

Topic 1 - Single Topic

Question #1

Topic 1

Which functions of an SDN architecture require southbound APIs to enable communication?

- A. SDN controller and the network elements
- B. management console and the SDN controller
- C. management console and the cloud
- D. SDN controller and the cloud

Correct Answer: A*Community vote distribution*

A (100%)

Thusi26 Highly Voted 2 years, 9 months ago

Software-defined southbound application program interfaces (SDN southbound APIs) are used to communicate between the SDN Controller and the switches and routers of the network.

upvoted 14 times

sull3y Highly Voted 1 year, 7 months ago

A

Southbound APIs are used to enable communication between the SDN controller and the network elements (such as switches, routers, etc.) in the network. The SDN controller uses these APIs to send commands and configuration instructions to the network elements, and to receive status and other information from them. This allows the SDN controller to centrally control and manage the network elements, and to dynamically adjust the network's behavior in response to changing conditions.

upvoted 5 times

Marshpillowz Most Recent 6 months, 2 weeks ago**Selected Answer: A**

Answer is 'A' as per the other responses.

upvoted 1 times

Naderelmansi 1 year, 10 months ago**Selected Answer: A**

southbound APIs are used to communicate between the SDN controller and the switches and routers within the infrastructure.

Chapter 3. Software-Defined Networking Security and Network Programmability

Official Cert Guide

upvoted 2 times

sheki2005 2 years, 4 months ago

A is correct

upvoted 2 times

Which two request methods of REST API are valid on the Cisco ASA Platform? (Choose two.)

- A. put
- B. options
- C. get
- D. push
- E. connect

Correct Answer: AC

Reference:

<https://www.cisco.com/c/en/us/td/docs/security/asa/api/qsg-asa-api.html>

Community vote distribution

AC (80%)

AE (20%)

sajoz123 Highly Voted 2 years, 8 months ago

ans is correct.

Available request methods are:

GET – Retrieves data from the specified object.

PUT – Adds the supplied information to the specified object; returns a 404 Resource Not Found error if the object does not exist.

POST – Creates the object with the supplied information.

DELETE – Deletes the specified object.

PATCH – Applies partial modifications to the specified object.

upvoted 10 times

abdulmalik_mail 2 years, 7 months ago

reference : <https://www.cisco.com/c/en/us/td/docs/security/asa/api/qsg-asa-api.html>

upvoted 3 times

Marshpillowz Most Recent 6 months, 2 weeks ago

Selected Answer: AC

A and C are correct answers.

Request Structure

Available request methods are:

GET – Retrieves data from the specified object.

PUT – Adds the supplied information to the specified object; returns a 404 Resource Not Found error if the object does not exist.

POST – Creates the object with the supplied information.

DELETE – Deletes the specified object.

PATCH – Applies partial modifications to the specified object.

upvoted 1 times

Anonymous983475 1 year, 7 months ago

Selected Answer: AC

Definitely A and C sajoz123 described exactly why.

upvoted 2 times

sull3y 1 year, 7 months ago

AC

GET and PUT are valid request methods of REST API that can be used on the Cisco ASA Platform. GET is used to retrieve information from the server, while PUT is used to update or replace existing information on the server.

The other options are not valid request methods of REST API on the Cisco ASA Platform.

upvoted 2 times

ross123 1 year, 8 months ago

Selected Answer: AC

Correct answer as per <https://www.cisco.com/c/en/us/td/docs/security/asa/api/qsg-asa-api.html>

upvoted 1 times

Naderelmansi 1 year, 10 months ago

Selected Answer: AE

The ASA REST API gives you programmatic access to managing individual ASAs through a Representational State Transfer (REST) API. The API allows external clients to perform CRUD (Create, Read, Update, Delete) operations on ASA resources; it is based on the HTTPS protocol and REST methodology.

All API requests are sent over HTTPS to the ASA, and a response is returned.
This section provides an overview of how requests are structured, and the expected responses,

Request Structure

Available request methods are:

GET – Retrieves data from the specified object.

PUT – Adds the supplied information to the specified object; returns a 404 Resource Not Found error if the object does not exist.

POST – Creates the object with the supplied information.

DELETE – Deletes the specified object.


PATCH – Applies partial modifications to the specified object.

upvoted 1 times

  **cyberwhizzy0** 1 year, 3 months ago

I guess you meant to write AC

upvoted 2 times

  **sheki2005** 2 years, 4 months ago

yes correct answers

upvoted 1 times

The main function of northbound APIs in the SDN architecture is to enable communication between which two areas of a network?

- A. SDN controller and the cloud
- B. management console and the SDN controller
- C. management console and the cloud
- D. SDN controller and the management solution

Correct Answer: D

Community vote distribution

D (100%)

Alee86 Highly Voted 2 years, 11 months ago

Correct answer is D: SDN Controller and the management solution

How Do Northbound APIs Work?

Northbound APIs are the link between the applications and the SDN controller. The applications can tell the network what they need (data, storage, bandwidth, and so on) and the network can deliver those resources, or communicate what it has.

upvoted 17 times

nomanlands Highly Voted 2 years, 2 months ago

Selected Answer: D

D

The management solution is the applications that are supporting and managing control over the network. "The Cloud" could be correct if some of those applications live in the cloud but isn't a complete answer. Applications and SDN Controller should really be an answer here because this is pretty vague and poor.

A should really be incorrect due to virtual switches and routers could live in "the cloud" but be a Southbound API so this is why I would completely remove A as an answer.

upvoted 5 times

Marshpillowz Most Recent 6 months, 2 weeks ago

Selected Answer: D

Answer is D.

Northbound APIs (SDN northbound APIs) are typically RESTful APIs that are used to communicate between the SDN controller and the services and applications running over the network.

upvoted 1 times

jCho 2 years, 3 months ago

Northbound interfaces define the way the SDN controller should interact with the application plane. Applications and services are things like load-balancers, firewalls, security services and cloud resources. The idea is to abstract the inner-workings of the network, so that application developers can 'hook' into the network and make changes to accommodate the needs of the application without having to understand exactly what that means for the network.

<https://www.econfgs.com/ccna-7-7-c-northbound-and-southbound-apis/>

A

upvoted 1 times

LippaCippa 2 years, 5 months ago

Correct answer is D:

From the official study Guide "Northbound APIs (SDN northbound APIs) are typically RESTful APIs that are used to communicate between the SDN controller and the services and applications running over the network. Such northbound APIs can be used for the orchestration and automation of the network components to align with the needs of different applications via SDN network programmability. In short, northbound APIs are basically the link between the applications and the SDN controller."

upvoted 3 times

bassfunk 2 years, 9 months ago

The answer should be B



<https://www.sdxcentral.com/networking/sdn/definitions/north-bound-interfaces-api/>

upvoted 1 times

Cock 2 years, 9 months ago

According to your website the answer should be A. Examples of the types of network applications that can be optimized via the northbound interface include load balancers, firewalls, or other software-defined security services, or orchestration applications across cloud resources.

upvoted 1 times


  **heamgu** 2 years, 10 months ago

Answer should be A:

SCOR Reference Book:

Northbound APIs (SDN northbound APIs) are typically RESTful APIs that are used to communicate between the SDN controller and the services and applications running over the network. Such northbound APIs can be used for the orchestration and automation of the network components to align with the needs of different applications via SDN network programmability. In short, northbound APIs are basically the link between the applications and the SDN controller. In modern environments, applications can tell the network devices (physical or virtual) what type of resources they need and, in turn, the SDN solution can provide the necessary resources to the application.

upvoted 2 times

  **NWguy** 2 years, 5 months ago

Answer should be D : SDN controller and management solution as cloud is to specific and the management solution can be on prem or a cisco cloud solution.

Your actually stating it in your reference:

In short, northbound APIs are basically the link between the applications and the SDN controller. In modern environments, applications can tell the network devices (physical or virtual) what type of resources they need and, in turn, the SDN solution can provide the necessary resources to the application.

upvoted 1 times

  **beeker98106** 2 years, 10 months ago

I'll go with A too. NB is basically everything but the infra components, not just the mgmt solution

upvoted 1 times

  **Amedeou** 3 years ago

answer should A

upvoted 2 times

Question #4

Topic 1

What is a feature of the open platform capabilities of Cisco DNA Center?

- A. application adapters
- B. domain integration
- C. intent-based APIs
- D. automation adapters

Correct Answer: C

Community vote distribution

C (100%)

  **Marshpillowz** 5 months, 1 week ago

Selected Answer: C

Intent APIs: The Intent APIs are northbound REST APIs that expose specific capabilities of Cisco DNA Center platform. The Intent APIs provide policy-based abstraction of business intent, allowing you to focus on an outcome to achieve instead of struggling with the mechanisms that implement that outcome. The APIs conform to the REST API architectural style. The APIs are simple, extensible, secure to use, and support the standard REST methods, which include the GET, POST, PUT, and DELETE operations through HTTPS.

upvoted 1 times

  **MPoels** 6 months, 2 weeks ago

Selected Answer: C

https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center-platform/2-3-7/user-guide/b-dnac-platform-ug-2-3-7/b-dnac-platform-ug-2-3-7-chapter-01.html#id_76824

<https://www.ciscolive.com/c/dam/r/ciscolive/emea/docs/2020/pdf/DEVNET-2087.pdf>

upvoted 1 times

  **samtestking** 7 months, 4 weeks ago

Really C?

upvoted 1 times

```
import requests

client_id = 'a1b2c3d4e5'

api_key = 'a1b2c3d4-e5f6-g7h8'

url = 'https://api.amp.cisco.com/v1/computers'

response = requests.get(url, auth=(client_id, api_key))


response_json = response.json()

for computer in response_json['data']:
    network_addresses = computer['network_addresses']
    for network_interface in network_addresses:
        mac = network_interface.get('mac')
        ip = network_interface.get('ip')
        ipv6 = network_interface.get('ipv6')
        print(mac, ip, ipv6)
```

Refer to the exhibit. What does the API do when connected to a Cisco security appliance?

- A. create an SNMP pull mechanism for managing AMP
- B. gather network telemetry information from AMP for endpoints
- C. get the process and PID information from the computers in the network
- D. gather the network interface information about the computers AMP sees

Correct Answer: D

 **corelan** 6 months, 2 weeks ago

My choose is D
upvoted 1 times

Which form of attack is launched using botnets?

- A. TCP flood
- B. DDOS
- C. DOS
- D. virus

Correct Answer: B

Community vote distribution

B (80%)

D (20%)

pohqinan Highly Voted 2 years, 8 months ago
<https://en.wikipedia.org/wiki/Botnet>

Correct answer DDOS
upvoted 9 times

Marshpillowz Most Recent 5 months, 1 week ago

Selected Answer: B

Answer is distributed denial of service (DDOS)
upvoted 1 times

MPoels 6 months, 2 weeks ago

Selected Answer: B

A botnet is a collection of compromised machines that the attacker can manipulate from a command-and-control (often referred to as a C2 or CnC) system to participate in a DDoS, send spam emails, and perform other illicit activities.
upvoted 1 times

zamkljo 1 year, 5 months ago

Selected Answer: B

Botnets – Short for “robot network,” these are networks of infected computers under the control of single attacking parties using command-and-control servers. Botnets are highly versatile and adaptable, able to maintain resilience through redundant servers and by using infected computers to relay traffic. Botnets are often the armies behind today's distributed denial-of-service (DDoS) attacks.

A botnet (short for “robot network”) is a network of computers infected by malware that are under the control of a single attacking party

<https://www.paloaltonetworks.com/cyberpedia/what-is-malware>

upvoted 2 times

sull3y 1 year, 7 months ago

B. DDOS

A Distributed Denial of Service (DDOS) attack is a type of cyber attack in which multiple systems, often compromised through malware and controlled remotely by attackers, known as “botnets”, flood the target website or network with a huge amount of traffic in order to overload the system and make it unavailable for legitimate users. The large number of systems participating in the attack amplifies the volume of traffic, making it very difficult for the targeted website or network to handle, resulting in a denial of service. Botnets are commonly used to launch DDoS attacks as they allow attackers to launch a much larger attack than they would be able to accomplish with a single system.

upvoted 3 times

royallyre20 1 year, 11 months ago

Selected Answer: D

There is no TCP Flood attack.there is TCP sync flood attack which is one of DDOS attack.

So answers is D

upvoted 1 times

In which form of attack is alternate encoding, such as hexadecimal representation, most often observed?

- A. smurf
- B. distributed denial of service
- C. cross-site scripting
- D. rootkit exploit

Correct Answer: C

Community vote distribution

C (100%)

Alee86 Highly Voted 2 years, 11 months ago

Cross site scripting (also known as XSS) occurs when a web application gathers malicious data from a user. The data is usually gathered in the form of a hyperlink which contains malicious content within it. The user will most likely click on this link from another website, instant message, or simply just reading a web board or email message.

Usually the attacker will encode the malicious portion of the link to the site in HEX (or other encoding methods) so the request is less suspicious looking to the user when clicked on.

For example the code below is written in hex:

```
<a href=&#x6A&#x61&#x76&#x61&#x73&#x63&#x72&#x69&#x70&#x74&#x3A&#x61&#x6C&#x65&#x72&#x74&#x28&#x27&#x58&#x53&#x53&#x27&#x29>Click Here</a>
```

is equivalent to:

```
<a href=javascript:alert('XSS')>Click Here</a>
```

Note: In the format "&#xhhhh", hhhh is the code point in hexadecimal form

upvoted 8 times

sull3y Most Recent 1 year, 7 months ago

C. cross-site scripting

Cross-site scripting (XSS) is a type of security vulnerability typically found in web applications, that allows an attacker to inject malicious code into a web page viewed by other users. One of the methods attackers use to evade detection and make the injected code more difficult to detect is by using alternate encoding, such as hexadecimal representation. This makes the code harder to read and understand, making it more difficult to detect and remove. This technique is often used in XSS attacks as it allows attackers to hide the malicious code and evade detection by security software and systems.

upvoted 4 times

heamgu 2 years, 7 months ago

Selected Answer: C

Ans: C

upvoted 2 times

abdulmalik_mail 2 years, 7 months ago

It's C

Reference : https://owasp.org/www-community/Double_Encoding

upvoted 3 times

ic0deem 3 years ago

It could be C but why not D?

upvoted 1 times

Raajaa 3 years, 2 months ago

not sure about the correct answer for this Q

upvoted 1 times

Max95 3 years, 3 months ago

There are some common characters sets that are used in Web applications attacks. For example, Path Traversal attacks use ../ (dot-dot-slash), while XSS attacks use < and > characters. These characters give a hexadecimal representation that differs from normal data.

https://owasp.org/www-community/Double_Encoding

upvoted 3 times

deathfrom 3 years, 3 months ago

Would somebody be able to explain why the answer is Cross Side Scripting please?

upvoted 1 times

Seawanderer 3 years, 2 months ago

A and B are wrong as related to ICMP or related network attacks

upvoted 1 times

Which flaw does an attacker leverage when exploiting SQL injection vulnerabilities?

- A. user input validation in a web page or web application
- B. Linux and Windows operating systems
- C. database
- D. web page images

Correct Answer: A

Reference:

https://tools.cisco.com/security/center/resources/sql_injection

Community vote distribution

A (100%)

kudlaaaty Highly Voted 4 years, 3 months ago

should be A
upvoted 19 times

eazy99 Highly Voted 2 years, 12 months ago

This is a tricky question, and I believe the provided answer is correct and here is why. They ask what is the flaw that caused the attacker to exploit this vulnerability?

I agree that the attacker uses the web application or the user input to exploit the vulnerability, and give commands to connect to the database and get everything needed about the database. But what where is the actual flaw? Was it A. the web application and the user input? No, it's not, or it would be XSS vulnerability. The attacker leveraged a flaw in the Database, using the web application or the user input as a way to communicate with the Database and extract all the info about the database. With that being said, I believe that the provided answer is correct, and I will go with C.

upvoted 9 times

Dorr20 1 year, 5 months ago

The database exploitation is the end result, it's not the flaw
upvoted 3 times

otzu1 2 years, 4 months ago

The flaw is in the web application/user input as it did not have input validation. The database.
upvoted 2 times

Rockbo47 Most Recent 12 hours, 1 minute ago

Selected Answer: A

As others have highlighted already, the "flaw" would refer to the vulnerability which in this example would be the user input validation (or lack of).

<https://www.cisco.com/c/en/us/support/docs/csa/cisco-sa-dcnm-sql-inj-OAQOObP.html>

This is also verified in the above link...

"CVE-2021-1248: Cisco DCNM SQL Injection Vulnerability

A vulnerability in a REST API endpoint of Cisco DCNM could allow an authenticated, remote attacker with administrative privileges to execute arbitrary SQL commands on an affected device.

This vulnerability is due to insufficient validation of user-supplied input to the API. An attacker with administrative privileges could exploit this vulnerability by sending a crafted request to the API"

upvoted 1 times

itsklk 1 year, 4 months ago

Selected Answer: A

Which "flaw" does. So its cause in my understanding
upvoted 1 times

nomanlands 2 years, 2 months ago

Selected Answer: A

Exploiting input validation at the source and destination. It isn't a flaw within the database itself.
upvoted 3 times

tom_1991 2 years, 3 months ago

I believe the answer is C. The Database is unable to sanitize the data sent to it through the web page/application as it relies heavily on the web page/application to sanitize the code. That is the databases flaw. The attacker is leveraging the fact that the database can't do anything to prevent

the attacker from sending the code.
Very tricky question...

upvoted 2 times

  **TesterDude** 2 years, 3 months ago



Selected Answer: A

Exploiting no data validation
upvoted 1 times

  **sheki2005** 2 years, 4 months ago

for me the answer is C, because you can have systems which is using web to connect into database, so all the queries are coming from web to database, the user wont exploit web but database through web, so for me I will go with Database instead of web.

upvoted 1 times

  **brownbear505** 2 years, 6 months ago


Selected Answer: A

To prevent SQL injection one means of preventing is input validation.
upvoted 1 times

  **elast1c** 2 years, 7 months ago

Selected Answer: A

definitely A
upvoted 1 times



  **urathod** 2 years, 8 months ago

Selected Answer: A

should be A
upvoted 1 times

  **efongvan** 2 years, 8 months ago

Answer is definitely A.
upvoted 2 times

  **PrinM** 2 years, 9 months ago

Selected Answer: A

should be A
upvoted 2 times

  **bassfunk** 2 years, 9 months ago



Selected Answer: A

Answer is definitely A. Input validation is the vulnerability, not the database.
upvoted 2 times


  **jaciro11** 2 years, 9 months ago

Selected Answer: A

The answer is A
upvoted 2 times

  **ExamP** 2 years, 12 months ago

A
<https://www.cisco.com/c/en/us/support/docs/csa/cisco-sa-dcnm-sql-inj-OAQOObP.html>
upvoted 2 times

  **Raajaa** 3 years, 2 months ago

I go with A
upvoted 2 times

What is the difference between deceptive phishing and spear phishing?

- A. Deceptive phishing is an attack aimed at a specific user in the organization who holds a C-level role.
- B. A spear phishing campaign is aimed at a specific person versus a group of people.
- C. Spear phishing is when the attack is aimed at the C-level executives of an organization.
- D. Deceptive phishing hijacks and manipulates the DNS server of the victim and redirects the user to a false webpage.

Correct Answer: B

Community vote distribution

B (100%)

fabio3wz **Highly Voted** 4 years ago

Nope, the answer should be B. You can easily google it, and you can find that Spear phishing relates to attacks targeted to individuals. Spear phishing always focuses on one victim
upvoted 24 times

sull3y **Highly Voted** 1 year, 7 months ago

B. A spear phishing campaign is aimed at a specific person versus a group of people.

Deceptive Phishing is a general term used to describe any type of phishing attack that uses deception to trick the victim into providing personal information or login credentials. It can be targeted at a large group of people, indiscriminately.

Spear Phishing is a targeted type of phishing attack that is aimed at a specific individual or group of people within an organization. It is more sophisticated than a general phishing attack and often uses personal information about the target to make the email or message appear legitimate. Spear phishing is also known to target specific roles or positions, such as C-level executives within an organization.

Deceptive Phishing does not hijack and manipulate the DNS server of the victim and redirect the user to a false webpage, this kind of attack is called "pharming" attack.
upvoted 5 times

Marshpillowz **Most Recent** 5 months, 1 week ago

Selected Answer: B

Answer is B - spear phishing targets a specific victim (normally high-level or authoritative figure).
upvoted 1 times

royallyre20 1 year, 11 months ago

Selected Answer: B

answer: B
upvoted 1 times

Wang87 2 years, 7 months ago

Selected Answer: B

Spear Phishing is targeted at one particular person who generally is C-Level but not necessarily. So correct answer is B
upvoted 2 times

efongvan 2 years, 8 months ago

Correct answer is B.
<https://terranosecurity.com/spear-phishing-vs-phishing/>
upvoted 1 times

eazy99 2 years, 12 months ago

The provided answer is correct B.
upvoted 2 times



myccnptest 3 years, 9 months ago

<https://www.tripwire.com/state-of-security/security-awareness/6-common-phishing-attacks-and-how-to-protect-against-them/>

So B
upvoted 3 times

tester90 4 years ago

Correct is C.
upvoted 1 times

  **5tuple** 3 years, 8 months ago
Wrong, that is Whaling
upvoted 6 times

Question #10

Topic 1

Which two behavioral patterns characterize a ping of death attack? (Choose two.)

- A. The attack is fragmented into groups of 16 octets before transmission.
- B. The attack is fragmented into groups of 8 octets before transmission.
- C. Short synchronized bursts of traffic are used to disrupt TCP connections.
- D. Malformed packets are used to crash systems.
- E. Publicly accessible DNS servers are typically used to execute the attack.

Correct Answer: *BD*

Reference:




https://en.wikipedia.org/wiki/Ping_of_death

Community vote distribution

BD (100%)

  **aalnman** Highly Voted  3 years, 2 months ago

B and D is correct. If you google either or both B and D you'll land on a Wikipedia page that confirms the information:
https://en.wikipedia.org/wiki/Ping_of_death#:~:text=Like%20other%20large%20but%20well,the%20injection%20of%20malicious%20code.
upvoted 8 times

  **sull3y** Highly Voted  1 year, 7 months ago

D. Malformed packets are used to crash systems.
B. The attack is fragmented into groups of 8 octets before transmission.



A Ping of death attack is a type of denial-of-service attack that sends malformed or oversized ping packets to a target network. The packets are typically fragmented into groups of 8 octets before transmission and when the target system reassembles the packets it can cause the system to crash or become unstable.

upvoted 6 times

  **Marshpillowz** Most Recent  5 months, 1 week ago

Selected Answer: *BD*


Answers are B and D as per other responses
upvoted 1 times

  **c3qu1** 6 months, 1 week ago

B and D is correct
upvoted 1 times

  **samtestking** 7 months, 3 weeks ago

Why Choose only two?
upvoted 1 times

  **DarexTech100** 8 months, 3 weeks ago

I'll th
upvoted 1 times

Which two mechanisms are used to control phishing attacks? (Choose two.)

- A. Enable browser alerts for fraudulent websites.
- B. Define security group memberships.
- C. Revoke expired CRL of the websites.
- D. Use antispam software.
- E. Implement email filtering techniques.

Correct Answer: AE

Community vote distribution

AE (100%)

heamgu Highly Voted 2 years, 7 months ago

Selected Answer: AE

Answer is A and E.

Reference:

<https://www.ncsc.gov.uk/guidance/phishing#downloads>

upvoted 5 times

Marshpillowz Most Recent 5 months, 1 week ago

Selected Answer: AE

A and E are the correct answers

upvoted 1 times

sull3y 1 year, 7 months ago

A. Enable browser alerts for fraudulent websites.

E. Implement email filtering techniques.

Phishing attacks are attempts to trick individuals into providing sensitive information such as passwords or credit card numbers by disguising as a trustworthy entity. Two common mechanisms used to control phishing attacks are:

Enable browser alerts for fraudulent websites: Some web browsers have built-in phishing filters that can detect and warn users when they visit a potentially fraudulent website.

Implement email filtering techniques: Email filters can help to identify and block phishing emails from reaching the inbox by using techniques such as keyword filtering, bayesian filtering, and sender reputation analysis.

upvoted 4 times

heamgu 2 years, 10 months ago

Answer is A and E.

Reference:

<https://www.ncsc.gov.uk/guidance/phishing#downloads>

upvoted 4 times

eazy99 2 years, 12 months ago

From the options provided, the best answer is AE, we would try to protect the employee from accessing any fraudulent websites used in the phishing emails, and try to filter emails to prevent such emails.

upvoted 3 times

Fazy 3 years ago

AE are correct

upvoted 4 times

Sarbi 3 years ago

B and D

upvoted 1 times

Which attack is commonly associated with C and C++ programming languages?

- A. cross-site scripting
- B. water holing
- C. DDoS
- D. buffer overflow

Correct Answer: D

Reference:

https://en.wikipedia.org/wiki/Buffer_overflow

Community vote distribution



Marshpillowz 5 months, 1 week ago

Selected Answer: D

D - buffer overflow is correct
upvoted 1 times

ama6 1 year, 7 months ago

d IS cORRECT
upvoted 4 times

sull3y 1 year, 7 months ago

D

A buffer overflow is a type of security vulnerability that occurs when a program tries to store more data in a buffer (a temporary storage area in memory) than it can hold. This can cause the extra data to overflow into adjacent memory areas, potentially corrupting or overwriting important data or instructions. In some cases, an attacker can use a buffer overflow to execute arbitrary code or take control of a program or system. C and C++ programming languages, due to their low-level manipulation of memory, are particularly susceptible to buffer overflow attacks.

upvoted 4 times

Which two prevention techniques are used to mitigate SQL injection attacks? (Choose two.)

- A. Check integer, float, or Boolean string parameters to ensure accurate values.
- B. Use prepared statements and parameterized queries.
- C. Secure the connection between the web and the app tier.
- D. Write SQL code instead of using object-relational mapping libraries.
- E. Block SQL code execution in the web application database login.

Correct Answer: AB

Reference:

https://en.wikipedia.org/wiki/SQL_injection

Community vote distribution



sull3y Highly Voted 1 year, 7 months ago

BE

Checking integer, float, or Boolean string parameters to ensure accurate values (Option A) can help prevent certain types of injection attacks, such as those that rely on unexpected input. However, it is not a comprehensive solution and can still be bypassed by a determined attacker.

Using prepared statements and parameterized queries (Option B) is a more robust method of preventing SQL injection attacks. These techniques separate the data and the SQL command, preventing attackers from injecting malicious code into the SQL command.

Blocking SQL code execution in the web application database login (Option E) is another robust method to mitigate SQL injection attacks. This technique ensures that no malicious SQL statements can be executed in the database.

Therefore, B and E are correct answers as they are more robust methods of preventing SQL injection attacks.

upvoted 5 times

sull3y 1 year, 7 months ago

Option C, Securing the connection between the web and the app tier, is important for overall security, but it is not directly related to preventing SQL injection attacks. Having a secure connection ensures that the data being transmitted between the web and app tier is protected, but it does not prevent attackers from injecting malicious code into the SQL command.

Option D, Writing SQL code instead of using object-relational mapping libraries, can help prevent SQL injection attacks by giving you more control over the SQL commands being executed, but it is not a guarantee. It is still possible to make mistakes in the SQL code that can lead to SQL injection vulnerabilities. Prepared statements and parameterized queries (Option B) is a more robust method of preventing SQL injection attacks, regardless of whether you are using an ORM library or writing raw SQL code.

In summary, B and E are the best options for preventing SQL injection attacks. While C and D may improve overall security, they do not directly address SQL injection vulnerabilities.

upvoted 1 times

Marshpillowz Most Recent 5 months, 1 week ago

Selected Answer: BE

B and E are correct as per sull3y's response

upvoted 1 times

nep1019 1 year, 1 month ago

According to Cisco's documentation: https://tools.cisco.com/security/center/resources/sql_injection.html

B and C are correct:

Parameterized queries in ASP.NET, prepared statements in Java, or similar techniques in other languages should be used comprehensively in addition to strict input validation.

Application layer protocol inspection performs deep packet inspection of traffic that transits the firewall. Using application layer protocol inspection on Cisco firewalls to mitigate SQL attacks against web servers is discussed in Cisco TAC Security Podcast Episode #16.

Only way to do the second, imo, is to secure the connection between the web and app tier (Application layer protocol inspection)

upvoted 1 times

nep1019 1 year, 1 month ago

Changing back to A and B based on this statement that comes at the beginning of the section on mitigating these attacks:

The primary approaches include validation of user-supplied data, in the form of whitelisting or blacklisting, and the construction of SQL statements such that user-supplied data cannot influence the logic of the statement.

Last sentence is all about the statements and A and B are directly about that so must be those two.

upvoted 1 times

  **Cokamaniako** 1 year, 2 months ago

Selected Answer: AB

Answer A and B

Parameterized statements

Main article: Prepared statement

With most development platforms, parameterized statements that work with parameters can be used (sometimes called placeholders or bind variables) instead of embedding user input in the statement. A placeholder can only store a value of the given type and not an arbitrary SQL fragment. Hence the SQL injection would simply be treated as a strange (and probably invalid) parameter value. In many cases, the SQL statement is fixed, and each parameter is a scalar, not a table. The user input is then assigned (bound) to a parameter

Pattern check

Integer, float or boolean, string parameters can be checked if their value is valid representation for the given type. Strings that must follow some strict pattern (date, UUID, alphanumeric only, etc.) can be checked if they match this pattern.

upvoted 1 times

  **Brain_Power** 1 year, 2 months ago

Selected Answer: BE

correct answer B & E

upvoted 1 times

  **maddy** 1 year, 3 months ago

B and E for me

https://en.wikipedia.org/wiki/SQL_injection#Mitigation

upvoted 2 times

  **Przemol** 1 year, 2 months ago

IT is B and D according to the URL provided.

Parameterized statements

Main article: Prepared statement

With most development platforms, parameterized statements that work with parameters can be used (sometimes called placeholders or bind variables) instead of embedding user input in the statement. A placeholder can only store a value of the given type and not an arbitrary SQL fragment. Hence the SQL injection would simply be treated as a strange (and probably invalid) parameter value. In many cases, the SQL statement is fixed, and each parameter is a scalar, not a table. The user input is then assigned (bound) to a parameter.[24]

Enforcement at the coding level



Using object-relational mapping libraries avoids the need to write SQL code. The ORM library in effect will generate parameterized SQL statements from object-oriented code.

upvoted 1 times

  **cyberwhizzy0** 1 year, 3 months ago

A and B is correct

upvoted 1 times


  **achille5** 1 year, 6 months ago

Selected Answer: BC

B. Prepared statements and parameterized queries are a way of separating the SQL code from the data that is being passed into the query. By doing this, the SQL injection attack is prevented because the attacker cannot inject any SQL code into the prepared statement or parameterized query.

C. Securing the connection between the web and the app tier is also an important prevention technique to mitigate SQL injection attacks. This is because an attacker can intercept network traffic and view the data that is being passed between the web and the app tier. By using SSL or TLS encryption, the data that is being passed between the two tiers is encrypted, making it much harder for an attacker to view or manipulate.


upvoted 1 times

  **achille5** 1 year, 6 months ago

After further reading i changed to A, B.

https://en.wikipedia.org/wiki/SQL_injection

upvoted 3 times

  **jienBoq** 1 year, 9 months ago

to me it's B and C as per this Cisco article:

https://tools.cisco.com/security/center/resources/sql_injection.html

"A SQL injection attack can be detected and potentially blocked at two locations in an application traffic flow: in the application and in the network."

"Parameterized queries in ASP.NET, prepared statements in Java, or similar techniques in other languages should be used comprehensively in addition to strict input validation."

A's wording doesn't necessary imply input validation

D doesn't make sense

E is not a solution which I've seen suggested anywhere.

upvoted 2 times

👤 **achille5** 1 year, 6 months ago

B. Prepared statements and parameterized queries are a way of separating the SQL code from the data that is being passed into the query. By doing this, the SQL injection attack is prevented because the attacker cannot inject any SQL code into the prepared statement or parameterized query.

C. Securing the connection between the web and the app tier is also an important prevention technique to mitigate SQL injection attacks. This is because an attacker can intercept network traffic and view the data that is being passed between the web and the app tier. By using SSL or TLS encryption, the data that is being passed between the two tiers is encrypted, making it much harder for an attacker to view or manipulate.

upvoted 2 times

👤 **JavierAcuna** 1 year, 9 months ago

Selected Answer: AB

Answer found in: https://tools.cisco.com/security/center/resources/sql_injection.html

upvoted 1 times

👤 **NikoNiko** 2 years, 2 months ago

Correct are A, B.

Countermeasure against SQLi:

..you should most definitely use ORM (Object-Relational Mappings) and prepared statements. = option B.

They take away the vast majority of SQL Injection risk, and are generally good software practices.

However, you shouldn't think that using these packages makes you completely immune.

Instead, you should also use input validation. This will keep malicious input out of your system to begin with, which is a great way to reduce risk. = option A

<https://snyk.io/blog/sql-injection-orm-vulnerabilities/>

upvoted 2 times

👤 **HilaM** 2 years, 2 months ago

A,B correct

Answer found in: https://tools.cisco.com/security/center/resources/sql_injection.html

upvoted 1 times

👤 **davezz** 1 year, 9 months ago

This is from this link: Parameterized queries in ASP.NET, prepared statements in Java, or similar techniques in other languages should be used comprehensively in addition to strict input validation. Each of these techniques performs all required escaping of dangerous characters before the SQL statement is passed to the underlying database system.

upvoted 1 times

👤 **aal** 2 years, 4 months ago

https://en.wikipedia.org/wiki/SQL_injection#Mitigation

Limiting the permissions on the database login used by the web application to only what is needed may help reduce the effectiveness of any SQL injection attacks that exploit any bugs in the web application.

upvoted 1 times

👤 **otzu1** 2 years, 4 months ago

yea i legit searched it's most def A/B the other option D is discussing the web application "login".

upvoted 1 times

👤 **Cock** 2 years, 9 months ago

Answers are A and B.

<https://www.softwaresecured.com/introduction-to-sql-injection-mitigation/>

upvoted 4 times

👤 **aalnman** 3 years, 2 months ago

This appears to be correct. I checked 3 other sites similar to this and all had the same answer. That said, I didn't research in the textbook or Cisco documentation.

upvoted 3 times

👤 **idto** 2 years, 9 months ago

I know this is a late response, but all sites share the same wrong answers because none of which have "real experts" answering these questions

upvoted 2 times

👤 **idto** 2 years, 9 months ago

Not saying the answers are incorrect, just saying we can't rely on the answers just because other websites say the same

upvoted 4 times

Which two kinds of attacks are prevented by multifactor authentication? (Choose two.)

- A. phishing
- B. brute force
- C. man-in-the-middle
- D. DDOS
- E. tear drop

Correct Answer: AB

Community vote distribution

AB (100%)

crh23 Highly Voted 4 years, 1 month ago

Its A and B cisco document

https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-mfa-password-security-infographic.pdf

upvoted 28 times

Benkelly18 Highly Voted 4 years, 1 month ago

mfa does not prevent phishing. I've seen phishing attacks where people managed to get them to send the code from the mfa device.

Basically one way is they send a marketing with a reply to unsubscribe, having already obtained the password, when someones texts stop or whatever they log in, and say please tell us the six digit code just messaged to your phone in order to unsubscribe.

It helps prevent as the above is quite uncommon but it doesn't prevent it.

upvoted 9 times

klu16 3 years ago

A, B and C are correct, but it matters what Cisco wants.

From Cisco website (about Trust Center): MFA protects against phishing, social engineering and password brute- force attacks and secures your logins from attackers exploiting weak or stolen credentials.

So it's simple for me, correct is A & B.

upvoted 7 times

bigdadzzz 3 years, 8 months ago

I'd classify that as a MitM attack (the bad actor is relaying between Authentication Service and the victim) where a general Phishing attack would be used to gather the password in the first place (cast a line with bait and see who bites).

In this context, the MFA would prevent the phishing attack from being successful, user pops in the username/password, but without the OTP, bad actor can't log in. It doesn't stop them from further social engineering to get the OTP as you describe, but it does prevent a credential harvesting attack from being successful.

upvoted 4 times

Marshpillowz Most Recent 5 months, 1 week ago

Selected Answer: AB

A and B are correct

upvoted 1 times

Rododendron2 5 months, 2 weeks ago

How can ever C be wrong ?

upvoted 1 times

sull3y 1 year, 7 months ago

A. Phishing

B. Brute force

upvoted 2 times

sis_net_sec 2 years, 1 month ago

AB is correct

upvoted 1 times

nomanlands 2 years, 2 months ago

Selected Answer: AB

Cisco answer is AB. Real life, mainly B and could help with A or C.

upvoted 1 times

[-]  **Cyril_the_Squirrel** 2 years, 2 months ago

B & C are Correct.

<https://www.fortinet.com/resources/cyberglossary/man-in-the-middle-attack>

upvoted 2 times


[-]  **philip8787** 2 years, 3 months ago

<https://duo.com/product/multi-factor-authentication-mfa/two-factor-authentication-2fa>

2FA protects against phishing, social engineering and password brute-force attacks and secures your logins from attackers exploiting weak or stolen credentials.

so A and B

upvoted 1 times

[-]  **Iron21** 2 years, 3 months ago

Its A and B

upvoted 1 times

[-]  **brownbear505** 2 years, 6 months ago

Selected Answer: AB

MFA protects against phishing, social engineering and password brute-force attacks and secures your logins from attackers exploiting weak or stolen credentials.

A teardrop attack is a denial-of-service (DoS) attack that involves sending fragmented packets to a target machine. Since the machine receiving such packets cannot reassemble them due to a bug in TCP/IP fragmentation reassembly, the packets overlap one another, crashing the target network device. This generally happens on older operating systems such as Windows 3.1x, Windows 95, Windows NT and versions of the Linux kernel prior to 2.1.63.

upvoted 2 times

[-]  **Wang87** 2 years, 7 months ago

Selected Answer: AB

Phishing is correct because here it means that even if someone phished your password MFA won't allow threat actors to exploit your passwords as 2nd step of authentication will prevent login.

upvoted 2 times

[-]  **jaciro11** 2 years, 9 months ago

Selected Answer: AB

Its A and B there is in CISCO documents

upvoted 2 times

[-]  **pfunkylol** 2 years, 9 months ago

Selected Answer: AB

Phishing attempts to get logon credentials just a brute force attempts to use credentials; multi-factor authentication means you need an additional factor (biometric / RSA token, etc.) to log in. Man-in-the-middle attacks can see the extra factor so it will not be mitigated by MFA (multi factor authentication). DDoS and Tear Drop are denial of services, again not affected by MFA.

upvoted 1 times

[-]  **heamgu** 2 years, 10 months ago

So if you are not sure what is the answer check this PDF from Cisco.

https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-top-10-cyber-tips.pdf

Answer is A and B.

upvoted 6 times

[-]  **Hormore** 2 years, 11 months ago

It's definitely A&B, MITM is getting the info inbetween the packet conversation... not when user are just trying to authenticate.

upvoted 2 times

[-]  **SirFrates24** 3 years, 2 months ago

MFA protects against phishing, social engineering and password bruteforce attacks and secures your logins from attackers exploiting weak or stolen credentials.

upvoted 3 times

What are two rootkit types? (Choose two.)

- A. registry
- B. buffer mode
- C. user mode
- D. bootloader
- E. virtual

Correct Answer: CD

Community vote distribution

CD (100%)

larn Highly Voted 2 years, 4 months ago

Selected Answer: CD

1. Kernel rootkit
 2. Hardware or firmware rootkit
 3. Hyper-V rootkits
 4. Bootloader rootkit or bootkit
 5. Memory rootkit
 6. User-mode or application rootkit
- upvoted 10 times

Cock Highly Voted 2 years, 9 months ago

C&D.

<https://heimdalsecurity.com/blog/rootkit/>

upvoted 5 times

Marshpillowz Most Recent 5 months, 1 week ago

Selected Answer: CD

User mode and bootloader - C and D

upvoted 1 times

sull3y 1 year, 7 months ago

C. User mode

D. Bootloader

A rootkit is a type of malicious software that is designed to hide itself and its activities from the system and its users. There are several types of rootkits, but the two most common are user-mode and bootloader rootkits.

A user-mode rootkit runs at the same privilege level as a normal application and is able to intercept and modify system calls made by other processes. It can also hide its presence by modifying the output of system commands such as "ps" or "netstat"

A bootloader rootkit infects the system's bootloader, which is the first piece of software that runs when a computer starts up. By infecting the bootloader, a rootkit can ensure that it is loaded before the operating system, making it difficult for the system to detect and remove it. Additionally, it can also hide its presence by modifying the output of system commands such as "ps" or "netstat"

Option A, registry, is a database in Windows operating systems that stores configuration settings and options for the operating system, applications, and users. Registry is not a type of rootkit.

upvoted 4 times

DeepaBP 2 years, 9 months ago

Please ignore the first comment

C & D is the correct answer, Kernel, user, bootloader and Memory are the 4 types of rootkits,

upvoted 5 times

DeepaBP 2 years, 9 months ago

B & C is the correct answer

kernel Rootkit, User Mode Rootkits, Buffer Mode Rootkit and Memory Rootkits are the four

upvoted 1 times

jonsmackface 2 years, 10 months ago

<https://en.wikipedia.org/wiki/Rootkit#Types>

User mode (C)

Bootkits (D)

upvoted 2 times

  **jairusster** 2 years, 11 months ago

User-mode or application rootkit - User-mode rootkits are simpler and easier to detect than kernel or boot record rootkits. This is because they hide within an application itself, and not system-critical files.

In other words, they operate at the level of standard programs such as Paint, Word, PC games and so on. This means a good antivirus or anti-rootkit program will probably find the malware and then remove it.

upvoted 1 times

  **Sarbi** 3 years ago

The correct answer is Bootloader and Virtual toll kit. There is no user-mode tool kit.

Hypervisor (Virtualized) Level Rootkits: Hypervisor (Virtualized) Level Rootkits are created by exploiting hardware features such as Intel VT or AMD-V (Hardware assisted virtualization technologies). Hypervisor level rootkits hosts the target operating system as a virtual machine and therefore they can intercept all hardware calls made by the target operating system.

Boot loader Level (Bootkit) Rootkits: Boot loader Level (Bootkit) Rootkits replaces or modifies the legitimate boot loader with another one thus enabling the Boot loader Level (Bootkit) to be activated even before the operating system is started. Boot loader Level (Bootkit) Rootkits are serious threat to security because they can be used to hack the encryption keys and passwords.

upvoted 3 times

  **capwapap555** 3 years ago

<https://resources.infosecinstitute.com/topic/rootkits-user-mode-kernel-mode-part-1/>

upvoted 1 times

How is DNS tunneling used to exfiltrate data out of a corporate network?

- A. It leverages the DNS server by permitting recursive lookups to spread the attack to other DNS servers
- B. It encodes the payload with random characters that are broken into short strings and the DNS server rebuilds the exfiltrated data
- C. It redirects DNS requests to a malicious server used to steal user credentials, which allows further damage and theft on the network
- D. It corrupts DNS servers by replacing the actual IP address with a rogue address to collect information or start other attacks

Correct Answer: B

Community vote distribution

B (81%)

C (19%)

Jetnor Highly Voted 2 years, 9 months ago

Selected Answer: B

I would go with B, based on the question .

because we are asked how is DNS tunneling used, and the attacker encodes text information in base64 to then send it to the malicious DNS server which is mentioned at the end of the question (DNS server rebuilds the exfiltrated data)

"C" does not explain how the information is encoded.

upvoted 7 times

Premium_Pils Most Recent 1 month ago

Selected Answer: B

Maybe it is just me, but I can't see how "redirection" would fit in. "attackers use the DNS protocol to embed data within packets in DNS queries", and get the data shipped out to the attackers DNS server. (not redirecting, just directing it to the malicious server) The data needs to be split into smaller chunks (to be protocol conform), and is often encoded with base64.

<https://www.akamai.com/glossary/what-is-dns-data-exfiltration>

<https://bluegoatcyber.com/blog/dns-exfiltration-with-base64-encoding-a-stealthy-data-theft-technique/>

I vote for B.

upvoted 1 times

Marshpillowz 5 months, 1 week ago

Selected Answer: B

B is correct

upvoted 1 times

klu16 6 months, 3 weeks ago

Well, for me it all depends if these answers are really worded like this. If so, then B cannot be correct, because DNS servers do not rebuild information (DNS server's role is to handle DNS queries and responses).

Option C seems to be the most logical, since the data is encoded, then the encoded payload is inserted into DNS queries and manipulated DNS packets are sent to a malicious DNS server controlled by the attacker.

I think I will go with answer C because of that.

upvoted 1 times

Cokamaniako 1 year, 2 months ago

Selected Answer: B

The DNS server can not rebuild information.

upvoted 1 times

littlewilly 1 year, 3 months ago

Selected Answer: C

This is C

upvoted 2 times

gamingoddess 1 year, 4 months ago

Selected Answer: B

Attackers can use outbound DNS requests to send encoded exfiltrated data to their infrastructure. The DNS tunneling client malware on the infected machine reads the data to be exfiltrated line by line, slices the data into small chunks and performs base64 encoding on each line. So, option B is the closest to describing how DNS tunneling is used to exfiltrate data out of a corporate network.

upvoted 1 times

stalkr3 1 year, 5 months ago

B is false imo - "It encodes the payload with RANDOM characters..." - What is the point of exfiltrating random characters?



upvoted 2 times

pioo1979 1 year, 6 months ago

I think the correct answer is C.

B - "It encodes the payload with RANDOM characters..." There is no sense to exfiltrate random data..

upvoted 1 times



  **sull3y** 1 year, 7 months ago

B. It encodes the payload with random characters that are broken into short strings and the DNS server rebuilds the exfiltrated data

DNS Tunneling is a technique used to exfiltrate data out of a corporate network by encoding the payload with random characters that are broken into short strings and then sending these strings as DNS queries. These queries are sent to a domain controlled by the attacker, which then rebuilds the exfiltrated data. This technique takes advantage of the fact that many corporate networks allow outgoing DNS queries, while other types of traffic may be blocked.

Option A, It leverages the DNS server by permitting recursive lookups to spread the attack to other DNS servers, is not exactly the way DNS Tunneling works, it's more about encoding data into DNS queries and exfiltrating it through this channel.



upvoted 4 times

  **sull3y** 1 year, 7 months ago

Option C, It redirects DNS requests to a malicious server used to steal user credentials, which allows further damage and theft on the network, is not exactly how DNS Tunneling works. This technique is more about exfiltrating data, not stealing credentials.

Option D, It corrupts DNS servers by replacing the actual IP address with a rogue address to collect information or start other attacks, is not exactly how DNS Tunneling works. DNS Tunneling is more about exfiltrating data, not corrupting DNS servers.

upvoted 1 times



  **Anonymous983475** 1 year, 7 months ago

Selected Answer: C

C should be the correct answer.

for more information watch this short vid <https://www.paloaltonetworks.com/cyberpedia/what-is-dns-tunneling>

upvoted 1 times

  **Anonymous983475** 1 year, 7 months ago

Actually jaciro11 is right, C is correct, but the keyword "redirect" makes it incorrect as the information is exfiltrated by being encoded in base64

upvoted 1 times


  **jaciro11** 2 years, 6 months ago

Selected Answer: B

Once the desired data is obtained, the payload encodes the data as a series of 32 characters broken into short strings...

The problem with answer C, is that this not only to get credentials

upvoted 2 times

  **brownb** 2 years, 9 months ago

Im leaning more toward C in this case. Is the point of the DNS attack not to redirect the victim to a server to then attempt to steal data?

upvoted 2 times

  **_nomad_** 2 years, 9 months ago

me too

upvoted 1 times

Which type of attack is social engineering?

- A. trojan
- B. MITM
- C. phishing
- D. malware

Correct Answer: C

Community vote distribution

C (100%)

luismg 1 week, 4 days ago

C is clear.

upvoted 1 times

Marshpillowz 5 months, 1 week ago

Selected Answer: C

C is correct

upvoted 1 times

sull3y 1 year, 7 months ago

C. Phishing

Social engineering is a type of attack that relies on manipulating people to gain access to sensitive information or resources. Social engineering attacks can take many forms, but the most common is phishing.

Phishing is a form of social engineering that uses email or other electronic communication methods to trick people into providing sensitive information or performing an action, such as clicking on a link that downloads malware. Phishing can take many forms, but the goal is always to trick people into giving up their personal information or taking actions that can compromise the security of their computer or network.

Option A, Trojan, is a type of malware that disguises itself as legitimate software in order to gain access to a system. It can be delivered via social engineering but it is not the same thing as social engineering.

upvoted 4 times

sull3y 1 year, 7 months ago

Option B, MITM (Man in the Middle) is a type of attack where an attacker intercepts communication between two parties to steal information. MITM can be performed via social engineering but it is not the same thing as social engineering.

Option D, Malware, is a software that is specifically designed to damage or disrupt computer systems. Malware can be delivered via social engineering but it is not the same thing as social engineering.

upvoted 1 times

idto 2 years, 9 months ago

Agreed. Definitely phishing.

upvoted 3 times

Thusi26 2 years, 9 months ago

Phishing is a form of social engineering. Phishing attacks use email or malicious websites to solicit personal information by posing as a trustworthy organization.

<https://us-cert.cisa.gov/ncas/tips/ST04-014>

upvoted 2 times

What are two DDoS attack categories? (Choose two.)

- A. protocol
- B. source-based
- C. database
- D. sequential
- E. volume-based

Correct Answer: AE

Community vote distribution

AE (100%)

SirFrates24 Highly Voted 3 years, 2 months ago

Volume Based Attacks. Includes UDP floods, ICMP floods, and other spoofed-packet floods. ...
Protocol Attacks. Includes SYN floods, fragmented packet attacks, Ping of Death, Smurf DDoS and more. ...
Application Layer Attacks.
upvoted 10 times

sull3y Highly Voted 1 year, 7 months ago

- A. protocol
- E. volume-based

DDoS (Distributed Denial of Service) attacks are a type of cyberattack that aims to disrupt the normal traffic of a targeted server, service, or network by overwhelming it with a flood of internet traffic. There are several categories of DDoS attacks, including:

A. Protocol: This type of DDoS attack targets the underlying communication protocols used by the targeted server or network, such as TCP, UDP, or ICMP.

E. Volume-based: This type of DDoS attack floods the targeted server or network with a large volume of traffic, such as a flood of packets, in order to overload and disrupt its normal functioning.
upvoted 5 times

Marshpillowz Most Recent 5 months, 1 week ago

Selected Answer: AE

A and E correct
upvoted 1 times

sheki2005 2 years, 4 months ago

A,E are correct answers
upvoted 2 times

heamgu 2 years, 10 months ago

Answer A and E.

There are three different general categories of DDoS attacks:

Volume-based DDoS attacks
Application DDoS attacks
Low-rate DoS (LDoS) attacks
https://tools.cisco.com/security/center/resources/guide_ddos_defense.html
upvoted 4 times

In which type of attack does the attacker insert their machine between two hosts that are communicating with each other?

- A. man-in-the-middle
- B. LDAP injection
- C. insecure API
- D. cross-site scripting

Correct Answer: A

Community vote distribution



Marshpillowz 5 months, 1 week ago

Selected Answer: A

A - MITM
upvoted 1 times

IETF1 9 months ago

A. man-in-the-middle
upvoted 1 times

Abdelmoneim656 10 months, 2 weeks ago

NNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
upvoted 1 times

How does Cisco Advanced Phishing Protection protect users?

- A. It utilizes sensors that send messages securely.
- B. It uses machine learning and real-time behavior analytics.
- C. It validates the sender by using DKIM.
- D. It determines which identities are perceived by the sender.

Correct Answer: B

Community vote distribution

B (100%)

SirFrates24 Highly Voted 3 years, 4 months ago

Cisco® Advanced Phishing Protection provides sender authentication and BEC detection capabilities. It uses advance machine learning techniques, real time behavior analytics, relationship modeling and telemetry to protect against identity deception–based threats.

answer should be B

upvoted 28 times

samismayilov 3 years, 4 months ago

correct . B

upvoted 3 times

Marshpillowz Most Recent 5 months, 1 week ago

Selected Answer: B

Answer is B

upvoted 1 times

sull3y 1 year, 7 months ago

B. It uses machine learning and real-time behavior analytics.

Cisco Advanced Phishing Protection uses machine learning to identify and analyze patterns in email and other online communication, and can detect and block phishing attempts in real-time. It also uses behavior analytics to identify anomalies and suspicious activity, helping to protect users from phishing attacks. The solution also integrates threat intelligence and machine learning to detect new types of malicious emails, and it also uses a combination of techniques, including URL and attachment scanning, to detect and block phishing attacks.

upvoted 3 times

surforlife 2 years, 2 months ago

You can configure mail policies to enable forwarding of message metadata to the Cisco Advanced Phishing Protection cloud service.

When you enable the Cisco AdvancedPhishingProtection cloud service on your email gateway, the following message headers are shared with the Cisco Advanced Phishing Protection Cloud service :

- dkim_selector
- last_hop_ip_address
- helo_domain
- dkim_result
- dkim_domain
- dmarc_result
- dkim_signatures
- to_header
- header_subject
- header_from
- message_id
- spf_result
- rcpt_to
- full_header_from
- mail_from
- Received-SPF
- Received-Header
- Authentication-Results
- reply_to
- original_sender
- received-timestamps
- Authentication-Results-original
- X-originating-ip

upvoted 1 times

Thumbzy_Thumbzy 2 years, 5 months ago

Funny enough, as much as B sounds correct but the flaw with that answer is that Cisco Advanced Phishing Protection doesn't provide "real-time behavior analytics" it actually bases it's data according to historic email data sent to organization. Check out below statement from the cisco webpage

The Advanced Phishing Protection engine on the email gateway checks the unique behavior of all legitimate senders, based on the historic email traffic to your organization. The cloud service interface of the Cisco Advanced Phishing Protection provides risk analysis to distinguish good messages from potentially malicious messages.

https://www.cisco.com/c/en/us/td/docs/security/esa/esa13-5/user_guide/b_ESA_Admin_Guide_13-5/m_advanced_phishing_protection.html
upvoted 2 times

  **migueli** 2 years, 1 month ago


D would be correct if it was "It determines which identities are perceived by the RECEIVER." but it's not so that leaves B as the most correct answer.

upvoted 1 times

  **davezz** 1 year, 9 months ago

Sorry, one more time. On the same link, it also says this in the section of "Benefits of Cisco Advanced Phishing Protection": Gain a real-time understanding of senders, learn, and authenticate email identities and behavioral relationships to protect against BEC attacks

upvoted 1 times

  **davezz** 1 year, 9 months ago

On the same link, it also says in the section of "Benefits of Cisco Advanced Phishing Protection": this Gain a real-time understanding of senders, learn, and authenticate email identities and behavioral relationships to protect against BEC attacks

upvoted 1 times

  **brownbear505** 2 years, 6 months ago

Selected Answer: B

Cisco Advanced Phishing Protection provides Business Email Compromise (BEC) and phishing detection capabilities. It detects identity deception-based threats by performing reputation checks on sender address by using advanced machine learning techniques and added intelligence. This intelligence continuously adapts to drive a real-time understanding of senders and provides enhanced protection.

https://www.cisco.com/c/en/us/td/docs/security/esa/esa13-5/user_guide/b_ESA_Admin_Guide_13-5/m_advanced_phishing_protection.html
upvoted 1 times

  **Wang87** 2 years, 7 months ago

Selected Answer: B

Phishing Defense provides sender authentication and BEC detection capabilities. It uses advance machine learning techniques, real time behavior analytics, relationship modeling and telemetry to protect against identity deception-based threats. This intelligence continuously adapts to drive a real-time understanding of senders, prevent breaches and provide enhanced protection

upvoted 2 times



  **ChrisElkin** 2 years, 7 months ago

Selected Answer: B

Answer D is a red herring. It references identities perceived by the sender, but the Cisco docs point to "identities the recipient perceives". The correct answer is B. Again Cisco docs reference three areas of machine learning:

<https://www.cisco.com/c/dam/en/us/products/collateral/security/cloud-email-security/at-a-glance-c45-740894.pdf>

upvoted 1 times

  **urathod** 2 years, 8 months ago

Selected Answer: B

Correct answer should be B



upvoted 2 times

  **jfuentesf** 2 years, 9 months ago

Selected Answer: B



Advanced Phishing Protection uses advance machine learning techniques. Answer B

upvoted 3 times

  **san111** 2 years, 10 months ago

It should be B

upvoted 2 times

  **u777** 3 years ago

Answer is B

It detects identity deception-based threats by performing reputation checks on sender address by using advanced machine learning techniques and added intelligence. This intelligence continuously adapts to drive a real-time understanding of senders and provides enhanced protection.

https://www.cisco.com/c/en/us/td/docs/security/esa/esa13-5/user_guide/b_ESA_Admin_Guide_13-5/m_advanced_phishing_protection.html

upvoted 1 times

👤 **shahed4062** 3 years ago
Answer is B Machine Learning
upvoted 4 times

👤 **Sarbi** 3 years ago
It should be B.
upvoted 1 times

👤 **kakakayayaya** 3 years, 4 months ago
<https://www.cisco.com/c/dam/en/us/products/collateral/security/cloud-email-security/at-a-glance-c45-740894.pdf>
"Determines which identities the recipient perceives is sending the message" - differ from this answer,
upvoted 2 times

👤 **nospampls** 3 years, 1 month ago
Phishing Defense leverages three areas of machine learning modeling.
• Determines which identities the recipient perceives is sending the message
• Analyzes the expected sending behavior for anomalies relative to that identity
upvoted 1 times

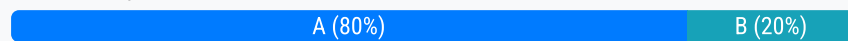
👤 **kakakayayaya** 3 years, 4 months ago
Wrong answer.
It's all about machine learning.
upvoted 4 times

How does DNS Tunneling exfiltrate data?

- A. An attacker registers a domain that a client connects to based on DNS records and sends malware through that connection.
- B. An attacker opens a reverse DNS shell to get into the client's system and install malware on it.
- C. An attacker sends an email to the target with hidden DNS resolvers in it to redirect them to a malicious domain.
- D. An attacker uses a non-standard DNS port to gain access to the organization's DNS servers in order to poison the resolutions.

Correct Answer: A

Community vote distribution



Alee86 Highly Voted 2 years, 11 months ago
Correct Answer A

The attacker registers a domain, such as badsite.com. The domain's name server points to the attacker's server, where a tunneling malware program is installed.

The attacker infects a computer, which often sits behind a company's firewall, with malware. Because DNS requests are always allowed to move in and out of the firewall, the infected computer is allowed to send a query to the DNS resolver. The DNS resolver is a server that relays requests for IP addresses to root and top-level domain servers.

The DNS resolver routes the query to the attacker's command-and-control server, where the tunneling program is installed. A connection is now established between the victim and the attacker through the DNS resolver. This tunnel can be used to exfiltrate data or for other malicious purposes. Because there is no direct connection between the attacker and victim, it is more difficult to trace the attacker's computer.

upvoted 15 times

davezz 2 years, 1 month ago
<https://www.paloaltonetworks.com/cyberpedia/what-is-dns-tunneling>
upvoted 2 times

ic0deem Highly Voted 3 years ago
None of the answers address the actual question.
upvoted 11 times

Marshpillowz Most Recent 5 months, 1 week ago
Selected Answer: A
Answer is A
upvoted 1 times

klu16 6 months, 3 weeks ago
Selected Answer: A
I would also go with answer A.
upvoted 1 times

jhorvat 1 year, 1 month ago
Selected Answer: A
A for sure
upvoted 1 times

Cokamaniako 1 year, 2 months ago
Selected Answer: A
The attacker registers a domain, such as badsite.com. The domain's name server points to the attacker's server, where a tunneling malware program is installed.
The attacker infects a computer, which often sits behind a company's firewall, with malware. Because DNS requests are always allowed to move in and out of the firewall, the infected computer is allowed to send a query to the DNS resolver. The DNS resolver is a server that relays requests for IP addresses to root and top-level domain servers.
upvoted 1 times

Brain_Power 1 year, 2 months ago
Selected Answer: B
I think B is the correct
upvoted 1 times

sull3y 1 year, 5 months ago
DNS tunneling is a technique used by attackers to exfiltrate data by encoding the data into DNS queries or responses. The attacker creates a covert communication channel between the victim's computer and a server controlled by the attacker. This technique uses the DNS protocol to bypass firewalls and other network security measures.

The correct answer is A. An attacker registers a domain that a client connects to based on DNS records and sends malware through that connection. The attacker creates a DNS tunnel by encoding the data in the DNS queries or responses that are sent to the server controlled by the attacker. The server then extracts the data from the queries or responses and sends it to the attacker.

upvoted 3 times

Smilebloke 2 years, 5 months ago

Dont think any of the answers are correct, DNS exfil wont deliver malware. Malware will use DNS tunneling to exfil data.

upvoted 9 times

ffsilveira10 11 months, 2 weeks ago

Perfect, I agree with you

upvoted 1 times

whiteherondance 2 years, 9 months ago

Does anyone else think this questions answers have been mixed up with Question 16?

upvoted 4 times

Question #22

Topic 1

An attacker needs to perform reconnaissance on a target system to help gain access to it. The system has weak passwords, no encryption on the VPN links, and software bugs on the system's applications. Which vulnerability allows the attacker to see the passwords being transmitted in clear text?

- A. unencrypted links for traffic
- B. weak passwords for authentication
- C. improper file security
- D. software bugs on applications

Correct Answer: A

Community vote distribution

A (100%)

Marshpillowz 5 months, 1 week ago

Selected Answer: A

A is correct

upvoted 1 times

Alizade 11 months, 2 weeks ago

Selected Answer: A

A. Unencrypted links for traffic

upvoted 1 times

sull3y 1 year, 7 months ago

A

Reconnaissance in this context refers to the process of gathering information about a target system in order to identify vulnerabilities that can be exploited. The attacker needs to know what weaknesses the system has, so they can plan their attack accordingly.

Answer A is correct because if the VPN links are not encrypted, then any data transmitted over those links, including passwords, can be intercepted and read by an attacker. This allows the attacker to see the passwords being transmitted in clear text and potentially use them to gain access to the system.

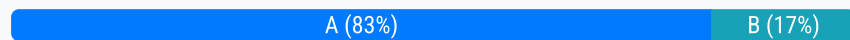
upvoted 1 times

A user has a device in the network that is receiving too many connection requests from multiple machines. Which type of attack is the device undergoing?

- A. SYN flood
- B. slowloris
- C. phishing
- D. pharming

Correct Answer: A

Community vote distribution



pohqinan Highly Voted 2 years, 8 months ago

Answer is A

Slowloris use a single machine to hold as many connections, The question is asking multi machine
[https://en.wikipedia.org/wiki/Slowloris_\(computer_security\)](https://en.wikipedia.org/wiki/Slowloris_(computer_security))

upvoted 7 times

Marshpillowz Most Recent 5 months, 1 week ago

Selected Answer: A

A is correct

upvoted 1 times

jienBoq 1 year, 7 months ago

Selected Answer: A

Slowloris attack originates from one machine. The question mentions multiple machines.

upvoted 1 times

GatPat 1 year, 8 months ago

Selected Answer: A

A SYN flood is a type of denial of service (DoS) attack that is designed to overwhelm a target device or network resource by flooding it with connection requests. In a SYN flood attack, the attacker sends a large number of SYN packets (a type of packet used to initiate a TCP connection) to the target device with spoofed source addresses.

upvoted 3 times

sis_net_sec 1 year, 11 months ago

Selected Answer: B

Slowloris is an application layer DDoS attack which uses partial HTTP requests to open connections between a single computer and a targeted Web server, then keeping those connections open for as long as possible, thus overwhelming and slowing down the target.

upvoted 1 times

Taibu 1 year, 5 months ago

Question is asking " from multiple machines"
Slowloris attacks are initiated from single machine.

upvoted 1 times

PrinM 2 years, 9 months ago

I think answer is B.

upvoted 1 times

PrinM 2 years, 9 months ago

It is A . Slowloris is a type of denial of service attack tool which allows a single machine to take down another machine's web server with minimal bandwidth.

upvoted 2 times

Which two preventive measures are used to control cross-site scripting? (Choose two.)

- A. Enable client-side scripts on a per-domain basis.
- B. Incorporate contextual output encoding/escaping.
- C. Disable cookie inspection in the HTML inspection engine.
- D. Run untrusted HTML input through an HTML sanitization engine.
- E. SameSite cookie attribute should not be used.

Correct Answer: *BD*

Community vote distribution

BD (100%)

[-] **dashiawia** Highly Voted 3 years, 7 months ago
Should be BD
upvoted 9 times

[-] **jfuentesf** Highly Voted 2 years, 9 months ago
Selected Answer: BD
https://en.wikipedia.org/wiki/Cross-site_scripting#Safely_validating_untrusted_HTML_input
B and D
upvoted 5 times

[-] **Marshpillowz** Most Recent 5 months, 1 week ago
Selected Answer: BD
B and D are correct
upvoted 1 times

[-] **sull3y** 1 year, 7 months ago
B. Incorporate contextual output encoding/escaping
D. Run untrusted HTML input through an HTML sanitization engine.

Cross-site scripting (XSS) is a type of security vulnerability that allows an attacker to inject malicious code into a web page viewed by other users. To prevent XSS attacks, it's important to properly handle user input and output on the server-side.

Incorporating contextual output encoding/escaping is an important preventive measure because it ensures that any user input that is included in the output of a web page is properly encoded and cannot be executed as code. This makes it difficult for an attacker to inject malicious code into the web page.

Running untrusted HTML input through an HTML sanitization engine is another important preventive measure because it ensures that any malicious code is removed from the input before it is processed by the server. This also makes it difficult for an attacker to inject malicious code into the web page.

upvoted 4 times

[-] **nomanlands** 2 years, 2 months ago
The cisco training material really only refers to input validation and scripts being executed. They don't really review running HTML through sanitation which seems more likely... I think A and B is what Cisco will look for but who knows
upvoted 1 times

[-] **jaciro11** 2 years, 6 months ago
Selected Answer: BD
It is B & D
upvoted 4 times

[-] **jaciro11** 2 years, 6 months ago
Selected Answer: BD
BD are correct
upvoted 3 times

[-] **mic9** 2 years, 7 months ago
A and B are correct because the question is asking how to prevent before cross scripting happens D its after it happens
upvoted 4 times

[-] **Dinges** 3 years, 2 months ago



ABD are all valid options. They request only two, so if we need to pick only the better options, we should choose BD:

While disabling scripts in general and enabling them on a per-domain basis, it does have some drawbacks for functionality. Users would be forced to enable scripting to have the site fully functional, which would make the user vulnerable to XSS attack again. Selectively disabling scripts is a good alternative, but is not in the question list of answers. That makes BD the better answer.

From https://en.wikipedia.org/wiki/Cross-site_scripting:

-The most significant problem with blocking all scripts on all websites by default is substantial reduction in functionality and responsiveness. Another problem with script blocking is that many users do not understand it, and do not know how to properly secure their browsers. Yet another drawback is that many sites do not work without client-side scripting, forcing users to disable protection for that site and opening their systems to vulnerabilities.

upvoted 4 times

  **Jayde** 3 years, 3 months ago

Unfortunately, A, B, D are all correct answers

https://en.wikipedia.org/wiki/Cross-site_scripting#Safely_validating_untrusted_HTML_input

upvoted 2 times

  **samismayilov** 3 years, 4 months ago

BD are correct

upvoted 3 times

  **juanlecho** 3 years, 5 months ago

I found this at the end of this article.

<https://spanning.com/blog/cross-site-scripting-web-based-application-security-part-3/>

according to that is BD

upvoted 4 times

  **bobby14** 3 years, 7 months ago

Very sad question, because A, B and D are correct answers.

<https://www.techknowlogy.in/security/cross-site-scripting-xss/>

upvoted 1 times

Which threat involves software being used to gain unauthorized access to a computer system?

- A. ping of death
- B. HTTP flood
- C. NTP amplification
- D. virus

Correct Answer: D

Community vote distribution



D (100%)

  **Marshpillowz** 5 months, 1 week ago

Selected Answer: D



D - Virus

upvoted 1 times

  **mm_cisco_2022** 1 year, 8 months ago

<https://www.techtarget.com/searchsecurity/definition/RAT-remote-access-Trojan>



upvoted 2 times

  **mm_cisco_2022** 1 year, 8 months ago

A RAT (remote access Trojan) is malware an attacker uses to gain full administrative privileges and remote control of a target computer.

Therefore virus is used to gain access for the target! select Virus is a correct option

upvoted 2 times

  **ureis** 1 year, 11 months ago

Selected Answer: D

D is correct

upvoted 1 times

  **chawiz** 2 years, 3 months ago

D is the answer

upvoted 1 times

Which two capabilities does TAXII support? (Choose two.)

- A. exchange
- B. pull messaging
- C. binding
- D. correlation
- E. mitigating

Correct Answer: AB

Community vote distribution

AB (100%)

statikd Highly Voted 3 years, 2 months ago

<https://docs.oasis-open.org/cti/taxii/v1.1.1/taxii-v1.1.1-part1-overview.html> "There are three Capabilities that the current version of TAXII supports: push messaging, pull messaging, and discovery." "Discovery does, however, allow for the automated exchange of information..." The correct answer is A and B

upvoted 10 times

karmaomar Highly Voted 3 years, 3 months ago

Correct answer is A& B .. Binding is not supported by TAXII

upvoted 7 times

Marshpillowz Most Recent 5 months, 1 week ago

Selected Answer: AB

A and B correct

upvoted 1 times

SegaMasterSystemAdmin 1 year, 6 months ago

This is a questions that shouldn't even be on this exam. The official guide points to a link for more info so this is BS

upvoted 2 times

sull3y 1 year, 7 months ago

A. exchange refers to the ability of TAXII to exchange Cyber Threat Intelligence (CTI) information between different systems and organizations in a secure and standardized way. This enables different CTI providers to share and consume information in a consistent and interoperable manner.

B. pull messaging refers to the ability of TAXII to use a pull-based messaging model, which allows a client to request specific CTI information from a server, rather than receiving unsolicited CTI information. This allows clients to only receive the CTI information that is relevant to them.

upvoted 2 times

ColonelSRW 2 years, 1 month ago

Not understanding how so many folks vote for A when the TAXII specifications on github repeatedly refer to the binding attributes in very obvious language. Not to mention that answer B is an exchange, so choosing A is redundant. Note that the Official Cert Guide provides a link to the github project as well.

upvoted 2 times

brownbear505 2 years, 6 months ago

Selected Answer: AB

Cisco ScanCenter allows you to pull information on incidents detected by CTA down to your client for further correlation analysis and archival. The service supports MITRE's Trusted Automated eXchange of Indicator Information (TAXII) standard for integration with your Security Information and Event Management (SIEM) system. The TAXII standard specifies transport mechanisms used to share cyber threat information between systems.

upvoted 2 times

elast1c 2 years, 7 months ago

Selected Answer: AB

Binding is not part of it:

"TAXII is bound to neither a particular network protocol nor to a particular message binding"

upvoted 1 times

jfuentesf 2 years, 9 months ago

Selected Answer: AB

TAXII is an exchange utility using Pull Messaging, Push Messaging, Discovery, and Query

upvoted 4 times

pfunkylol 2 years, 9 months ago

Selected Answer: AB

TAXII - Trusted Automated eXchange of Indicator Information. TAXII is an exchange utility using Pull Messaging, Push Messaging, Discovery, and Query.

upvoted 2 times

Alee86 2 years, 11 months ago

Correct Answer B, C

TAXII implementers have a great deal of flexibility in choosing which TAXII Capabilities they support. As noted earlier, TAXII is bound to neither a particular network protocol nor to a particular message binding. In order to facilitate automated communication, TAXII includes the ability to discover the specific TAXII Services a TAXII user (or group of TAXII users) fields, as well as their network address and supported bindings. This does not remove the need for human involvement in the establishment of sharing agreements - sharing agreement negotiation is outside the scope of TAXII. Discovery does, however, allow for the automated exchange of information about which TAXII Capabilities a Producer might support and the technical mechanisms they employ in doing so.

upvoted 3 times

Alee86 2 years, 11 months ago

I meant A and B are correct

upvoted 3 times

Sarbi 3 years ago

The Correct answer is A and B. Tax11 supports pull, push, and discovery. So discovery means exchange. <https://www.forumstandaardisatie.nl/open-standaarden/stix-en-taxii>

upvoted 1 times

Dinges 3 years, 2 months ago

B and C are correct

TAXII does not offer the exchange of the information as a service, enables the exchange, through its services that standardize information. The Standardization is accomplished through bindings, which TAXII defines: Message Binding Specification, Protocol Binding Specification, Content Binding Reference.

<http://docs.oasis-open.org/cti/taxii/v1.1.1/taxii-v1.1.1-part2-services.html>

The Discovery Service provides a requester with a list of TAXII Services and how these Services can be invoked (i.e., the address of the TAXII Daemon that implements that service and the bindings that Daemon supports).

https://taxiiproject.github.io/releases/1.1/TAXII_Overview.pdf

Trusted Automated eXchange of Indicator Information (TAXII™) defines a set of services and message exchanges that, when implemented, enable sharing of actionable cyber threat information across organization and product/service boundaries. TAXII, through its member specifications, defines concepts, protocols and messages to exchange cyber threat information for the detection, prevention, and mitigation of cyber threats. TAXII is not an information sharing initiative...

upvoted 2 times

Dinges 3 years, 2 months ago

I gained new insight:

STIX is structured languages to standardise threat information. Taxii is a protocol for automated exchange of this information.

<https://www.forumstandaardisatie.nl/open-standaarden/stix-en-taxii>

its AB

upvoted 3 times

samismayilov 3 years, 4 months ago

A & B

upvoted 1 times

bobby14 3 years, 7 months ago

There are three Capabilities that the current version of TAXII supports: push messaging, pull messaging, and discovery

upvoted 2 times

NOPT4U 3 years, 6 months ago

And so the right answer is ????

upvoted 2 times

CISCO_CCNP 3 years, 10 months ago

Correct B

and C

upvoted 3 times

thegreek1 3 years, 10 months ago

With the definition listed below: How does C, D, and E communicate that information?

STIX is the critical threat information. TAXII is the protocol to communicate it.

Trusted Automated Exchange of Intelligence Information (TAXII) is an application layer protocol specially designed to enable the exchange of STIX objects for facilitating cyber threat intel sharing and communication.

TAXII runs over HTTPS which also makes it secure and suitable for building online services that can consume and process STIX objects. It provides the developers an ability to build TAXII servers and TAXII clients which can communicate with each other in a request/response manner.

upvoted 2 times

 **NOPT4U** 3 years, 6 months ago

And so for you is A&B?

upvoted 2 times

Which two conditions are prerequisites for stateful failover for IPsec? (Choose two.)

- A. Only the IKE configuration that is set up on the active device must be duplicated on the standby device; the IPsec configuration is copied automatically.
- B. The active and standby devices can run different versions of the Cisco IOS software but must be the same type of device.
- C. The IPsec configuration that is set up on the active device must be duplicated on the standby device.
- D. Only the IPsec configuration that is set up on the active device must be duplicated on the standby device; the IKE configuration is copied automatically.
- E. The active and standby devices must run the same version of the Cisco IOS software and must be the same type of device.

Correct Answer: CE

Reference:

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_vpnav/configuration/15-mt/sec-vpn-availability-15-mt-book/sec-state-fail-ipsec.html

Community vote distribution

CE (100%)

mlu Highly Voted 4 years, 2 months ago
CE

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_vpnav/configuration/15-mt/sec-vpn-availability-15-mt-book/sec-state-fail-ipsec.html#:~:text=Stateful%20failover%20for%20IPsec%20requires,accelerator%20or%20identical%20encryption%20accelerators.
Restrictions for Stateful Failover for IPsec
When configuring redundancy for a VPN, the following restrictions apply:

Both the active and standby devices must run the identical version of the Cisco IOS software, and both the active and standby devices must be connected via a hub or switch.
upvoted 20 times

DJO_2020 Highly Voted 3 years, 10 months ago
C and E

Restrictions for Stateful Failover for IPsec

When configuring redundancy for a VPN, the following restrictions apply:

Both the active and standby devices must run the identical version of the Cisco IOS software, and both the active and standby devices must be connected via a hub or switch.
upvoted 7 times

Marshpillowz Most Recent 5 months, 1 week ago

Selected Answer: CE

C and E are correct
upvoted 1 times

sull3y 1 year, 7 months ago
CE

Stateful failover for IPsec is a feature that allows for a standby device to take over the responsibilities of an active device in the event of a failure. In order for this to happen, certain conditions must be met:

-The IPsec configuration that is set up on the active device must be duplicated on the standby device. This includes the IPsec policies, access control lists, and other settings that are required for the IPsec connections to function.

-The active and standby devices must run the same version of the Cisco IOS software and must be the same type of device. This is necessary to ensure that the standby device is capable of handling the same IPsec connections as the active device and that any issues can be resolved with the same software version.
upvoted 2 times

surforlife 2 years, 1 month ago

Device Requirements

Stateful failover for IPsec requires that your network contains two identical routers that are available to be either the primary or secondary device. Both routers should be the same type of device, have the same CPU and memory, and have either no encryption accelerator or identical encryption accelerators.

Restrictions for Stateful Failover for IPsec

When configuring redundancy for a VPN, the following restrictions apply:

Both the active and standby devices must run the identical version of the Cisco IOS software, and both the active and standby devices must be connected via a hub or switch.

"C and E"

upvoted 1 times

  **nomanlands** 2 years, 2 months ago

Selected Answer: CE

CE because even if sometimes B may work, it's definitely not best practice and you shouldn't be doing it.

upvoted 1 times

  **breezer** 2 years, 5 months ago

Technically B and C are correct.. When the FW HA is upgraded, for a time being both the units are running different OS versions. Still the failover is stateful

upvoted 1 times

  **breezer** 2 years, 5 months ago


Also the doc does not mention that they need to be on same version:

Device Requirements

Stateful failover for IPsec requires that your network contains two identical routers that are available to be either the primary or secondary device. Both routers should be the same type of device, have the same CPU and memory, and have either no encryption accelerator or identical encryption accelerators.

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_vpnnav/configuration/15-mt/sec-vpn-availability-15-mt-book/sec-state-fail-ipsec.html#GUID-484562B6-A113-4901-A630-37869F8494D8

upvoted 1 times

  **brownbear505** 2 years, 6 months ago

Selected Answer: CE

Prerequisites for Stateful Failover for IPsec

Complete, Duplicate IPsec and IKE Configuration on the Active and Standby Devices

Both the active and standby devices must run the identical version of the Cisco IOS software, and both the active and standby devices must be connected via a hub or switch.

upvoted 2 times

  **CipherTrumpet** 2 years, 8 months ago

Selected Answer: CE

Review the prerequisites

upvoted 2 times

  **urathod** 2 years, 8 months ago

Selected Answer: CE

Should be C & E

upvoted 3 times

  **shaanthom** 2 years, 8 months ago

C,E

Prerequisites for Stateful Failover for IPsec

Complete, Duplicate IPsec and IKE Configuration on the Active and Standby Devices

This document assumes that you have a complete IKE and IPsec configuration.

The IKE and IPsec configuration that is set up on the active device must be duplicated on the standby device. That is, the crypto configuration must be identical with respect to Internet Security Association and Key Management Protocol (ISAKMP) policy, ISAKMP keys (preshared), IPsec profiles, IPsec transform sets, all crypto map sets that are used for stateful failover, all access control lists (ACLs) that are used in match address statements on crypto map sets, all AAA configurations used for crypto, client configuration groups, IP local pools used for crypto, and ISAKMP profiles.

upvoted 2 times

  **pfunkylol** 2 years, 9 months ago

Selected Answer: CE



The IKE and IPsec configuration that is set up on the active device must be duplicated on the standby device. Both the active and standby devices must run the identical version of the Cisco IOS software, and both the active and standby devices must be connected via hub or switch. Stateful failover for IPsec requires that your network contains two identical routers that are available to be either the primary or secondary device.

upvoted 2 times

  **djreymix** 2 years, 11 months ago



CE absolutely

upvoted 1 times

  **Raajaa** 3 years, 2 months ago



C and E for sure

upvoted 2 times

  **aalnman** 3 years, 2 months ago

C & E are the correct answer. I deploy Cisco firewalls for a living and C & E are absolutely the correct answers.

upvoted 1 times

  **Zoli6** 3 years, 3 months ago

C and E are correct.

Device Requirements

Stateful failover for IPsec requires that your network contains



two identical routers that are available to be either the primary or secondary device. Both routers should be the same type of device, have the same CPU and memory, and have either no encryption accelerator or identical encryption accelerators.

Restrictions for Stateful Failover for IPsec

When configuring redundancy for a VPN, the following restrictions apply:

Both the active and standby devices must run the identical version of the Cisco IOS software, and both the active and standby devices must be connected via a hub or switch.

upvoted 3 times

  **thefiresays** 3 years, 6 months ago

C & E. Follow the linked document and read the "Prerequisites" section

upvoted 4 times

Which algorithm provides encryption and authentication for data plane communication?

- A. AES-GCM
- B. SHA-96
- C. AES-256
- D. SHA-384

Correct Answer: A

Community vote distribution

A (100%)

Kris92 Highly Voted 3 years, 6 months ago

It is A, AES-GCM can do encryption like all other AES and has an authentication tag, rest of the options can be used for encryption or authentication, but not both.

In cryptography, Galois/Counter Mode (GCM) is a mode of operation for symmetric-key cryptographic block ciphers which is widely adopted for its performance. GCM throughput rates for state-of-the-art, high-speed communication channels can be achieved with inexpensive hardware resources.[1] The operation is an authenticated encryption algorithm designed to provide both data authenticity (integrity) and confidentiality.

https://en.wikipedia.org/wiki/Galois/Counter_Mode

upvoted 12 times

Vic25H Highly Voted 4 years, 1 month ago

It's A because of the GCM, this mode of block ciphers provide confidentiality and integrity. AES-256 refers to the CBC mode because it's the default mode in Cisco.

https://en.wikipedia.org/wiki/Galois/Counter_Mode

https://en.wikipedia.org/wiki/Block_cipher_mode_of_operation

upvoted 6 times

Marshpillowz Most Recent 5 months, 1 week ago

Selected Answer: A

Answer is A - AES GCM

upvoted 1 times

sull3y 1 year, 7 months ago

A. AES-GCM (Advanced Encryption Standard-Galios/Counter Mode) is the correct answer because it provides both encryption and authentication for data plane communication. It uses the Advanced Encryption Standard (AES) algorithm for encryption and the Galios/Counter Mode (GCM) for authentication. GCM is a block cipher mode of operation that provides both confidentiality and integrity for data. It uses a unique initialization vector (IV) for each message and also a unique authentication tag for each message. GCM is considered to be a very secure algorithm that is resistant to tampering and replay attacks.

upvoted 2 times

sull3y 1 year, 7 months ago

AES-256 provides encryption for the data, but it does not provide authentication for the data. Authentication is a process of proving the integrity and origin of the data. It ensures that the data has not been tampered with and that it came from a trusted source. To provide both encryption and authentication for data, AES-256 can be combined with a separate authentication algorithm such as GCM (Galois/Counter Mode) or HMAC (Hash-based Message Authentication Code).

upvoted 1 times

johnsonwale 2 years, 10 months ago

It's A.

upvoted 3 times

naddaf 4 years, 1 month ago

In the Cisco SD-WAN network for unicast traffic, data plane encryption is done by AES-256-GCM, a symmetric-key algorithm that uses the same key to encrypt outgoing packets and to decrypt incoming packets. Each router periodically generates an AES key for its data path (specifically, one key per TLOC) and transmits this key to the vSmart controller in OMP route packets, which are similar to IP route updates. These packets contain information that the vSmart controller uses to determine the network topology, including the router's TLOC (a tuple of the system IP address and traffic color) and AES key. The vSmart controller then places these OMP route packets into reachability advertisements that it sends to the other routers in the network. In this way, the AES keys for all the routers are distributed across the network. Even though the key exchange is symmetric, the routers use it in an asymmetric fashion. The result is a simple and scalable key exchange process that uses the Cisco vSmart Controller.

https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/security/vedge/security-book/security-overview.html#id_112385


upvoted 2 times

Gurak 4 years, 1 month ago

Could someone tell me if I'm wrong? I see AES-256

<https://sdwan->

docs.cisco.com/Product_Documentation/Software_Features/Release_18.1/05Security/01Security_Overview/Data_Plane_Security_Overview#:~:text=duplicates%20encrypted%20packets.,Data%20Plane%20Authentication%20and%20Encryption,each%20other%20over%20this%20connection.
upvoted 1 times

 **Max95** 3 years, 3 months ago
AES-256 should be refer to control plane
upvoted 1 times

Question #29

Topic 1

DRAG DROP -

Drag and drop the capabilities from the left onto the correct technologies on the right.

Select and Place:

detection, blocking, tracking, analysis, and remediation to protect against targeted persistent malware attacks	Next Generation Intrusion Prevention System
superior threat prevention and mitigation for known and unknown threats	Advanced Malware Protection
application-layer control and ability to enforce usage and tailor detection policies based on custom applications and URLs	application control and URL filtering
combined integrated solution of strong defense and web protection, visibility, and controlling solutions	Cisco Web Security Appliance

Correct Answer:

detection, blocking, tracking, analysis, and remediation to protect against targeted persistent malware attacks	superior threat prevention and mitigation for known and unknown threats
superior threat prevention and mitigation for known and unknown threats	detection, blocking, tracking, analysis, and remediation to protect against targeted persistent malware attacks
application-layer control and ability to enforce usage and tailor detection policies based on custom applications and URLs	application-layer control and ability to enforce usage and tailor detection policies based on custom applications and URLs
combined integrated solution of strong defense and web protection, visibility, and controlling solutions	combined integrated solution of strong defense and web protection, visibility, and controlling solutions

 **pohqinan** Highly Voted 2 years, 6 months ago

Key word:

prevention = Next generation intrusion prevention system
Protect = Advanced Malware Protection
Application Layer = Application control and URL filtering
Combined integrated = Cisco web security Appliance
upvoted 13 times

Which two key and block sizes are valid for AES? (Choose two.)

- A. 64-bit block size, 112-bit key length
- B. 64-bit block size, 168-bit key length
- C. 128-bit block size, 192-bit key length
- D. 128-bit block size, 256-bit key length
- E. 192-bit block size, 256-bit key length

Correct Answer: CD

Reference:

https://en.wikipedia.org/wiki/Advanced_Encryption_Standard

Community vote distribution

CD (100%)

Marshpillowz 5 months, 1 week ago

Selected Answer: CD

C and D are correct

upvoted 1 times

sull3y 1 year, 7 months ago

C. 128-bit block size, 192-bit key length

D. 128-bit block size, 256-bit key length

AES (Advanced Encryption Standard) is a symmetric-key encryption algorithm that supports several key and block sizes. The most commonly used key sizes for AES are 128-bit, 192-bit, and 256-bit. The block size is always fixed at 128-bit.

AES-128 uses a 128-bit key length and 128-bit block size

AES-192 uses a 192-bit key length and 128-bit block size

AES-256 uses a 256-bit key length and 128-bit block size

Option A and B are not correct because AES does not support 64-bit block size.

Option E is not correct because AES does not support 192-bit block size

AES-128, AES-192, and AES-256 are the valid key sizes for AES. The block size is always fixed at 128-bit.

upvoted 3 times

nomanlands 2 years, 2 months ago

Selected Answer: CD

128 block size is defined in the AES standard

upvoted 1 times

abdulmalik_mail 2 years, 7 months ago

correct, It's CD

upvoted 3 times

Which two descriptions of AES encryption are true? (Choose two.)

- A. AES is less secure than 3DES.
- B. AES is more secure than 3DES.
- C. AES can use a 168-bit key for encryption.
- D. AES can use a 256-bit key for encryption.
- E. AES encrypts and decrypts a key three times in sequence.

Correct Answer: *BD*

Reference:

https://gpdb.docs.pivotal.io/43190/admin_guide/topics/ipsec.html

Community vote distribution



BD (100%)

  **Marshpillowz** 5 months, 1 week ago

Selected Answer: *BD*

B and D are correct

upvoted 1 times

  **sull3y** 1 year, 7 months ago

B. AES is more secure than 3DES.

D. AES can use a 256-bit key for encryption.

AES (Advanced Encryption Standard) is a widely used symmetric-key encryption algorithm that is considered to be more secure than its predecessor, 3DES (Triple Data Encryption Standard). AES uses a fixed block size of 128 bits and support key sizes of 128,192, and 256 bits.

AES is considered to be more secure than 3DES because it uses a larger block size and key size, which makes it more resistant to brute-force attacks. AES uses a complex substitution-permutation network (SPN) structure which is more secure than the Feistel network of 3DES.

Option A is not correct because AES is more secure than 3DES.

Option C is not correct because AES does not support a 168-bit key size.

Option E is not correct because AES uses only one round of encryption and decryption, not three times.

AES-128, AES-192, and AES-256 are the valid key sizes for AES. The block size is always fixed at 128-bit.

upvoted 2 times

  **abdulmalik_mail** 2 years, 7 months ago

Correct, It's BD

Reference : https://en.wikipedia.org/wiki/Advanced_Encryption_Standard

upvoted 3 times

What is a language format designed to exchange threat intelligence that can be transported over the TAXII protocol?

- A. STIX
- B. XMPP
- C. pxGrid
- D. SMTP

Correct Answer: A

Reference:

https://www.cisco.com/c/en/us/td/docs/security/web_security/scancenter/administrator/guide/b_ScanCenter_Administrator_Guide/b_ScanCenter_Administrator_Guide_chapter_0100011.pdf

Community vote distribution

A (100%)

—  **sull3y** Highly Voted 1 year, 7 months ago

A. STIX (Structured Threat Information eXpression) is a language format designed to exchange threat intelligence that can be transported over the TAXII (Trusted Automated eXchange of Indicator Information) protocol. STIX enables organizations to share cyber threat intelligence, such as information about malware, vulnerabilities, and indicators of compromise, in a structured and machine-readable format. It allows for the exchange of information about the cyber threats, including details on the threat actors, their tools, and tactics, techniques and procedures (TTPs).

upvoted 5 times

—  **Marshpillowz** Most Recent 5 months, 1 week ago

Selected Answer: A

A - STIX

upvoted 1 times

DRAG DROP -

Drag and drop the descriptions from the left onto the correct protocol versions on the right.

Select and Place:

standard includes NAT-T	IKEv1
uses six packets in main mode to establish phase 1	
uses four packets to establish phase 1 and phase 2	IKEv2
uses three packets in aggressive mode to establish phase 1	
uses EAP for authenticating remote access clients	

Correct Answer:

standard includes NAT-T	IKEv1
uses six packets in main mode to establish phase 1	uses six packets in main mode to establish phase 1
uses four packets to establish phase 1 and phase 2	uses three packets in aggressive mode to establish phase 1
uses three packets in aggressive mode to establish phase 1	IKEv2
uses EAP for authenticating remote access clients	standard includes NAT-T
	uses four packets to establish phase 1 and phase 2
	uses EAP for authenticating remote access clients

pfunkylol Highly Voted 2 years, 9 months ago
 correct.
 upvoted 6 times

Marshpillowz Most Recent 5 months, 1 week ago
 Correct!
 upvoted 2 times

Which VPN technology can support a multivendor environment and secure traffic between sites?

- A. SSL VPN
- B. GET VPN
- C. FlexVPN
- D. DMVPN

Correct Answer: C

Reference:

https://www.cisco.com/c/en/us/products/collateral/routers/asr-1000-series-aggregation-services-routers/data_sheet_c78-704277.html

Community vote distribution



nomanlands Highly Voted 2 years, 2 months ago

Selected Answer: C

SSL VPN is a remote access VPN, not a S2S vpn. The question is specifically looking to connect sites.

The below comes from the link that is supplied with the answer as well which should've made this very obvious.

"Third-party compatibility: As the IT world transitions to cloud- and mobile-based computing, more and more VPN routers and VPN endpoints from different vendors are required. The Cisco IOS FlexVPN solution provides compatibility with any IKEv2-based third-party VPN vendors, including native VPN clients from Apple iOS and Android devices."

upvoted 9 times

Marshpillowz Most Recent 5 months, 1 week ago

Selected Answer: C

C - FlexVPN

upvoted 1 times

Cokamaniako 1 year, 2 months ago

Selected Answer: C

• Third-party compatibility: As the IT world transitions to cloud- and mobile-based computing, more and more VPN routers and VPN endpoints from different vendors are required. The Cisco IOS FlexVPN solution provides compatibility with any IKEv2-based third-party VPN vendors, including native VPN clients from Apple iOS and Android devices.

upvoted 1 times

sull3y 1 year, 7 months ago

C. FlexVPN is a VPN technology that can support a multivendor environment and secure traffic between sites.

FlexVPN is a Cisco's IOS-based VPN solution that simplifies the configuration and deployment of VPNs. It provides a unified configuration model that simplifies the process of configuring VPNs across multiple vendors, making it a good choice for multivendor environments.

FlexVPN can support various types of VPNs such as site-to-site, remote access, and Easy VPN remote connections. It also supports various protocols such as IKEv2, SSL, and IPsec.

FlexVPN uses a simplified and unified configuration model, which reduces the complexity of the VPN deployment and allows for easy troubleshooting and maintenance. It also includes advanced features such as IPsec IKEv2, FlexVPN-Cisco Easy VPN, which is a simplified VPN solution for branch offices and teleworkers.

In summary, FlexVPN is a Cisco's VPN technology that simplifies the configuration and deployment of VPNs across multiple vendors and provide a secure traffic between sites, it's a great choice for multivendor environments.

upvoted 2 times

smartcarter 2 years, 1 month ago

"FlexVPN relies on open-standards-based IKEv2 as a security technology and provides on top of it many Cisco® specific enhancements to provide high levels of security, added value, and competitive differentiations".

https://www.cisco.com/c/en/us/products/collateral/routers/asr-1000-series-aggregation-services-routers/data_sheet_c78-704277.html

FlexVpn supports open source standard - Ikev2 which is also supported by other vendors.

C is in order.

upvoted 2 times

nemeses667 2 years, 1 month ago

Can't be A, that is RA - C

• Third-party compatibility: As the IT world transitions to cloud- and mobile-based computing, more and more VPN routers and VPN endpoints

from different vendors are required. The Cisco IOS FlexVPN solution provides compatibility with any IKEv2-based third-party VPN vendors, including native VPN clients from Apple iOS and Android devices.

upvoted 1 times

  **cbadea** 2 years, 2 months ago

Selected Answer: A

A is correct

upvoted 1 times

  **Kevbo02** 2 years, 5 months ago

"FlexVPN is a framework to configure IPsec VPNs on CISCO IOS devices". Since it is a multi-vendor environment the answer is A.

upvoted 2 times

  **asdasd123123iu** 2 years, 3 months ago

In question there is an information about multivendor environment so I understand that Palo Alto, Fortinet and Cisco must support it. B, C and D are Cisco property so only answer A left.

upvoted 2 times

  **royallyre20** 1 year, 11 months ago

question ask about between sites, ssl vpn is use for remote .So answer is C .



upvoted 1 times

  **e_mwas** 2 years, 5 months ago

Selected Answer: C

I change my answer to C

upvoted 3 times

  **mecacig953** 2 years, 5 months ago

Selected Answer: C

FlexVPN was created to simplify the deployment of VPNs, to address the complexity of multiple solutions, and as a unified ecosystem to cover all types of VPN: remote access, teleworker, site to site, mobility, managed security services, and

others.https://www.cisco.com/c/en/us/products/collateral/routers/asr-1000-series-aggregation-services-routers/data_sheet_c78-704277.html

upvoted 1 times

  **e_mwas** 2 years, 6 months ago

I would go with A, the rest seems like cisco proprietary

upvoted 1 times

  **haiderzaid** 1 year, 5 months ago

ssl vpn is for remote access not site to site

upvoted 1 times

  **mmenen** 2 years, 5 months ago

Please keep in mind this is a Cisco Exam ;-)

upvoted 3 times

Which technology must be used to implement secure VPN connectivity among company branches over a private IP cloud with any-to-any scalable connectivity?

- A. DMVPN
- B. FlexVPN
- C. IPsec DVTI
- D. GET VPN

Correct Answer: D

Community vote distribution

D (100%)

Raajaa Highly Voted 3 years, 2 months ago

D is the answer
upvoted 9 times

Kris92 Highly Voted 3 years, 6 months ago

you can use DMVPN with private IPs also
GET VPN is more scalable and needs less resources, but can't be used on internet because IP preservation
I think they expect GET VPN here
upvoted 5 times

Marshpillowz Most Recent 5 months, 1 week ago

Selected Answer: D

D - GetVPN
upvoted 1 times

aal 2 years, 4 months ago

Why not FlexVPN, it can also be used in private networks?
upvoted 1 times

NikoNiko 2 years, 2 months ago

Also DMVPN can be used but GET VPN is better solution.
upvoted 1 times

roolmereyes 1 year, 1 month ago

Because FlexVPN does not support Full Mesh Topology
upvoted 1 times

otzu1 2 years, 4 months ago

Cisco's Group Encrypted Transport VPN (GETVPN) provides a collection of features and capabilities to protect IP multicast group traffic or unicast traffic over a private WAN.

Note "Private"

From the OCG
upvoted 2 times

neta1o 2 years, 8 months ago

This seems to confirm D
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_getvpn/configuration/xr-3s/sec-get-vpn-xr-3s-book/sec-get-vpn.html
upvoted 2 times

thefiresays 3 years, 5 months ago

Over a private line is what they want you to associate GET with.
upvoted 3 times

Javimc 3 years, 7 months ago

Why not DMVPN?
upvoted 1 times

bobby14 3 years, 7 months ago

because over a private IP cloud, not public IP like internet.

upvoted 6 times

Question #36

Topic 1

What is a commonality between DMVPN and FlexVPN technologies?

- A. FlexVPN and DMVPN use the new key management protocol, IKEv2
- B. FlexVPN and DMVPN use IS-IS routing protocol to communicate with spokes
- C. IOS routers run the same NHRP code for DMVPN and FlexVPN
- D. FlexVPN and DMVPN use the same hashing algorithms

Correct Answer: C

Reference:

<https://packetpushers.net/cisco-flexvpn-dmvpn-high-level-design/#:~:text=In%20its%20essence%2C%20FlexVPN%20is,both%20are%20Cisco's%20proprietary%20technologies>

Community vote distribution

C (100%)

thefiresays Highly Voted 3 years, 5 months ago

I'm thinking this question should be: what is NOT a commonality?

IS-IS routing is not a commonality.

Both FlexVPN and DMVPN are compatible with IKEv2, both use NHRP, and they can use the same hashing algorithms.

upvoted 7 times

Dinges 3 years, 2 months ago

The key is necessity.

Both are compatible with IKEv2, but flexVPN supports ONLY IKEv2, where dmvpn also supports IKEv1. So they dont necessarily have the IKE version in communality. Same with Hashing. While they both support the same pool of algorithms, that doesnt necessarily mean that they use the same algorithm in a particular setup.

upvoted 4 times

Marshpillowz Most Recent 5 months, 1 week ago

Selected Answer: C

C appears to be most accurate

upvoted 1 times

otzu1 2 years, 4 months ago

FlexVPN uses NHRP for name resolution I believe. If you pay close attention to the option, it's saying it's the IOS is running the same NHRP being used, which is accurate as it's the build on the IOS.

FlexVPN NHRP is primarily used to establish spoke to spoke communication.

upvoted 1 times

abdulmalik_mail 2 years, 7 months ago

correct, it's C,

FlexVPN is based on these same fundamental technologies with DMVPN using IPSEC, GRE and NHRP

Reference : <https://community.cisco.com/t5/network-security/what-is-the-difference-between-dmvpn-and-flexvpn/td-p/3438913>

upvoted 4 times

Steve122 2 years, 10 months ago

Closest answer is C, both use NHRP

upvoted 1 times

Raajaa 3 years, 2 months ago

not clear with the Q

upvoted 1 times

Which protocol provides the strongest throughput performance when using Cisco AnyConnect VPN?

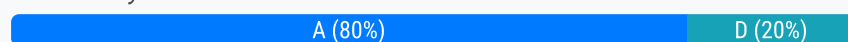
- A. DTLSv1
- B. TLSv1
- C. TLSv1.1
- D. TLSv1.2

Correct Answer: A

Reference:

<https://www.cisco.com/c/en/us/support/docs/security/anyconnect-secure-mobility-client/215331-anyconnect-implementation-and-performanc.html>

Community vote distribution



Husein2024 3 months, 1 week ago

DTLS is UDP based which allows it to outperform TLS (TCP based)
upvoted 1 times

Marshpillowz 5 months, 1 week ago

Selected Answer: A

A - DTLS
upvoted 1 times

ch1be2les3 8 months, 3 weeks ago

Selected Answer: D

The ciphers available are TLS 1.2, DTLS 1.2 and IKEv2. A,B and C are not available on the system. If A was DTLSv1.2 then I think A would be the best choice.
upvoted 1 times

sull3y 1 year, 7 months ago

A. DTLSv1 (Datagram Transport Layer Security version 1) provides the strongest throughput performance when using Cisco AnyConnect VPN.

According to the Cisco document, DTLS (Datagram Transport Layer Security) is the default protocol used by the Cisco AnyConnect VPN Client for SSL connections, it can provide a better throughput performance compared to TLS (Transport Layer Security). DTLS uses UDP as the transport protocol, and it is designed for use in situations where the underlying transport protocol is unreliable, this allows DTLS to be more efficient than TCP-based TLS, especially in situations where network conditions are less than ideal.

DTLS is a variation of the TLS protocol that is optimized for use over unreliable networks and is implemented on top of the User Datagram Protocol (UDP) to provide a more efficient and faster data transfer. It provides similar security to TLS and it is used by Cisco AnyConnect VPN client to secure communications between the VPN client and the VPN server.

upvoted 4 times

mecacig953 2 years, 5 months ago

Selected Answer: A

A is correct

By default, group policies on ASAs are configured to attempt establishing a DTLS tunnel. If UDP 443 traffic is blocked between the VPN headend and the AnyConnect client, it will automatically fallback to TLS. It is recommended to use DTLS or IKEv2 to increase maximum VPN throughput performance. DTLS offers better performance than TLS due to less protocol overhead. IKEv2 also offers better throughput than TLS. Additionally, using AES-GCM ciphers may slightly improve performance. These ciphers are available in TLS 1.2, DTLS 1.2 and IKEv2.

upvoted 3 times

Which group within Cisco writes and publishes a weekly newsletter to help cybersecurity professionals remain aware of the ongoing and most prevalent threats?

- A. Talos
- B. PSIRT
- C. SCIRT
- D. DEVNET

Correct Answer: A

Community vote distribution

A (100%)

Marshpillowz 5 months, 1 week ago

Selected Answer: A

A - Cisco Talos
upvoted 1 times

Alizade 11 months, 2 weeks ago

Selected Answer: A

A. Talos
upvoted 1 times

sull3y 1 year, 7 months ago

A. Talos is a group within Cisco that writes and publishes a weekly newsletter to help cybersecurity professionals remain aware of the ongoing and most prevalent threats.

Talos is a Cisco's threat intelligence team that focuses on identifying and analyzing cyber threats, vulnerabilities, and incidents. They publish a weekly newsletter called the Talos Threat Intelligence Report, which provides information on the latest threats, vulnerabilities, and trends in the cyber security industry. The report also includes technical details and recommendations for mitigating the identified threats.

The Talos Threat Intelligence Report is widely read by cybersecurity professionals and organizations worldwide, as it provides valuable information on the latest threats and vulnerabilities, which helps them to better protect their networks and systems.

upvoted 4 times

mm_cisco_2022 1 year, 8 months ago

Sign Up for Weekly Intelligence Updates from the Talos Security Intelligence and Research Group
<https://engage2demand.cisco.com/subscribetalosthreatsource>
upvoted 2 times

Raajaa 3 years, 2 months ago

A is the answer
upvoted 4 times

When Cisco and other industry organizations publish and inform users of known security findings and vulnerabilities, which name is used?

- A. Common Vulnerabilities, Exploits and Threats
- B. Common Vulnerabilities and Exposures
- C. Common Exploits and Vulnerabilities
- D. Common Security Exploits

Correct Answer: B

Community vote distribution

B (100%)

[-] **👤 Raajaa** **Highly Voted** 3 years, 2 months ago

B is the answer
upvoted 5 times

[-] **👤 johnsonwale** **Highly Voted** 2 years, 10 months ago

It's B.
https://en.wikipedia.org/wiki/Common_Vulnerabilities_and_Exposures
upvoted 5 times

[-] **👤 Marshpillowz** **Most Recent** 5 months, 1 week ago

Selected Answer: B

B is correct
upvoted 1 times

[-] **👤 mhd96far** 5 months, 4 weeks ago

Selected Answer: B

The Common Vulnerabilities and Exposures (CVE) system is a widely adopted standard for identifying and naming security vulnerabilities. It provides a unique identifier (CVE ID) for each known vulnerability, along with additional information about the vulnerability, such as its severity, affected software versions, and potential impact. This standardized approach allows organizations to reference and communicate about vulnerabilities consistently across different platforms and vendors.

upvoted 1 times

[-] **👤 sull3y** 1 year, 5 months ago

B:When Cisco and other industry organizations publish and inform users of known security findings and vulnerabilities, the name used is B. Common Vulnerabilities and Exposures (CVE).

CVE is a standardized naming convention used to identify and track publicly disclosed cybersecurity vulnerabilities and exposures. It provides a unique identifier for each vulnerability and is used by organizations to reference and communicate about specific vulnerabilities.

upvoted 3 times

Which two features of Cisco DNA Center are used in a Software Defined Network solution? (Choose two.)

- A. accounting
- B. assurance
- C. automation
- D. authentication
- E. encryption

Correct Answer: BC

Reference:

<https://www.cisco.com/c/en/us/products/cloud-systems-management/dna-center/index.html>

Community vote distribution

BC (100%)

Raajaa Highly Voted 3 years, 2 months ago

B and C
upvoted 7 times

thefiresays Highly Voted 3 years, 5 months ago

Design
Automation
Provision
Assurance
upvoted 6 times

Marshpillowz Most Recent 5 months, 1 week ago

Selected Answer: BC

B and C are correct
upvoted 1 times

sull3y 1 year, 7 months ago

C. automation
B. assurance

Cisco DNA Center is a network management platform that provides a centralized, programmable, and automated approach to managing and automating the network. The two features that are used in a Software Defined Network solution are Automation and Assurance.

Automation: Cisco DNA Center allows for the automation of network configuration and management, which can improve the speed and efficiency of managing the network. Automating repetitive tasks and reducing manual configuration errors can lead to increased network uptime, improved security, and better network performance.

Assurance: Cisco DNA Center provides real-time monitoring and analytics for the network, which can be used to proactively identify and resolve issues. This feature allows for the assurance of network performance, security and compliance. With the network's real-time telemetry and historical data, it can identify issues, troubleshoot and resolve them quickly, which ensures a smooth network operation.

upvoted 6 times

What provides the ability to program and monitor networks from somewhere other than the DNAC GUI?

- A. ASDM
- B. NetFlow
- C. API
- D. desktop client

Correct Answer: C

Community vote distribution



[-] **👤 Raajaa** **Highly Voted** 👍 3 years, 2 months ago

API...C is the answer
upvoted 7 times

[-] **👤 Marshpillowz** **Most Recent** 🕒 5 months, 1 week ago

Selected Answer: C

C - API
upvoted 1 times

What is a function of 3DES in reference to cryptography?

- A. It encrypts traffic.
- B. It creates one-time use passwords.
- C. It hashes files.
- D. It generates private keys.

Correct Answer: A

Community vote distribution

A (100%)

Raajaa Highly Voted 3 years, 2 months ago

A is the answer
upvoted 6 times

Marshpillowz Most Recent 5 months, 1 week ago

Selected Answer: A

A - encryption
upvoted 1 times

sull3y 1 year, 7 months ago

A. It encrypts traffic.

3DES (Triple Data Encryption Standard) is a symmetric-key block cipher algorithm that is used to encrypt data. It uses the same key for encrypting and decrypting data, and it is considered to be more secure than its predecessor, the Data Encryption Standard (DES), as it applies the DES algorithm three times in succession to the data, which makes it more resistant to cryptographic attacks.

3DES is widely used in various applications such as virtual private networks (VPNs), electronic commerce (e-commerce), and other secure communications systems, to encrypt and protect data in transit.

It is important to note that 3DES is considered less secure than AES (Advanced Encryption Standard) which is now widely recommended.
upvoted 3 times

Which two activities can be done using Cisco DNA Center? (Choose two.)

- A. DHCP
- B. design
- C. accounting
- D. DNS
- E. provision

Correct Answer: BE

Reference:

https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/1-2-1/user_guide/b_dnac_ug_1_2_1/b_dnac_ug_1_2_chapter_00.pdf

Community vote distribution

BE (100%)

[-] **Cock** Highly Voted 2 years, 9 months ago
Design Automation Provision Assurance
upvoted 10 times

[-] **Wang87** Highly Voted 2 years, 7 months ago
Selected Answer: BE
DNAC can be used for Design and Provision B & E are Correct answers
upvoted 5 times

[-] **Marshpillowz** Most Recent 5 months, 1 week ago
Selected Answer: BE
B and E are correct
upvoted 1 times

[-] **sull3y** 1 year, 7 months ago
B. design
E. provision

Cisco DNA Center is a network management platform that provides a centralized, programmable, and automated approach to managing and automating the network. The two activities that can be done using Cisco DNA Center are design and provision.

Design: Cisco DNA Center provides an intuitive and visual interface for designing, modeling, and simulating the network. It allows network administrators to create and test network configurations before deploying them to the production network. This feature can help to improve the speed and efficiency of managing the network.

Provision: Cisco DNA Center provides an automated approach to provisioning and configuring network devices. It allows network administrators to automate repetitive tasks such as configuring network devices, and reducing manual configuration errors can lead to increased network uptime, improved security, and better network performance.

upvoted 4 times

Which PKI enrollment method allows the user to separate authentication and enrollment actions and also provides an option to specify HTTP/TFTP commands to perform file retrieval from the server?

- A. terminal
- B. selfsigned
- C. url
- D. profile

Correct Answer: D

Community vote distribution

D (100%)

Stardec Highly Voted 2 years, 10 months ago

D.

Certificate Enrollment Profiles

Certificate enrollment profiles allow users to specify certificate authentication, enrollment, and reenrollment parameters when prompted. The values for these parameters are referenced by two templates that make up the profile. One template contains parameters for the HTTP request that is sent to the CA server to obtain the certificate of the CA (also known as certificate authentication); the other template contains parameters for the HTTP request that is sent to the CA for certificate enrollment.

upvoted 9 times

Marshpillowz Most Recent 5 months, 1 week ago

Selected Answer: D

D - profile

upvoted 1 times

Raajaa 3 years, 2 months ago

D is the correct answer

upvoted 2 times

cwolf 3 years, 3 months ago

D seems correct

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_pki/configuration/15-mt/sec-pki-15-mt-book/sec-cert-enroll-pki.html#GUID-CF1092E8-D696-491E-A1E2-302CAF9FBB64

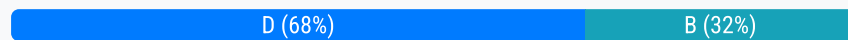
upvoted 4 times

Which type of API is being used when a security application notifies a controller within a software-defined network architecture about a specific security threat?

- A. southbound API
- B. westbound API
- C. eastbound API
- D. northbound API

Correct Answer: D

Community vote distribution



eazy99 Highly Voted 2 years, 12 months ago

Don't over think it guys, the provided answer is correct. The security application which is the (northbound) is the one who is notifying, (sending the notification to the southbound)

upvoted 10 times

Premium_Pils Most Recent 1 month ago

Selected Answer: B

I go with B. For me Northbound would be to control policies and simplify the management actions. Westbound is to integrate the controller with other devices, and use inputs received from other devices.

upvoted 1 times

ffsilveira10 4 months, 3 weeks ago

Selected Answer: B

I would go with B.

upvoted 2 times

Marshpillowz 5 months, 1 week ago

Selected Answer: D

Answer is D

upvoted 1 times

eriksm 11 months ago

Selected Answer: D

Northbound API: Intent-based API
Southbound API: controllers -> devices

upvoted 1 times

jku2cya 1 year, 2 months ago

Selected Answer: D

D - application is north of the controller

upvoted 3 times

appfw 1 year, 5 months ago

Answer is D:

Northbound APIs --> communication between Applications and the SDN Controller
Southbound APIs --> communication between Network Devices and the SDN Controller

upvoted 3 times

Carlis 1 year, 5 months ago

Intent (Northbound) APIs

- used to enforce the configurations and settings
- creating and managing sites
- retrieving network health information
- policy creation
- Rest APIs
- Common in web services
- Use HTTP requests for data transfer
- GET, PUT, POST and DELETE requests

Integration (Westbound) APIs:

- Integrate controller with other platforms
- Communicate with third-party IT service management solutions
- Ticket and request automation

- Publish the network data, events and notifications to the external systems



Multivendor Support (Southbound) APIs:

- Multivendor Software Development Kit (SDK)
- SDKs can include multiple APIs
- SDKs allow for management of non-Cisco devices

Events and Notifications (Eastbound) APIs:

- Allow external systems to take action against notifications
- Especially useful for security compliance

upvoted 2 times

  **Carlis** 1 year, 5 months ago

I would go for Westbound

upvoted 2 times

  **ddev3737** 1 year, 7 months ago

Sorry meant Northbound APIs are typically used to communicate between the SDN controller and the services and applications running over the network. However, in the context of the question provided, a security application is notifying the controller about a specific security threat, which would be accomplished through a Southbound API. Northbound APIs are generally used for different purposes such as automation and orchestration of the network components, whereas Southbound APIs are used for communication between the controller and the underlying network devices.

upvoted 1 times

  **ddev3737** 1 year, 7 months ago

How about this info? Northbound APIs (SDN northbound APIs) are typically RESTful APIs that are used to communicate between the SDN controller and the services and applications running over the network. Such northbound APIs can be used for the orchestration and automation of the network components to align with the needs of different applications via SDN network programmability. In short, northbound APIs are basically the link between the APPLICATIONS and the SDN controller.

upvoted 1 times

  **GatPat** 1 year, 8 months ago

Selected Answer: D

NorthBound API for sure



upvoted 2 times

  **SulSulEi** 2 years ago

Answer is D, check quick video below,

<https://youtu.be/BUuNgQn3uNc>

upvoted 3 times

  **getafix** 2 years, 2 months ago

Selected Answer: D

Northbound APIs (SDN northbound APIs) are typically RESTful APIs that are used to communicate between the SDN controller and the services and applications running over the network. Such northbound APIs can be used for the orchestration and automation of the network components to align with the needs of different applications via SDN network programmability. In short, northbound APIs are basically the link between the applications and the SDN controller. In modern environments, applications can tell the network devices (physical or virtual) what type of resources they need and, in turn, the SDN solution can provide the necessary resources to the application.

From the Cisco OCG. Answer is D since the question talks about a security application

upvoted 2 times

  **TesterDude** 2 years, 3 months ago

Selected Answer: D

It's D.

Northbound APIs (SDN northbound APIs) are typically RESTful APIs that are used to communicate between the SDN controller and the services and applications running over the network. Such northbound APIs can be used for the orchestration and automation of the network components to align with the needs of different applications via SDN network programmability. In short, northbound APIs are basically the link between the APPLICATIONS and the SDN controller.

Santos, Omar. CCNP and CCIE Security Core SCOR 350-701 Official Cert Guide (p. 118). Pearson Education. Kindle Edition.

upvoted 3 times

  **awsnoob1** 2 years, 4 months ago

Answer should be B , the difference between Northbound and Westbound API interfaces is very clear from the bellow link :

<https://blogs.cisco.com/networking/with-apis-cisco-dna-center-can-improve-your-competitive-advantage>

upvoted 1 times

  **Sattm1** 2 years, 4 months ago

Selected Answer: B

Westbound should be right:

Northbound - intent-based management user to controller

Southbound - Controller to network elements

Eastbound - Controller to other Applications

Westbound - Other software to Controller

<https://developer.cisco.com/docs/dna-center/#!cisco-dna-center-platform-overview/intent-api-northbound>

upvoted 1 times

  **ospf858** 2 years, 5 months ago

Answer should B.

<https://blogs.cisco.com/networking/with-apis-cisco-dna-center-can-improve-your-competitive-advantage>

upvoted 1 times

An organization has two machines hosting web applications. Machine 1 is vulnerable to SQL injection while machine 2 is vulnerable to buffer overflows. What action would allow the attacker to gain access to machine 1 but not machine 2?

- A. sniffing the packets between the two hosts
- B. sending continuous pings
- C. overflowing the buffer's memory
- D. inserting malicious commands into the database

Correct Answer: D

Community vote distribution

D (100%)

Raajaa Highly Voted 3 years, 2 months ago

D is the answer
upvoted 10 times

eazy99 Highly Voted 2 years, 12 months ago

Yup, D it is
upvoted 5 times

Marshpillowz Most Recent 5 months, 1 week ago

Selected Answer: D

D is right
upvoted 1 times

eriksm 11 months ago

Selected Answer: D

D is the right answer
upvoted 1 times

Alizade 11 months, 2 weeks ago

Selected Answer: D

D. inserting malicious commands into the database
upvoted 1 times

sull3y 1 year, 7 months ago

D. inserting malicious commands into the database.

SQL injection is a type of security vulnerability that allows an attacker to insert malicious code into an SQL statement, allowing them to gain unauthorized access to a database or manipulate its data. This can be done by exploiting vulnerabilities in the way that user input is handled by a web application. So by inserting malicious commands into the database hosted on Machine 1, an attacker can gain access to the database and potentially steal or manipulate data.

On the other hand, a buffer overflow is a type of security vulnerability that occurs when more data is written to a buffer than it can hold. This can cause the program to crash or execute arbitrary code, allowing an attacker to gain control of the affected machine. However, in this scenario, Machine 2 is vulnerable to buffer overflows, so overflowing the buffer's memory on Machine 2 would allow the attacker to gain access to Machine 2 but not to Machine 1.

upvoted 4 times

What is the function of SDN southbound API protocols?

- A. to allow for the static configuration of control plane applications
- B. to enable the controller to use REST
- C. to enable the controller to make changes
- D. to allow for the dynamic configuration of control plane applications

Correct Answer: C

Community vote distribution

C (100%)

statikd Highly Voted 3 years, 2 months ago

Official Cert Guide: "Southbound APIs enable SDN controllers to dynamically make changes based on real-time demands and scalability needs." But... the Northbound APIs communicates with the control plane applications, not the Southbound APIs. So technically C is still correct, even though Southbound APIs make dynamic changes it still makes changes, hence does not have to say it makes the changes dynamically. This is one of them questions to catch you off guard. The key is the control plane applications. Northbound also uses the REST.

upvoted 7 times

Marshpillowz Most Recent 5 months, 1 week ago

Selected Answer: C

C appears most accurate here

upvoted 1 times

jku2cya 1 year, 2 months ago

Selected Answer: C

C is the best amongst a bunch of really bad alternatives.

Don't think its B as there is mention of REST but not REST API. Don't think its either A or D because SDN controllers either control north (application) or south (network/switch)

upvoted 1 times

sull3y 1 year, 7 months ago

C. to enable the controller to make changes. The southbound API protocol of a Software-Defined Network (SDN) enables communication between the SDN controller and the networking devices, such as switches and routers, in the network. This allows the controller to make changes and manage the network's configuration.

upvoted 4 times

getafix 2 years, 2 months ago

Selected Answer: C

In an SDN architecture, southbound APIs are used to communicate between the SDN controller and the switches and routers within the infrastructure. These APIs can be open or proprietary. Southbound APIs enable SDN controllers to dynamically make changes based on real-time demands and scalability needs. OpenFlow and Cisco OpFlex provide southbound API capabilities.

Above is an extract from the OCG (Official Cert Guide for the exam).

upvoted 3 times

TesterDude 2 years, 3 months ago

Selected Answer: C

C
Southbound APIs enable SDN controllers to dynamically make changes based on real-time demands and scalability needs. OpenFlow and Cisco OpFlex provide southbound API capabilities.

Santos, Omar. CCNP and CCIE Security Core SCOR 350-701 Official Cert Guide (p. 118). Pearson Education. Kindle Edition.

upvoted 2 times

Thusi26 2 years, 12 months ago



C

How Do SDN Southbound APIs Work?

Southbound APIs facilitate control over the network and enable the SDN Controller to dynamically make changes according to real-time demands and needs.

OpenFlow, which was developed by the Open Networking Foundation (ONF), is the first and probably most well-known southbound interface. OpenFlow defines the way the SDN Controller should interact with the forwarding plane to make adjustments to the network, so it can better adapt to changing business requirements. With OpenFlow, entries can be added and removed to the internal flow-table of switches and routers to make the network more responsive to real-time traffic demands.

upvoted 4 times

  **Raajaa** 3 years, 2 months ago



I go with C as only Northbound APIs deals with control plane

upvoted 4 times

  **bazinga31** 3 years, 2 months ago

C? But it allows the controller to [dynamically] make changes. Doesn't mention about the control plane?

upvoted 1 times

  **SirFrates24** 3 years, 3 months ago

Southbound APIs facilitate control over the network and enable the SDN Controller to dynamically make changes according to real-time demands and needs. D is the correct answer

upvoted 2 times

  **SirFrates24** 3 years, 2 months ago

i stand corrected. C is the answer

upvoted 1 times

  **rad9899** 3 years, 4 months ago

D. to allow for the dynamic configuration of control plane applications
its correct

upvoted 3 times

DRAG DROP -

Drag and drop the threats from the left onto examples of that threat on the right.

Select and Place:

DoS/DDoS	A stolen customer database that contained social security numbers and was published online.
insecure APIs	A phishing site appearing to be a legitimate login page captures user login information.
data breach	An application attack using botnets from multiple remote locations that flood a web application causing a degraded performance or a complete outage.
compromised credentials	A malicious user gained access to an organization's database from a cloud-based application programming interface that lacked strong authentication controls.

Correct Answer:

DoS/DDoS	data breach
insecure APIs	compromised credentials
data breach	DoS/DDoS
compromised credentials	insecure APIs

Marshpillowz 5 months, 1 week ago

Answer is correct
upvoted 2 times

mm_cisco_2022 1 year, 8 months ago

1 - 3
2 - 4
3 - 1
4 - 2
upvoted 2 times

sis_net_sec 1 year, 11 months ago

1-3
2-4
3-1
4-2
upvoted 2 times

Kyle1776 2 years, 6 months ago

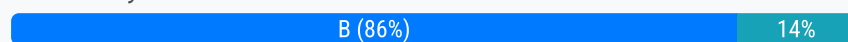
1-3
2-4
3-1
4-2
upvoted 3 times

What is the difference between Cross-site Scripting and SQL Injection attacks?

- A. Cross-site Scripting is when executives in a corporation are attacked, whereas SQL Injection is when a database is manipulated.
- B. Cross-site Scripting is an attack where code is executed from the server side, whereas SQL Injection is an attack where code is executed from the client side.
- C. Cross-site Scripting is a brute force attack targeting remote sites, whereas SQL Injection is a social engineering attack.
- D. Cross-site Scripting is an attack where code is injected into a database, whereas SQL Injection is an attack where code is injected into a browser.

Correct Answer: B

Community vote distribution



jaciro11 Highly Voted 2 years, 6 months ago

Selected Answer: B

Cross-site Scripting is an attack where code is executed from the server side, whereas SQL Injection is an attack where code is executed from the client side.

upvoted 9 times

sull3y Highly Voted 1 year, 7 months ago

The correct answer is: B. Cross-site Scripting is an attack where code is executed from the client side, whereas SQL Injection is an attack where code is executed from the server side.

In Cross-site scripting (XSS) the attacker injects malicious code into a web page viewed by other users, the code is executed by the client's browser. SQL Injection is a server-side attack, where the attacker manipulates an SQL statement by injecting malicious code into the query. The malicious code is executed on the server, often with the goal of accessing or modifying sensitive data in the database

upvoted 5 times

Husein2024 Most Recent 3 months, 1 week ago

The answer is B

upvoted 1 times

Marshpillowz 5 months, 1 week ago

Selected Answer: B

B is correct

upvoted 1 times

squirrelzzz 5 months, 4 weeks ago

SQL is injected in browser and runs on server. XSS is injected in browser and loaded into server database then executes on clients browser

upvoted 1 times

jku2cya 1 year, 2 months ago

Selected Answer: B

Can't be A because XSS is not whaling.

Can't be D because XSS because code is injected into the web app and not database: <https://owasp.org/www-community/attacks/xss/> ; and SQL Injection is more about browser input rather than injecting code into a browser: https://owasp.org/www-community/attacks/SQL_Injection

upvoted 2 times

ddev3737 1 year, 7 months ago

Option A is the closest to being correct, as executives in a corporation can be considered targeted users of a website, and XSS is a client-side vulnerability that targets other users of the application.

So, to summarize:

XSS is a client-side vulnerability where malicious code is injected into a website and targets other users of the application, including executives in a corporation.

SQLi is a server-side vulnerability where an attacker can manipulate the database of a website by injecting malicious SQL commands.

upvoted 2 times

psuoh 1 year, 7 months ago

Answer B appears to be the Cisco's choice as correct.

Key Concepts of XSS

XSS is a web-based attack performed on vulnerable web applications.

In XSS attacks, the victim is the user and not the application.

In XSS attacks, malicious content is delivered to users using JavaScript.

upvoted 2 times

👤 **tom_1991** 2 years, 3 months ago

I would say D is most accurate. For XSS malicious links can be inserted into databases, If webpages store and pull links to append to their HTML (instead of manually typing each one in their code `click me`) so when an unsuspecting user download the page and pulls the links from the database, they unknowingly pull those malicious links as well.

The reason why it isn't B is because XSS isn't executed on the server, it is executed on the clients browser when the user initially downloads the HTML page and all associated scripts (.js .css etc). SQL code is sent from the user using HTML form (POST) submission and executed on the server when the server opens a connection to the database and executes the SQL commands.

The answer could equally be A as well however, XSS isn't just targeted at executives, It could be targeted at anyone providing there is a vulnerability to exploit.

upvoted 3 times

👤 **Metgatz** 2 years, 4 months ago

Selected Answer: D

D Explanation:

Therefore only answer D is left. In XSS, an attacker will try to inject his malicious code (usually malicious links) into a database. When other users follow his links, their web browsers are redirected to websites where attackers can steal data from them. In a SQL Injection, an attacker will try to inject SQL code (via his browser) into forms, cookies, or HTTP headers that do not use data sanitizing or validation methods of GET/POST parameters.

Note: The main difference between a SQL and XSS injection attack is that SQL injection attacks are used to steal information from databases whereas XSS attacks are used to redirect users to websites where attackers can steal data from them.

upvoted 3 times

👤 **brownbear505** 2 years, 6 months ago

Selected Answer: B

An attacker can use XSS to send a malicious script to an unsuspecting user. The end user's browser has no way to know that the script should not be trusted, and will execute the script. Because it thinks the script came from a trusted source, the malicious script can access any cookies, session tokens, or other sensitive information retained by the browser and used with that site. These scripts can even rewrite the content of the HTML page.

upvoted 2 times

👤 **Wang87** 2 years, 7 months ago

Selected Answer: B

Answer is B as XSS happens when Client is exploited and used to run code on another site. 2nd part where SQL injection happens from client end and run on server. Notice the wording it says FROM client which is correct.

upvoted 4 times

👤 **Brumik** 2 years, 7 months ago

If anything definitely A. XSS is a client side side attack, the code is executed from the clients browser. SQL injection is a server side attack, code is executed on the server side. B is wrong. C+D are completely wrong.

upvoted 2 times

👤 **bassfunk** 2 years, 8 months ago

B is correct. The key word there is "from". They are talking about the origin of the code not where it's being executed.

upvoted 4 times

👤 **rbrain** 2 years, 8 months ago

Yes indeed, it should be B

upvoted 2 times

👤 **duck_hat** 2 years, 10 months ago

I think maybe can mean stored XSS and SQL inject

A SQL injection attack consists of insertion or "injection" of a SQL query via the input data from the client to the application.

https://owasp.org/www-community/attacks/SQL_Injection

upvoted 1 times

👤 **jaciro11** 2 years, 10 months ago

Its B

The only problem with A is @Cross-site Scripting is when executives in a corporation are attacked@

upvoted 3 times

👤 **eazy99** 2 years, 12 months ago

This question is so bad, but I would go with A and here is why. First, all other options is messed up and obviously wrong without questioning.

Now, if we look at A, the second part is perfect description for SQL " SQL Injection is when a database is manipulated"

So what about XSS? I would say that because all other options are wrong that leaves us to the fact that when XSS are performed on the corporation internal website, executives and everyone else is attacked.

I'm assuming this is why they chose A, the rest of options is so bad.

upvoted 3 times

DRAG DROP -

Drag and drop the common security threats from the left onto the definitions on the right.

Select and Place:

phishing	a software program that copies itself from one computer to another, without human interaction
botnet	unwanted messages in an email inbox
spam	group of computers connected to the Internet that have been compromised by a hacker using a virus or Trojan horse
worm	fraudulent attempts by cyber criminals to obtain private information

Correct Answer:

phishing	worm
botnet	spam
spam	botnet
worm	phishing

flash007 5 months, 1 week ago

Worm copies to other devices
upvoted 2 times

Marshpillowz 5 months, 1 week ago

Answer is correct
upvoted 2 times

mbaviskar01 1 year, 7 months ago

1 —> 4
2 —> 3
3 —> 2
4 —> 1
upvoted 2 times

Which type of dashboard does Cisco DNA Center provide for complete control of the network?

- A. distributed management
- B. service management
- C. application management
- D. centralized management

Correct Answer: D

Community vote distribution

D (100%)

sull3y Highly Voted 1 year, 7 months ago

D. centralized management.

Cisco DNA Center provides a centralized management dashboard that allows network administrators to have complete control over the network. The dashboard provides a single point of access to manage and monitor all aspects of the network, including devices, users, applications, and services. It allows administrators to easily configure, troubleshoot, and optimize their network, ensuring that it is running at peak performance.

upvoted 5 times

Marshpillowz Most Recent 5 months, 1 week ago

Selected Answer: D

D - centralized

upvoted 1 times

```
import requests
url = https://api.amp.cisco.com/v1/computers
headers = {
    'accept': 'application/json',
    'Content-type': 'application/json',
    'authorization': "Basic <API Credentials",
    'cache-control': "no-cache",
}
response = requests.request("GET", url, headers=headers)
print(response.text)
```

Refer to the exhibit. What will happen when this Python script is run?

- A. The list of computers, policies, and connector statuses will be received from Cisco AMP.
- B. The list of computers and their current vulnerabilities will be received from Cisco AMP.
- C. The compromised computers and malware trajectories will be received from Cisco AMP.
- D. The compromised computers and what compromised them will be received from Cisco AMP.

Correct Answer: A

Community vote distribution

A (100%)

iluvmicrosoft 5 months ago

im struggling with this one, all the other json scripts that print multiple records have a for loop:

```
for computer in response_json['data']:
    hostname = computer['hostname']
    print(hostname)
```

how is it printing more than 1 line?

upvoted 1 times

ffsilveira10 4 months, 3 weeks ago

Because it is doing an API call without any filter, so in that case it will return all computers.

upvoted 1 times

Marshpillowz 5 months, 1 week ago

Selected Answer: A

A is correct

upvoted 1 times

otzu1 2 years, 4 months ago

A

[https://api-docs.amp.cisco.com/api_actions/details?](https://api-docs.amp.cisco.com/api_actions/details?api_action=GET+%2Fv1%2Fcomputers&api_host=api.amp.cisco.com&api_resource=Computer&api_version=v1)

[api_action=GET+%2Fv1%2Fcomputers&api_host=api.amp.cisco.com&api_resource=Computer&api_version=v1](https://api-docs.amp.cisco.com/api_actions/details?api_action=GET+%2Fv1%2Fcomputers&api_host=api.amp.cisco.com&api_resource=Computer&api_version=v1)

upvoted 4 times

```
import requests
client_id = '<Client ID>'
api_key = '<API Key>'
url = 'https://api.amp.cisco.com/v1/computers'
response = requests.get(url, auth=(client_id, api_key))
response_json = response.json()
for computer in response_json['data']:
    hostname = computer['hostname']
    print(hostname)
```

Refer to the exhibit. What will happen when the Python script is executed?

- A. The hostname will be printed for the client in the client ID field.
- B. The hostname will be translated to an IP address and printed.
- C. The script will pull all computer hostnames and print them.
- D. The script will translate the IP address to FQDN and print it.

Correct Answer: C

Community vote distribution

C (100%)

Marshpillowz 5 months, 1 week ago

Selected Answer: C

C is correct

upvoted 1 times

red_sparrow_Gr 9 months, 1 week ago

I believe that the correct answer is A.

The for response is for a specific client_ID.....

upvoted 2 times

MPoels 6 months, 2 weeks ago

Answer C is right. The answer to the question of what a client ID is:

API credentials (API Client ID & API Key) will allow other programs to retrieve and modify your Cisco AMP for Endpoints data. It is functionally equivalent to a username and password, and should be treated as such.

<https://www.cisco.com/c/en/us/support/docs/security/amp-endpoints/201121-Overview-of-the-Cisco-AMP-for-Endpoints.html>

upvoted 1 times

With which components does a southbound API within a software-defined network architecture communicate?

- A. applications
- B. controllers within the network
- C. appliances
- D. devices such as routers and switches

Correct Answer: D

Community vote distribution

D (100%)

Raajaa Highly Voted 3 years, 2 months ago

D is the answer
upvoted 10 times

flash007 Most Recent 5 months, 1 week ago

Southbound is when it goes to the network devices
upvoted 1 times

Marshpillowz 5 months, 1 week ago

Selected Answer: D

D is correct
upvoted 1 times

alexyoizat24 1 year, 4 months ago

D is correct since SBI(southboundinterface) mainly deals with data plane(network device)

<https://www.ciscopress.com/articles/article.asp?p=2995354&seqNum=2>

https://ptgmedia.pearsoncmg.com/images/chap16_9781587147135/elementLinks/16fig05_alt.jpg

upvoted 1 times

achille5 1 year, 6 months ago

Selected Answer: D

A southbound API within a software-defined network architecture typically communicates with devices such as routers and switches
upvoted 2 times

dr4gn00t 2 years, 7 months ago

I think D is the right answer but C is correct also since the question is SDN in general, not just Cisco solutions.
upvoted 1 times

flejd 2 years, 8 months ago

B. Controller to network devices.
upvoted 2 times

asdasd123123iu 2 years, 3 months ago

No, answer B is 'controllers within the network'. Correct is D
upvoted 3 times

Which method is used to deploy certificates and configure the supplicant on mobile devices to gain access to network resources?

- A. BYOD onboarding
- B. MAC authentication bypass
- C. client provisioning
- D. Simple Certificate Enrollment Protocol

Correct Answer: D

Community vote distribution



karmaomar Highly Voted 3 years, 3 months ago
correct answer is A. BYOD onboarding
upvoted 22 times

Tuxinator Highly Voted 1 year, 7 months ago
Selected Answer: C
C.

The method used to deploy certificates and configure the supplicant on mobile devices to gain access to network resources is C) client provisioning.

Client provisioning is a process of deploying network settings, certificates, and other configuration information to mobile devices to enable them to securely connect to a network. This process involves configuring the supplicant, which is the client software that communicates with the network, to use the appropriate authentication methods and credentials required to access network resources.

BYOD onboarding is a process that enables personal devices to connect to a corporate network, and it may include client provisioning as one of its steps. MAC authentication bypass is a method of granting network access based on the device's MAC address, without requiring any authentication credentials. Simple Certificate Enrollment Protocol (SCEP) is a protocol used for certificate management, but it is not specifically related to configuring the supplicant or deploying network settings to mobile devices.
upvoted 9 times

nseguy 1 year, 4 months ago
Thank you, ChatGPT?
upvoted 2 times

mhd96far 5 months, 4 weeks ago
do not trust chat gpt on questions like that, especially for Cisco exams, it makes a lot of mistakes
upvoted 2 times

ffsilveira10 Most Recent 4 months, 3 weeks ago
Selected Answer: D
I would go with D.

a) the question don't say nothing if the device is corporate owned or not. So BYOD it doesn't make sense.
b) authentication bypass certainly is not a method to deploy certificates.
c) client provisioning is not related to certificates deployment.
upvoted 3 times

Marshpillowz 5 months, 1 week ago
Selected Answer: A
I think A - BYOD
upvoted 1 times

4pelos 6 months, 1 week ago
Correct answer A:

When supporting personal devices on a corporate network, you must protect network services and enterprise data by authenticating and authorizing users (employees, contractors, and guests) and their devices. Cisco ISE provides the tools you need to allow employees to securely use personal devices on a corporate network.

Guests can add their personal devices to the network by running the native supplicant provisioning (Network Setup Assistant), or by adding their devices to the My Devices portal.

Because native supplicant profiles are not available for all devices, users can use the My Devices portal to add these devices manually; or you can configure Bring Your Own Device (BYOD) rules to register these devices.

Reference: https://www.cisco.com/c/en/us/td/docs/security/ise/2-4/admin_guide/b_ISE_admin_guide_24/m_ise_devices_byod.html
upvoted 2 times

  **petestudies** 9 months ago

Selected Answer: D

D for sure. I have done this.
upvoted 1 times

  **KnackerTopf1** 9 months, 2 weeks ago

Selected Answer: C

It is not byod, since it's not explicitly stating that it's about employees own devices, but its rather just client provisioning
upvoted 1 times

  **kylesam2017** 12 months ago

'D' is perhaps the right answer, after all. Simple Certificate Enrollment Protocol (SCEP): SCEP is a protocol that allows mobile devices to request and obtain digital certificates from a certificate authority (CA). The certificates can then be used for authentication and secure network access.
upvoted 1 times

  **jhorvat** 1 year ago

Selected Answer: D

Simple Certificate Enrollment Protocol (SCEP)--A Cisco-developed enrollment protocol that uses HTTP to communicate with the CA or registration authority (RA). SCEP is the most commonly used method for sending and receiving requests and certificates.
upvoted 1 times

  **jhorvat** 1 year, 1 month ago

Selected Answer: C

C for sure
upvoted 1 times

  **ums008** 1 year, 2 months ago



Selected Answer: C

I will go with C:

based on Tuxzinator's response

BYOD encompasses a broader set of activities including client provisioning.

This makes Client Provisioning the more specific answer
upvoted 2 times

  **jku2cya** 1 year, 2 months ago


Selected Answer: D

I thought it would be D - SCEP

<https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine-software/116068-configure-product-00.html>


"At the heart of the BYOD solution is the network supplicant provisioning process, which seeks to distribute the requisite certificates to employee-owned devices. In order to satisfy this requirement, a Microsoft Certificate Authority (CA) can be configured in order to automate the certificate enrollment process with the SCEP."

upvoted 1 times

  **seb008** 1 year, 2 months ago

The answer is C client provisioning

The method used to deploy certificates and configure the supplicant on mobile devices to gain access to network resources is client provisioning
upvoted 1 times

  **Jessie45785** 1 year, 3 months ago

Selected Answer: A



A- is correct answer:

<https://community.cisco.com/t5/security-knowledge-base/cisco-ise-byod-prescriptive-deployment-guide/ta-p/3641867#toc-hId-748642240>

Endpoint Onboarding

When leveraging ISE for BYOD, there are few actions that the endpoint needs to perform, which includes starting the communication with proper ISE node via the BYOD portal, creating digital certificate pairs, submitting certificate signing request, and configuring network profile. Some O/S has provisions for such functions natively while others require downloading and running an application temporarily to assist with the flow. Aside from Apple mobile devices (iOS), ISE leverages Network Setup Assistant (NSA or AKA Supplicant Provisioning Wizard (SPW)) to ease the BYOD flow for the users. NSA is an application that is downloaded to the endpoint either from the ISE itself or from app store for each of the endpoint types. NSA assists the user to generate certificate pair, install signed certificate, and configure network and proxy settings on the endpoint.

upvoted 1 times

  **gc999** 1 year, 3 months ago

Selected Answer: D

The question doesn't mention the device is the user owned device. If it is the user-owned device, then BYOD onboarding is the option. I choose Option D because

Simple Certificate Enrollment Protocol allows devices to easily enroll for a certificate by using a URL and a shared secret to communicate with a PKI. Mobile Device Management (MDM) software commonly uses SCEP for devices by pushing a payload containing the SCEP URL and shared secret to managed devices.

<https://www.securew2.com/blog/simple-certificate-enrollment-protocol-scep-explained>

upvoted 1 times

  **aliasger52** 1 year, 2 months ago

Mobile always cover under BYOD... thus answer is A

upvoted 1 times

  **aliasger52** 1 year, 2 months ago

Also note that question is asked about methods not protocols

upvoted 1 times

  **Naderelmansi** 1 year, 5 months ago

Selected Answer: D

D is correct:

At the heart of the BYOD solution is the network supplicant provisioning process, which seeks to distribute the requisite certificates to employee-owned devices. In order to satisfy this requirement, a Microsoft Certificate Authority (CA) can be configured in order to automate the certificate enrollment process with the SCEP.

<https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine-software/116068-configure-product-00.html>

upvoted 1 times

  **loser4fun** 1 year, 6 months ago

Answer is C

The method used to deploy certificates and configure the supplicant on mobile devices to gain access to network resources is client provisioning.

Client provisioning is a process where network administrators deploy certificates and configure the supplicant on mobile devices to allow access to network resources. This process involves configuring security policies, installing security certificates, configuring the wireless settings, and verifying the configuration of the mobile device.

BYOD onboarding refers to the process of enrolling personal mobile devices into an enterprise network. MAC authentication bypass is a process that allows clients to connect to a network without authentication by whitelisting the client's MAC address. Simple Certificate Enrollment Protocol (SCEP) is a protocol used to manage and distribute digital certificates.

upvoted 1 times

What are two characteristics of Cisco DNA Center APIs? (Choose two.)

- A. They are Cisco proprietary.
- B. They do not support Python scripts.
- C. They view the overall health of the network.
- D. They quickly provision new devices.
- E. Postman is required to utilize Cisco DNA Center API calls.

Correct Answer: CD

Community vote distribution

CD (100%)

Dinges Highly Voted 3 years, 2 months ago

C and D are correct

-Use the Know Your Network REST methods to GET information about clients, sites, topology, devices, and issues: Retrieve network health information and site and network physical, Layer 2, Layer 3, and VLAN information.

-Configuration Templates with the Template Programmer/Editor is a centralized CLI-management tool that facilitates design and provisioning of workflows in Cisco DNA Center.

<https://developer.cisco.com/docs/dna-center/#!cisco-dna-center-platform-overview/intent-api-northbound>

Postman is not required: Python, SDK and postman can be used.

<https://robertcsapo.medium.com/3-simple-ways-to-use-cisco-dna-center-platform-apis-7eee49b76287>

These APIs can be open or proprietary.

<https://www.ciscopress.com/articles/article.asp?p=3004581&seqNum=2>

upvoted 16 times

kornman Highly Voted 3 years, 2 months ago

I believe C & D are correct

upvoted 5 times

Marshpillowz Most Recent 5 months, 1 week ago

Selected Answer: CD

C and D are correct

upvoted 1 times

Naderelmansi 1 year, 5 months ago

Selected Answer: CD

It is C and D

upvoted 2 times

mecacig953 2 years, 5 months ago

Selected Answer: CD

Postman is not required

upvoted 4 times

brownbear505 2 years, 6 months ago

Selected Answer: CD

<https://www.ciscolive.com/c/dam/r/ciscolive/emea/docs/2019/pdf/LTRNMS-2500-LG.pdf>

upvoted 3 times

Wang87 2 years, 7 months ago

Selected Answer: CD

C & D are correct

upvoted 3 times

efongvan 2 years, 8 months ago

c and d are correct.No doubt.

upvoted 2 times



eazy99 2 years, 12 months ago



I believe C and D



upvoted 2 times

Sarbi 3 years ago

c and d are correct.No doubt
upvoted 2 times

  **Sarbi** 3 years ago
C and D are Correct
upvoted 2 times

  **aalnman** 3 years, 2 months ago
C and D
upvoted 4 times

  **itisfakemallo** 3 years, 2 months ago
Vote for C and D
upvoted 4 times

A company discovered an attack propagating through their network via a file. A custom file detection policy was created in order to track this in the future and ensure no other endpoints execute to infected file. In addition, it was discovered during testing that the scans are not detecting the file as an indicator of compromise. What must be done in order to ensure that the policy created is functioning as it should?

- A. Create an IP block list for the website from which the file was downloaded.
- B. Block the application that the file was using to open.
- C. Upload the hash for the file into the policy.
- D. Send the file to Cisco Threat Grid for dynamic analysis.

Correct Answer: C

Community vote distribution

C (100%)

zeroCOOL Highly Voted 3 years ago

i would go with C here because it looks like they are referring to the "custom detection list" from FMC(Firepower) which is part of the File Policy. With this you can do the following:

Override File Disposition Using Custom Lists

If a file has a disposition in the AMP cloud that you know to be incorrect, you can add the file's SHA-256 value to a file list that overrides the disposition from the cloud:

To treat a file as if the AMP cloud assigned a clean disposition, add the file to the clean list.

To treat a file as if the AMP cloud assigned a malware disposition, add the file to the custom detection list.

On subsequent detection, the device either allows or blocks the file without reevaluating the file's disposition. You can use the clean list or custom detection list per file policy.

https://www.cisco.com/c/en/us/td/docs/security/firepower/623/configuration/guide/fpmc-config-guide-v623/file_policies_and_advanced_malware_protection.html

upvoted 7 times

Marshpillowz Most Recent 5 months, 1 week ago

Selected Answer: C

C is correct

upvoted 1 times

Naderelmansi 1 year, 5 months ago

Selected Answer: C

The correct answer is C. Upload the hash for the file into the policy.

Option A is not an appropriate response to ensure the policy is functioning, as it involves blocking an IP address rather than detecting the file.

Option B is also not an appropriate response, as blocking the application used to open the file may not prevent the file from being downloaded or executed on the endpoint.

Option D is a good practice for threat analysis, but it does not address the issue of the custom file detection policy not detecting the file as an indicator of compromise. Uploading the hash of the file into the policy is a more direct approach to ensuring the policy is functioning as it should.

upvoted 2 times

sull3y 1 year, 7 months ago

C. Upload the hash for the file into the policy.

When a custom file detection policy is created in order to track a specific file, it is necessary to ensure that the file is being properly detected by the security scans. One way to do this is by uploading the hash of the file into the policy. The hash, also known as a digital fingerprint, is a unique identification code that is specific to a file. By including the hash of the infected file in the policy, the scans will be able to detect the file based on its unique characteristics, even if the file has been modified or renamed. This ensures that the policy is functioning as it should and that the infected file will be detected in the future.

Although options like blocking the application that the file was using to open, sending the file to Cisco Threat Grid for dynamic analysis or creating an IP block list for the website from which the file was downloaded are good options to prevent the attack but they are not related to the custom file detection policy functionality.

upvoted 4 times

Emlia1 1 year, 9 months ago

It should be D

upvoted 1 times

  **sis_net_sec** 1 year, 11 months ago

The correct answer is D

upvoted 2 times

  **otzu1** 2 years, 4 months ago

C,

configuring the policy doesn't imply it was configured correctly, add the file hash using sha 256/

OCG:

Simple custom detection allows you to add file signatures, while the advanced custom detections are more like traditional antivirus signatures. Creating a simple custom detection is similar to adding new entries to a blacklist. You define one or more files that you are trying to quarantine by building a list of SHA-256 hashes. If you already have the SHA-256 hash of a file, you can paste that hash directly into the UI, or you can upload files directly and allow the cloud to create the SHA-256 hash for you. To create a simple custom detection, navigate to Outbreak Control > Custom Detections > Simple and the list of all existing simple custom detections appears, as shown in Figure 11-3. To add a new one, you must type it in the Name box and click Save, as shown in Figure 11-3.

upvoted 2 times

  **Wang87** 2 years, 7 months ago

Selected Answer: C


Answer is C because question is regarding making custom policy work. By adding hash of file the policy will start working as it should. What must be done in order to ensure that the policy created is functioning as it should?

upvoted 4 times

  **dr4gn00t** 2 years, 7 months ago

Exactly. I was first going with D, but after rereading the question C is best answer. You need to add hash for the custom policy to work. By uploading file to ThreatGrid, it would be detected dynamically but it wouldn't fix the custom detection policy, and this is what is been asked.



upvoted 1 times

  **Cock** 2 years, 8 months ago

Selected Answer: C

I prefer C



upvoted 4 times

  **Jetnor** 2 years, 9 months ago

I would vote for D

Because these products are designed to work in automatic way so we have to send file to 'threat grid' , and threat grid will automatically update the hash value to AMP database where our device gets updates about threats.

upvoted 1 times

  **zheka** 2 years, 9 months ago

For both AMP for endpoints and AMP under Firepower there's no way upload the hash for the file into the policy. This gives us an option of D - dynamic analysis with threat grid

upvoted 1 times

  **flejd** 2 years, 8 months ago

You are wrong. Within Objects Tab you can find FILE LIST and in there a CUSTOM DETECTION LIST in which you can add/calculate a SH256 checksum.

upvoted 2 times

  **flejd** 2 years, 8 months ago

but in the question they mention that the custom detection list is already prepared so its not C

upvoted 1 times

  **GatPat** 1 year, 8 months ago

But then it also says - "What must be done in order to ensure that the policy created is functioning as it should?" So it would be C to make the policy work

upvoted 2 times

  **NullNull88** 2 years, 9 months ago

Definitely no to A and B. Also not D because we are not sending every single file to threat-grid for analysis as this is not necessary. See documentation on Custom Detection Lists. Answer is C

upvoted 2 times

[-] 👤 **brownb** 2 years, 9 months ago

Im thinking D. If the file is still considered unknown then the hash failed to get a positive ID through AMP so it needs dynamic analysis by sending it to threat grid for sandboxing.

upvoted 1 times

[-] 👤 **eazy99** 2 years, 12 months ago

I believe the answer is C, they already created a custom file, and the scans can't discover it, so they need to upload the hash for the scans to detect it because the scans needs some help to identify the malicious file, and nothing better than the hash in this scenario.

upvoted 4 times

[-] 👤 **ic0deem** 3 years ago

I vote for D, since this is Cisco exam and traditional IoCs are not seemed effective

upvoted 1 times

[-] 👤 **Sarbi** 3 years ago

I think it is A

upvoted 1 times

```

import http.client
import base64
import ssl
import sys

host = sys.argv[1]#"10.10.10.240"
user = sys.argv[2]#"ersad"
password = sys.argv[3]#"Password1"

conn = http.client.HTTPSConnection("{}:9060".format(host),
context=ssl.SSLContext(ssl.PROTOCOL_TLSv1_2))

creds = str.encode(':'.join((user, password)))
encodedAuth = bytes.decode(base64.b64encode(creds))

headers = {
    'accept': "application/json",
    'authorization': " ".join(("Basic",encodedAuth)),
    'cache-control': "no-cache",
}

conn.request("GET", "/ers/config/internaluser/", headers=headers)

res = conn.getresponse()
data = res.read()

print("Status: {}".format(res.status))
print("Header:\n{}".format(res.header))
print("Body:\n{}".format(data.decode("utf-8")))

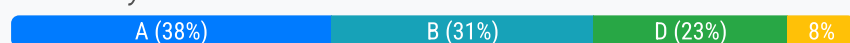
```

Refer to the exhibit. What does the Python script accomplish?

- A. It authenticates to a Cisco ISE server using the username or ersad.
- B. It lists the LDAP users from the external identity store configured on Cisco ISE.
- C. It authenticates to a Cisco ISE with an SSH connection.
- D. It allows authentication with TLSv1 SSL protocol.

Correct Answer: A

Community vote distribution



zeroC00L Highly Voted 2 years, 11 months ago

i would go with "A" here because:

- B cant be correct the GET is going after /ers/config/internaluser which is ISE own User DB
- C cant be correct we we take a lookat the "context=" part we see the connection will be build by using the SSL Library
- D cant be correct again if we look at the "context" part we see they take the TLSv1.2 from the ssl library not TLSv1

upvoted 15 times

4pelos Most Recent 6 months, 1 week ago

Correct answer B

Note: The purpose of this Python script is used to get the guest users through ISE External RESTful Services (ERS) API. ERS is designed to allow external clients to perform CRUD (Create, Read, Update, Delete) operations on Cisco ISE resources.

upvoted 1 times

blacknblue8 1 year, 2 months ago

Selected Answer: A

Option A is the correct one, the answer has a typo .. as I check on other website the "or" should be "of"

upvoted 3 times

Odorka222 1 year, 4 months ago

Selected Answer: D

it is the same code from cisco web pages :-)

<https://developer.cisco.com/docs/identity-services-engine/latest/#!/internal-users-get-user-by-id/execution>

upvoted 1 times

iluvmicrosoft 5 months ago

its eerily similar tho.. and more interesting when you read what the purpose of the script is - thank you!

upvoted 1 times

  **HDragovich** 1 year, 4 months ago

not the same
look at "context"part its TLSv1_2 not TLSV1
upvoted 1 times

  **Jessie45785** 1 year, 4 months ago

code is not the same, under your link you can clearly see that ssl.PROTOCOL_TLSv1 is listed as a context, in presented question you have ssl.PROTOCOL_TLSv1_2

... additionally it clearly tell you what this script is used for:

```
#####  
# #  
# This script demonstrates how to use the ISE ERS internal users #  
# API by executing a Python script. #  
# #
```

```
.  
. .
```


```
user = sys.argv[2] # "ersad"
```

```
os "A" is the correct answer
```

upvoted 1 times


  **stalkr3** 1 year, 5 months ago

I think D is the correct one.
TLS is backwards-compatible. "After upgrading the default to 1.2, systems using 1.1 and 1.0 will continue to function, so if any of your processing requires 1.0 and 1.1, it will remain available."
upvoted 2 times

  **Jessie45785** 1 year, 5 months ago

Selected Answer: A

I am sorry I have to correct myself A is correct - but the word "or" is probably a typo
upvoted 2 times


  **Jessie45785** 1 year, 5 months ago

Selected Answer: D

Correct answers is D
- A - make nonsense whatsoever
- B - It is NOT external LDAP but internal DB
- C - it is NOT SSH but restapi Call



D - is Correct TLSv1_2 are allowed!

upvoted 2 times

  **Jessie45785** 1 year, 5 months ago

Selected Answer: C

see @GetPat - it is clearly C
upvoted 1 times

  **GatPat** 1 year, 8 months ago

This code imports the http.client, base64, ssl, and sys modules. The http.client module is used to create an HTTP connection, the base64 module is used to encode the user credentials, and the ssl module is used to create an SSL context. The sys module is used to access command line arguments passed to the script.



The code sets the host, user, and password variables to the values of the first, second, and third command-line arguments respectively.

It creates an HTTPS connection to the specified host on port 9060 using the http.client.HTTPSConnection class, passing the hostname and port to the constructor and specifying that the connection should use the SSL/TLS protocol version 1.

The user credentials are then concatenated and encoded using the base64 module. The encoded credentials are saved in the encodedAuth variable.

In summary, this code creates an HTTPS connection to a specified host, using a specified username and password, encoded with base64, and using SSL/TLS protocol version 1.

upvoted 4 times

  **otzu1** 2 years, 4 months ago

A
"the" username "or" ersad. I think the sysarg function can prompt if i'm not mistaking
upvoted 2 times

  **stalkr3** 1 year, 5 months ago

How does the function takes ersad from the comment?

upvoted 2 times

  **ilikevenice** 2 years, 5 months ago

This is part of the `get-all-internal-users.py` script, to extract all internal users from ISE.

<https://developer.cisco.com/docs/identity-services-engine/v1/#!/internal-users-get-all-users/get-all-internal-userspy-source-code>

upvoted 2 times

  **jaciro11** 2 years, 6 months ago

Selected Answer: B

A discarded

C and D also

upvoted 4 times

  **jaciro11** 2 years, 6 months ago



user `ersad` is a comment on the code, so A cannot be

upvoted 4 times

  **dr4gn00t** 2 years, 7 months ago

It is A. Only mistake is that user `ersad` is only a comment in the script. It will use what ever username is given as a second argument.

upvoted 3 times

  **gabbar** 2 years, 11 months ago

Correct answer should be D

upvoted 1 times

  **jaciro11** 2 years, 10 months ago

Man the AUTH is doing with TLSv1.2 WTF

Answer is A

upvoted 4 times

  **asdasd123123iu** 2 years, 3 months ago

A is incorrect because `'ersad'` is commented. B is correct answer.

upvoted 2 times

  **alexozgat24** 1 year, 4 months ago

so i got the point why you are pointing for `#` comment out but - it is basically not comment out it's for reference `sys.argv[1]` is calling out `ersad`. after all other options I think A is make more sense. if the line was starting with `#user=sys.argv[1]` i would get your point.

upvoted 1 times

  **stalkr3** 1 year, 5 months ago

TLS v1.2 is backwards compatible with v1.0

upvoted 1 times

What is a difference between GETVPN and IPsec?

- A. GETVPN is used to build a VPN network with multiple sites without having to statically configure all devices.
- B. GETVPN is based on IKEv2 and does not support IKEv1.
- C. GETVPN provides key management and security association management.
- D. GETVPN reduces latency and provides encryption over MPLS without the use of a central hub.

Correct Answer: D

Community vote distribution



Alee86 Highly Voted 2 years, 8 months ago

GETVPN Simplifies branch-to-branch instantaneous communications - Ensures low latency and jitter by enabling full-time, direct communications between sites, without requiring transport through a central hub

Maximizes security - Provides encryption for MPLS networks while maintaining network intelligence such as full-mesh connectivity, natural routing path, and quality of service (QoS)

Complies with governmental regulation and privacy laws - Helps you meet security compliance and internal regulation by encrypting all WAN traffic

Offers management flexibility - Eliminates complex peer-to-peer key management with group encryption keys
upvoted 11 times

hdrnzenlaorljol 1 year, 4 months ago

GETVPN Simplifies branch-to-branch instantaneous communications - Ensures low latency and jitter by enabling full-time, direct communications between sites, without requiring transport through a central hub

Maximizes security - Provides encryption for MPLS networks while maintaining network intelligence such as full-mesh connectivity, natural routing path, and quality of service (QoS)

Complies with governmental regulation and privacy laws - Helps you meet security compliance and internal regulation by encrypting all WAN traffic

Offers management flexibility - Eliminates complex peer-to-peer key management with group encryption keys
upvoted 1 times

Rododendron2 Most Recent 2 months, 4 weeks ago

Selected Answer: C

How can GETVPN reduce latency ? If I will not setup GETVPN, I will have to go via central hub ? No, so why the latency here. C is right answer , D is cisco marketing
upvoted 1 times

RemiK 3 months ago

Selected Answer: A

I'll definitely answer A on this one. This looks like the fundamental difference between the two.
upvoted 1 times

XvidalX 6 months ago

Selected Answer: D

D
"Helps ensure low latency and jitter by enabling full-time, direct communications between sites, without requiring transport through a central hub"
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_getvpn/configuration/xs-3s/sec-get-vpn-xe-3s-book/sec-get-vpn.html
upvoted 2 times

4pelos 6 months, 1 week ago

Answer correct D.
Checked with securitytut
upvoted 1 times

Stevens0103 8 months, 2 weeks ago

Selected Answer: D

D. 100% correct.

"Helps ensure low latency and jitter by enabling full-time, direct communications between sites, without requiring transport through a central hub"

"GET-based networks can be used in a variety of WAN environments, including IP and MPLS. MPLS VPNs that use this encryption technology are highly scalable, manageable, and cost-effective, and they meet government-mandated encryption requirements."

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_getvpn/configuration/xr-3s/sec-get-vpn-xr-3s-book/sec-get-vpn.html

upvoted 1 times

  **hdrnzenlaorljol** 1 year, 4 months ago

Selected Answer: D

GETVPN Simplifies branch-to-branch instantaneous communications - Ensures low latency and jitter by enabling full-time, direct communications between sites, without requiring transport through a central hub

Maximizes security - Provides encryption for MPLS networks while maintaining network intelligence such as full-mesh connectivity, natural routing path, and quality of service (QoS)

Complies with governmental regulation and privacy laws - Helps you meet security compliance and internal regulation by encrypting all WAN traffic

Offers management flexibility - Eliminates complex peer-to-peer key management with group encryption keys

upvoted 1 times

  **DaelsBae** 1 year, 7 months ago

Selected Answer: C


C is correct and D is wrong. GETVPN can reduce latency as it allows encrypted traffic to be transported over a pre-existing MPLS network. However, it does not necessarily eliminate the use of a central hub. In GETVPN, a group of routers called Key Servers act as a central hub for key management and security association management. So while GETVPN can provide encryption over MPLS, the use of a central hub is a key component of its design.

upvoted 4 times

  **Rododendron2** 2 months, 4 weeks ago

key servers are for management - not hub (= packets traverse via hub), nothing to do with data path and nothing to do with latency

upvoted 2 times

  **Net4dd** 1 year, 8 months ago

This one is C

upvoted 1 times

  **GatPat** 1 year, 8 months ago

Selected Answer: D

Helps ensure low latency and jitter by enabling full-time, direct communications between sites, without requiring transport through a central hub

upvoted 1 times

  **Emlia1** 1 year, 8 months ago

Selected Answer: D

I prefer D

upvoted 1 times

  **Jamesy** 1 year, 11 months ago

C is the correct answer. Cheers

upvoted 1 times

  **surforlife** 2 years, 2 months ago



'B' is correct answer. Question is regarding IPSEC differences. GET VPN currently supports only IKEv1.

upvoted 3 times

  **nemeses667** 2 years, 1 month ago

It does https://content.cisco.com/chapter.sjs?uri=/searchable/chapter/content/en/us/td/docs/ios-xml/ios/sec_conn_getvpn/configuration/xr-16-6/sec-get-vpn-xr-16-6-book/sec-get-vpn-gikev2.html.xml

upvoted 2 times

  **psuoh** 1 year, 7 months ago

Yep..."The GETVPN G-IKEv2 feature implements Internet Key Exchange version 2 (IKEv2) protocol on GETVPN thereby allowing GETVPN to derive the benefits of IKEv2."

upvoted 1 times

  **Fragalot** 2 years, 10 months ago

I believe it's C as it does use a central hub for key management and security association.



https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_getvpn/configuration/xr-16-11/sec-get-vpn-xr-16-11-book/sec-get-vpn.html

upvoted 2 times

  **Fragalot** 2 years, 9 months ago



Must have been asleep when looking into this. It's D.

upvoted 3 times

  **psuoh** 1 year, 7 months ago

Cisco wants you to choose D

upvoted 1 times

  **psuoh** 1 year, 7 months ago

"..Cisco Group Encrypted Transport VPN provides the following benefits:

Provides data security and transport authentication, helping to meet security compliance and internal regulation by encrypting all WAN traffic

Enables high-scale network meshes and eliminates complex peer-to-peer key management with group encryption keys

For Multiprotocol Label Switching (MPLS) networks, maintains network intelligence such as full-mesh connectivity, natural routing path, and quality of service (QoS)

Grants easy membership control with a centralized key server

Helps ensure low latency and jitter by enabling full-time, direct communications between sites, without requiring transport through a central hub

Reduces traffic loads on customer premises equipment (CPE) and provider-edge (PE) encryption devices by using the core network for replication of multicast traffic, avoiding packet replication at each individual peer site.."

upvoted 1 times

Question #60

Topic 1

Which algorithm provides asymmetric encryption?

- A. 3DES
- B. RC4
- C. AES
- D. RSA

Correct Answer: D

Community vote distribution

D (100%)

  **Marshpillowz** 5 months, 1 week ago

Selected Answer: D

D is correct



upvoted 1 times

  **Naderelmansi** 1 year, 5 months ago

Selected Answer: D

The most widely used asymmetric encryption algorithm is RSA (Rivest-Shamir-Adleman) algorithm.

upvoted 2 times

  **sull3y** 1 year, 7 months ago

D. RSA

RSA is an algorithm that provides asymmetric encryption, which means that it uses a pair of keys, one for encryption and one for decryption. Data is encrypted with the public key and can only be decrypted with the corresponding private key. RSA is widely used in various applications, such as digital signatures, software protection, and secure communications.

3DES, RC4, and AES are symmetric encryption algorithms which means they use the same key for encryption and decryption.

3DES is a symmetric-key block cipher that applies the Data Encryption Standard (DES) algorithm three times to each data block.

RC4 is a symmetric stream cipher, it's known for its simplicity and speed

AES is a symmetric block cipher that supports key sizes of 128, 192, and 256 bits.

upvoted 3 times

  **migueli** 2 years, 1 month ago

Selected Answer: D

<https://www.cisco.com/c/en/us/products/security/encryption-explained.html#~types-of-encryption>

RSA is asymmetric cryptography, so there is one public key and one private key.

upvoted 2 times

What is a difference between an XSS attack and an SQL injection attack?

- A. SQL injection is a hacking method used to attack SQL databases, whereas XSS attack can exist in many different types of applications.
- B. XSS attacks are used to steal information from databases, whereas SQL injection attacks are used to redirect users to websites where attackers can steal data from them.
- C. XSS is a hacking method used to attack SQL databases, whereas SQL injection attacks can exist in many different types of applications.
- D. SQL injection attacks are used to steal information from databases, whereas XSS attacks are used to redirect users to websites where attackers can steal data from them.

Correct Answer: D

Community vote distribution

D (100%)

Marshpillowz 5 months, 1 week ago

Selected Answer: D

D is correct

upvoted 1 times

sull3y 1 year, 7 months ago

D. SQL injection attacks are used to steal information from databases, whereas XSS attacks are used to redirect users to websites where attackers can steal data from them.

Cross-site scripting (XSS) is a type of security vulnerability that allows attackers to inject malicious code into a website, which can be executed by unsuspecting users when they visit the website. The malicious code can be used to steal information from the user's browser, such as login credentials or personal information. XSS attacks can exist in many different types of applications, including web-based applications, mobile apps, and even PDFs.

SQL injection is a type of attack that targets SQL databases. The attacker injects malicious SQL code into a web application's input fields, which can be executed by the database. This can allow the attacker to steal sensitive information from the database, such as login credentials, credit card numbers, and other sensitive data. SQL injection attacks can exist in many different types of applications that use SQL databases, including web-based applications, mobile apps, and even PDFs.

upvoted 2 times

networkhanim 1 year, 3 months ago

According your comment, "XSS can exist in many different types of applications" This is true in A. So why is the answer not A?

upvoted 2 times

GatPat 1 year, 8 months ago

Selected Answer: D

Should be D

upvoted 2 times

NullNull88 2 years, 9 months ago

There can be no other answer,.. D

upvoted 4 times

kapplejacks 2 years, 11 months ago

Answer: D

If it said for A "web applications" sure thats a good fit but applications are not subjected to XSS, only web applications are. A is invalid, answer D!

upvoted 3 times

eazy99 2 years, 12 months ago

A and D are correct, but D is better answer.

upvoted 1 times

Jayde 3 years ago

I believe A is the answer

upvoted 3 times

What is a difference between a DoS attack and DDoS attack?

- A. A DoS attack is where a computer is used to flood a server with TCP packets, whereas DDoS attack is where a computer is used to flood a server with UDP packets.
- B. A DoS attack is where a computer is used to flood a server with UDP packets, whereas DDoS attack is where a computer is used to flood a server with TCP packets.
- C. A DoS attack is where a computer is used to flood a server with TCP and UDP packets, whereas DDoS attack is where a computer is used to flood multiple servers that are distributed over a LAN.
- D. A DoS attack is where a computer is used to flood a server with TCP and UDP packets, whereas DDoS attack is where multiple systems target a single system with a DoS attack.

Correct Answer: D

Community vote distribution

D (100%)

—  **sull3y** Highly Voted 1 year, 7 months ago

D. A DoS attack is where a computer is used to flood a server with TCP and UDP packets, whereas DDoS attack is where multiple systems target a single system with a DoS attack.

A Denial of Service (DoS) attack is a type of cyber attack in which a single system floods a server with a large number of packets, overwhelming the server and causing it to become unavailable to legitimate users. The goal of a DoS attack is to prevent legitimate users from accessing the targeted server by consuming its resources or causing it to crash.

A Distributed Denial of Service (DDoS) attack is a more sophisticated form of a DoS attack. In a DDoS attack, multiple systems, often compromised through malware, are used to flood a single server with packets, overwhelming it and making it unavailable to legitimate users. The goal of a DDoS attack is the same as a DoS attack, but the scale of the attack is much larger and the resources used to launch the attack are distributed across multiple systems. This makes DDoS attacks much harder to detect and mitigate.

upvoted 6 times

—  **Marshpillowz** Most Recent 5 months, 1 week ago

Selected Answer: D

D is correct

upvoted 1 times

—  **Naderelmansi** 1 year, 5 months ago

Selected Answer: D

The correct answer is D.

A Denial of Service (DoS) attack and a Distributed Denial of Service (DDoS) attack are both types of attacks that aim to overwhelm a system or network, making it unavailable to users. However, the key difference between the two is the number of attacking systems involved.

A DoS attack is typically launched from a single source, such as a single computer, and is intended to overwhelm a targeted system or network with traffic, making it unavailable to users. A DDoS attack, on the other hand, is launched from multiple systems, often a large number of compromised systems that form a botnet, and is intended to overwhelm the targeted system or network with a massive volume of traffic.

upvoted 3 times

What are two advantages of using Cisco AnyConnect over DMVPN? (Choose two.)

- A. It provides spoke-to-spoke communications without traversing the hub.
- B. It enables VPN access for individual users from their machines.
- C. It allows multiple sites to connect to the data center.
- D. It allows different routing protocols to work over the tunnel.
- E. It allows customization of access policies based on user identity.

Correct Answer: BE

Cisco Anyconnect is a Remote access VPN client based solution where users can install the client on their machines and can connect to the respective VPN devices (ASA/FTD/Router). In order to secure connectivity for Anyconnect Users, one can also create custom access policies to ensure proper conditions are met before access is granted to the VPN user.

Community vote distribution

BE (100%)

Marshpillowz 5 months, 1 week ago

Selected Answer: BE

B and E are correct
upvoted 1 times

sull3y 1 year, 5 months ago

The two advantages of using Cisco AnyConnect over DMVPN are:

B. It enables VPN access for individual users from their machines. AnyConnect provides a client-based VPN solution that allows individual users to securely access the corporate network from their own machines or devices, whereas DMVPN is a site-to-site VPN solution that requires network devices to establish a secure tunnel between them.

E. It allows customization of access policies based on user identity. AnyConnect provides a robust identity-based access control solution, allowing network administrators to define different access policies for different users or groups of users. DMVPN does not provide such granular control over access policies.

upvoted 3 times

pioo1979 1 year, 6 months ago

Is there any situation when I have to choose between Anyconnect and DMVPN?

upvoted 3 times

Karitza 7 months, 4 weeks ago

No, because there are different types of vpn. Anyconnect application is used for remote access vpn to a concentrator la cisco ASA or cisco Secure Firewall and DVPN si a type of vpn that is applied in a hub and spoke topology (DMVPN only works for cisco).

upvoted 1 times

What is the difference between a vulnerability and an exploit?

- A. A vulnerability is a weakness that can be exploited by an attacker.
- B. A vulnerability is a hypothetical event for an attacker to exploit.
- C. An exploit is a hypothetical event that causes a vulnerability in the network.
- D. An exploit is a weakness that can cause a vulnerability in the network.

Correct Answer: A

Reference:

<https://debricked.com/blog/what-is-security-weakness/#:~:text=A%20vulnerability%20is%20a%20weakness,when%20it%20can%20be%20exploited.&text=This%20is%20a%20%E2%80%9Ccommunity%2Ddeveloped,of%20common%20software%20security%20weaknesses%E2%80%9D>

Community vote distribution

A (100%)

Naderelmansi Highly Voted 1 year, 5 months ago

Selected Answer: A

The correct answer is A.

A vulnerability is a weakness or flaw in a system, software, or network that can be exploited by an attacker to compromise the security or functionality of the system. A vulnerability can be caused by a variety of factors, including coding errors, misconfigurations, or design flaws.

An exploit, on the other hand, is a tool or technique used by an attacker to take advantage of a vulnerability and gain unauthorized access or control over the target system. An exploit can be a piece of software, a script, or a command that leverages a vulnerability to execute malicious code or actions on the target system.

Therefore, the difference between a vulnerability and an exploit is that a vulnerability is a weakness that can be exploited by an attacker, while an exploit is the means by which an attacker takes advantage of a vulnerability to compromise the system.

upvoted 5 times

Marshpillowz Most Recent 5 months, 1 week ago

Selected Answer: A

A is correct here

upvoted 1 times

Felice44 1 year, 6 months ago

Selected Answer: A

No doubt, the vulnerability creates access to the exploit

upvoted 3 times

What is the term for having information about threats and threat actors that helps mitigate harmful events that would otherwise compromise networks or systems?

- A. threat intelligence
- B. Indicators of Compromise
- C. trusted automated exchange
- D. The Exploit Database

Correct Answer: A

Reference:

https://en.wikipedia.org/wiki/Cyber_threat_intelligence

Community vote distribution

A (100%)

[-] **Marshpillowz** 5 months, 1 week ago

Selected Answer: A

A is correct

upvoted 1 times

[-] **Naderelmansi** 1 year, 5 months ago

Selected Answer: A

The correct answer is A.

The term for having information about threats and threat actors that helps mitigate harmful events that would otherwise compromise networks or systems is "threat intelligence." Threat intelligence refers to the knowledge and insights gained from analyzing and understanding potential threats and threat actors, including their tactics, techniques, and procedures (TTPs).

By leveraging threat intelligence, organizations can better understand the risks they face and take proactive steps to prevent or mitigate potential attacks. Threat intelligence can come from a variety of sources, including open-source intelligence, commercial threat intelligence feeds, and internal security operations.

upvoted 3 times

[-] **Felice44** 1 year, 6 months ago

Selected Answer: A

Certainly A

upvoted 3 times

```
crypto ikev2 name-mangler MANGLER
dn organization-unit
```

Refer to the exhibit. An engineer is implementing a certificate based VPN. What is the result of the existing configuration?

- A. Only an IKEv2 peer that has an OU certificate attribute set to MANGLER establishes an IKEv2 SA successfully.
- B. The OU of the IKEv2 peer certificate is used as the identity when matching an IKEv2 authorization policy.
- C. The OU of the IKEv2 peer certificate is set to MANGLER.
- D. The OU of the IKEv2 peer certificate is encrypted when the OU is set to MANGLER.

Correct Answer: B

Community vote distribution

B (100%)

Smilebloke Highly Voted 2 years, 4 months ago

B:

Configuring the IKEv2 Name Mangler

Perform this task to specify the IKEv2 name mangler, which is used to derive a name for authorization requests and obtain AAA preshared keys. The name is derived from specified portions of different forms of remote IKE identities or the EAP identity.

```
enable
configure terminal
crypto ikev2 name-mangler mangler-name
dn {common-name | country | domain | locality | organization | organization-unit | state}
eap {all | dn {common-name | country | domain | locality | organization | organization-unit | state} | prefix | suffix {delimiter { . | @ | \}}}
email {all | domain | username}
fqdn {all | domain | hostname}
end
dn = Derives the name from any of the noted fields in the remote identity of type DN
common-name
country
domain
locality
organization
organization-unit
state
```

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_ike2vpn/configuration/xr-16-10/sec-flex-vpn-xr-16-10-book/sec-cfg-flex-serv.html

upvoted 5 times

Marshpillowz Most Recent 5 months, 1 week ago

Selected Answer: B

B is correct

upvoted 1 times

Naderelmansi 1 year, 5 months ago

Selected Answer: B

The correct answer is B.

The "match identity certificate" command in the IKEv2 authorization policy is used to specify that the OU (Organizational Unit) attribute of the IKEv2 peer certificate should be used as the identity when matching the policy. The OU attribute is set to "MANGLER" in this case.

So, when an IKEv2 peer with a certificate that has an OU attribute of "MANGLER" attempts to establish an IKEv2 SA, the router will use the OU attribute as the identity when matching the authorization policy. If the policy is a match, the SA will be established successfully.

upvoted 3 times

Which kind of API that is used with Cisco DNA Center provisions SSIDs, QoS policies, and update software versions on switches?

- A. event
- B. intent
- C. integration
- D. multivendor

Correct Answer: B

Cisco is moving towards intent based networking and DNA center is a new addition to the solution offerings from Cisco.

Community vote distribution

B (100%)

Marshpillowz 5 months, 1 week ago

Selected Answer: B

B is correct

upvoted 1 times

Carlis 1 year, 5 months ago

event - eastbound

intent - northbound

integration - westbound

multivendor - southbound

upvoted 3 times

Naderelmansi 1 year, 5 months ago

Selected Answer: B

Therefore, the correct answer is B, Intent API.

The API used with Cisco DNA Center to provision SSIDs, QoS policies, and update software versions on switches is the Cisco DNA Center Intent API. This API allows network administrators to automate network infrastructure tasks by expressing their intent through high-level policies rather than low-level device-specific configuration commands. The Cisco DNA Center Intent API uses RESTful APIs to provide a standardized interface for interacting with the network infrastructure. It allows network administrators to define their intent using JSON-based data models and use those models to provision, configure, and manage the network infrastructure.

upvoted 2 times

loser4fun 1 year, 6 months ago

B. Intent

Intent API is a type of API that allows developers to program the desired intent for the network rather than the specific configuration details. Intent API simplifies the process of network automation by abstracting the complexity of device-specific configurations and providing a more natural and intuitive way to interact with the network.

Cisco DNA Center uses Intent API to provide a simplified way to configure and manage network devices. With Intent API, administrators can specify the intent of the configuration, such as creating a new SSID or updating a QoS policy, and DNA Center takes care of the underlying device-specific configurations.

upvoted 1 times

sull3y 1 year, 7 months ago

B. intent

Cisco DNA Center uses Intent APIs to provision SSIDs, QoS policies, and update software versions on switches. Intent APIs allow the network administrator to define high-level policies, such as "this SSID should have these characteristics" or "this switch should run this version of software," and the Cisco DNA Center platform automatically translates those policies into the necessary low-level configurations on the network devices. This simplifies the management of the network and allows for a more automated and consistent provisioning process.

upvoted 3 times

A network engineer needs to select a VPN type that provides the most stringent security, multiple security associations for the connections, and efficient VPN establishment with the least bandwidth consumption. Why should the engineer select either FlexVPN or DMVPN for this environment?

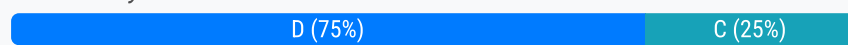
- A. DMVPN because it uses multiple SAs and FlexVPN does not.
- B. DMVPN because it supports IKEv2 and FlexVPN does not.
- C. FlexVPN because it supports IKEv2 and DMVPN does not.
- D. FlexVPN because it uses multiple SAs and DMVPN does not.

Correct Answer: D

Reference:

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_ike2vpn/configuration/xr-16-12/sec-flex-vpn-xr-16-12-book/sec-cfg-flex-serv.html

Community vote distribution



  **Smilebloke** Highly Voted  2 years, 4 months ago

IKEv2 Multi-SA


The IKEv2 Multi-SA feature allows an IKEv2 Dynamic Virtual Tunnel Interface (DVTI) session on the IKEv2 responder to support multiple IPsec Security Associations (SA). The maximum number of IPsec SAs per DVTI session is either obtained from AAA authorization or configured on the IPsec profile. The value from AAA has a higher priority. Any change to the max-flow-limit argument in the IPsec profile is not applied to the current session but is applied to subsequent sessions. The IKEv2 Multi-SA feature makes the configuration of the IKEv2 profile in the IPsec profile optional. This optional configuration allows IPsec DVTI sessions using the same virtual template to have different IKEv2 profiles, thus saving the number of virtual template configurations.

Note

The IKEv2 Multi-SA feature allows multiple IPsec SAs that have non-any-any proxies. However, when the IPsec SA proxies are any-any, a single IPsec SA is allowed.

For more information, see the "Multi-SA Support for Dynamic Virtual Tunnel Interfaces for IKEv2" module in the Security for VPNs with IPsec Configuration Guide.


upvoted 6 times

  **Nonono2** Most Recent  2 months, 1 week ago

Selected Answer: C

The answer is C

upvoted 1 times

  **jku2cya** 1 year, 2 months ago



Selected Answer: D

DMVPN can be configured with IKEv2, so answer is not C.

I wasn't able to find Cisco documentation to back this up, but found this configuration example:

<https://journey2theccie.wordpress.com/2020/03/13/ikev1-ikev2-configuration-in-dmvpn/>



upvoted 3 times

  **alexyoizat24** 1 year, 4 months ago

Really like the comment on following link for this discussion, per say- it looks like Answer is C

<https://community.cisco.com/t5/network-security/what-is-the-difference-between-dmvpn-and-flexvpn/td-p/3438913>



upvoted 1 times

  **psuoh** 1 year, 7 months ago

What is the difference between FlexVPN and DMVPN?

IPSec: One key difference between FlexVPN and default Dynamic Multipoint VPN (DMVPN) is the protocol used for negotiating IPsec Security Associations (SAs). While DMVPN defaults to using Internet Key Exchange version 1 (IKEv1), FlexVPN utilizes IKEv2.

upvoted 2 times

  **psuoh** 1 year, 7 months ago

ANswer is C

upvoted 1 times

  **johnnybgud** 1 year, 7 months ago

But DMVPN definitely support IKEv2, and Answer C says "...DMVPN does not". Therefore answer is likely D.

upvoted 4 times

Interface	MAC Address	Method	Domain	Status	Fg Session ID
Gi4/15	0050.b6d4.8a60	dot1x	DATA	Auth	0A02198200001
Gi8/43	0024.c4fe.1832	dot1x	VOICE	Auth	0A02198200000
Gi10/25	0026.7391.bbd1	dot1x	DATA	Auth	0A02198200001
Gi8/28	0026.0b5e.51d5	dot1x	VOICE	Auth	0A02198200000
Gi4/13	0025.4593.e575	dot1x	VOICE	Auth	0A02198200000
Gi10/23	0025.8418.217f	dot1x	VOICE	Auth	0A02198200000
Gi7/4	0025.8418.1bc7	dot1x	VOICE	Auth	0A02198200000
Gi7/7	0026.0b5e.50fb	dot1x	VOICE	Auth	0A02198200000
Gi8/14	c85b.7604.fa1d	dot1x	DATA	Auth	0A02198200001
Gi10/29	0026.0b5e.528a	dot1x	VOICE	Auth	0A02198200000
Gi4/2	0026.0b5e.4f9f	dot1x	VOICE	Auth	0A02198200000
Gi10/30	0025.4593.e5ac	dot1x	VOICE	Auth	0A02198200000
Gi8/29	68bd.aba5.2e44	dot1x	VOICE	Auth	0A02198200000
Gi7/4	54ee.75db.d766	dot1x	DATA	Auth	0A02198200001
Gi2/34	e804.62eb.a658	dot1x	VOICE	Auth	0A02198200000
Gi10/22	482a.e307.d9c8	dot1x	DATA	Auth	0A02198200001
Gi9/22	0007.b00c.8c35	mab	DATA	Auth	0A02198200000

Refer to the exhibit. Which command was used to generate this output and to show which ports are authenticating with dot1x or mab?

- A. show authentication registrations
- B. show authentication method
- C. show dot1x all
- D. show authentication sessions

Correct Answer: D

Community vote distribution

D (100%)

examShark Highly Voted 4 years, 3 months ago

D is correct
upvoted 20 times

dzef13 Highly Voted 3 years, 3 months ago

D is correct answer
upvoted 5 times

Marshpillowz Most Recent 5 months, 1 week ago

Selected Answer: D

D is correct
upvoted 1 times

Totosos1 1 year, 5 months ago

Selected Answer: D

Absolutely 'D' is the answer here:

https://www.ciscozine.com/basic-throubleshooting-dot1x-via-cli/?utm_content=cmp-true

upvoted 1 times

surforlife 2 years, 1 month ago

D=correct
Usage Guidelines

Use the show authentication sessions command to display information about all current Auth Manager sessions. To display information about specific Auth Manager sessions, use one or more of the keywords.

Examples

The following example shows how to display all authentication sessions on the switch:

Device# show authentication sessions

```
Interface MAC Address Method Domain Status Session ID
Gi1/48 0015.63b0.f676 dot1x DATA Authz Success 0A3462B1000000102983C05C
```

Gi1/5 000f.23c4.a401 mab DATA Authz Success 0A3462B1000000D24F80B58
Gi1/5 0014.bf5d.d26d dot1x DATA Authz Success 0A3462B1000000E29811B94
upvoted 2 times

  **nenotronix** 2 years, 2 months ago



D is the correct answer
"show authentication sessions"

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/security/s1/sec-s1-xe-3se-3850-cr-book/sec-s1-xe-3se-3850-cr-book_chapter_01.html
upvoted 2 times

  **Jardator** 2 years, 4 months ago

Selected Answer: D

<https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/12-2/50sg/configuration/guide/Wrapper-46SG/dot1x.html#wp1133930>
upvoted 1 times

  **otzu1** 2 years, 4 months ago

D

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/security/s1/sec-s1-xe-3se-3850-cr-book/sec-s1-xe-3se-3850-cr-book_chapter_01.html#wp3404908137

Ctrl F "show authentication sessions"
upvoted 2 times

  **brownbear505** 2 years, 6 months ago

Selected Answer: D

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/security/s1/sec-s1-xe-3se-3850-cr-book/sec-s1-xe-3se-3850-cr-book_chapter_01.html#wp3404908137
upvoted 4 times

  **MoBreezy** 2 years, 7 months ago

Selected Answer: D

The only way to display the above output on a catalyst switch is to enter the show authentication sessions command and nothing else.

100% going with D
upvoted 3 times

  **Sun2sun** 2 years, 7 months ago

Selected Answer: D

D is correct
upvoted 3 times

  **NullNull88** 2 years, 9 months ago

D is the correct answer
upvoted 3 times

  **pfunkylol** 2 years, 9 months ago

Selected Answer: D

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/security/s1/sec-s1-xe-3se-3850-cr-book/sec-s1-xe-3se-3850-cr-book_chapter_01.html#wp3404908137
upvoted 4 times

  **Cisco_SecCol** 2 years, 11 months ago

D is correct. https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/security/s1/sec-s1-xe-3se-3850-cr-book/sec-s1-xe-3se-3850-cr-book_chapter_01.html#wp3404908137
upvoted 3 times

  **Sarbi** 3 years ago

D is correct.
The following example shows how to display all authentication sessions on the switch:

Device# show authentication sessions

```
Interface MAC Address Method Domain Status Session ID
Gi1/48 0015.63b0.f676 dot1x DATA Authz Success 0A3462B1000000102983C05C
Gi1/5 000f.23c4.a401 mab DATA Authz Success 0A3462B1000000D24F80B58
Gi1/5 0014.bf5d.d26d dot1x DATA Authz Success 0A3462B10
```


upvoted 3 times

  **yenp** 3 years, 2 months ago

answer is D Displaying the Summary of All Auth Manager Sessions on the Switch
Enter the following:

```
Switch# show authentication sessions
Interface MAC Address Method Domain Status Session ID
```


Gi1/48 0015.63b0.f676 dot1x DATA Authz Success 0A3462B1000000102983C05C
Gi1/5 000f.23c4.a401 mab DATA Authz Success 0A3462B10000000D24F80B58
Gi1/5 0014.bf5d.d26d dot1x DATA Authz Success 0A3462B10000000E29811B94
upvoted 5 times

  **Raajaa** 3 years, 2 months ago

Answer is D
upvoted 4 times

Question #70

Topic 1

```
snmp-server group SNMP v3 auth access 15
```

Refer to the exhibit. What does the number 15 represent in this configuration?

- A. privilege level for an authorized user to this router
- B. access list that identifies the SNMP devices that can access the router
- C. interval in seconds between SNMPv3 authentication attempts
- D. number of possible failed attempts until the SNMPv3 user is locked out

Correct Answer: B

Community vote distribution

B (100%)

  **Cisco_SecCol** **Highly Voted**  2 years, 11 months ago

B is correct. <https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/snmp/configuration/xe-16/snmp-xe-16-book/nm-snm-cfg-snm-support.html#GUID-10FB2FAD-39A6-41D8-AB14-0C4B6E20911F>
upvoted 7 times

  **Marshpillowz** **Most Recent**  5 months, 1 week ago

Selected Answer: B

B is correct
upvoted 1 times

What is the result of running the crypto isakmp key ciscXXXXXXXX address 172.16.0.0 command?

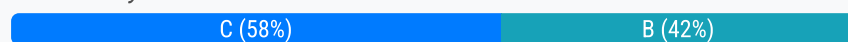
- A. authenticates the IKEv2 peers in the 172.16.0.0/16 range by using the key ciscXXXXXXXX
- B. authenticates the IP address of the 172.16.0.0/32 peer by using the key ciscXXXXXXXX
- C. authenticates the IKEv1 peers in the 172.16.0.0/16 range by using the key ciscXXXXXXXX
- D. secures all the certificates in the IKE exchange by using the key ciscXXXXXXXX

Correct Answer: B

Reference:

<https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/security/a1/sec-a1-cr-book/sec-cr-c4.html#wp6039879000>

Community vote distribution



Ampersand Highly Voted 3 years, 5 months ago

B is correct. When you use "address" it is referring to the remote peer you share the key with. If you want to add more than 1 ip add, you will have to use group key.

upvoted 17 times

nospampls 3 years, 1 month ago

C is correct

did this ins GNS3

```
R1(config)#crypto isakmp key 123123 address 172.16.0.0
R1(config)#end
R1#show crypto isakmp key
Keyring Hostname/Address Preshared Key
```

```
default 172.16.0.0 [255.255.0.0] 123123
```

same as Seawanderer did

upvoted 15 times

jaciro11 2 years, 9 months ago

Man this is not true...

upvoted 3 times

kwong328 1 year, 6 months ago

You are correct, I have verified in IOU. because the command "crypto isakmp key ciscXXXXXXXX address 172.16.0.0" did not specified the mask, the router will take is as /16, unless you specify the mask as "crypto isakmp key ciscXXXXXXXX address 172.16.0.0 255.255.255.0", the router will take it as /24.

upvoted 2 times

thefiresays Highly Voted 3 years, 6 months ago

It's weird that they used a network address, but this command authenticates a single VPN peer. Leaving B correct.

upvoted 9 times

loiphin 2 years, 8 months ago

This is not always a network address... for example on this subnet 172.16.4.0/23, 172.16.5.0 is a valid IP address, and nothing to do with network address. It just looks weird because people tend to subnet on /24's mostly.

upvoted 4 times

luismg Most Recent 1 week, 3 days ago

Selected Answer: C

it is an IKE v1 command so the answer is C

upvoted 1 times

Rockbo47 1 month ago

Selected Answer: C

isakmp command refers to IKEv1 and without specifying a mask it will use the default classful mask which in this case would be 255.255.0.0 for 172.16.0.0. So answer C is absolutely the correct answer. nospampls also demonstrates this with output.

upvoted 1 times

c3qu1 6 months ago

C is correct, the command `crypto isakmp key ciscXXXXXXXX address 172.16.0.0 0.0.255.255` authenticates IKEv1 peers in the 172.16.0.0/16 range by using the preshared key `ciscXXXXXXXX`.

upvoted 1 times

  **xziomal9** 10 months, 2 weeks ago

Selected Answer: C

Answer C

upvoted 2 times

  **squirrel49** 10 months, 3 weeks ago

Selected Answer: C

The command `crypto isakmp key` you provided is related to IKEv1, not IKEv2. IKEv1 (Internet Key Exchange version 1) is configured using `crypto isakmp` commands, whereas IKEv2 (Internet Key Exchange version 2) is configured using `crypto ikev2` commands.

If you want to configure a pre-shared key for IKEv1, the `crypto isakmp key` command is used as shown in your original question. If you want to configure a pre-shared key for IKEv2, you would use `crypto ikev2 keyring` and `crypto ikev2 profile` commands. The distinction is important because the two versions of IKE have different configurations and characteristics.

So IMHO - C is the right answer!

upvoted 1 times

  **RafaelSTI** 1 year, 1 month ago

C is correct, o IOS assumes a /16 mask if you omit the mask, like when you put at the and 0.0.0.0 and the IOS assumes a /0 mask (any). I test in the lab:

...

```
Router(config)# crypto isakmp key Mudar@123 address 172.16.0.0
Router(config)#do show crypto isakmp key
Keyring Hostname/Address Preshared Key
```

```
default 172.16.0.0 [255.255.0.0] Mudar@123
```

```
Router(config)#
```

upvoted 3 times

  **nep1019** 1 year, 1 month ago

Selected Answer: B

Some of you are overthinking this. Go here: https://www.cisco.com/c/en/us/td/docs/ios/12_2/security/command/reference/srfike.html#wp1017897

Search: `crypto isakmp key` and read. When you enter the peer using address, the mask is optional if you want to specify the subnet. If you specify no subnet then the address is to a single peer. In this case, 172.16.0.0/32 leaving B the only correct answer.



upvoted 1 times

  **nep1019** 1 year, 1 month ago

Explanation from the source:

mask (Optional) Specify the subnet address of the remote peer. (The argument can be used only if the remote peer ISAKMP identity was set with its IP address.)

upvoted 1 times

  **fdl543** 1 year, 1 month ago

Selected Answer: B

B is always correct. Using IKEv1 or IKEv2. C will fail if I use IKEv2...

upvoted 1 times

  **wizzlewazzle** 1 year, 3 months ago

With the address keyword, you can also use the mask argument to indicate the remote peer ISAKMP identity will be established using the preshared key only. If the mask argument is used, preshared keys are no longer restricted between two users.

Note

If you specify mask, you must use a subnet address. (The subnet address 0.0.0.0 is not recommended because it encourages group preshared keys, which allow all peers to have the same group key, thereby reducing the security of your user authentication.)

upvoted 1 times

  **G33** 1 year, 3 months ago

C is correct

Apart from reasons already given by other C campaigners

`ikev2` uses a different format for keys

```
crypto ikev2 keyring IKEv2-KEYRING
```

```
peer 1.2.3.4
```

```
address 1.2.3.4
```

```
pre-shared-key cisco123
```

apart from that whe you actually run the command in a lab it results in

```
172.16.0.0 [255.255.0.0]
```

It assumes a subnet for anything that ends in .0


upvoted 2 times

  **Kromwall** 1 year, 3 months ago

Selected Answer: B

B is correct

upvoted 1 times

  **gc999** 1 year, 3 months ago

Selected Answer: B

This question is tricky, it is testing the concept I believe. According to the CLI, it should be "peer". In Option B, it is 172.16.0.0/32 "peer", but in Option C, it is 172.16.0.0 "range". No matter then can be reachable, I will select the one with "peer".

upvoted 1 times

  **haiderzaid** 1 year, 5 months ago

B

"If the mask argument is used, preshared keys are no longer restricted between two users" so its restricted to 172.16.0.0

https://www.cisco.com/c/en/us/td/docs/ios/12_2/security/command/reference/srfike.html

upvoted 1 times

  **haiderzaid** 1 year, 5 months ago

i tested it on a real router and the output was
Keyring Hostname/Address Preshared Key

```
default 172.16.0.0 [255.255.0.0] cisco
```



but if i use 172.0.0.1

```
Keyring Hostname/Address Preshared Key
```

```
default 172.16.0.1 cisco
```



weird thing , not B

upvoted 2 times

  **angry** 1 year, 6 months ago

C is the correct answer!

upvoted 6 times

  **angry** 1 year, 6 months ago

B is correct!

upvoted 2 times

Which command enables 802.1X globally on a Cisco switch?

- A. dot1x system-auth-control
- B. dot1x pae authenticator
- C. authentication port-control auto
- D. aaa new-model

Correct Answer: A

Reference:

https://www.cisco.com/c/en/us/td/docs/routers/nfvis/switch_command/b-nfvis-switch-command-reference/802_1x_commands.html

Community vote distribution

A (100%)

Marshpillowz 5 months, 1 week ago

Selected Answer: A

A is correct

upvoted 1 times

bobie 1 year, 3 months ago

Selected Answer: A

The command to globally enable 802.1x authentication on the switch, use the dot1x system-auth-control command in Global Configuration mode.

<https://www.cisco.com/c/en/us/support/docs/smb/switches/cisco-small-business-300-series-managed-switches/smb5635-configure-global-802-1x-properties-on-a-switch-through-the-c.html>

upvoted 1 times

Cnoteone 1 year, 10 months ago

To enable 802.1X globally, use the dot1x system-auth-control command in switch configuration mode. To restore the default configuration, use the no form of this command.

dot1x system-auth-control

upvoted 2 times

leowulf 1 year, 11 months ago

I will go with A

Step 3. To globally enable 802.1x authentication on the switch, use the dot1x system-auth-control command in Global Configuration mode.

<https://www.cisco.com/c/en/us/support/docs/smb/switches/cisco-small-business-300-series-managed-switches/smb5635-configure-global-802-1x-properties-on-a-switch-through-the-c.html>

upvoted 3 times

SulSulEi 2 years ago

Selected Answer: A

A is the answer, no doubt

upvoted 3 times

Odorka222 2 years ago

B is answer, https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_8021x/configuration/xe-3se/3850/sec-user-8021x-xe-3se-3850-book/config-ieee-802x-pba.html

D - only enable AAA not 802.1x

upvoted 1 times

surforlife 2 years, 1 month ago

The following example shows how to enable IEEE 802.1X and AAA on Fast Ethernet port 2/1 and how to verify the configuration:

Note

In this example the Ethernet interface is configured as an access port by using the switchport mode access command in interface configuration mode. The Ethernet interface can also be configured as a trunk port using the switchport mode trunk command in interface configuration mode.

Device> enable

Device# configure terminal

Device(config)# dot1x system-auth-control



Device(config)# aaa new-model



Device(config)# aaa authentication dot1x default group radius

Device(config)# interface fastethernet2/1



```
Device(config-if)# switchport mode access
Device(config-if)# authentication port-control auto
Device(config-if)# dot1x pae authenticator
Device(config-if)# end
```

"A" looks like correct answer
upvoted 3 times

  **ureis** 1 year, 11 months ago
this is not globally
upvoted 1 times

  **nenotronix** 2 years, 2 months ago
correct answer is D
"aaa new-model"

<https://www.cisco.com/c/en/us/support/docs/security-vpn/terminal-access-controller-access-control-system-tacacs-/10384-security.html>
upvoted 1 times

  **ureis** 1 year, 11 months ago
Man this is for authentication not for dot1x
upvoted 3 times

What is a characteristic of Dynamic ARP Inspection?

- A. DAI determines the validity of an ARP packet based on valid IP to MAC address bindings from the DHCP snooping binding database.
- B. In a typical network, make all ports as trusted except for the ports connecting to switches, which are untrusted.
- C. DAI associates a trust state with each switch.
- D. DAI intercepts all ARP requests and responses on trusted ports only.

Correct Answer: A

Community vote distribution

A (100%)

Sarbi Highly Voted 3 years ago

The correct answer is A.

Dynamic ARP Inspection

To prevent ARP poisoning attacks such as the one described in the previous section, a switch must ensure that only valid ARP requests and responses are relayed. DAI prevents these attacks by intercepting all ARP requests and responses. Each of these intercepted packets is verified for valid MAC address to IP address bindings before the local ARP cache is updated or the packet is forwarded to the appropriate destination. Invalid ARP packets are dropped.

DAI determines the validity of an ARP packet based on valid MAC address to IP address bindings stored in a trusted database. This database is built at runtime by DHCP snooping, provided that it is enabled on the VLANs and on the switch in question. In addition, DAI can also validate ARP packets against user-configured ARP ACLs in order to handle hosts that use statically configured IP addresses.

DAI can also be configured to drop ARP packets when the IP addresses in the packet are invalid or when the MAC addresses in the body of the ARP packet do not match the addresses specified in the Ethernet header.

upvoted 6 times

Marshpillowz Most Recent 5 months, 1 week ago

Selected Answer: A

A is correct

upvoted 1 times

Thusi26 2 years, 3 months ago

A is the correct answer

upvoted 2 times

otzu1 2 years, 4 months ago

OSG:

Dynamic ARP inspection (DAI) is a security feature that validates ARP packets in a network. DAI intercepts, logs, and discards ARP packets with invalid IP-to-MAC address bindings. This capability protects the network from some man-in-the-middle attacks.

DAI determines the validity of an ARP packet based on valid IP-to-MAC address bindings stored in a trusted database, the DHCP snooping binding database. As described in the previous section, this database is built by DHCP snooping if DHCP snooping is enabled on the VLANs and on the switch. If the ARP packet is received on a trusted interface, the switch forwards the packet without any checks. On untrusted interfaces, the switch forwards the packet only if it is valid.

A

upvoted 2 times

nickanme 2 years, 11 months ago

https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750x_3560x/software/release/12-2_58_se/configuration/guide/3750xscg/swdynarp.html#wp1039773

upvoted 1 times

nickanme 2 years, 11 months ago

@ Amedeou

In non-DHCP environments, dynamic ARP inspection can validate ARP packets against user-configured ARP access control lists (ACLs) for hosts with statically configured IP addresses. You define an ARP ACL by using the `arp access-list acl-name global` configuration command. For configuration information, see the "Configuring ARP ACLs for Non-DHCP Environments" section. The switch logs dropped packets. For more information about the log buffer, see the "Logging of Dropped Packets" section.

upvoted 1 times

  **Amedeou** 3 years ago

what happen if there is no DHCP involved ?

upvoted 1 times

Question #74

Topic 1

Which statement about IOS zone-based firewalls is true?

- A. An unassigned interface can communicate with assigned interfaces
- B. Only one interface can be assigned to a zone.
- C. An interface can be assigned to multiple zones.
- D. An interface can be assigned only to one zone.

Correct Answer: D

Reference:

<https://www.cisco.com/c/en/us/support/docs/security/ios-firewall/98628-zone-design-guide.html>

Community vote distribution



D (100%)

  **Marshpillowz** 5 months, 1 week ago

Selected Answer: D

D is correct

upvoted 1 times

  **sull3y** 1 year, 7 months ago

D

Rules For Zone-Based Policy Firewall Application

Router network interface memberships in zones is subject to several rules that govern interface behavior, as is the traffic that moves between zone member interfaces:

A zone must be configured before interfaces can be assigned to the zone.

An interface can be assigned to only one security zone.

All traffic to and from a given interface is implicitly blocked when the interface is assigned to a zone, except traffic to and from other interfaces in the same zone, and traffic to any interface on the router.

Traffic is implicitly allowed to flow by default among interfaces that are members of the same zone.

In order to permit traffic to and from a zone member interface, a policy that allows or inspects traffic must be configured between that zone and any other zone.

The self-zone is the only exception to the default deny all policy. All traffic to any router interface is allowed until traffic is explicitly denied.

upvoted 4 times

  **Here_comes_MrLamb** 5 months, 3 weeks ago

D correct!!

<https://www.cisco.com/c/en/us/support/docs/security/ios-firewall/98628-zone-design-guide.html#anc11>

upvoted 1 times

  **Cnoteone** 1 year, 10 months ago

D for me

upvoted 2 times

  **BloodyBronco** 2 years, 6 months ago

D is correct

upvoted 4 times

When wired 802.1X authentication is implemented, which two components are required? (Choose two.)

- A. authentication server: Cisco Identity Service Engine
- B. supplicant: Cisco AnyConnect ISE Posture module
- C. authenticator: Cisco Catalyst switch
- D. authenticator: Cisco Identity Services Engine
- E. authentication server: Cisco Prime Infrastructure

Correct Answer: AC

Reference:

<https://www.lookingpoint.com/blog/ise-series-802.1x>

Community vote distribution

AC (100%)

Rockbo47 1 month ago

Selected Answer: AC

Out of the provided options, A and C are the correct choices. B is there to catch you out because whilst a supplicant is required, the ISE Posture module is not

upvoted 1 times

Marshpillowz 5 months, 1 week ago

Selected Answer: AC

A and C are correct

upvoted 1 times

Which SNMPv3 configuration must be used to support the strongest security possible?

- A. asa-host(config)#snmp-server group myv3 v3 priv asa-host(config)#snmp-server user andy myv3 auth sha cisco priv des ciscXXXXXXXXX
asa-host(config)#snmp-server host inside 10.255.254.1 version 3 andy
- B. asa-host(config)#snmp-server group myv3 v3 noauth asa-host(config)#snmp-server user andy myv3 auth sha cisco priv aes 256
ciscXXXXXXXXX asa-host(config)#snmp-server host inside 10.255.254.1 version 3 andy
- C. asa-host(config)#snmp-server group myv3 v3 noauth asa-host(config)#snmp-server user andy myv3 auth sha cisco priv 3des
ciscXXXXXXXXX asa-host(config)#snmp-server host inside 10.255.254.1 version 3 andy
- D. asa-host(config)#snmp-server group myv3 v3 priv asa-host(config)#snmp-server user andy myv3 auth sha cisco priv aes 256
ciscXXXXXXXXX asa-host(config)#snmp-server host inside 10.255.254.1 version 3 andy

Correct Answer: D

Community vote distribution

D (100%)

sull3y Highly Voted 1 year, 7 months ago

D. asa-host(config)#snmp-server group myv3 v3 priv asa-host(config)#snmp-server user andy myv3 auth sha cisco priv aes 256 ciscXXXXXXXXX asa-host(config)#snmp-server host inside 10.255.254.1 version 3 andy

SNMPv3 offers three security levels: noAuthNoPriv, authNoPriv, and authPriv. The strongest security possible is achieved by using the authPriv security level. This level requires both an authentication and a privacy (encryption) protocol.

Option D is using the authPriv security level, it uses the AES256 for encryption which is considered a stronger encryption algorithm than 3DES, and it uses the SHA for authentication which is considered a stronger authentication algorithm than MD5.

It is important to note that the real configuration may vary depending on the device and the vendor.

upvoted 5 times

Marshpillowz Most Recent 5 months, 1 week ago

Selected Answer: D

D is correct

upvoted 1 times

xziomal9 10 months, 2 weeks ago

Selected Answer: D

A.

asa-host(config)#snmp-server group myv3 v3 priv
asa-host(config)#snmp-server user andy myv3 auth sha cisco priv des ciscXXXXXXXXX
asa-host(config)#snmp-server host inside 10.255.254.1 version 3 andy

B.

asa-host(config)#snmp-server group myv3 v3 noauth
asa-host(config)#snmp-server user andy myv3 auth sha cisco priv aes 256 ciscXXXXXXXXX
asa-host(config)#snmp-server host inside 10.255.254.1 version 3 andy

C.

asa-host(config)#snmp-server group myv3 v3 noauth
asa-host(config)#snmp-server user andy myv3 auth sha cisco priv 3des ciscXXXXXXXXX
asa-host(config)#snmp-server host inside 10.255.254.1 version 3 andy

D.

asa-host(config)#snmp-server group myv3 v3 priv
asa-host(config)#snmp-server user andy myv3 auth sha cisco priv aes 256 ciscXXXXXXXXX
asa-host(config)#snmp-server host inside 10.255.254.1 version 3 andy

upvoted 2 times

psuoh 1 year, 7 months ago

D is better Cisco answer

AES allows you to choose a 128-bit, 192-bit or 256-bit key, making it exponentially stronger than the 56-bit key of DES. Encryption is also much faster in AES vs. DES, making it ideal for applications, firmware and hardware that require low latency or high throughput.

privacy in SNMP-server user (Optional) Specifies the use of the User-based Security Model (USM) for SNMP version 3 for SNMP message level security.

upvoted 2 times

Under which two circumstances is a CoA issued? (Choose two.)

- A. A new authentication rule was added to the policy on the Policy Service node.
- B. An endpoint is deleted on the Identity Service Engine server.
- C. A new Identity Source Sequence is created and referenced in the authentication policy.
- D. An endpoint is profiled for the first time.
- E. A new Identity Service Engine server is added to the deployment with the Administration persona.

Correct Answer: *BD*

Reference:

https://www.cisco.com/en/US/docs/security/ise/1.0/user_guide/ise10_prof_pol.html

Community vote distribution

BD (100%)

aadach Highly Voted 4 years, 1 month ago

The profiler service implements the CoA in the following cases:

- Static assignment of an endpoint
- An exception action is configured
- An endpoint is profiled for the first time
- Endpoint deleted
upvoted 31 times

ozone1864 Highly Voted 4 years, 1 month ago

Its B & D

upvoted 11 times

Premium_Pils Most Recent 1 month ago

Change of Authorization (CoA)

upvoted 1 times

Marshpillowz 5 months, 1 week ago

Selected Answer: BD

B and D correct

upvoted 1 times

Nizar_Makarem 2 years, 10 months ago

BD are correct

upvoted 3 times

Raajaa 3 years, 2 months ago

B and D is the answer

upvoted 3 times

thegreek1 3 years, 10 months ago

https://www.cisco.com/en/US/docs/security/ise/1.0/user_guide/ise10_prof_pol.html

aadach 2 months, 1 week ago

The profiler service implements the CoA in the following cases:

- Static assignment of an endpoint
- An exception action is configured
- An endpoint is profiled for the first time
- Endpoint deleted
upvoted 3 times

naddaf 4 years, 1 month ago

i think its A & C

upvoted 1 times

Question #78

Topic 1

Which ASA deployment mode can provide separation of management on a shared appliance?

- A. DMZ multiple zone mode
- B. transparent firewall mode
- C. multiple context mode
- D. routed mode

Correct Answer: C

Community vote distribution

C (100%)

molinux Highly Voted 2 years, 9 months ago

Yes. Multicontext
upvoted 5 times

Marshpillowz Most Recent 5 months, 1 week ago

Selected Answer: C

C multi-context
upvoted 1 times

sull3y 1 year, 7 months ago

C. multiple context mode

The Cisco ASA firewall supports several deployment modes, one of them is multiple context mode also known as Security Contexts mode. This mode allows for the separation of management on a shared appliance by creating multiple virtual firewalls, each with its own security policies, interfaces, and administrators. This allows for a more granular control of network access and security, as well as logical separation of different security zones on the same physical appliance.

This deployment mode is typically used in large enterprises or service providers to provide secure multitenancy, segregating different customers or departments on the same device while keeping their security policies separate.

upvoted 4 times

```

Sysauthcontrol      Enabled
Dot1x Protocol Version 3

Dot1x Info for GigabitEthernet1/0/12
-----
PAE                  = AUTHENTICATOR
PortControl          = FORCE_AUTHORIZED
ControlDirection    = Both
HostMode             = SINGLE_HOST
QuietPeriod          = 60
ServerTimeout        = 0
SuppTimeout          = 30
ReAuthMax            = 2
MaxReq               = 2
TxPeriod             = 30

```

Refer to the exhibit. Which command was used to display this output?

- A. show dot1x all
- B. show dot1x
- C. show dot1x all summary
- D. show dot1x interface gi1/0/12

Correct Answer: A

Reference:

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_8021x/configuration/x3se/3850/sec-user-8021x-xe-3se-3850-book/config-ieee-802x-pba.html

Community vote distribution

A (100%)

CiscoTech Highly Voted 4 years, 2 months ago

It is. A

The following example displays show dot1x all command output:

```
Device# show dot1x all
```

```

Sysauthcontrol Enabled
Dot1x Protocol Version 2
Dot1x Info for FastEthernet1
-----
PAE = AUTHENTICATOR
PortControl = AUTO
ControlDirection = Both
HostMode = MULTI_HOST
ReAuthentication = Disabled
QuietPeriod = 60
ServerTimeout = 30
SuppTimeout = 30
ReAuthPeriod = 3600 (Locally configured)
ReAuthMax = 2
MaxReq = 2
TxPeriod = 30
RateLimitPeriod = 0
Device-871#

```

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_8021x/configuration/x3se/3850/sec-user-8021x-xe-3se-3850-book/config-ieee-802x-pba.html

upvoted 20 times

moiz_109 Highly Voted 4 years, 2 months ago

No. It's A

upvoted 8 times

Marshpillowz Most Recent 5 months, 1 week ago

Selected Answer: A

A is correct

upvoted 1 times

[-] 👤 **Ferdaush** 8 months, 4 weeks ago

It is: A

upvoted 1 times

[-] 👤 **Totosos1** 1 year, 5 months ago

Selected Answer: A

Definitely 'A':

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_8021x/configuration/x3e/3850/sec-user-8021x-xe-3se-3850-book/config-ieee-802x-pba.html

upvoted 1 times

[-] 👤 **zheka** 2 years, 9 months ago

I configured only one port on the real switch for dot1x together with the global dot1x authentication. Ran two commands to show the difference, see below and make a correct decision for the correct answer.

```
2960_SW3(config-if)#do sh dot1x all
Sysauthcontrol Enabled
Dot1x Protocol Version 3
```

Dot1x Info for GigabitEthernet1/0/45

```
-----
PAE = AUTHENTICATOR
QuietPeriod = 60
ServerTimeout = 0
SuppTimeout = 30
ReAuthMax = 2
MaxReq = 2
TxPeriod = 30
```

```
2960_SW3(config-if)#do sh dot1x int gig1/0/45
```

Dot1x Info for GigabitEthernet1/0/45

```
-----
PAE = AUTHENTICATOR
QuietPeriod = 60
ServerTimeout = 0
SuppTimeout = 30
ReAuthMax = 2
MaxReq = 2
TxPeriod = 30
```

upvoted 6 times

[-] 👤 **Raajaa** 3 years, 2 months ago

Answer is A

upvoted 4 times

[-] 👤 **juanlecho** 3 years, 5 months ago

```
xxxxxx-xxxx-xxxx-sw1#show interface gigabitEthernet 1/0/1
```

Dot1x Info for GigabitEthernet1/0/1

```
-----
PAE = AUTHENTICATOR
QuietPeriod = 60
ServerTimeout = 0
SuppTimeout = 30
ReAuthMax = 2
MaxReq = 2
TxPeriod = 10
```

□

```
xxxxxx-xxxx-xxxx-sw1#
```

CCC

```
xxxx-xxxx-xxxx-sw1#show dot1x all
```

```
Sysauthcontrol Enabled
Dot1x Protocol Version 3
```

Dot1x Info for GigabitEthernet1/0/1

```
-----
PAE = AUTHENTICATOR
QuietPeriod = 60
ServerTimeout = 0
SuppTimeout = 30
ReAuthMax = 2
MaxReq = 2
TxPeriod = 10
```

Dot1x Info for GigabitEthernet1/0/2

```
-----
PAE = AUTHENTICATOR
QuietPeriod = 60
```

ServerTimeout = 0
SuppTimeout = 30
ReAuthMax = 2
MaxReq = 2
TxPeriod = 10



!!!!!!!!!! ANSWER IS A !!!!!!!

upvoted 2 times

  **Jeeves69** 3 years, 6 months ago

A is the correct answer, because only the 'show dot1x all' command shows the 'Sysauthcontrol' status and Dot1x Protocol Version

upvoted 5 times

  **Kris92** 3 years, 6 months ago

A should show all interfaces, D only for specific interface, so both are correct, would go with D if I have to choose

To display the IEEE 802.1X administrative and operational status for the switch, use the show dot1x all [details | statistics | summary] command in privileged EXEC configuration mode.

To display the IEEE 802.1X administrative and operational status for a specific port, use the show dot1x interface type number command in privileged EXEC configuration mode. For detailed information about the fields in these displays, see the command reference for this release.

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_8021x/configuration/x-3se/3850/sec-user-8021x-xe-3se-3850-book/config-ieee-802x-pba.html

upvoted 1 times

  **Javimc** 3 years, 7 months ago

No, is A. With D you don't have sysauthcontrol info

upvoted 4 times

  **Vic25H** 4 years, 2 months ago

Should be D

<https://guides.co/g/cisco-trustsec-failed-authentications-and-authorizations/10982>

upvoted 3 times

What is a characteristic of Cisco ASA NetFlow v9 Secure Event Logging?

- A. It tracks flow-create, flow-teardown, and flow-denied events.
- B. It provides stateless IP flow tracking that exports all records of a specific flow.
- C. It tracks the flow continuously and provides updates every 10 seconds.
- D. Its events match all traffic classes in parallel.

Correct Answer: A

Reference:

<https://www.cisco.com/c/en/us/td/docs/security/asa/asa92/configuration/general/asa-general-cli/monitor-nse.html>

Community vote distribution

A (100%)

Marshpillowz 5 months, 1 week ago

Selected Answer: A

A is correct

upvoted 1 times

sull3y 1 year, 7 months ago

A. It tracks flow-create, flow-teardown, and flow-denied events.

Cisco ASA NetFlow v9 Secure Event Logging is a feature that allows the ASA to export detailed information about network traffic flow and security events to a NetFlow collector for analysis. The exported information includes information about flow-create, flow-teardown and flow-denied events, which provide insight into the behavior of the traffic passing through the firewall.

This feature also allows for the collection of detailed information about the traffic passing through the firewall which can be used for security incident investigations, capacity planning and troubleshooting.

It does not provide stateless IP flow tracking that exports all records of a specific flow (B) or tracks the flow continuously and provides updates every 10 seconds (C) and also it does not match all traffic classes in parallel (D)

upvoted 2 times

surforlife 2 years, 2 months ago

A is correct.

In stateful flow tracking, tracked flows go through a series of state changes. NSEL events are used to export data about flow status and are triggered by the event that caused the state change.

The significant events that are tracked include flow-create, flow-teardown, and flow-denied (excluding those flows that are denied by EtherType ACLs). In addition, the ASA and ASASM implementation of NSEL generates periodic NSEL events, flow-update events, to provide periodic byte counters over the duration of the flow. These events are usually time-driven, which makes them more in line with traditional NetFlow; however, they may also be triggered by state changes in the flow.

upvoted 3 times

Cyril_the_Squirrel 2 years, 2 months ago

This is Correct

upvoted 1 times

A network engineer has entered the snmp-server user andy myv3 auth sha cisco priv aes 256 cisc0383320506 command and needs to send SNMP information to a host at 10.255.254.1. Which command achieves this goal?

- A. snmp-server host inside 10.255.254.1 snmpv3 andy
- B. snmp-server host inside 10.255.254.1 version 3 myv3
- C. snmp-server host inside 10.255.254.1 snmpv3 myv3
- D. snmp-server host inside 10.255.254.1 version 3 andy

Correct Answer: D

Reference:

https://www.cisco.com/c/m/en_us/techdoc/dc/reference/cli/nxos/commands/sm/snmp-server-host.html

Community vote distribution

D (100%)

Jeeves69 Highly Voted 3 years, 6 months ago

Correct answer is D

See:

<https://www.networkstraining.com/how-to-configure-snmp-on-cisco-asa-5500-firewall/>

And:

https://www.cisco.com/c/en/us/td/docs/security/asa/snmp/snmpv3_tools/snmpv3_1.html

upvoted 23 times

Marshpillowz Most Recent 5 months, 1 week ago

Selected Answer: D

D is correct

upvoted 1 times

Terry0987 1 year, 9 months ago

** CORRECT answer is D ***

snmp-server host interface { hostname | ip_address } [trap | poll] [community community-string] [version { 1 | 2c | 3 username }] [udp-port port]

upvoted 2 times

hz033 2 years, 4 months ago

Selected Answer: D

ASA(config)# snmp-server host inside 10.255.254.1 version 3 ?

configure mode commands/options:

Current available user name(s):

ASA(config)# snmp-server host inside 10.255.254.1 version 3 andy

require "Current available user name(s):"

so D is correct

upvoted 3 times

rbrain 2 years, 7 months ago

Selected Answer: D

D is correct

upvoted 4 times

zheka 2 years, 9 months ago

An attempt to add the SNMP server with the command on the ASA firewall:

See what the firewall expect as the input

fw(config)# snmp-server host inside 172.16.0.94 ver 3 ?

configure mode commands/options:

Current available user name(s):

snmpuser

upvoted 1 times



Sarbi 3 years ago

Anser D is correct.



snmp-server enable traps

!


```
! ...or insted select just some traps, for example:
! snmp-server enable traps envmon fan shutdown supply temperature status ospf cpu
!
snmp-server group trapgroup v3 priv
snmp-server user trapuser trapgroup v3 auth sha AuthPass priv 3des PrivPass
snmp-server host 10.1.1.161 traps version 3 priv trapuser
upvoted 2 times
```

  **Sarbi** 3 years ago



The correct answer is D
upvoted 2 times

  **jshow** 3 years, 2 months ago

100% D
For community-string, when version 1 or version 2c is specified, enter the password-like community string sent with the notification operation.
When version 3 is specified, enter the SNMPv3 username

https://www.cisco.com/c/en/us/td/docs/routers/ir910/software/release/1_1/configuration/guide/ir910scg/swsnmp.html

upvoted 2 times

  **Zoli6** 3 years, 2 months ago

Configuration Example of SNMP v3

Currently the most secure SNMP version is v3. To configure this version you need first to create an SNMP group, then an SNMP server and lastly a host (NMS) which will communicate with the firewall for management purposes.

Let's configure SNMP v3 with the example below:

```
ASA(config)# snmp-server enable
```

```
ASA(config)# snmp-server group snmpgroup v3 auth <- create v3 group with authentication
```

```
ASA(config)# snmp-server user administrator snmpgroup v3 auth sha strongpass <- create user "administrator" belonging to group "snmpgroup"
```

```
ASA(config)#snmp-server host inside 10.1.1.1 version 3 administrator <- specify the NMS host
```

Correct answer is D, administrator here is equal to andy

upvoted 3 times

  **deathfrom** 3 years, 3 months ago

You associate the SNMP host config with a user not a group. D is the correct answer

upvoted 4 times

  **CyberG** 3 years, 4 months ago

B is correct myv3 is the host, Andy is an user on host myv3

upvoted 1 times

  **nemeses667** 2 years, 1 month ago

myv3 is the snmp v3 group name. D is the correct answer

upvoted 1 times

An engineer wants to generate NetFlow records on traffic traversing the Cisco ASA. Which Cisco ASA command must be used?

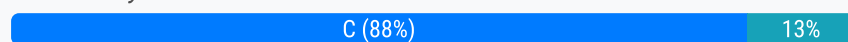
- A. flow exporter <name>
- B. ip flow-export destination 1.1.1.1 2055
- C. flow-export destination inside 1.1.1.1 2055
- D. ip flow monitor <name> input

Correct Answer: C

Reference:

https://www.cisco.com/c/en/us/td/docs/security/asa/special/netflow/guide/asa_netflow.html

Community vote distribution



Marshpillowz 5 months, 1 week ago

Selected Answer: C

C is correct

upvoted 1 times

yong08321 1 year, 4 months ago

The correct Cisco ASA command to generate NetFlow records on traffic traversing the device is "flow-export destination inside 1.1.1.1 2055".

The "flow-export destination inside" command is used to specify the IP address and port number of the NetFlow collector that will receive the exported flow data. In this case, the collector is located on the inside interface of the ASA. The IP address "1.1.1.1" and port number "2055" are just examples and should be replaced with the actual IP address and port number of the collector.

Option A, "flow exporter <name>", is used to configure the NetFlow exporter parameters, such as the version, transport protocol, and template options. Option B, "ip flow-export destination 1.1.1.1 2055", is a command used on Cisco routers to configure the NetFlow collector destination. Option D, "ip flow monitor <name> input", is a command used on Cisco routers to enable NetFlow data export for the specified flow monitor. These commands are not used on the Cisco ASA.

upvoted 1 times

surforlife 2 years, 2 months ago

"C" should be the correct answer.

Add an NSEL collector to which NetFlow packets may be sent.

flow-export destination interface-name ipv4-address | hostname udp-port

Example:

```
ciscoasa(config)# flow-export destination inside 209.165.200.225 2002
```

The destination keyword indicates that a NSEL collector is being configured. The interface-name argument is the name of the ASA and ASA Services Module interface through which the collector is reached. The ipv4-address argument is the IP address of the machine running the collector application. The hostname argument is the destination IP address or name of the collector. The udp-port argument is the UDP port number to which NetFlow packets are sent.

You can configure a maximum of five collectors. After a collector is configured, template records are automatically sent to all configured NSEL collectors.

upvoted 3 times

Pwned 2 years, 3 months ago

Selected Answer: C

C is correct

<https://support.auvik.com/hc/en-us/articles/360025289112-How-to-configure-NetFlow-on-Cisco-ASA-firewalls>

upvoted 3 times

jaciro11 2 years, 6 months ago

Selected Answer: C

ASA do it like C

upvoted 3 times


Jetnor 2 years, 9 months ago

Selected Answer: D

Correct answer should be D,

if we want to enable netflow to record traffic data we should apply monitor command on interface.

upvoted 1 times

 **Jetnor** 2 years, 9 months ago

Nevermind, Answer is C since this is an ASA. on switches we use monitor

upvoted 6 times

Which two tasks allow NetFlow on a Cisco ASA 5500 Series firewall? (Choose two.)

- A. Define a NetFlow collector by using the flow-export command
- B. Create a class map to match interesting traffic
- C. Create an ACL to allow UDP traffic on port 9996
- D. Enable NetFlow Version 9
- E. Apply NetFlow Exporter to the outside interface in the inbound direction

Correct Answer: AB

Community vote distribution

AB (100%)

Jeeves69 Highly Voted 3 years, 6 months ago

The Correct Answer is A and B.

Reference: https://www.cisco.com/c/en/us/td/docs/security/asa/special/netflow/guide/asa_netflow.html#pgfid-1330480

upvoted 20 times

Raajaa Highly Voted 3 years, 2 months ago

A and B is the correct answer

upvoted 5 times

Marshpillowz Most Recent 5 months, 1 week ago

Selected Answer: AB

A and B are correct

upvoted 1 times

yong08321 1 year, 4 months ago

Selected Answer: AB

The two tasks that are required to enable NetFlow on a Cisco ASA 5500 Series firewall are:

B. Create a class map to match interesting traffic: A class map is used to identify the interesting traffic for which NetFlow data needs to be exported. It can be based on various parameters such as source and destination IP address, protocol, port numbers, etc.

A. Define a NetFlow collector by using the flow-export command: This command is used to configure the NetFlow exporter parameters, such as the version, transport protocol, and template options. It also specifies the IP address and port number of the NetFlow collector that will receive the exported flow data.

upvoted 1 times

brownbear505 2 years, 6 months ago

Selected Answer: AB

The Correct Answer is A and B. Reference: https://www.cisco.com/c/en/us/td/docs/security/asa/special/netflow/guide/asa_netflow.html#pgfid-1330480

upvoted 5 times

coentror 2 years, 9 months ago

access-list global_mpc extended permit ip any any

!

flow-export destination inside 192.168.1.13 2055

!

class-map global_class

match access-list global_mpc

upvoted 1 times

Sarbi 3 years ago

A and B is the correct answer

upvoted 4 times

jmosilva 3 years, 1 month ago

A and B

"Flow-export actions are not supported in interface-based policies. You can configure flow-export actions in a class-map only with the match

access-list, match any, or class-default commands. You can only apply flow-export actions in a global service policy. "

upvoted 5 times

```
HQ_Router(config)# username admin5 privilege 5
HQ_Router(config)#privilege interface level 5 shutdown
HQ_Router(config)#privilege interface level 5 ip
HQ_Router(config)#privilege interface level 5 description
```

Refer to the exhibit. A network administrator configures command authorization for the admin5 user. What is the admin5 user able to do on HQ_Router after this configuration?

- A. set the IP address of an interface
- B. add subinterfaces
- C. complete no configurations
- D. complete all configurations

Correct Answer: C

Community vote distribution

C (100%)

dansecu Highly Voted 3 years, 4 months ago

the answer is C because the below line is missing from privilege configuration and the user will not be able to reach the interface config level:
privilege exec level 5 configure terminal
upvoted 19 times

Raajaa Highly Voted 3 years, 2 months ago

C is the answer
upvoted 5 times

Marshpillowz Most Recent 5 months, 1 week ago

Selected Answer: C

C is correct
upvoted 1 times

sull3y 1 year, 7 months ago

C. complete no configurations

Based on the given exhibit, the admin5 user has been given command authorization for only the "show" command. This means that the admin5 user is only able to view the current configurations and status of the router, but not make any changes or modifications. Therefore, the admin5 user would not be able to set the IP address of an interface, add subinterfaces, or complete any configurations other than "show" commands.
upvoted 4 times

psuoh 1 year, 7 months ago

Example
So for example, consider the following set of privileges:

privilege interface level 5 shutdown

privilege interface level 5 ip address

privilege interface level 5 ip

privilege interface level 5 bandwidth

privilege configure level 5 interface

privilege exec level 5 show running-config

privilege exec level 5 show

The command show running-config will now display:

Current configuration : 425 bytes

!

boot-start-marker

boot-end-marker

```
!  
!  
!  
!  
!  
interface Loopback0  
ip address 10.255.255.1 255.255.255.255  
!  
interface FastEthernet0/0  
no ip address  
!  
interface FastEthernet0/1  
no ip address  
shutdown  
!  
interface Serial1/0  
bandwidth 512  
ip address 10.0.0.1 255.255.255.0  
!  
interface Serial1/1  
no ip address  
shutdown  
!  
interface Serial1/2  
no ip address  
shutdown  
!  
interface Serial1/3  
no ip address  
shutdown  
!  
!  
end
```

upvoted 2 times

  **BloodyBronco** 2 years, 4 months ago

Selected Answer: C

definitely C!

upvoted 4 times

  **brownbear505** 2 years, 6 months ago

Selected Answer: C

Needed:

Privilege exec level 5 configure terminal

Privilege configure level 5 interface

upvoted 2 times

  **Sun2sun** 2 years, 7 months ago

Selected Answer: C

C. complete no configurations
upvoted 3 times

  **Gaborimbo22** 3 years, 5 months ago

letter C is the correct
upvoted 4 times

A network engineer is configuring DMVPN and entered the `crypto isakmp key cisc0383320506 address 0.0.0.0` command on host A. The tunnel is not being established to host B. What action is needed to authenticate the VPN?

- A. Change the password on host A to the default password
- B. Enter the command with a different password on host B
- C. Enter the same command on host B
- D. Change isakmp to ikev2 in the command on host A

Correct Answer: C

Community vote distribution

C (100%)

Marshpillowz 5 months, 1 week ago

Selected Answer: C

C is correct

upvoted 1 times

sull3y 1 year, 7 months ago

C. Enter the same command on host B

The `crypto isakmp key` command is used to set the shared secret key for Internet Security Association and Key Management Protocol (ISAKMP) on a router. In order for the VPN tunnel to be established between host A and host B, the same shared secret key must be configured on both hosts. In this case, the network engineer needs to enter the same `crypto isakmp key` command, with the same password, on host B as they did on host A. This will ensure that both hosts are using the same shared secret key for authentication and the tunnel will be established. The other options A, B and D are not correct.

upvoted 3 times

psuoh 1 year, 7 months ago

The question should say the `crypto isakmp key cisc0383320506 address 0.0.0.0 0.0.0.0`

Example

Add dynamic pre-shared keys for all the remote VPN !--- routers and the hub router.

```
crypto isakmp key cisco123 address 0.0.0.0 0.0.0.0
```

upvoted 1 times

Net4dd 1 year, 8 months ago

C. Is true <https://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/29240-dcmvpn.html>

upvoted 2 times

dr4gn00t 2 years, 7 months ago

C is correct answer according to DMVPN configuration examples in cert guide

upvoted 2 times

Laryoul 2 years, 8 months ago

For me the good answer is C.

Enter 0.0.0.0 on a this command line could be done on Hub and Spoke.

Hub configuration is done on `ip nhrp`.

https://www.cisco.com/c/en/us/td/docs/ios/12_2/security/command/reference/srfike.html#wp1017897

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_dmvpn/configuration/15-mt/sec-conn-dmvpn-15-mt-book/sec-conn-dmvpn-dmvpn.html#GUID-BDBD63D7-C9FD-490F-B1AF-EFC38B6B497B

upvoted 2 times

loiphin 2 years, 8 months ago

I would say its A, because if you entered the same command on Host B, they would never establish a tunnel. `crypto isakmp key xxx 0.0.0.0` is only ever used on hubs. If you use the same command on a spoke they will never connect to each other.

upvoted 1 times

DarkestHour 2 years, 2 months ago

How would spoke to spoke tunnels ever be encrypted then?

upvoted 1 times

nomad 2 years, 9 months ago

0.0.0.0 adres wth! threw me off :P

upvoted 1 times

Question #86

Topic 1

How many interfaces per bridge group does an ASA bridge group deployment support?

- A. up to 16
- B. up to 2
- C. up to 4
- D. up to 8

Correct Answer: C

Community vote distribution

C (100%)

Moll Highly Voted 2 years, 10 months ago

C should be the only valid answer given the history of the SW versions..

<https://www.cisco.com/c/en/us/td/docs/security/asa/asa97/configuration/general/asa-97-general-config/intro-fw.html>

upvoted 7 times

u777 Highly Voted 3 years ago

C is the correct answer for Cisco ASA up to version 9.4 (up to 4 interfaces per bridge group)

<https://www.cisco.com/c/en/us/td/docs/security/asa/asa94/config-guides/cli/general/asa-94-general-config/interface-routed-tfw.html>

With Cisco ASA version 9.6 the correct answer is up to 64 interfaces per bridge group !!!

No such number there !!!

<https://www.cisco.com/c/en/us/td/docs/security/asa/asa96/configuration/general/asa-96-general-config/interface-routed-tfw.html>

upvoted 5 times

Marshpillowz Most Recent 5 months, 1 week ago

Selected Answer: C

C is correct

upvoted 1 times

denverfly 2 years, 6 months ago

C is the correct answer for Cisco ASA up to version 9.4.....The bridge group maximum was increased from 8 to 250 bridge groups. You can configure up to 250 bridge groups in single mode or per context in multiple mode, with 4 interfaces maximum per bridge group.We modified the following commands: interface bvi, bridge-group.

upvoted 5 times

Raajaa 3 years, 2 months ago

C is the correct answer

upvoted 2 times

Barish 3 years, 4 months ago

C is the correct Answ - You can assign up to 4 interfaces to a bridge group. You cannot assign the same interface to more than one bridge group.

<https://www.cisco.com/c/en/us/td/docs/security/asa/asa94/config-guides/cli/general/asa-94-general-config/interface-routed-tfw.html>

upvoted 2 times

kakakayayaya 3 years, 4 months ago

For Information:

You can assign up to 64 interfaces to a bridge group. You cannot assign the same interface to more than one bridge group.

https://www.cisco.com/c/en/us/td/docs/security/asa/asa97/configuration/general/asa-97-general-config/interface-routed-tfw.html#concept_0545A38665F04B78B993BAC61725B26D

???

upvoted 2 times

Seawanderer 3 years, 2 months ago

The problem with evolving technologies is that the exams can't change at the same speed of the software. You are looking at ASA 9.7, but the 9.4 had different specs

upvoted 3 times

A network administrator configures Dynamic ARP Inspection on a switch. After Dynamic ARP Inspection is applied, all users on that switch are unable to communicate with any destination. The network administrator checks the Interface status of all interfaces, and there is no err-disabled interface. What is causing this problem?

- A. DHCP snooping has not been enabled on all VLANs
- B. Dynamic ARP inspection has not been enabled on all VLANs
- C. The ip arp inspection limit command is applied on all interfaces and is blocking the traffic of all users
- D. The no ip arp inspection trust command is applied on all user host interfaces

Correct Answer: D

Community vote distribution

A (85%)

D (15%)

[-] **Jeeves69** Highly Voted 3 years, 6 months ago

The correct answer should be A. DHCP Snooping has not been enabled on all VLANs.

DHCP Snooping is a prerequisite for Dynamic ARP Inspection (DAI). When DHCP Snooping is enabled the 'no ip arp inspection trust' command only ensures that DAI will do its job, blocking invalid traffic.

upvoted 20 times

[-] **brownbear505** Highly Voted 2 years, 6 months ago

Selected Answer: A

DAI requires DHCP Snooping

upvoted 7 times

[-] **xzioma19** Most Recent 10 months, 2 weeks ago

Answer D

upvoted 1 times

[-] **DWizard** 1 year, 2 months ago

Selected Answer: D

The right answer is D. DAI can obtain its IP-MAC information from DHCP snooping or from ACLs statically configured by the admin, it could work without DHCP snooping, however, by default all the interfaces become untrusted, and you have to manually set the "no ip arp inspection trust" command on interfaces connecting to other switches, even if those switches do not support DAI, so the answer is D. You can read this, it's carefully explained:

<https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/12-2/25ew/configuration/guide/conf/dynarp.html>

upvoted 1 times

[-] **webwalker00** 1 year, 4 months ago

Selected Answer: A

DHCP snooping is required for DAI.

upvoted 2 times

[-] **achille5** 1 year, 6 months ago

Selected Answer: D

no err-disabled interfaces indicates that the problem may not be related to a physical or link-level issue, which could be the case with DHCP snooping misconfiguration. Likely option D as the cause of the problem.

upvoted 1 times

[-] **amtf8888** 1 year, 8 months ago

Selected Answer: A

a is correct

upvoted 1 times

[-] **sis_net_sec** 1 year, 11 months ago

Selected Answer: A

<https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipaddr/command/ipaddr-cr-book/ipaddr-i1.html#wp2458863701>

the command "no ip arp inspection trust" means the port is not trusted in DAI. This means that it will inspect packets from the port for appropriate entries in the DHCP Snooping table. This is the default state.

https://www.cisco.com/en/US/docs/switches/lan/catalyst3850/software/release/3.2_0_se/multiboo

k/configuration_guide/b_consolidated_config_guide_3850_chapter_0110111.html
err-disable on a port due to DAI comes from exceeding a rate limit.



upvoted 1 times

  **jaciro11** 2 years, 10 months ago

In a typical network configuration, you configure all switch ports connected to host ports as untrusted and configure all switch ports connected to switches as trusted. With this configuration, all ARP packets entering the network from a given switch bypass the security check. It is unnecessary to perform a validation at any other place in the VLAN or in the network. You configure the trust setting by using the ip arp inspection trust interface configuration command.

Answer is D

upvoted 1 times

  **birdman6709** 3 years ago



I think the issue here is the wording, the question is looking for what is causing the problem. With 'no ip arp inspection trust' enabled on all user ports, the switch is intercepting the ARP request and responses, and if there is no valid IP-to-MAC binding, the traffic is dropped and logged. So I think the answer should be D based on that.

upvoted 1 times

  **birdman6709** 3 years ago



I take that back actually, the answer is A. Since all the ports are untrusted anyways, as soon as DAI is enabled without DHCP snooping, they would drop since there is no IP-to-MAC binding. Adding the DHCP snooping in this case would fix the issue.

upvoted 6 times

  **zap_pap** 3 years, 1 month ago

The answer is D. It is tricky "no ip arp inspection trust" -> Trust removed from all interfaces -> Interfaces disabled.

upvoted 1 times

  **jshow** 3 years, 2 months ago

Its A

Dynamic ARP inspection depends on the entries in the DHCP snooping binding database to verify IP-to-MAC address bindings in incoming ARP requests and ARP responses. Make sure to enable DHCP snooping to permit ARP packets that have dynamically assigned IP addresses. When DHCP snooping is disabled or in non-DHCP environments, use ARP ACLs to permit or to deny packets.

upvoted 4 times

  **Dinges** 3 years, 2 months ago

A NOT NECESSARILY TRUE: DHCP snooping is not REQUIRED, when ARP ACLs are configured. Also not enabling DHCP snooping only on some vlans would not cause ALL users, connected to the switch being unable to communicate.


B NOT TRUE Not enabling DAI on a VLAN simply exempts the VLAN from DAI, it will not block traffic

C TRUE: Rate-limit exceed can put the interface in err-disabled state. Even if its not configured by admin; it is set at 15 ARP pps by default, but admin could have configured it with even lower limit, or an actual DOS attack has ocured.

D NOT TRUE: No ip arp inspection trust command MUST be applied on all user HOST interfaces. Only ports leading to the DHCP server should be set as trusted (EXCEPT if the upstream switch does not have DAI enabled, then leave it as untrusted and apply ARP ACLs locally).

<https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/12-2/25ew/configuration/guide/conf/dynarp.html>

upvoted 1 times

  **Dinges** 3 years, 2 months ago

CORRECTION:



The question explicitly mentions that no interface is in err-disabled state, so C cannot be the correct answer.

D is not the cause: Packets arriving on trusted interfaces bypass all DAI validation checks, while those arriving on untrusted interfaces go through the DAI validation process.

So, to me, that leaves on A as a possible answer.


Im going with A

upvoted 6 times

  **FN21** 3 years, 4 months ago

D is correct. DHCP snooping is not a prerequisite for Dynamic ARP. The question is tricky though. Since it doesn't mention about configuring DHCP snooping, issuing the "no ip arp inspection trust" command surely will kill all connections. All interfaces have become untrusted and Dynamic ARP doesn't have a DHCP snooping database to compare to.

upvoted 3 times

  **statikd** 3 years, 2 months ago

Wrong. All switch ports connected to hosts should be untrusted. The only trusted ports should be ports connected to other switches. By default switch ports are untrusted. DHCP snooping works in conjunction with Dynamic ARP inspection. The answer is A

upvoted 3 times

  **dansecu** 3 years, 4 months ago

Jeeves69 provided correct answer. it is A

DHCP Snooping should be enable globally and on VLANs. The IP-MAC pair is checed by DAI in DHCP database.

Answer D is related to hosts interfaces and they should be always untrusted.

upvoted 3 times

  **thefiresays** 3 years, 5 months ago

D is correct. By default all interfaces will be untrusted. You must have trusted interfaces facing other network devices. Interfaces connected to hosts are untrusted and will validate DHCP table bindings to decide whether to forward/drop.

What Jeeves wrote is true. But not enabling DHCP snooping would not break connectivity.

What is a difference between FlexVPN and DMVPN?

- A. DMVPN uses only IKEv1. FlexVPN uses only IKEv2
- B. FlexVPN uses IKEv2. DMVPN uses IKEv1 or IKEv2
- C. DMVPN uses IKEv1 or IKEv2. FlexVPN only uses IKEv1
- D. FlexVPN uses IKEv1 or IKEv2. DMVPN uses only IKEv2

Correct Answer: B

Community vote distribution

B (100%)

[-] **Raajaa** Highly Voted 3 years, 2 months ago

B is the correct answer
upvoted 5 times

[-] **Marshpillowz** Most Recent 5 months, 1 week ago

Selected Answer: B

B is correct
upvoted 1 times

[-] **Alizade** 11 months, 2 weeks ago

Selected Answer: B

B. FlexVPN uses IKEv2. DMVPN uses IKEv1 or IKEv2.
upvoted 2 times

[-] **sull3y** 1 year, 7 months ago

B. FlexVPN uses IKEv2. DMVPN uses IKEv1 or IKEv2

FlexVPN is a Cisco VPN solution that simplifies the deployment of VPNs using a centralized VPN management model. It uses IKEv2 as the default key exchange protocol to provide secure and flexible VPN connections. FlexVPN is supported on Cisco IOS XE and Cisco IOS software platforms.

DMVPN (Dynamic Multipoint Virtual Private Network) is a Cisco VPN solution that enables the creation of VPNs with dynamic spoke-to-spoke connections. It uses IKEv1 or IKEv2 as the key exchange protocol to provide secure VPN connections. DMVPN is supported on Cisco IOS, Cisco IOS XE and Cisco IOS XR software platforms.

upvoted 3 times

DRAG DROP -

Drag and drop the capabilities of Cisco Firepower versus Cisco AMP from the left into the appropriate category on the right.

Select and Place:

provides detection, blocking, tracking, analysis and remediation to protect against targeted persistent malware attacks	Cisco Firepower
provides superior threat prevention and mitigation for known and unknown threats	
provides outbreak control through custom detections	
provides the root cause of a threat based on the indicators of compromise seen	Cisco AMP
provides the ability to perform network discovery	
provides intrusion prevention before malware compromises the host	

Correct Answer:



provides detection, blocking, tracking, analysis and remediation to protect against targeted persistent malware attacks	Cisco Firepower provides superior threat prevention and mitigation for known and unknown threats provides the ability to perform network discovery provides intrusion prevention before malware compromises the host
provides superior threat prevention and mitigation for known and unknown threats	
provides outbreak control through custom detections	
provides the root cause of a threat based on the indicators of compromise seen	Cisco AMP provides detection, blocking, tracking, analysis and remediation to protect against targeted persistent malware attacks provides outbreak control through custom detections provides the root cause of a threat based on the indicators of compromise seen
provides the ability to perform network discovery	
provides intrusion prevention before malware compromises the host	

AMP provides intrusion prevention before malware compromises the host

The answer is wrong!!!

<https://essextec.com/wp-content/uploads/2018/03/Cisco-AMP-for-Endpoints-At-a-Glance.pdf>

upvoted 1 times

  **Cock** 2 years, 8 months ago

I am incorrect. The answer provided is correct

upvoted 6 times

An engineer needs behavioral analysis to detect malicious activity on the hosts, and is configuring the organization's public cloud to send telemetry using the cloud provider's mechanisms to a security device. Which mechanism should the engineer configure to accomplish this goal?

- A. sFlow
- B. NetFlow
- C. mirror port
- D. VPC flow logs

Correct Answer: D

Community vote distribution

D (100%)

acc2326 Highly Voted 3 years, 3 months ago
correct answer is D - VPC flow logs
upvoted 9 times

jaciro11 Highly Voted 2 years, 10 months ago
Its D

I totally remember when I configure the first time the Stealthwatch Cloud
upvoted 9 times

Nonono2 Most Recent 2 months ago
Selected Answer: D
VPC flow logs
upvoted 1 times

Marshpillowz 5 months, 1 week ago
Selected Answer: D
D is correct
upvoted 1 times

psuoh 1 year, 7 months ago
A, B, C are for data networks containing switches and routers

VPC slow log is meant for cloud based network like AWS.

Now, Secure Cloud Analytics (formerly Stealthwatch Cloud) can automatically retrieve VPC Flow Logs as a primary or supplementary data source for entity modeling. This means you can now monitor network activity in a cloud environment and increase your security.
upvoted 2 times

Rhoads 1 year, 8 months ago
Selected Answer: D
Using the cloud provider..
upvoted 2 times

sis_net_sec 2 years, 1 month ago
Selected Answer: D
Stealthwatch Cloud can be deployed without software agents, relying on the native AWS Virtual Private Cloud (VPC) flow logs.
<https://aws.amazon.com/marketplace/pp/prodview-woiawecmdlezq>
upvoted 3 times

semi1750 2 years, 4 months ago
D - VPC flow logs is answer

The question asks "public cloud" and cisco made the following explanation.

Cisco Telemetry Broker

The Cisco Telemetry Broker is capable of ingesting network telemetry from a variety of telemetry sources, transforming their data formats, and then forwarding that telemetry to one or multiple destinations. For example, it can ingest any of the following:



- On-premises network telemetry, including NetFlow, SYSLOG, and IPFIX
- Cloud-based telemetry sources, such as AWS VPC flow logs and Azure NSG flow logs

And it can forward that telemetry to any or all of the following example destinations:

- Analytics platforms, such as Hadoop
- Network management and automation platforms, such as Cisco DNA Center
- Security Information and Event Management (SIEM) platforms
- Storage/smart capture, such as Cisco Security Analytics and Logging (On-premises)

<https://www.cisco.com/c/en/us/products/collateral/security/stealthwatch/datasheet-c78-739398.html>

upvoted 3 times



  **brownbear505** 2 years, 6 months ago

Selected Answer: D

Specifically, AWS VPC Flow Logs contain the following information:



- Which IP entities are communicating inside and outside the VPC
- Which protocols (such as TCP and UDP) are being used
- How much traffic is sent and received by each entity
- Whether the flow was allowed or blocked by the security policy

upvoted 3 times

  **psuoh** 1 year, 7 months ago

<https://www.cisco.com/c/en/us/products/collateral/security/stealthwatch-cloud/at-a-glance-c45-739851.html>

upvoted 1 times

  **Minion2021** 2 years, 6 months ago

Correct answer is D

upvoted 2 times

  **dr4gn00t** 2 years, 7 months ago

This is a tricky question. VPC is valid option only for AWS (Azure and Google uses different terms), and AWS doesn't send telemetry to Stealthwatch. Stealthwatch fetch logs from AWS via API. I think B is therefore most valid answer.

upvoted 4 times

  **neta1o** 2 years, 7 months ago

Looks like this solution supports Azure and AWS. Based on the docs for Azure setup it doesn't look like they refer to the logs as VPC Flow Logs (AWS). So based on that I'd stick with B. <https://www.cisco.com/c/en/us/support/security/stealthwatch-cloud/products-installation-guides-list.html#pcm>

upvoted 3 times

  **VI_Vershinin** 3 years, 1 month ago

It's B

From the book SCOR 350-701:

Stealthwatch Cloud is a Software as a Service (SaaS) cloud solution. You can use Stealthwatch Cloud to monitor many different public cloud environments, such as Amazon's AWS, Google Cloud Platform, and Microsoft Azure. All of these cloud providers support their own implementation of NetFlow:



■ ■ In Amazon AWS, the equivalent of NetFlow is called VPC Flow Logs. You can obtain detailed information about VPC Flow Logs in AWS at <https://docs.aws.amazon.com/vpc/latest/userguide/flow-logs.html>.

■ ■ Google Cloud Platform also supports VPC Flow Logs (or Google-branded GPC Flow Logs). You can obtain detailed information about VPC Flow Logs in Google Cloud Platform at <https://cloud.google.com/vpc/docs/using-flow-logs>.

■ ■ In Microsoft's Azure, traffic flows are collected in Network Security Group (NSG) flow logs. NSG flow logs are a feature of Network Watcher. You can obtain additional information about Azure's NSG flow logs and Network Watcher at <https://docs.microsoft.com/en-us/azure/network-watcher/network-watcher-nsg-flow-logging-overview>

com/en-us/azure/network-watcher/network-watcher-nsg-flow-logging-overview

upvoted 4 times

  **Dinges** 3 years, 2 months ago

Its D



<https://aws.amazon.com/marketplace/pp/prodview-woiawecmdlezq>

upvoted 3 times

  **SirFrates24** 3 years, 2 months ago


Not seeing anything related to PUBLIC CLOUD and vpc

upvoted 1 times

  **Stardec** 2 years, 10 months ago

<https://www.cisco.com/c/en/us/products/collateral/security/stealthwatch-cloud/at-a-glance-c45-739850.html>

upvoted 1 times

  **yenp** 3 years, 2 months ago


correct answer is b : In AWS environments, Cisco Stealthwatch Cloud can be deployed without software agents, relying on the native AWS Virtual Private Cloud (VPC) flow logs. Deployment can be accomplished in minutes by simply giving Cisco Stealthwatch Cloud read-only access to these VPC flow logs. In addition to VPC flows logs, other AWS telemetry data can also be used. GCP also uses VPC flow logs for rapid deployment and integration. Currently for Microsoft Azure environments, Cisco Stealthwatch Cloud relies first on a Linux-based software appliance, called the Observable Networks Appliance (ONA), and second on a third-party host-based NetFlow exporter such as Ziften or FlowTraq.

upvoted 2 times

  **Maleck** 3 years, 2 months ago

You mean Correct answer is D from your explanation

upvoted 3 times

  **wfexco** 3 years, 3 months ago

Answer is D - Stealthwatch Cloud can be deployed without software agents, relying on the native AWS Virtual Private Cloud (VPC) flow logs
upvoted 4 times

  **statikd** 3 years, 2 months ago

How is it VPC flow logs when this question is an organization's public cloud, not a private cloud?
upvoted 1 times

  **itisfakemaiol** 3 years, 2 months ago

VPC flow logs are the feature of the public clouds, like AWS
upvoted 2 times

Question #91

Topic 1

An engineer is trying to securely connect to a router and wants to prevent insecure algorithms from being used. However, the connection is failing. Which action should be taken to accomplish this goal?

- A. Generate the RSA key using the crypto key generate rsa command.
- B. Configure the port using the ip ssh port 22 command.
- C. Enable the SSH server using the ip ssh server command.
- D. Disable telnet using the no ip telnet command.

Correct Answer: A



Community vote distribution

A (100%)

  **Marshpillowz** 5 months, 1 week ago

Selected Answer: A

A is correct
upvoted 1 times

  **OZ1** 1 year, 2 months ago

Selected Answer: A

Generate the RSA key using the crypto key generate rsa command.
upvoted 1 times

  **gondohwe** 1 year, 3 months ago

scenario: enabling ssh, setting ssh version to 2 and configuring vty lines to support only ssh connections
(config)#hostname FUNTECH-ROUTER
#ip domain name FUNTECH.com
#crypto key generate rsa (choose key length of your choice after entering this command)
#ip ssh version 2
#line vty 0 4
#transport input ssh
#password cisco
#exit
...of all the provided answers A would make sense
upvoted 3 times

```

Info: New SMTP ICID 30 interface Management (192.168.0.100)
      address 10.128.128.200 reverse dns host unknown verified no
Info: ICID 30 ACCEPT SG SUSPECTLIST match sbrs[none] SBRS None
Info: ICID 30 TLS success protocol TLSv1 cipher
      DHE-RSA-AES256-SHA
Info: SMTP Auth: (ICID 30) succeeded for user: cisco using
      AUTH mechanism: LOGIN with profile: ldap_smtp
Info: MID 80 matched all recipients for per-recipient policy
      DEFAULT in the outbound table

```

Refer to the exhibit. Which type of authentication is in use?

- A. POP3 authentication
- B. SMTP relay server authentication
- C. external user and relay mail authentication
- D. LDAP authentication for Microsoft Outlook

Correct Answer: D

Community vote distribution

D (50%) B (36%) 14%

jaciro11 Highly Voted 2 years, 10 months ago

Okay okay TEAM

We will clarify the image:

LDAP AUTH Its is true is the action committed for External user and relay mail auth.

And the question ask Told "Which Type of authentication is in use "

D is the answer

<https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118545-technote-esa-00.html>

This document describes how to configure LDAP SMTPAUTH to authenticate external users and relay mail.

;)

upvoted 12 times

naipoom Highly Voted 2 years, 5 months ago

C

<https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118545-technote-esa-00.html>

upvoted 6 times

Marshpillowz Most Recent 5 months, 1 week ago

Selected Answer: D

I think D

upvoted 1 times

LTLnetworker 8 months ago

Selected Answer: D

<https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118545-technote-esa-00.html>

upvoted 2 times

Stevens0103 8 months, 1 week ago

Selected Answer: D

C is the object to be authenticated, not a type of authentication.

"Configure LDAP SMTPAUTH To Authenticate External Users and Relay Mail"

<https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118545-technote-esa-00.html>

upvoted 3 times

petestudies 9 months ago

Selected Answer: C

C. external user and relay mail authentication

<https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118545-technote-esa-00.html>

Wed Sep 12 07:59:41 2007 Info: SMTP Auth: (ICID 36) succeeded for user: jsmith using
AUTH mechanism: LOGIN with profile: ldap_smtp

upvoted 1 times

  **xziomal9** 10 months, 2 weeks ago

Answer B

upvoted 1 times

  **fdl543** 1 year, 1 month ago

Selected Answer: B

B is correct. The problem with D is "for Microsoft Outlook" because LDAP does not restrict to Microsoft Outlook only...

upvoted 1 times

  **jku2cya** 1 year, 2 months ago

Selected Answer: D

jaciro11 has the correct Troubleshooting Technote to reference link.

It also has similar example logs, without the timestamps and it misses the "<<<SNIP FOR BREVITY>>>".

upvoted 1 times

  **littlewilly** 1 year, 3 months ago

Selected Answer: C

Answer is C- this has nothing to do with outlook

upvoted 1 times

  **Carlis** 1 year, 5 months ago

Selected Answer: B

SMTP Authentication using LDAP as Profile Type has been configured on Cisco ESA.

Another tricky Cisco question, where the correct answer is what cisco wants to see.



It authenticates External users and Relay Mail, using LDAP profile type as authentication mechanism for SMTP Authentication (as stated in the log).

Info: SMTP Auth: (ICID 30) succeeded for user: cisco using AUTH mechanism: LOGIN with profile: ldap_smtp

For me the correct answer is B.

<https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118545-technote-esa-00.html>

upvoted 4 times

  **sull3y** 1 year, 7 months ago

D. LDAP authentication for Microsoft Outlook

The exhibit refers to "AUTH Mechanism:LOGIN with profile: ldap_smtp", which indicates that the authentication mechanism in use is LDAP (Lightweight Directory Access Protocol) and the profile used is "ldap_smtp". This means that users are being authenticated against an LDAP directory before they are allowed to send mail via SMTP, which is typically used for Microsoft Outlook.

upvoted 3 times

  **edu_web** 1 year, 10 months ago

Why not B?



<https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118570-qa-esa-00.html>

upvoted 2 times

  **smartcarter** 2 years, 1 month ago



C is not a kind of authentication supported by the ESA. D is the answer as clearly shown in log.

upvoted 1 times

  **zheka** 2 years, 9 months ago

So, why do you say it is D if C clearly says "External user and relay mail authentication" and the document you are referring to has exactly the same title? Moreover, it says about Outlook Express not Microsoft Outlook.

upvoted 2 times

  **eazy99** 2 years, 11 months ago

I believe the answer is D.

The question says what type of Authentication used, not for who.

So we used LDAP authentication for the external users (answer C).

Personally I would go with the Answer D.

upvoted 5 times

  **zeroC00L** 3 years ago

i would go with C here because if you put "external user and relay mail authentication" into google you find a cisco document about the ESA where there example CLI output looks pretty much the same as in the question -> <https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118545-technote-esa-00.html>

upvoted 4 times

```
ip dhcp snooping
ip dhcp snooping vlan 41,44
!
interface GigabitEthernet1/0/1
description Uplink_To_Distro_Switch_g1/0/11
switchport trunk native vlan 999
switchport trunk allowed vlan 40,41,44
switchport mode trunk
```

Refer to the exhibit. An organization is using DHCP Snooping within their network. A user on VLAN 41 on a new switch is complaining that an IP address is not being obtained. Which command should be configured on the switch interface in order to provide the user with network connectivity?

- A. ip dhcp snooping limit 41
- B. ip dhcp snooping verify mac-address
- C. ip dhcp snooping trust
- D. ip dhcp snooping vlan 41

Correct Answer: C

Community vote distribution

C (100%)

zheka Highly Voted 2 years, 9 months ago

Even though the correct answer is C the entire question and especially exhibit is stupid. We do not know where the DHCP server is. It could be on the same switch or the other switch reachable via the shown interface. If it is on the same switch then adding "ip dhcp snooping trust" on port 41 won't help because it needs added on the port where DHCP server is connected.

An untrusted port is a port that does not accept DHCP server messages. In other words, if a device is connected to an untrusted port, it can obtain IP configuration from the DHCP server but it cannot offer an IP configuration.

A trusted port is a port that accepts DHCP server messages. In other words, a DHCP server can provide IP configuration only if it is connected to a trusted port.

upvoted 16 times

asd123123iu 2 years, 3 months ago

I add that command from D is already visible in configuration and answer A i think is incorrect so B and C left. C work like zheka described so theoretically should resolve problem. B I'm not sure if it has any impact for clients, it's just security feature.

upvoted 1 times

psuoh 1 year, 7 months ago

perhaps it is using IP DHCP RELAY command...

upvoted 1 times

Wdgbill Highly Voted 2 years, 1 month ago

note here that the config is for the trunk port to a distribution switch and switch to switch ports need to be set to trusted. No detailed information but the possibility exists that the DHCP server is on another switch so without the trunk between switches being trusted no DHCP offers would transit the link

upvoted 5 times

Marshpillowz Most Recent 5 months, 1 week ago

Selected Answer: C

C is correct

upvoted 1 times


```

> show crypto ipsec sa
interface: Outside
  Crypto map tag: CSM_Outside_map, seq num: 1, local addr:
  209.165.200.225

  access-list CSM_IPSEC_ACL_1 extended permit ip 10.0.11.0
  255.255.255.0 10.0.10.0 255.255.255.0
  local ident (addr/mask/prot/port) : (10.0.11.0/255.255.255.0/0/0)
  remote ident (addr/mask/prot/port) : (10.0.10.0/255.255.255.0/0/0)
  current_peer: 209.165.202.129

  #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
  #pkts decaps: 17, #pkts decrypt : 17, #pkts verify: 17
  #pkts compressed: 0, #pkts decompressed: 0
  #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp
  failed: 0
  #pre-frag successes: 0, #pre-frag failures: 0, #fragments
  created : 0
  #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing
  reassembly: 0
  #TFC rcvd: 0, #TFC sent: 0
  #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
  #send errors: 0, #recv errors: 0

  local crypto endpt.: 209.165.200.225/500, remote crypto endpt.:
  209.165.202.129/500
  path mtu 1500, ipsec overhead 55(36), media mtu 1500
  PMTU time remaining (sec): 0, DF policy: copy-df
  ICMP error validation: disabled, TFC packets: disabled
  current outbound spi : B6F5EA53
  current inbound spi : 84348DEE

```

Refer to the exhibit. Traffic is not passing through IPsec site-to-site VPN on the Firepower Threat Defense appliance. What is causing this issue?

- A. Site-to-site VPN preshared keys are mismatched.
- B. Site-to-site VPN peers are using different encryption algorithms.
- C. No split-tunnel policy is defined on the Firepower Threat Defense appliance.
- D. The access control policy is not allowing VPN traffic in.

Correct Answer: D

Community vote distribution

D (100%)

kerniger Highly Voted 3 years ago

A - vpn is established
 B - vpn is established
 C - Split Tunneling has nothing to do with a site-to-site VPN.
 D - we see traffic is coming in but no traffic is going into the tunnel so its likely a access policy wrong or missing
 upvoted 27 times

zap_pap Highly Voted 3 years, 1 month ago



A & B are ruled out by #pkts encaps #pkts decaps: traffic is flowing based on these lines, so the VPN is established.
 #pkts decaps: 17 - we are getting traffic in, so it is not blocked by the ACL.
 Only C is left.
 upvoted 11 times

jmosilva 3 years, 1 month ago

Perfect explanation! I agree with C
 upvoted 3 times

gondohwe 1 year, 3 months ago

no no my friend...split-tunneling doesnt prevent vpns from operating but define what traffic should use the vpn tunnel and what traffic shouldnt so forget C...on FTD devices access policies shld also properly permit traffic provide vpn has been configured proper way...D sounds better
 upvoted 2 times

  **gondohwe** 1 year, 3 months ago
split-tunneling is never heard of in site 2 site vpns
upvoted 2 times

  **Rockbo47** Most Recent 1 month ago

Selected Answer: D

As others have pointed out also, the correct answer can only be D for the reasons provided by others however there MUST be a typo in D because traffic is being successfully received as indicated by the decaps and decrypt packets. So the actual correct answer would be "The access control policy is not allowing VPN traffic OUT."

upvoted 1 times

  **Marshpillowz** 5 months, 1 week ago

Selected Answer: D

D is correct



upvoted 1 times

  **Alizade** 11 months, 2 weeks ago

Selected Answer: D



D. The access control policy is not allowing VPN traffic in.

upvoted 2 times

  **intirt** 1 year, 9 months ago

D is correct

upvoted 2 times

  **ureis** 1 year, 11 months ago

crypto map is not matching with ALC, so D is correct

upvoted 2 times

  **getafix** 2 years, 3 months ago

Selected Answer: D

A - cannot be true since the tunnel is established as we can see pkts decrypted and pkts encrypted --> zero

B: Same as above, tunnel is up so Phase1 and Phase2 are both up and interesting traffic is passing

C: Split tunneling works for remote access VPNs. It defines what traffic, when a user connects to a remote access VPN server, should go inside the VPN and what traffic should go out via his local home router.

D: Since there are no encapsulations happening encaps:0bytes.....it evidently shows a problem with the access list


upvoted 7 times

  **somaao** 2 years, 5 months ago

Selected Answer: D



pkts encap are 0 , so D

upvoted 4 times

  **killbots** 2 years, 5 months ago

I say its D. Split-Tunneling is only relevant to Remote Access VPNs not S2S. only one that makes sense is D.

upvoted 3 times

  **zheka** 2 years, 9 months ago

Maybe it is another example of the stupid question/exhibit or a tricky one.

If VPN is established and especially Phase 2 with all security associations created then two firewall peers negotiated everything which is matching.

Of course nothing to do with split-tunneling on the site-to-site tunnel. The only explanation for this asymmetry of counters for packets entering the tunnel and exiting is either missing NAT exemption rules or indeed access control policy rule which should be configured only if we stopped trusting the traffic that exits the tunnel (former sysopt connection permit-vpn)

upvoted 1 times

  **zeroCOOL** 3 years ago

i would go with D and hoping this is just a typo (and it meant actually "out") because it seems to be the "less" wrong answer.

C makes no sense from both wording and technically. If you do something wrong according to what to send into the tunnel it would either not come up at all or would throw errors about "proxy identity mismatch" (we dont have debugs so this cant be validated)

upvoted 6 times

  **Sarbi** 3 years ago

I agreed with C and VPN tunnel is established only traffic is not passing.

upvoted 1 times

  **Narcolepto** 3 years, 2 months ago

I think the answer is D because if you look carefully at the access-list it is incorrectly formatted. There is an extra period between the mask of the source and the ip of the destination instead of a space - 255.255.255.0.10.0.10.0 instead of 255.255.255.0 10.0.10.0


upvoted 2 times

  **Dead_Adriano** 3 years, 2 months ago



This might me just a typo.

In the next lines of the output, traffic selectors (local and remote idents) are parsed correctly.

upvoted 1 times

  **Raajaa** 3 years, 2 months ago

D is the answer
upvoted 1 times

  **Barish** 3 years, 4 months ago

Answer D is correct
upvoted 2 times

  **Minipaf** 3 years, 4 months ago

Hello, can anyone explain this answer ? I find that answer D makes more sense. thanks!
upvoted 1 times

  **cciewannab** 2 years, 12 months ago

A and B are incorrect because we can see the tunnel is up. We know it is up because we have 17 decap packets. This means traffic is coming from the peer to the ASA and it decrypts and sends it according to the routing table. C is incorrect because that is related to remote-access VPNs, not S2S VPNs. Since we have no encaps - which is traffic entering the ASA, being encrypted, and sent out the tunnel - this likely means the ASA has an inbound access-list on the 'inside' or whatever interface not allowing the interesting traffic in. So the traffic blocked entering into the ASA never giving it an option to be encrypted. D is therefore the answer.
upvoted 6 times


```

*Jun 30 16:52:33.287: ISAKMP: (1002) : retransmitting phase 1 MM_KEY_ECH...
*Jun 30 16:52:33.287: ISAKMP: (1002) : incrementing error counter on sa, attempt 4
of 5: retransmit phase 1
*Jun 30 16:52:33.287: ISAKMP: (1002) : retransmitting phase 1 MM_KEY_EXCH
*Jun 30 16:52:33.287: ISAKMP: (1002) : sending packet to 10.10.12.2 my_port 500
peer_port 500 (I) MM_KEY_EXCH
*Jun 30 16:52:33.291: ISAKMP: (1002) : Sending an IKE IPv4 Packet.
*Jun 30 16:52:33.791: ISAKMP: (1002) : received packet from 10.10.12.2 dport 500
sport 500 Global (I) MM_KEY_EXCH
*Jun 30 16:52:33.795: ISAKMP: (1002) : phase 1 packet is a duplicate of a previous
packet
R1#
*Jun 30 16:52:33.795: ISAKMP: (1002) : retransmission skipped for phase 1 (time
since last transmission 504)
R1#
*Jun 30 16:52:40.183: ISAKMP: (1001) : purging SA., SA=68CEE058, delme=68CEE058
R1#
*Jun 30 16:52:43.291: ISAKMP: (1002) : retransmitting phase 1 MM_KEY_EXCH...
*Jun 30 16:52:43.291: ISAKMP: (1002) : incrementing error counter on sa, attempt 5
of 5: retransmit phase 1
*Jun 30 16:52:43.295: ISAKMP: (1002) : retransmitting phase 1 MM_KEY_EXCH
*Jun 30 16:52:43.295: ISAKMP: (1002) : sending packet to 10.10.12.2 my_port 500
peer_port 500 (I) MM_KEY_EXCH
*Jun 30 16:52:43.295: ISAKMP: (1002) :Sending an IKE IPv4 Packet.
R1#
*Jun 30 16:52:53.299: ISAKMP: (1002) : retransmitting phase 1 MM_KEY_EXCH...
*Jun 30 16:52:53.291: ISAKMP: (1002) :peer does not do paranoid keepalives.

*Jun 30 16:52:53.299: ISAKMP: (1002) :deleting SA reason "Death by retransmission
P1" state (I) MM_KEY_EXCH (peer 10.10.12.2)
*Jun 30 16:52:53.303: ISAKMP: (1002) :deleting SA reason "Death by retransmission
P1" state (I) MM_KEY_EXCH (peer 10.10.12.2)
*Jun 30 16:52:53.307: ISAKMP: Unlocking peer struct 0x68287318 for
isadb_mark_sa_deleted {}, count 0
*Jun 30 16:52:53.307: ISAKMP: Deleting peer node by peer_reap for 10.10.12.2:
68287318
*Jun 30 16:52:53.311: ISAKMP: (1002) :deleting node 79875537 error FALSE reason "IKE
deleted"
R1#
*Jun 30 16:52:53.311: ISAKMP: (1002) :deleting node -484575753 error FALSE reason
"IKE deleted"
*Jun 30 16:52:53.315: ISAKMP: (1002) :Input = IKE_MSG_INTERNAL, IKE_PHASE1_DEL
*Jun 30 16:52:53.319: ISAKMP: (1002) :Old State = IKE_I_M5 New State = IKE_DEST_SA

```

Refer to the exhibit. A network administrator configured a site-to-site VPN tunnel between two Cisco IOS routers, and hosts are unable to communicate between two sites of VPN. The network administrator runs the debug crypto isakmp sa command to track VPN status. What is the problem according to this command output?

- A. interesting traffic was not applied
- B. encryption algorithm mismatch
- C. authentication key mismatch
- D. hashing algorithm mismatch

Correct Answer: C

Community vote distribution

C (77%)

B (23%)

dr4gn00t Highly Voted 2 years, 7 months ago

Selected Answer: C

Googling for MM_KEY_EXCH retransmission seems to indicate mismatch between shared secret
upvoted 19 times

denverfly Highly Voted 2 years, 7 months ago

Answer:C

<https://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/5409-ipsec-debug-00.html>

n the show crypto isakmp sa output, the state should always be QM_IDLE. If the state is MM_KEY_EXCH, it means either the configured pre-shared key is not correct or the peer IP addresses are different.

upvoted 13 times

CyberSecurity80 2 years, 6 months ago

I agree with this. Even though the command is "show crypto isakmp sa" not "debug crypto isakmp sa command" but same idea
upvoted 1 times

  **Premium_Pils** Most Recent 1 month ago

Selected Answer: C

based on below explanation for MM_KEY_EXCH retransmission
upvoted 1 times



  **Marshpillowz** 5 months, 1 week ago

Selected Answer: C

C is correct
upvoted 1 times

  **JavierAcuna** 1 year, 4 months ago

C MM_KEY_EXCH ANswer is C
upvoted 2 times

  **Carlis** 1 year, 5 months ago

MM_KEY_EXCH indicates key exchange mismatch
MM_NO_STATE would indicate isakmp policy mismatch (e.g. encryption)
upvoted 3 times

  **iratus_umbra** 1 year, 5 months ago

Selected Answer: C

100% C is correct.
upvoted 1 times

  **Vlad_Is_Love_ua** 1 year, 6 months ago

Selected Answer: C


C is CORRECT, because MM_KEY_EXCH = MisMatch Key Exchange
upvoted 2 times

  **Stevens0103** 8 months, 1 week ago



MM_KEY_EXCH = Main Mode Key Exchange
upvoted 1 times

  **ddev3737** 1 year, 7 months ago

C because B would right but paranoid keepalives message only occurs after MM_KEY_EXC error message
upvoted 2 times

  **Stevens0103** 8 months, 1 week ago

Keepalives are messages exchanged between the peers to ensure that the VPN tunnel is still alive and functioning. The "paranoid keepalives" message suggests that the peer (10.10.12.2) does not support or engage in the paranoid keepalives mechanism. The "MM_KEY_EXCH" messages, on the other hand, specifically refer to Main Mode Key Exchange during IKE negotiation. These messages are part of the process of establishing a secure communication channel between the VPN peers. They are distinct aspects of the overall VPN establishment process.
upvoted 1 times



  **psuoh** 1 year, 7 months ago

More likely mismatched authentication key issue...
<https://www.networkworld.com/article/2288666/chapter-4--common-ipsec-vpn-issues.html?page=3>
upvoted 1 times

  **Emlia1** 1 year, 9 months ago

Selected Answer: C

It's C
upvoted 2 times

  **Hereim** 1 year, 11 months ago

It should be B - since the error message states "peer does not do paranoid keepalives" meaning PFS is tuned on at one end and off on the other end. If it was key mismatch we should see that in the debug.
upvoted 1 times

  **SulSulEi** 2 years ago

Selected Answer: C



Answet is C, please check below,
<https://www.google.com/amp/s/www.networkworld.com/article/2288666/chapter-4--common-ipsec-vpn-issues.amp.html>
upvoted 2 times

  **surforlife** 2 years, 1 month ago

all over the retry MM_KEY_EXCH, it means Mismatch Key Exchange!
"C" is correct
upvoted 2 times



  **west33637** 1 year, 9 months ago

thats main mode key exchange. not mismatch
upvoted 1 times

  **Bezos** 2 years, 2 months ago

Selected Answer: C

C is the answer <https://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/5409-ipsec-debug-00.html>
upvoted 3 times

  **getafix** 2 years, 3 months ago

Selected Answer: B

Debugging isakmp logs show the actual message of key mismatch if there is a key mismatch. The exhibit in the question does not show the "key mismatch" message.

The resulting logs would be due to a proposal mismatch

upvoted 2 times

  **Sattm1** 2 years, 4 months ago

Selected Answer: C

B and D show specific items that could be wrong - but we don't know which (or it could be mismatched secrets/auth methods).

Here's a very basic ISAKMP config:

C is the generic key mismatch - aka ISAKMP has failed- and that's all we see in the logs

```
R3(config)# crypto isakmp policy 10
R3(config-isakmp)# authentication pre-share
R3(config-isakmp)# encryption 3des
R3(config-isakmp)# hash sha
R3(config-isakmp)# group 2
```

upvoted 2 times

Which policy represents a shared set of features or parameters that define the aspects of a managed device that are likely to be similar to other managed devices in a deployment?

- A. group policy
- B. access control policy
- C. device management policy
- D. platform settings policy

Correct Answer: D

Reference:



https://www.cisco.com/c/en/us/td/docs/security/firepower/622/configuration/guide/fpmc-config-guide-v622/platform_settings_policies_for_managed_devices.pdf

Community vote distribution

D (100%)

  **Vic25H** Highly Voted  4 years, 2 months ago

It's platform SETTINGS policy
upvoted 10 times



  **Seawanderer** 3 years, 2 months ago

close enough :-)
upvoted 2 times

  **Marshpillowz** Most Recent  5 months, 1 week ago

Selected Answer: D

D is correct
upvoted 1 times

  **sull3y** 1 year, 7 months ago

D:https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Platform_Settings_Policies_for_Managed_Devices.pdf
upvoted 3 times

The Cisco ASA must support TLS proxy for encrypted Cisco Unified Communications traffic.
Where must the ASA be added on the Cisco UC Manager platform?

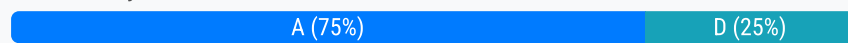
- A. Certificate Trust List
- B. Endpoint Trust List
- C. Enterprise Proxy Service
- D. Secured Collaboration Proxy

Correct Answer: A

Reference:

<https://www.cisco.com/c/en/us/td/docs/security/asa/special/unified-communications/guide/unified-comm/unified-comm-tlsproxy.html>

Community vote distribution



— **surforlife** Highly Voted 2 years, 2 months ago

"A" is correct.

The security appliance acts as a TLS proxy between the Cisco IP Phone and Cisco UCM. The proxy is transparent for the voice calls between the phone and the Cisco UCM. Cisco IP Phones download a Certificate Trust List from the Cisco UCM before registration which contains identities (certificates) of the devices that the phone should trust, such as TFTP servers and Cisco UCM servers. To support server proxy, the CTL file must contain the certificate that the security appliance creates for the Cisco UCMS.

upvoted 5 times

— **red_sparrow_Gr** Highly Voted 10 months, 2 weeks ago

Selected Answer: A

Incorporating the Firewall into the Unified Communications System

Configuring the ASA is not enough to fully incorporate the firewall into the Cisco Unified Communications system. You must also add the ASA to the Certificate Trust List (CTL) using the Cisco Certificate Trust List Client, which is part of the Unified Communications Manager.

<https://www.cisco.com/c/en/us/td/docs/security/asa/special/unified-communications/unified-communications-guide/tls-proxy-for-encrypted-voice-inspection.html?bookSearch=true>

upvoted 5 times

— **Marshpillowz** Most Recent 5 months, 1 week ago

Selected Answer: A

I think A

upvoted 1 times

— **Alizade** 11 months, 2 weeks ago

Selected Answer: D

The ASA must be added to the Cisco UC Manager platform as the Secured Collaboration Proxy.

upvoted 2 times

— **DWizard** 1 year, 2 months ago

This question is horrible. It is about where to put the certificate or is it about the option in the menu in the CUCM to configure the TLS proxy or anything else?

upvoted 1 times

Which two application layer preprocessors are used by Firepower Next Generation Intrusion Prevention System? (Choose two.)

- A. SIP
- B. inline normalization
- C. SSL
- D. packet decoder
- E. modbus


Correct Answer: AC


Reference:


https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Application_Layer_Preprocessors.html


Community vote distribution

AC (100%)

- [-]  **[Removed]** Highly Voted 2 years, 11 months ago

A&C
https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Application_Layer_Preprocessors.html
upvoted 9 times
- [-]  **Marshpillowz** Most Recent 5 months, 1 week ago

Selected Answer: AC
A and C are correct
upvoted 1 times
- [-]  **roolmereyes** 1 year, 1 month ago

These are all available preprocessors:
The DCE/RPC Preprocessor
The DNS Preprocessor
The FTP/Telnet Decoder
The HTTP Inspect Preprocessor
The Sun RPC Preprocessor
The SIP Preprocessor
The GTP Preprocessor
The IMAP Preprocessor
The POP Preprocessor
The SMTP Preprocessor
The SSH Preprocessor
The SSL Preprocessor
upvoted 1 times
- [-]  **sull3y** 1 year, 7 months ago

A. SIP
C. SSL

SIP (Session Initiation Protocol) Preprocessor and SSL (Secure Sockets Layer) Preprocessor are two of the application layer preprocessors that are used by Firepower Next Generation Intrusion Prevention System (NGIPS). SIP preprocessor inspects and analyzes SIP traffic, and SSL preprocessor inspects and analyzes SSL traffic. These preprocessors work in conjunction with the overall NGIPS system to provide a comprehensive security solution for protecting networks from a variety of attacks.
upvoted 4 times

Which feature is configured for managed devices in the device platform settings of the Firepower Management Center?

- A. quality of service
- B. time synchronization
- C. network address translations
- D. intrusion policy

Correct Answer: B

Community vote distribution

B (100%)

  **crh23** Highly Voted  4 years, 1 month ago

Correct B

Synchronizing Time on Classic Devices

https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Firepower_Software_Platform_Settings.html#task_EF18AE3D5CA9457AB65791B9654FD46C

upvoted 6 times

  **Marshpillowz** Most Recent 5 months, 1 week ago

Selected Answer: B

B is correct

upvoted 1 times

Which information is required when adding a device to Firepower Management Center?

- A. username and password
- B. encryption method
- C. device serial number
- D. registration key

Correct Answer: D

Reference:

https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Device_Management_Basics.html#ID-2242-0000069d

Community vote distribution

D (100%)

  **pfunkylol** Highly Voted  2 years, 9 months ago

correct.



upvoted 7 times

  **Marshpillowz** Most Recent  5 months, 1 week ago

Selected Answer: D

D is correct

upvoted 1 times

  **gc999** 1 year, 5 months ago

Selected Answer: D

https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Device_Management_Basics.html
Please refer to the procedure Step 5 when adding devices to the FMC.

upvoted 4 times

  **Toni_Su91** 1 year, 6 months ago

> configure manager add [IP address] [KEY]

upvoted 3 times

What can be integrated with Cisco Threat Intelligence Director to provide information about security threats, which allows the SOC to proactively automate responses to those threats?

- A. Cisco Umbrella
- B. External Threat Feeds
- C. Cisco Threat Grid
- D. Cisco Stealthwatch

Correct Answer: B

Community vote distribution

B (100%)

— **CiscoTech** **Highly Voted** 4 years, 2 months ago

I think the answer is B.

<https://www.cisco.com/c/en/us/support/docs/storage-networking/security/214859-configure-and-troubleshoot-cisco-threat.html>

upvoted 18 times

— **brownbear505** **Highly Voted** 2 years, 6 months ago

Selected Answer: B

https://www.cisco.com/c/en/us/td/docs/security/firepower/623/configuration/guide/fpmc-config-guide-v623/cisco_threat_intelligence_director_tid.html

upvoted 5 times

— **Marshpillowz** **Most Recent** 5 months, 1 week ago

Selected Answer: B

B is correct

upvoted 1 times

— **Sun2sun** 2 years, 7 months ago

Selected Answer: B

should be B

upvoted 2 times

— **pr0fectus** 2 years, 8 months ago

TID is used to leverage external threat feeds. ThreatGrid is already integrated with the AMP capability of FTD.

upvoted 1 times

— **Moll** 2 years, 10 months ago

Answer should be B

<https://www.ciscolive.com/c/dam/r/ciscolive/emea/docs/2020/pdf/BRKDEV-2456.pdf>

Page 28

Cisco Threat Intelligence Director (TID)

Step 1

Ingest third-party Cyber Threat Intelligence (CTI)

Step 2

Publish observables to sensors

Step 3

Detect and alert on incidents

upvoted 3 times

— **Moll** 2 years, 10 months ago

Answer should be B

<https://blogs.cisco.com/developer/automate-threat-intelligence-using-cisco-threat-intelligence-director>

upvoted 3 times

— **zeroC00L** 2 years, 11 months ago



i would go with B here. Because the TID is used if you want to use external (not cisco provided) Security Information / Observables, in addition to what you get from cisco ->

"The Cisco Threat Intelligence Director (TID) operationalizes threat intelligence data, helping you aggregate intelligence data, configure defensive actions, and analyze threats in your environment. This feature is intended to supplement other Firepower functionality, offering an additional line of defense against threats"

https://www.cisco.com/c/en/us/td/docs/security/firepower/623/configuration/guide/fpmc-config-guide-v623/cisco_threat_intelligence_director_tid.html

and for AMP you dont need the TID. AMP(for Networks) comes with its own configuration o the FMC for example where you can define the cloud you want to use etc.

upvoted 2 times

  **Sarbi** 3 years ago


It looks to me C.As it the cisco exam.Cisco treat grid

upvoted 2 times

  **andrewj511** 3 years ago



"Secure Malware Analytics (formerly Threat Grid) combines advanced sandboxing with threat intelligence into one unified solution to protect organizations from malware."

upvoted 2 times

  **Raajaa** 3 years, 2 months ago

B sounds correct to me

upvoted 2 times

  **Kris92** 3 years, 6 months ago

I went with C at first, but B makes more sense.

External threat feed is a option on ESA, but I don't see any example of using TID.

TID is usually added to FP in intelligence sources.

upvoted 1 times

  **user636** 3 years, 8 months ago

The answer is B, there no possibility to integrate ThreatGrid with TID at all. You could check the administration guide of TID.

upvoted 5 times

  **JAckThePip** 3 years, 9 months ago

The answer is B:

[https://www.cisco.com/c/en/us/td/docs/security/esa/esa12-](https://www.cisco.com/c/en/us/td/docs/security/esa/esa12-0/user_guide/b_ESA_Admin_Guide_12_0/b_ESA_Admin_Guide_12_0_chapter_0110001.html)

[0/user_guide/b_ESA_Admin_Guide_12_0/b_ESA_Admin_Guide_12_0_chapter_0110001.html](https://www.cisco.com/c/en/us/td/docs/security/esa/esa12-0/user_guide/b_ESA_Admin_Guide_12_0/b_ESA_Admin_Guide_12_0_chapter_0110001.html)

upvoted 2 times



  **myccnptest** 3 years, 9 months ago

Looks like it might be "B"

https://www.cisco.com/c/en/us/td/docs/security/firepower/623/configuration/guide/fpmc-config-guide-v623/cisco_threat_intelligence_director__tid_.html

Feature introduced: Lets you use threat intelligence from external sources to identify and process threats.

upvoted 4 times

  **avl83** 4 years, 1 month ago

the answer is C. More information take a look in, chapter 11, page 654, book "ccnp and ccie security Core"

upvoted 2 times

  **essie007** 3 years, 11 months ago

The question is about the TID, not CTR. Correct answer is BB

upvoted 6 times

Which Cisco command enables authentication, authorization, and accounting globally so that CoA is supported on the device?

- A. aaa server radius dynamic-author
- B. auth-type all
- C. aaa new-model
- D. ip device-tracking

Correct Answer: A

Community vote distribution

C (68%) A (32%)

Ampersand Highly Voted 3 years, 5 months ago

aaa new-model
Enables authentication, authorization, and accounting (AAA) globally.

aaa server radius dynamic-author
Sets up the local AAA server for the dynamic authorization service, which must be enabled to support the CoA functionality to push the policy map in an input and output direction, and enters dynamic authorization local server configuration mode.

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_aaa/configuration/15-sy/sec_usr_aaa-15-sy-book/sec-rad-coa.html
upvoted 25 times

Rockbo47 Most Recent 1 month ago

Selected Answer: C

The question is "Which Cisco command enables authentication, authorization, and accounting globally" - the rest is irrelevant here. With that being the case, the only correct answer is C. Once AAA is enabled globally, THEN you would use the command "aaa server radius dynamic-author" to enable CoA

upvoted 1 times

Tthurston1 1 month, 4 weeks ago

Selected Answer: C

To enable AAA, you need to configure the 'aaa new-model' command in global configuration mode. Until this command is enabled, ALL OTHER AAA commands are hidden.

<https://www.cisco.com/c/en/us/support/docs/security-vpn/terminal-access-controller-access-control-system-tacacs-/10384-security.html>
upvoted 1 times

Korndal 2 months, 1 week ago

Selected Answer: C

It's C. you cannot enable anything without first issuing "aaa new-model". So all AAA commands are not available before you add "aaa new-model" therefore the answer is C

upvoted 2 times

XvidalX 6 months, 1 week ago

Selected Answer: C

simple.. dynamic author enables COA , aaa new model permits COA to be enabled..
C is the correct.

upvoted 2 times

xziomal9 10 months, 2 weeks ago

Answer C
upvoted 1 times

jpapas 1 year, 1 month ago

Selected Answer: A

Guys,
you need reverse logic here.
> if you issue an "aaa new-model" you don't have CoA support as is disabled by default on all devices.
> if you issue "aaa server radius dynamic-author" this will activate CoA globally (assuming that aaa new-model is already there)

upvoted 4 times

jpapas 1 year, 1 month ago

... and says "so that CoA >>IS<< supported..."
so the command activated CoA.

If the Q wording was different i.e.

"... so that to be able to support CoA..." , then the right answer would be C "aaa new-model" (but not with the above wording, which makes A the correct answer).

upvoted 1 times

  **cyberwhizzy0** 1 year, 1 month ago

Selected Answer: C

Step 3

aaa new-model

Example:

Device(config)# aaa new-model

Enables authentication, authorization, and accounting (AAA) globally.

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_aaa/configuration/15-sy/sec_usr_aaa-15-sy-book/sec-rad-coa.html

upvoted 1 times

  **Leogxn** 1 year, 1 month ago


Selected Answer: A

aaa new-model

Enables authentication, authorization, and accounting (AAA) globally

I think the aaa server radius dynamic-author command has to be enabled globally to support the CoA

upvoted 2 times

  **jku2cya** 1 year, 2 months ago

Selected Answer: A

Exactly what Ampersand and Jessie45785 said

upvoted 2 times

  **Jessie45785** 1 year, 3 months ago

Selected Answer: A

A is correct answer don't be fooled:

Proof:

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/security/a1/sec-a1-xe-3se-3850-cr-book/sec-a1-xe-3se-3850-cr-book_chapter_01.html#wp4234596077

aaa new-model:

To enable the authentication, authorization, and accounting (AAA) access control model, issue the aaa new-model command in global configuration mode. To disable the AAA access control model, use the no form of this command.

aaa server radius dynamic-author:

(to facilitate interaction with an external policy server)

To configure a device as an authentication, authorization, and accounting (AAA) server to facilitate interaction with an external policy server, use the aaa server radius dynamic-author command in global configuration mode. To remove this configuration, use the no form of this command.

upvoted 2 times

  **YooAndI** 1 year, 4 months ago

It's C. Cisco states that Step 3: aaa new-model "Enables authentication, authorization, and accounting (AAA) globally."

This command goes before Step 4: aaa server radius dynamic-author, which "Enters dynamic authorization local server configuration mode and specifies a RADIUS client from which a device accepts Change of Authorization (CoA) and disconnect requests. Configures the device as a AAA server to facilitate interaction with an external policy server."

So the command aaa new-model is needed BEFORE aaa server radius dynamic-author, in order for it to function. Answer is C.

Source: Cisco RADIUS Change of Authorization paper - https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_aaa/configuration/xe-16-10/sec_usr_aaa-xe-16-10-book/sec-rad-coa.pdf

upvoted 1 times

  **stalkr3** 1 year, 5 months ago

Selected Answer: C

aaa server radius dynamic-author does not enable aaa globally. Therefore C

upvoted 1 times

  **Jessie45785** 1 year, 5 months ago

Selected Answer: C

definitely C

upvoted 1 times

  **Tuxzinator** 1 year, 7 months ago

Selected Answer: C

So both commands, "aaa new-model" and "aaa server radius dynamic-author," can be used to enable CoA on a Cisco device, but they serve different purposes. The "aaa new-model" command is used to enable AAA globally on the device, while the "aaa server radius dynamic-author" command is used to configure a RADIUS server for dynamic authorization.

upvoted 2 times

Emlia1 1 year, 9 months ago

Selected Answer: C

I prefer C

upvoted 2 times

Martian89 1 year, 10 months ago

Selected Answer: C

Tried now You cant use the command "aaa server radius dynamic-author" without using "aaa new model" first.

Suggesting that You have to first issue aaa new model to allow AAA globally on the switch so the COA is supported (so that You can put in the server command and anything else)

upvoted 4 times

Question #103

Topic 1

What is a characteristic of Firepower NGIPS inline deployment mode?

- A. ASA with Firepower module cannot be deployed
- B. It cannot take actions such as blocking traffic
- C. It is out-of-band from traffic
- D. It must have inline interface pairs configured

Correct Answer: D

Community vote distribution

D (100%)

surforlife **Highly Voted** 2 years, 2 months ago

"D"

<https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/200924-configuring-firepower-threat-defense-int.html#anc2>

upvoted 6 times

Marshpillowz **Most Recent** 5 months, 1 week ago

Selected Answer: D

I think D

upvoted 1 times

LTLnetworker 8 months ago

Inline pairs should not be confused with IPS inline mode.

<https://community.cisco.com/t5/security-blogs/demystifying-firepower-deployment-modes/bc-p/4994822#M2570>

<https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/200924-configuring-firepower-threat-defense-int.html>

Without any inline pairs, an FTD in routed mode usually performs IPS functions in inline mode (i. e. capable of dropping packets if intrusion is detected).

None of the answers are correct.

upvoted 1 times

A mall provides security services to customers with a shared appliance. The mall wants separation of management on the shared appliance. Which ASA deployment mode meets these needs?

- A. routed mode
- B. multiple zone mode
- C. multiple context mode
- D. transparent mode

Correct Answer: C

Community vote distribution

C (100%)

Marshpillowz 5 months, 1 week ago

Selected Answer: C

C is correct

upvoted 1 times

gondohwe 1 year, 3 months ago

multi-context mode allows creation of several firewall instances within a single physical firewall for multi-tenancy purposes

upvoted 1 times

gondohwe 1 year, 3 months ago

C is the correct choice

upvoted 1 times

What is managed by Cisco Security Manager?

- A. Cisco WLC
- B. Cisco ESA
- C. Cisco WSA
- D. Cisco ASA

Correct Answer: D

Community vote distribution

D (100%)

  **[Removed]**  2 years, 11 months ago

Cisco Security Manager provides a comprehensive management solution for:
Cisco ASA 5500 Series Adaptive Security Appliances
Cisco intrusion prevention systems 4200 and 4500 Series Sensors
Cisco AnyConnect Secure Mobility Client

Answer: D

<https://www.cisco.com/c/en/us/products/security/security-manager/index.html>



upvoted 6 times

  **Marshpillowz**  5 months, 1 week ago

Selected Answer: D

D is correct

upvoted 1 times

  **sull3y** 1 year, 7 months ago

D: Cisco Security Manager (CSM) is a security management solution for Cisco security devices, such as Cisco ASA, Cisco Firepower, and Cisco ISR. It is used to manage and configure Cisco security devices, including firewall policies, VPNs, and intrusion prevention. CSM provides a centralized management platform that allows network administrators to manage multiple Cisco security devices from a single console, including device discovery, inventory management, policy provisioning and compliance reporting. With CSM, administrators can deploy consistent security policies across multiple devices, reducing the risk of security breaches and simplifying security management.

upvoted 1 times



  **TesterDude** 2 years, 3 months ago

Based on the wording, I think bhh2020 is right; however, I believe the wording on the test will be "Cisco Content Security Manager Appliance (SMA)", which is covered heavily in the book and manages ESA and WSA:

"Cisco Content SMA provides centralized management and monitoring (reporting) of Cisco WSAs and Cisco ESAs. The Cisco SMA simplifies the planning and administration of Cisco ESA and Cisco WSA deployments."

Santos, Omar. CCNP and CCIE Security Core SCOR 350-701 Official Cert Guide (p. 624). Pearson Education. Kindle Edition.

upvoted 2 times

  **Mjestic** 1 year, 10 months ago

"Security Manager" is different compared to "Security Management Appliance" which you refers to. On Cisco site they are different. Manager/Management... tricky but not the same word.

D is the correct one.

upvoted 1 times

An organization is trying to improve their Defense in Depth by blocking malicious destinations prior to a connection being established. The solution must be able to block certain applications from being used within the network. Which product should be used to accomplish this goal?

- A. Cisco Firepower
- B. Cisco Umbrella
- C. Cisco ISE
- D. Cisco AMP

Correct Answer: A

Community vote distribution



aalman Highly Voted 3 years, 2 months ago

Answer = B

I work with Umbrella and Firepower daily. You can do this with Firepower, Umbrella whole existence is for blocking DNS connections to malicious sites before they are made, and blocking applications from launching on the internal network. For example, our users can't access Pandora, FB, Google Docs while on our internal network based on a policy configured in Umbrella.

upvoted 17 times

AS04 Highly Voted 3 years, 1 month ago

A is correct, Firepower has AVC feature that can block traffic based on application.

upvoted 7 times

west33637 1 year, 9 months ago

B is correct. AVC on Firepower can not block applications from being used within the network. Firepower can only block these applications if they pass through the firewall. Umbrella can block connections to malicious sites before the connection is made based on the DNS lookup. Umbrella also installs an endpoint supplicant or can be used as an Anyconnect module. This way you can push an application policy to the endpoints blocking even applications 'within the network'. Same as aalman, I have used this at work and at home.

upvoted 7 times

Premium_Pils Most Recent 1 month ago

Selected Answer: B

Block the process right at the beginning, i.e. at the DNS request step, before making a connection to the bad website. - B

upvoted 1 times

4pelos 6 months, 1 week ago

Correct answer B.

Checked in securitytut

upvoted 2 times

xziomal9 10 months, 2 weeks ago

Answer B

upvoted 1 times

jorg32 1 year, 1 month ago

Selected Answer: B

Umbrella, is trying to block the start of the conversation with bad websites, why block the application when you know you can block way earlier on the traffic flow?

upvoted 1 times

Jessie45785 1 year, 3 months ago

Selected Answer: D

The solution must be able to block certain applications from being used within the network

I really think it is D cause:

- NGFW cannot stop it in L2
- Umbrella can block only DNS protocol - what about all the other ones - wont be able to detect it
- WSA - proxy will definitely will not help here

... but AMP can block application from being able to start hence cutting it from TCP stack and fulfilling a requirement of "blocking malicious destinations prior to a connection being established"



but it is Cisco so you never know :/

upvoted 2 times

F0rtyx40 1 year, 3 months ago

It's B, Umbrella can block the connection before firepower L7 application detectors kick in.

upvoted 1 times

  **gc999** 1 year, 4 months ago



I think most of us already get the keywords here "prior to a connection being established" and "within the network". Can I make an example that if there are two internal users, let say User-1 and User-2, within the network, which solution can block the certain application being send from User-1 to User-2?

upvoted 1 times

  **SegaMasterSystemAdmin** 1 year, 4 months ago

This is a tricky one, the question is weird because the keywords are "prior to a connection being established" and "must be able to block certain applications". It is true that Umbrella blocks the DNS traffic so that it does that take care of "prior to a connection being established". However, Umbrella does not block the application itself just the DNS traffic, so if the application does not utilize DNS and is IP based, it will not block anything, Firepower on the other hand can block the applications and with a "Block with Reset" it does not allow any connection to be established. Also, both can block based on malicious destination. I will still go with B though.

upvoted 1 times

  **KPzee** 1 year, 5 months ago



A is correct a firewall will block certain applications that might already be on the network.

upvoted 1 times

  **Toni_Su91** 1 year, 6 months ago



Prior to a connection being established - This is classic Umbrella - DNS security is first line of defence.

upvoted 2 times

  **sull3y** 1 year, 7 months ago

The answer is B. Cisco Umbrella. Cisco Umbrella is a cloud-based security solution that provides advanced threat protection and blocks malicious destinations before a connection is established. It uses DNS-layer security to block requests to known malicious domains and IPs, and it also has the capability to block certain applications from being used within the network. By implementing Cisco Umbrella, the organization can improve their defense in depth by preventing malicious traffic from entering the network, thus reducing the risk of a successful cyber attack.

upvoted 2 times

  **psuoh** 1 year, 7 months ago



I think A is the Cisco's correct answer.

the question asks "within the network". Umbrella would do on and off the network/app blocking. Similarly, firepower can do network/app block for the network.

Umbrella would be a overkill for a "organization".

<https://community.cisco.com/t5/network-security/firepower-or-umbrella-for-blocking-urls-applications-ip/td-p/4430076>

upvoted 2 times

  **ureis** 1 year, 8 months ago

I managing a Umbrella of our costumer and this is what Umbrella is showing to us when i go to "DNS POLICIES":

"Control Applications - Select applications or application categories you'd like to block or Allow for the users in your organization"

In other hand you can do the same on Firepower ACP blocking applications.

Maybe the magic word here be:

"prior to a connection being established"

I'll choose B

upvoted 4 times

  **Emlia1** 1 year, 9 months ago

Selected Answer: B

It's B

upvoted 2 times

  **west33637** 1 year, 9 months ago

Selected Answer: B

B is correct. AVC on Firepower can not block applications from being used 'within the network'. Firepower can only block these applications if they pass through the firewall. Umbrella can block connections to malicious sites before the connection is made based on the DNS lookup. Umbrella also installs an endpoint supplicant or can be used as an Anyconnect module. This way you can push an application policy to the endpoints blocking even applications 'within the network'. Same as aalman, I have used this at work and at home.

upvoted 3 times

An engineer notices traffic interruptions on the network. Upon further investigation, it is learned that broadcast packets have been flooding the network. What must be configured, based on a predefined threshold, to address this issue?

- A. Storm Control
- B. embedded event monitoring
- C. access control lists
- D. Bridge Protocol Data Unit guard

Correct Answer: A

Community vote distribution



Marshpillowz 5 months, 1 week ago

Selected Answer: A

A - Storm Control
upvoted 1 times

sis_net_sec 2 years, 1 month ago

correct Answer is A

Explanation:

<https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/eem/command/eem-cr-book/eem-cr-e1.html>

upvoted 2 times

What is a feature of Cisco NetFlow Secure Event Logging for Cisco ASAs?

- A. Multiple NetFlow collectors are supported.
- B. Advanced NetFlow v9 templates and legacy v5 formatting are supported.
- C. Secure NetFlow connectors are optimized for Cisco Prime Infrastructure
- D. Flow-create events are delayed.

Correct Answer: A

Community vote distribution

D (50%) A (50%)

Reece_S Highly Voted 3 years, 1 month ago

A is the answer. While events can be delayed they are not delayed by default. The flow-create event is exported as soon as the flow is created if the flow-export delay flow-create command is not configured.

upvoted 13 times

Smilebloke 2 years, 5 months ago

https://www.cisco.com/c/en/us/td/docs/security/asa/asa91/asdm71/general/asdm_71_general_config/monitor_nsel.pdf

upvoted 2 times

ureis 1 year, 8 months ago

Multiple NetFlow collectors are supported in "Flexible Netflow"

upvoted 1 times

jaciro11 Highly Voted 2 years, 6 months ago

Selected Answer: D

Delays the export of flow-create events.

upvoted 5 times

Marshpillowz Most Recent 5 months, 1 week ago

Selected Answer: A

I think A is most accurate

upvoted 1 times

Stevens0103 8 months ago

Selected Answer: A

The option D's wording implies that flow-create events are always delayed and this default action is a feature. However, flow-create events are actually optional and it is exactly this optionality makes it a feature.

https://www.cisco.com/c/en/us/td/docs/security/asa/asa91/configuration/general/asa_91_general_config/monitor_nsel.html

upvoted 2 times

Stevens0103 8 months ago

correction: "...delayed flow-create events is actually optional..."

upvoted 1 times

nep1019 1 year, 1 month ago

Selected Answer: A

Whew this is a hard question. Is A because as previously mentioned, delaying the export of flow-create events is NOT a default action. A is the "more correct" answer. Cisco exams are a racket.

upvoted 4 times

jpapas 1 year, 1 month ago

Selected Answer: D

Question translates to : "What is a feature [only] of Cisco NSEL ?"

> A , its true for all Netflow implementations : IOS/IOS-XR/IOS-XE etc

> B,C are wrong

D is true and exists only on ASA's NSEL. So is the correct answer (even if delay is optional).

ref: https://www.cisco.com/c/en/us/td/docs/security/asa/asa91/configuration/general/asa_91_general_config/monitor_nsel.html

upvoted 2 times

jku2cya 1 year, 2 months ago

Selected Answer: D

Multiple references to the correct information "Delays the export of flow-create events"
upvoted 1 times

dabance 1 year, 2 months ago

D.
https://www.cisco.com/c/en/us/td/docs/security/asa/asa91/asdm71/general/asdm_71_general_config/monitor_nsel.pdf
Ref: page 2
upvoted 1 times

gc999 1 year, 3 months ago

Selected Answer: D

https://www.cisco.com/c/en/us/td/docs/security/asa/asa91/asdm71/general/asdm_71_general_config/monitor_nsel.html#:~:text=Delays%20the%20export%20of%20flow%2Dcreate%20events
upvoted 1 times

gc999 1 year, 3 months ago

Selected Answer: D

Some guys already pointed out the main point in the link
"https://www.cisco.com/c/en/us/td/docs/security/asa/asa91/asdm71/general/asdm_71_general_config/monitor_nsel.pdf"

The ASA and ASASM implementations of NSEL provide the following major functions:
- Delays the export of flow-create events

I don't see any related keyword "Multiple" for Netflow in the document.
upvoted 1 times

gc999 1 year, 3 months ago

Besides, "Multiple NetFlow collectors are supported" is not a kind of core feature.
From the link "<https://www.cisco.com/c/en/us/td/docs/security/asa/asa92/configuration/general/asa-general-cli/monitor-nsel.html>", it said it can support to send to "different" collectors, but it still cannot send to "multiple" collectors once it matches.
upvoted 1 times

Emlia1 1 year, 9 months ago

D could be
upvoted 2 times

francojaraba 2 years, 1 month ago

Selected Answer: A

Answer is A.

Based on the link -https://www.cisco.com/c/en/us/td/docs/security/asa/asa91/asdm71/general/asdm_71_general_config/monitor_nsel.pdf. What is delayed is the export not the flow-create.
upvoted 2 times

ureis 1 year, 8 months ago

Multiple NetFlow collectors are supported in "Flexible Netflow"
upvoted 1 times

Pwned 2 years, 3 months ago

Selected Answer: A

A is the correct answer
upvoted 1 times

semi1750 2 years, 5 months ago

Feature History for NSEL - NetFlow Filtering 8.1(2)
You can filter NetFlow events based on traffic and event type, then send records to different collectors. For example, you can log all flow-create events to one collector, and log flow-denied events to a different collector.

https://www.cisco.com/c/en/us/td/docs/security/asa/asa91/asdm71/general/asdm_71_general_config/monitor_nsel.pdf
upvoted 1 times

wowako 2 years, 8 months ago

I think. The correct answer is D because "OPTIONAL: Configure a delay for flow-create NSEL events in seconds. Increasing flow-create delay will cause fewer NSEL events to be exported to NetVizura NetFlow collector. E.g. setting delay to 120 will cause only one NSEL event to be exported, for flows shorter than 2 minutes."
<https://confluence.netvizura.com/display/NVUG/Configuring+Cisco+ASAs+for+NSEL+Export>
upvoted 2 times

zheka 2 years, 9 months ago

I now eliminate D as the good answer, it is notorious Cisco's trick to make us fail, Dinges is right, it can delay the export of events, not the flow of events.
upvoted 1 times

zheka 2 years, 9 months ago

Maybe on the real exam they will ask to select two options, then A and D would be just the right choice
upvoted 1 times

Question #109

Topic 1

What is a key difference between Cisco Firepower and Cisco ASA?

- A. Cisco Firepower provides identity based access control while Cisco ASA does not.
- B. Cisco AS provides access control while Cisco Firepower does not.
- C. Cisco ASA provides SSL inspection while Cisco Firepower does not.
- D. Cisco Firepower natively provides intrusion prevention capabilities while Cisco ASA does not.

Correct Answer: D

Community vote distribution

D (100%)

  **sull3y** Highly Voted 1 year, 7 months ago

Cisco Firepower and Cisco ASA are both network security products offered by Cisco, but they have different capabilities and are typically used for different purposes.

Cisco ASA (Adaptive Security Appliance) is a firewall and VPN device that provides perimeter security for networks. It can be used to control access to resources, block unauthorized traffic, and create secure VPN connections. ASA does not provide intrusion prevention capabilities, it is focused on network perimeter security.

Cisco Firepower, on the other hand, is a more advanced security product that provides both firewall and intrusion prevention capabilities. It is designed to protect networks from advanced threats, such as malware and zero-day attacks. Firepower uses a combination of technologies, such as threat intelligence and machine learning, to detect and block malicious traffic. Firepower includes features such as advanced malware protection, threat hunting, and incident response capabilities.

upvoted 5 times

  **Marshpillowz** Most Recent 5 months, 1 week ago

Selected Answer: D

D is correct

upvoted 1 times

DRAG DROP -

Drag and drop the suspicious patterns for the Cisco Tetration platform from the left onto the correct definitions on the right.

Select and Place:

privilege escalation	Tetration platform learns the normal behavior of users.
user login suspicious behavior	Tetration platform is armed to look at sensitive files.
interesting file access	Tetration platform watches user access failures and methods
file access from a different user	Tetration platform watches for movement in the process lineage tree.

Correct Answer:

privilege escalation	file access from a different user
user login suspicious behavior	interesting file access
interesting file access	user login suspicious behavior
file access from a different user	privilege escalation

  **Kyle1776** Highly Voted 2 years, 6 months ago


Privilege escalation: Watches for privilege changes from a lower privilege to a higher privilege in the process lineage tree.

User login suspicious behavior: Cisco Secure Workload platform watches user login failures and user login methods.

Interesting file access: Cisco Secure Workload platform can be armed to look at sensitive files.

File access from a different user: Cisco Secure Workload platform learns the normal behavior of which file is accessed by which user.

<https://www.cisco.com/c/en/us/products/collateral/data-center-analytics/tetration-analytics/white-paper-c11-740380.html>
upvoted 9 times

  **MPoels** 6 months, 1 week ago

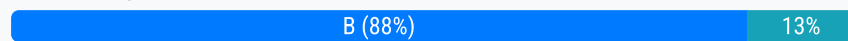
https://web.archive.org/web/20191129023324/https://www.cisco.com/c/en/us/products/collateral/data-center-analytics/tetration-analytics/white-paper-c11-740380.html#_Toc509550184
upvoted 1 times

What is a benefit of using Cisco FMC over Cisco ASDM?

- A. Cisco FMC uses Java while Cisco ASDM uses HTML5.
- B. Cisco FMC provides centralized management while Cisco ASDM does not.
- C. Cisco FMC supports pushing configurations to devices while Cisco ASDM does not.
- D. Cisco FMC supports all firewall products whereas Cisco ASDM only supports Cisco ASA devices.

Correct Answer: B

Community vote distribution



RemiK 3 months ago

Selected Answer: D

Am I the only one who has already managed several ASAs via ASDM? "Managing multiple ASAs" is not another definition of "centralized management"? Although, I agree, the possibility of a new "centralized management" apparatus is a far cry from what ASDM proposes.

B says "Cisco ASDM does not"

Regarding this, D seems the correct one

upvoted 1 times

Marshpillowz 5 months, 1 week ago

Selected Answer: B

B is correct

upvoted 1 times

KPzee 1 year, 5 months ago

B is correct. FMC allows for centralized management of many devices e.g if there is several firepower NGFW devices, they can be managed via a single FMC device whereas ASDM can only manage a single appliance.

upvoted 3 times

sull3y 1 year, 7 months ago

B: Cisco FMC provides centralized management, meaning that it allows administrators to manage multiple firewall devices from a single console. This can improve efficiency and reduce the potential for errors that can occur when managing multiple devices individually. Cisco ASDM, on the other hand, is a device-specific management tool that can only be used to manage a single Cisco ASA device at a time.

upvoted 3 times

MUKD 2 years, 3 months ago

Selected Answer: B

its B.FMC cannot manage ASA

upvoted 3 times

pr0fectus 2 years, 8 months ago

Selected Answer: B

Let's not complicate the question. Main question is "what is the benefit". FMC does provide centralized management of FTDs/FirePOWER service (note that FMC cannot manage ASA) while ASDM can only manage one ASA w/ FirePOWER service at a time.

upvoted 3 times

zheka 2 years, 9 months ago

But if by centralized management they mean managing IPS, AVC, AMP and all other security components then of course it is B

upvoted 2 times

zheka 2 years, 9 months ago

Disagree about D, FMC doesn't support firewalls running ASA code, it has to be FTD only. The term "centralized management" is vague. What do they mean by it? Managing more than one device? You can manage more than one ASA from ASDM by the way. But you can't push configuration from ASDM to ASA, it's instantaneous change without going through "Deploy/push" procedure. I'm not sure if it is a benefit or not, to me rather architectural feature. So I'm inclined to think it is C

upvoted 1 times

shaikat 2 years, 9 months ago

I think B is more appropriate. Because ASA is not used for centralized management for all firewalls but only for a ASA management.

upvoted 2 times

Thusi26 2 years, 9 months ago

D should be it. Both ASA and FMC are being used for centralized management.

upvoted 1 times

  **pr0fectus** 2 years, 8 months ago

Need to be careful in reading the choices. Note that FMC can only manage FirePOWER services of ASA (not the ASA) and Firepower appliance onboarded with FTD.

upvoted 1 times

  **bob511** 2 years, 6 months ago

connection manager in ASDM i dont think would be considered CM as you have to relogin to each firewall you want to manage

upvoted 1 times

  **1M4hqQ9G** 2 years, 4 months ago

You need CSM to manage multiple ASA. ASDM cant manage multiple ASA.

upvoted 1 times

Question #112

Topic 1

Which product allows Cisco FMC to push security intelligence observable to its sensors from other products?

- A. Threat Intelligence Director
- B. Encrypted Traffic Analytics.
- C. Cognitive Threat Analytics.
- D. Cisco Talos Intelligence

Correct Answer: A

Community vote distribution



  **Marshpillowz** 5 months, 1 week ago

Selected Answer: A

A is correct



upvoted 1 times

  **sull3y** 1 year, 7 months ago

A. Threat Intelligence Director

Cisco FMC's Threat Intelligence Director allows security teams to integrate security intelligence observables from various sources, such as Cisco Talos, into their Cisco FMC environment. This allows the FMC to push updated security intelligence to its sensors, enabling them to better detect and respond to potential threats.

upvoted 4 times

  **Jamesy** 1 year, 11 months ago

A is correct. Cheers

upvoted 3 times

  **freddycisco** 3 years, 1 month ago

How does it work?

As shown in the image, on the FMC you have to configure sources from where you would like to download threat intelligence information. The FMC then pushes that information (observables) to sensors. When the traffic matches the observables, the incidents appear in the FMC user interface (GUI).

<https://www.cisco.com/c/en/us/support/docs/storage-networking/security/214859-configure-and-troubleshoot-cisco-threat.html>

upvoted 2 times

A Cisco FirePower administrator needs to configure a rule to allow a new application that has never been seen on the network. Which two actions should be selected to allow the traffic to pass without inspection? (Choose two.)

- A. permit
- B. allow
- C. reset
- D. trust
- E. monitor

Correct Answer: *BD*

Community vote distribution



rad9899 Highly Voted 3 years, 4 months ago

- D. trust
- E. monitor

upvoted 26 times

loiphin 2 years, 8 months ago

In case you are still nery about the above answers, then this diagram will calm your nerves :)

https://www.cisco.com/c/en/us/td/docs/security/firepower/610/configuration/guide/fpmc-config-guide-v61/access_control_rules.html#ID-2190-0000005

upvoted 9 times

Fugashi 2 years, 3 months ago

https://www.cisco.com/c/en/us/td/docs/security/firepower/610/configuration/guide/fpmc-config-guide-v61/access_control_rules.html?bookSearch=true#ID-2190-0000023b

There is an exception, however. If a Monitor rule contains layer 7 conditions—such as an application condition—the system allows early packets to pass and the connection to be established (or the SSL handshake to complete)

upvoted 2 times

west33637 Highly Voted 1 year, 7 months ago

Selected Answer: DE

create a monitor rule that matches the application. Then create a trust rule right below it.

upvoted 6 times

mhd96far Most Recent 5 months, 3 weeks ago

Selected Answer: DE

never seen on the network

upvoted 1 times

Pakawat 8 months, 3 weeks ago

Selected Answer: DE

Trust and Monitor

upvoted 1 times

xziomal9 10 months, 1 week ago

Answer DE

upvoted 1 times

HOUSSE 11 months, 2 weeks ago

TRUST AND MONITOR

ALLOW IS NOT A GOOD ANSWER BECAUSE TRAFFIC WILL PASS UNDER INSPECTION

upvoted 1 times

Pakawat 11 months, 3 weeks ago

Selected Answer: DE



Trust and Monitor as the question mention that "without inspection".

upvoted 1 times

F0rtyx40 1 year, 2 months ago

D and E , allow rules are still subject to L7 processing

upvoted 1 times

  **bobie** 1 year, 3 months ago

Selected Answer: BD

The allow action, If it does only file inspection, intrusion inspection, or neither, it signifies that it will not be inspected because the application is unknown.

Without a doubt, the trust action is one of the proper answers.

upvoted 1 times



  **YooAndI** 1 year, 4 months ago

Step 1: Monitor

Step 2: Trust --> No inspection --> Reaches Destination

Allow is further down on the process, Step 4, after Step 3: Block.

upvoted 2 times

  **psuoh** 1 year, 7 months ago

The system does not perform deep inspection on trusted, blocked, or encrypted traffic.

You monitor to log the session to use when "configuring a rule to allow a new application..."

upvoted 2 times

  **Emlia1** 1 year, 9 months ago



D, E

Explanation

Each rule also has an action, which determines whether you monitor, trust, block, or allow matching traffic.

Note: With action "trust", Firepower does not do any more inspection on the traffic. There will be no intrusion protection and also no file-policy on this traffic.

upvoted 1 times

  **dique** 2 years, 1 month ago

D and E (Trust and monitor.)

upvoted 1 times

  **otzu1** 2 years, 4 months ago

D/E

https://www.cisco.com/c/en/us/td/docs/security/firepower/610/configuration/guide/fpmc-config-guide-v61/access_control_rules.html

upvoted 1 times

  **breezer** 2 years, 5 months ago



Dont put too much strain in the question.. Monitor action is only used to log traffic.. it in itself cannot allow or block.. Answer is Allow and Trust

upvoted 2 times

  **guest_user** 2 years, 4 months ago

There is an exception, however. If a Monitor rule contains layer 7 conditions—such as an application condition—the system allows early packets to pass and the connection to be established (or the SSL handshake to complete). This occurs even if the connection should be blocked by a subsequent rule; this is because these early packets are not evaluated against subsequent rules.


upvoted 1 times

  **rbrain** 2 years, 7 months ago

Selected Answer: BD

Trust & Monitor

upvoted 4 times

  **rbrain** 2 years, 7 months ago

D&E ofcourse

upvoted 2 times

  **pr0fectus** 2 years, 8 months ago

Selected Answer: BD

Key term is "pass without inspection"

upvoted 4 times

What is a characteristic of a bridge group in a Cisco ASA Firewall running in transparent mode?

- A. It has an IP address on its BVI interface and is used for management traffic.
- B. It allows ARP traffic with a single access rule.
- C. It includes multiple interfaces and access rules between interfaces are customizable.
- D. It is a Layer 3 segment and includes one port and customizable access rules.

Correct Answer: C

Community vote distribution

C (71%) A (29%)

leptonius Highly Voted 3 years ago

It's C

<https://www.cisco.com/c/en/us/td/docs/security/asa/asa94/config-guides/cli/general/asa-94-general-config/intro-fw.html>

upvoted 11 times

sull3y Highly Voted 1 year, 7 months ago

C. It includes multiple interfaces and access rules between interfaces are customizable.

In transparent mode, a Cisco ASA firewall acts as a bridge instead of a router. A bridge group is a collection of interfaces that are bridged together and forward traffic between them. A bridge group in transparent mode includes multiple interfaces, and the access rules between interfaces are customizable, meaning that the administrator can configure filtering and access control policies to restrict traffic between different interfaces. This allows the firewall to forward traffic between different VLANs or segments while still applying security policies.

upvoted 6 times

ytsionis Most Recent 12 months ago

C is the correct.

++if you configure an access control rule to block Questionable sites (level 5), it also blocks all 4,3,2, through Untrusted (level 1) sites. (Firepower Management Center Configuration Guide, Version 6.5)

https://www.cisco.com/c/en/us/td/docs/security/firepower/650/configuration/guide/fpmc-config-guide-v65/url_filtering.html#id_17110

upvoted 1 times

Jessie45785 1 year, 5 months ago

Selected Answer: A

NOT C - access rules between interfaces are customizable - how they can be since they are bridged !?!

upvoted 1 times

Jessie45785 1 year, 4 months ago

C - IS CORRECT - I have to correct myself, indeed C is correct:

<https://www.cisco.com/c/en/us/td/docs/security/asa/asa97/configuration/firewall/asa-97-firewall-config/access-rules.html>

Extended access rules (Layer 3+ traffic) assigned to Bridge Virtual Interfaces (BVI; routed mode)—If you name a BVI, you can apply separate rule sets in the inbound and outbound direction, and you can also apply rule sets to the bridge group member interfaces. When both the BVI and member interface have access rules, the order of processing depends on direction. Inbound, the member access rules are evaluated first, then the BVI access rules. Outbound, the BVI rules are considered first, then the member interface rules.

upvoted 1 times

kjubo 1 year, 10 months ago

Selected Answer: C

BVI interface is not used for management purpose. But we can add a separate Management slot/port interface that is not part of any bridge group, and that allows only management traffic to the ASA.

upvoted 3 times

leowulf 1 year, 12 months ago

I believe answer is C

<https://integratingit.wordpress.com/2021/05/30/asa-transparent-mode/#:~:text=Bridge%20groups%20are%20used%20to,the%20ASA%20to%20pass%20traffic.>

upvoted 2 times

getafix 2 years, 2 months ago

Selected Answer: C

A bridge group is a group of interfaces that the ASA bridges instead of routes. Bridge groups are only supported in Transparent Firewall Mode. Like any other firewall interfaces, access control between interfaces is controlled, and all of the usual firewall checks are in place.

Each bridge group includes a Bridge Virtual Interface (BVI). The ASA uses the BVI IP address as the source address for packets originating from the bridge group. The BVI IP address must be on the same subnet as the bridge group member interfaces. The BVI does not support traffic on secondary networks; only traffic on the same network as the BVI IP address is supported.

Only bridge group member interfaces are named and can be used with interface-based features.

<https://www.cisco.com/c/en/us/td/docs/security/asa/asa94/config-guides/cli/general/asa-94-general-config/intro-fw.html#ID-2106-00000012>

While we can use BVIs for Firewall Management purposes, it isn't ONLY used for management.

Answer C seems correct

upvoted 2 times

  **Metgatz** 2 years, 4 months ago

Selected Answer: A

A bridge group is a group of interfaces that the ASA bridges instead of routes. Bridge groups are supported in both transparent and routed firewall mode. Like any other firewall interfaces, access control between interfaces is controlled, and all of the usual firewall checks are in place

upvoted 1 times

  **dr4gn00t** 2 years, 7 months ago

Why not A? BVI can be assigned IP and be used for management afaik

upvoted 2 times

  **Laryoul** 2 years, 5 months ago

I think that in case of multiple bridge group, this answer as no sense ... there is only one route table.

upvoted 1 times

  **beeker98106** 2 years, 10 months ago

more specific from below doc:

About Bridge Groups

A bridge group is a group of interfaces that the ASA bridges instead of routes. Bridge groups are only supported in Transparent Firewall Mode. Like any other firewall interfaces, access control between interfaces is controlled, and all of the usual firewall checks are in place

upvoted 1 times

While using Cisco Firepower's Security Intelligence policies, which two criteria is blocking based upon? (Choose two.)

- A. IP addresses
- B. URLs
- C. port numbers
- D. protocol IDs
- E. MAC addresses

Correct Answer: AB

Community vote distribution

AB (100%)

  **idto** Highly Voted  2 years, 9 months ago

Selected Answer: AB

"Block specific IP addresses, URLs, or domain names using a manually-created list or feed (for IP addresses, you can also use network objects or groups.)"

Source: https://www.cisco.com/c/en/us/td/docs/security/firepower/623/configuration/guide/fpmc-config-guide-v623/security_intelligence_blacklisting.html#ID-2192-0000002b



upvoted 6 times

  **Marshpillowz** Most Recent  5 months, 1 week ago

Selected Answer: AB

A and B

upvoted 1 times

  **sull3y** 1 year, 7 months ago

- A. IP addresses
- B. URLs

Cisco Firepower's Security Intelligence policies allows to block traffic based on IP addresses and URLs. IP addresses can be used to block traffic from specific IPs or ranges of IPs, or to block traffic that is going to specific IPs or ranges of IPs. URLs can be used to block traffic to specific websites or web pages, or to block traffic that is coming from specific websites or web pages.

upvoted 3 times

What features does Cisco FTDv provide over Cisco ASA v?

- A. Cisco FTDv provides 1GB of firewall throughput while Cisco ASA v does not.
- B. Cisco FTDv runs on VMware while Cisco ASA v does not.
- C. Cisco FTDv runs on AWS while Cisco ASA v does not.
- D. Cisco FTDv supports URL filtering while Cisco ASA v does not.

Correct Answer: D

Reference:

<https://www.ciscolive.com/c/dam/r/ciscolive/apjc/docs/2018/pdf/BRKSEC-2064.pdf>

Community vote distribution

D (100%)

Marshpillowz 5 months, 1 week ago

Selected Answer: D

D is correct

upvoted 1 times

sull3y 1 year, 7 months ago

D. Cisco FTDv supports URL filtering while Cisco ASA v does not.

Cisco FTDv (Firepower Threat Defense Virtual) is a next-generation firewall (NGFW) solution that provides advanced security features and capabilities beyond what is offered by Cisco ASA v (Adaptive Security Appliance Virtual). One key feature that Cisco FTDv provides over Cisco ASA v is support for URL filtering. This feature allows administrators to block or allow traffic to specific websites or web pages, based on predefined policies. Additionally, FTDv provides a centralized management platform for firewall, VPN, and advanced threat protection services, while ASA v is a traditional firewall with VPN capabilities. Both Cisco FTDv and ASA v run on VMware and AWS, and both support 1GB of firewall throughput.

upvoted 2 times

psuoh 1 year, 7 months ago

<https://www.cisco.com/c/en/us/products/collateral/security/adaptive-security-virtual-appliance-asav/adapt-security-virtual-appliance-ds.html>

upvoted 1 times

psuoh 1 year, 7 months ago

<https://www.cisco.com/c/en/us/products/collateral/security/adaptive-security-virtual-appliance-asav/adapt-security-virtual-appliance-ds.html>

upvoted 1 times

Raajaa 3 years, 2 months ago

D is the answer

upvoted 3 times

A network engineer is deciding whether to use stateful or stateless failover when configuring two Cisco ASAs for high availability. What is the connection status in both cases?

- A. need to be reestablished with stateful failover and preserved with stateless failover
- B. preserved with both stateful and stateless failover
- C. need to be reestablished with both stateful and stateless failover
- D. preserved with stateful failover and need to be reestablished with stateless failover

Correct Answer: D

Community vote distribution

D (100%)

—  **sull3y** Highly Voted 1 year, 7 months ago

D. preserved with stateful failover and need to be reestablished with stateless failover

In stateful failover, the primary and secondary devices share state information, meaning that they have the same view of the current connections and the connection status is preserved. If the primary device fails, the secondary device takes over and continues to manage the existing connections without interruption. In contrast, In stateless failover, the primary and secondary devices do not share state information, meaning that they have different views of the connections. If the primary device fails, the secondary device takes over but the connection status need to be reestablished.

upvoted 5 times

—  **Marshpillowz** Most Recent 5 months, 1 week ago

Selected Answer: D

D is correct

upvoted 1 times

—  **johnnybgud** 1 year, 3 months ago

Selected Answer: D

D.

Stateful = Maintain Sessions

Stateless = Sessions need to be reestablished

upvoted 2 times

Which term describes when the Cisco Firepower downloads threat intelligence updates from Cisco Talos?

- A. authoring
- B. consumption
- C. sharing
- D. analysis

Correct Answer: B

Community vote distribution

B (100%)

dzef13 Highly Voted 3 years, 3 months ago

we will showcase Cisco Threat Intelligence Director (CTID) an exciting feature on Cisco's Firepower Management Center (FMC) product offering that automates the operationalization of threat intelligence. TID has the ability to consume threat intelligence via STIX over TAXII and allows uploads/downloads of STIX and simple blacklists.

Reference: <https://blogs.cisco.com/developer/automate-threat-intelligence-using-cisco-threat-intelligencedirector> - Answer B Consumption
upvoted 18 times

Marshpillowz Most Recent 5 months, 1 week ago

Selected Answer: B

B is correct

upvoted 1 times

yong08321 1 year, 4 months ago

Selected Answer: B

The correct answer is B. Consumption.

Cisco Firepower is a security solution that provides threat detection, prevention, and response capabilities for networks. One of the key features of Firepower is its integration with Cisco Talos, a global threat intelligence organization that provides real-time information on the latest security threats and vulnerabilities.

When Firepower downloads threat intelligence updates from Talos, this process is called consumption. Firepower uses this information to update its own threat intelligence database and to identify and block any new threats that may be present on the network.

Authoring refers to the process of creating or writing security rules and policies for a network. Sharing refers to the ability to share threat intelligence and other security information with other organizations or security solutions. Analysis refers to the process of examining and interpreting security data to identify potential threats or vulnerabilities.

upvoted 1 times

haiderzaid 1 year, 5 months ago

The process of downloading these updates is commonly referred to as "threat intelligence consumption"

upvoted 1 times

Emlia1 1 year, 9 months ago

Selected Answer: B

It's B

upvoted 2 times

francojaraba 2 years, 1 month ago

The answer is consumption (B) - <https://blogs.cisco.com/developer/automate-threat-intelligence-using-cisco-threat-intelligence-director>
"TID has the ability to consume threat intelligence via STIX over TAXII and allows uploads/downloads of STIX and simple blacklists"

upvoted 3 times

francojaraba 2 years, 1 month ago

"Cisco Talos Intelligence Group (Talos) feeds—Talos provides access to regularly updated security intelligence feeds. Sites representing security threats such as malware, spam, botnets, and phishing appear and disappear faster than you can update and deploy custom configurations. The system downloads feed updates regularly, and thus new threat intelligence is available without requiring you to redeploy the configuration." - <https://www.cisco.com/c/en/us/td/docs/security/firepower/640/fdm/fptd-fdm-config-guide-640/fptd-fdm-sec-intel.html>

upvoted 2 times

Laryoul 2 years, 5 months ago

Selected Answer: B



like all people say correct answer is B

upvoted 4 times

  **efongvan** 2 years, 8 months ago



B is correct answer.

upvoted 4 times

  **Sarbi** 3 years ago



The correct answer is consumption only.

upvoted 3 times

  **Seawanderer** 3 years, 2 months ago

While I can't find any reference at all, "sharing" makes more sense to me. Firepower is not consuming anything (yet), but Talos is sharing the intelligence with other devices.

upvoted 1 times

  **Raajaa** 3 years, 2 months ago



B looks correct

upvoted 4 times

  **statikd** 3 years, 2 months ago

I wonder how Analysis was chosen as the answer. I can not find any good answer online or in the official cert guide. Closest thing is from <https://blogs.cisco.com/developer/automate-threat-intelligence-using-cisco-threat-intelligence-director>

upvoted 1 times

  **entitty** 3 years, 3 months ago

I leaning toward consumption - B

upvoted 3 times

An administrator is configuring a DHCP server to better secure their environment. They need to be able to rate-limit the traffic and ensure that legitimate requests are not dropped. How would this be accomplished?

- A. Set a trusted interface for the DHCP server.
- B. Set the DHCP snooping bit to 1.
- C. Enable ARP inspection for the required VLAN.
- D. Add entries in the DHCP snooping database.

Correct Answer: A

Community vote distribution



zheka Highly Voted 2 years, 9 months ago

Folks, we have lots of wrong answers verified and provided by "experts", there's no need to supply wrong answers by ourselves here. You can't add entries to DHCP snooping database. It's wrong answer. The only case when you create mapping of IP to MAC and VLAN and port is configuring "ip source guard" but it is not the same as DHCP snooping.

Unless you explicitly configure a rate limit on an interface, changing the trust state of the interface also changes its rate limit to the default value for that trust state. After you configure the rate limit, the interface retains the rate limit even when its trust state is changed
https://content.cisco.com/chapter.sjs?uri=/searchable/chapter/www.cisco.com/content/dam/en/us/td/docs/switches/lan/catalyst4500/XE35-0XO/configuration/guide/dhcp.fm/jcr:content/renditions/config_dhcp.html.xml
 upvoted 14 times

Rododendron2 4 months, 1 week ago

Not valid comment

You can add entries manually:

Router# ip dhcp snooping binding mac_address vlan vlan_ID ip_address interface ifname expiry lease_in_seconds
 eg. https://www.cisco.com/en/US/docs/general/Test/dwerblo/broken_guide/snoodhcp.pdf
 command.
 upvoted 2 times

BoxX 1 year, 2 months ago

If you won't to configure DAI (Dynamic ARP Inspection) and IP Source Guard (IPSG) you must add statically assigned IP addresses to the DHCP snooping database, as DAI and IPSG are using it.

Depending on platform and version you can add static entries into the DHCP snooping database:
 - Router# ip dhcp snooping binding binding_id vlan vlan_id interface interface expiry lease_time
 - Switch# ip dhcp snooping binding mac-addr vlan vlan ipaddr interface ifname expiry lease-in-seconds

Please, do not call someone "expert" just because you are not.
 upvoted 2 times

Random000 1 year, 11 months ago

So, it's A ?
 upvoted 6 times

psuoh 1 year, 7 months ago

Answer is C
 upvoted 2 times

Rododendron2 Most Recent 4 months, 1 week ago

Selected Answer: D

It's possible to do this with D , eg. downloading the snooping database from tftp server (taken from DHCP server)... but cumbersome ... I am not sure if enough answer shall be A or D
 source - any IOS , IIS-XE, NX-OS ... DHCP snooping config guide ... <https://www.cisco.com/c/en/us/td/docs/dcn/nx-os/nexus3548/103x/configuration/security/cisco-nexus-3548-nx-os-security-configuration-guide-103x/m-configuring-dhcp-snooping.pdf>
 upvoted 1 times

4pelos 6 months, 1 week ago

Correct answer A
 Checked with securitytut
 upvoted 1 times

xziomal9 10 months ago

Selected Answer: C

Answer C
upvoted 1 times



  **kvothe86** 1 year ago

Answer is not A, I know because this is one of my few mistakes a couple of days ago. Admin, if you are reading this please provide the correct answer and I ask you not to post this comment
upvoted 1 times

  **Cokamaniako** 1 year, 2 months ago

Aswer A

The DHCP snooping feature determines whether traffic sources are trusted or untrusted. An untrusted source may initiate traffic attacks or other hostile actions. To prevent such attacks, the DHCP snooping feature filters messages and rate-limits traffic from untrusted sources.
upvoted 1 times

  **BoxX** 1 year, 2 months ago

Vote for A

Ensure that legitimate requests are not dropped (without trusted interface the traffic is dropped). This will also satisfy the request "able to rate-limit the traffic". "Able to", meaning it can be configured.
upvoted 2 times



  **Bandito** 1 year, 3 months ago

ARP inspection rate-limits ARP packets, not DHCP requests. I vote for A
upvoted 1 times



  **gc999** 1 year, 3 months ago

Selected Answer: A

I choose "A". The question said "An administrator is configuring a DHCP server", the DHCP server is a new setup, so it should not have trust interface before, we need to setup it once the DHCP server is newly installed.
upvoted 2 times

  **gc999** 1 year, 3 months ago

Finally, I choose "C". The rate limiting would not be enabled by default when ip dhcp snooping is configured. However, it will be enabled on untrust interface once the arp inspection is enabled.
upvoted 1 times

  **gc999** 1 year, 3 months ago

Please refer to this video at 13:22
https://www.youtube.com/watch?v=HwbTKalvL6s&ab_channel=Jeremy%27sITLab
upvoted 1 times

  **Jessie45785** 1 year, 3 months ago

Selected Answer: C

DHCP snooping has no default rate limit



<https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/12-2SXF/native/configuration/guide/swcg/snoodhcp.pdf>

hence only C make sense
upvoted 1 times

  **Dorr20** 1 year, 4 months ago

Selected Answer: C



As zheka said, answer is C
upvoted 1 times

  **angry** 1 year, 6 months ago

D is the correct answer!
A enable trust on the interface connected to the DHCP server. the trust statement has nothng to do with rate limit!
C is also not correct! you can't set rate limit on ARP inspection.
But with D,
Switch(config-if)#ip dhcp snooping limit rate ?
<1-2048> DHCP snooping rate limit
Switch(config-if)#ip dhcp snooping limit rate
upvoted 1 times



  **Totosos1** 1 year, 5 months ago

D is saying to add entries in the DHCP Snooping DB, you're statement is for setting the rate limit? It's still not clear what the answer is here!
upvoted 1 times

  **psuoh** 1 year, 7 months ago

Selected Answer: C

Answer is C
upvoted 1 times

  **psuoh** 1 year, 7 months ago


Answer is C

Setting a trusted interface is setting rate limit to unlimited so A is wrong.

DAI performs validation checks in the CPU, so the number of incoming ARP packets is rate-limited to prevent a denial of service attack. By default, the rate for untrusted interfaces is set to 15 packets per second, whereas trusted interfaces have no rate limit.

<https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/12-2/25ew/configuration/guide/conf/dynarp.html#75013>

upvoted 1 times

  **Emlia1** 1 year, 9 months ago

Selected Answer: A

A is correct

upvoted 4 times

  **Jamesy** 1 year, 11 months ago

A is the correct answer. Cheers

upvoted 3 times

  **GOD_ELESTAR** 2 years, 2 months ago

A is correct

(config-if)#ip dhcp snooping limit rate ?

<1-2048> DHCP snooping rate limit

upvoted 3 times

What is a prerequisite when integrating a Cisco ISE server and an AD domain?

- A. Configure a common administrator account.
- B. Place the Cisco ISE server and the AD server in the same subnet.
- C. Synchronize the clocks of the Cisco ISE server and the AD server.
- D. Configure a common DNS server.

Correct Answer: C

Reference:

<https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/215233-identity-service-engine-ise-and-active.html#anc1>

Community vote distribution

C (100%)

Marshpillowz 5 months, 1 week ago

Selected Answer: C

C is correct

upvoted 1 times

F0rtyx40 1 year, 3 months ago

This is a tricky one because DNS records are also crucial, A will break more functionality for sure.

upvoted 1 times

F0rtyx40 1 year, 3 months ago

I mean C *

upvoted 1 times

sis_net_sec 1 year, 11 months ago

C is correct answer

The following are the prerequisites to integrate Active Directory with Cisco ISE. + Use the Network Time Protocol (NTP) server settings to synchronize the time between the Cisco ISE server and Active Directory. You can configure NTP settings from Cisco ISE CLI. + If your Active Directory structure has multidomain forest or is divided into multiple forests, ensure that

Get Latest & Actual 350-701 Exam's Question and Answers from Passleader.

<http://www.passleader.com>

99

trust relationships exist between the domain to which Cisco ISE is connected and the other domains that have user and machine information to which you need access. For more information on establishing trust relationships, refer to Microsoft Active Directory documentation. + You must have at least one global catalog server operational and accessible by Cisco ISE, in the domain to which you are joining Cisco ISE.

Reference: [https://www.cisco.com/c/en/us/td/docs/security/ise/2-](https://www.cisco.com/c/en/us/td/docs/security/ise/2-0/ise_active_directory_integration/b_ISE_AD_integration_2x.html#reference_8DC463597A644A5C9CF5D582B77BB24F)

[0/ise_active_directory_integration/b_ISE_AD_integration_2x.html#reference_8DC463597A644A5C9CF5D582B77BB24F](https://www.cisco.com/c/en/us/td/docs/security/ise/2-0/ise_active_directory_integration/b_ISE_AD_integration_2x.html#reference_8DC463597A644A5C9CF5D582B77BB24F)

upvoted 2 times

harvey227 2 years, 1 month ago

Answer is C. Otherwise you may get Kerberos Auth errors due to clock skew

upvoted 3 times

When configuring ISAKMP for IKEv1 Phase 1 on a Cisco IOS router, an administrator needs to input the command `crypto isakmp key cisco address 0.0.0.0`.

The administrator is not sure what the IP address in this command is used for. What would be the effect of changing the IP address from 0.0.0.0 to 1.2.3.4?

- A. The key server that is managing the keys for the connection will be at 1.2.3.4.
- B. The address that will be used as the crypto validation authority.
- C. All IP addresses other than 1.2.3.4 will be allowed.
- D. The remote connection will only be allowed from 1.2.3.4.

Correct Answer: D

  **illwill** 9 months, 1 week ago

"D" is the correct answer because mask is optional and only needed if the peer device is using the mask command.

(Optional) Specify the subnet address of the remote peer. (The argument can be used only if the remote peer ISAKMP identity was set with its IP address.)



https://www.cisco.com/c/en/us/td/docs/ios/12_2/security/command/reference/srfike.html#wp1017897

upvoted 1 times

  **gondohwe** 1 year, 3 months ago

the command "crypto isakmp key xxxx address x.x.x.x " is used to specify the shared secret and the peer is expected at the other end of the connecton.....so D is the right choice

upvoted 2 times

  **Anonymous983475** 1 year, 7 months ago

I think none of the answers are correct or the question itself is wrong.

If you do not add a subnet mask at the end of the command the default class is assumed.

The default class for 1.2.3.4 is class A, which has mask 255.0.0.0 or 8 bits.

This means that all addresses from the 1.0.0.0/8 network will be accepted for authentication with that key.

upvoted 3 times

A network administrator is configuring SNMPv3 on a new router. The users have already been created, however an additional configuration is needed to facilitate access to the SNMP views. What must the administrator do to accomplish this?

- A. define the encryption algorithm to be used by SNMPv3
- B. set the password to be used for SNMPv3 authentication
- C. map SNMPv3 users to SNMP views
- D. specify the UDP port used by SNMP

Correct Answer: C

Community vote distribution

C (83%) B (17%)

kornman Highly Voted 3 years, 2 months ago

I think the correct answer is C - <https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/snmp/configuration/x3e/snmp-x3e-book/nm-snmp-snmpv3-comm-supp.html>
upvoted 14 times

jaciro11 2 years, 10 months ago

<https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/snmp/configuration/15-e/snmp-15-e-book.pdf> C is true
upvoted 2 times

thetaken Highly Voted 3 years, 1 month ago

It looks like none of the options given make sense: A and B are part of the user creation command, C does not make any sense since views can be assigned to groups, not users and D is wrong because it only makes sense if a SNMP host is being configured.
upvoted 6 times

bobie Most Recent 1 year, 3 months ago

Selected Answer: B

I'll go with B because I believe the user is using the noAuth command.

The following example shows how to configure a remote user to receive traps at the "noAuthNoPriv" security level when the SNMPv3 security model is enabled:

```
Device(config)# snmp-server group group1 v3 noauth
Device(config)# snmp-server user remoteuser1 group1 remote 10.12.8.4
Device(config)# snmp-server host 10.12.8.4 informs version 3 noauth remoteuser config
```

upvoted 1 times

psuoh 1 year, 7 months ago

Selected Answer: C

<https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/snmp/configuration/x3e/snmp-x3e-book/nm-snmp-snmpv3-comm-supp.html>
upvoted 1 times

sis_net_sec 1 year, 11 months ago

Yes Tjhe correct Answer is C
<https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/snmp/configuration/15-e/snmp-15-e-book.pdf>
upvoted 1 times

nomanlands 2 years, 2 months ago

Selected Answer: C

"however an additional configuration is needed to facilitate access to the SNMP views" Need to give the user or groups access to the view
upvoted 1 times

surforlife 2 years, 2 months ago

"B"
For requests to be authenticated, the manager and the agent must share knowledge of the authentication password associated with the username. For requests to be encrypted, the manager and the agent must additionally share knowledge of the privacy password associated with the username.
upvoted 1 times

haiderzaid 1 year, 5 months ago

setting the password for SNMPv3 authentication is also a required step in configuring SNMPv3, but it is not directly related to facilitating access to SNMP views,
upvoted 1 times

- surforlife** 2 years, 2 months ago
"B" The secure management of SNMPv3 is an important enabling technology for safe configuration and control operations. SNMPv3 provides security with authentication and privacy, and its administration offers logical contexts, view-based access control, and remote configuration.
upvoted 1 times
- killbots** 2 years, 4 months ago
Selected Answer: C
I agree with C. You can assign users or groups to views
upvoted 3 times
- semi1750** 2 years, 5 months ago
agreed with C according to the following link:

"specify what View we want associated with this Group"
<https://www.cbttuggets.com/blog/technology/networking/how-to-configure-snmpv3-and-how-it-works>

Answer D is for server engine ID.
Answer A and B are part of user configuration
upvoted 2 times
- denverfly** 2 years, 7 months ago
It is A
• 2.8 Configure secure network management of perimeter security and infrastructure devices (secure device management, SNMPv3, views, groups, users, authentication, and encryption, secure logging, and NTP with authentication)
upvoted 2 times
- zheka** 2 years, 9 months ago
Agree with C, here's what Cisco document says about it:
To configure a Simple Network Management Protocol Version 3 (SNMPv3) server user, specify an SNMP group or a table that maps SNMPv3 users to SNMP views.
upvoted 1 times
- coentror** 2 years, 9 months ago
It is C, on Cisco site:
"To configure a Simple Network Management Protocol Version 3 (SNMPv3) server user, specify an SNMP group or a table that maps SNMPv3 users to SNMP views."
upvoted 1 times
- u777** 3 years ago
The question is what is SNMP v3 according to Cisco (table 3):
The SNMP Version 3 feature is used to provide secure access to devices by authenticating and encrypting data packets over the network.
<https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/snmp/configuration/xe-3se/5700/snmp-xe-3se-5700-book/nm-snmp-snmpv3.pdf>
Then we need to provide SNMP Priv mode with both authentication and encryption, that is answer A+B. or only A if we consider the authentication is already provided.
upvoted 1 times
- kerniger** 3 years ago
I think you have to configure a view to be able to configure a group. You need a group to be able to configure a user. The PW and encryption is set while creating the user.
So if the user is already created, a group and a view is also created.
This leaves me with D which makes me not happy.
upvoted 1 times
- Reece_S** 3 years, 1 month ago
This question is too vague to properly answer. When you create the user, you assign them to the group and this provides access to the view. C would be plausible if you mapped users to views but you don't map users to views, you assign users to groups which provides access to views. The group and user option would be enough in a NoAuth model. The answer wording is questionable C but it could be the answer based on NoAuth.

Since we don't know the model that is being used. It's hard to say. With AuthNoPriv you would need the auth password. With AuthPriv you would need both the auth password and encryption. However in no case would just the encryption be enough by itself to allow access. For A to be correct, we'd have to assume that the user has been assigned to the group and that the auth password is correct.
upvoted 1 times
- Reece_S** 3 years, 1 month ago
Correction. C Could not be the answer at all. The question clearly states that the user has been created. The user is assigned to a group when the command is entered to create the user. Views are provided based on the group.
upvoted 1 times
- klu16** 3 years ago
Yeah, vague... But I would go with option B here.
upvoted 2 times
- Moll** 2 years, 9 months ago

Agree with B

Configuring SNMP Version 3

When you configure SNMPv3 and you want to use the SNMPv3 security mechanism for handling SNMP packets, you must establish SNMP groups and users with passwords.

SNMPv3 is a security model. A security model is an authentication strategy that is set up for a user and the group in which the user resides.

No default values exist for authentication or privacy algorithms when you configure the snmp-server group command. Also, no default passwords exist.

<https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/snmp/configuration/12-4t/snmp-12-4t-book/nm-snmp-cfg-snmp-support.html>

upvoted 2 times

DRAG DROP -

Drag and drop the NetFlow export formats from the left onto the descriptions on the right.

Select and Place:

Version 1	appropriate only for legacy systems
Version 5	appropriate only for the main cache
Version 8	introduced extensibility
Version 9	introduced support for aggregation caches

Correct Answer:

Version 1	Version 1
Version 5	Version 5
Version 8	Version 9
Version 9	Version 8

Reference:

<https://www.ciscolive.com/c/dam/r/ciscolive/emea/docs/2015/pdf/BRKNMS-3132.pdf>

  **Laryoul** Highly Voted  2 years, 8 months ago

Version 1 is for legacy systems

Version 5 export format is suitable only for the main cache

Version 8 export format is available only for aggregation caches

Version 9 the format is extensible

<https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/netflow/configuration/15-mt/nf-15-mt-book/cfg-nflow-data-expt.html>

upvoted 9 times

  **ddev3737** Most Recent  1 year, 7 months ago

so version 9 introduced extensibility indeed

upvoted 1 times

  **ddev3737** 1 year, 7 months ago

Version 9

You need to export data from various technologies, such as Multicast, DoS, IPv6, and BGP next hop. This format accommodates new NetFlow-supported technologies such as Multicast, MPLS, and BGP next hop.

The Version 9 export format supports export from the main cache and from aggregation caches.

Version 8

You need to export data from aggregation caches. The Version 8 export format is available only for export from aggregation caches.

Version 5

You need to export data from the NetFlow main cache, and you are not planning to support new features.

Version 5 export format does not support export from aggregation caches.

Version 1

You need to export data to a legacy collection system that requires Version 1 export format. Otherwise, do not use Version 1 export format. Use Version 9 or Version 5 export format.

upvoted 1 times

Edit AnyConnect Connection Profile: DefaultRAGroup

Basic

- Advanced
 - General
 - Client Addressing
 - Authentication
 - Secondary Authentication
 - Authorization
 - Accounting
 - Group Alias/Group URL

Name: DefaultRAGroup

Aliases:

Authentication

Method: AAA

AAA Server Group: LOCAL **Manage...**

Use LOCAL if Server Group fails

SAML Identity Provider

SAML Server: --- None --- **Manage...**

Client Address Assignment

DHCP Servers:

None DHCP Link DHCP Subnet

Client Address Pools: **Select...**

Client IPv6 Address Pools: **Select...**

Default Group Policy

Group Policy: DfitGrpPolicy **Manage...**

(Following fields are linked to attribute of the group policy selected above.)

Enable SSL VPN client protocol

Enable IPsec(IKEv2) client protocol

DNS Servers:

WINS Servers:

Domain Name:

Find:

Next **Previous**

OK **Cancel** **Help**

Refer to the exhibit. When configuring a remote access VPN solution terminating on the Cisco ASA, an administrator would like to utilize an external token authentication mechanism in conjunction with AAA authentication using machine certificates. Which configuration item must be modified to allow this?

- A. Method
- B. SAML Server
- C. AAA Server Group
- D. Group Policy

Correct Answer: C

Community vote distribution

A (83%) C (17%)

aalman Highly Voted 3 years, 2 months ago

C - is correct. Method (A) is already specified in the question if you read it closely. It wants external tokens when the configuration is set to local. C is what needs to be changed.

upvoted 9 times

Reece_S **Highly Voted** 3 years, 1 month ago

AAA server group is correct. It's looking for what to use in conjunction with AAA. The method is already selected. Most likely you will change the "local" under server group to "ldap" to use AD for authentication rather than local creds defined on the ASA.

upvoted 9 times

Reece_S 3 years, 1 month ago

Yea its method. I re-read the question. It wants to use local & another method. So you'll need to select Both in the drop-down.

upvoted 7 times

Premium_Pils **Most Recent** 1 month ago

Selected Answer: C

C - AAA method is already set, but "local" needs to be changed - as mentioned below

upvoted 1 times

xziomal9 10 months, 1 week ago

Answer A

upvoted 1 times

862e76c 10 months, 1 week ago

Selected Answer: A

Method offers following options to select:

- AAA
- AAA and certificate
- Certificate only
- SAML
- Multiple certificates and AAA
- Multiple certificates

In order to utilize an external token authentication mechanism in conjunction with AAA authentication using machine certificates you must change the method to "AAA and certificate". Answer is A = Method.

upvoted 4 times

Rockbo47 1 week, 2 days ago

Correct, a lot of people are overlooking the fact that it states "utilize an external token authentication mechanism in conjunction with AAA authentication USING MACHINE CERTIFICATES"

upvoted 1 times

rishard 1 year, 2 months ago

Thx @psuoh for the YT link.

Answer A it is - Method.

upvoted 1 times

Jessie45785 1 year, 3 months ago

Selected Answer: C

C - to my understanding secondary authentication tokens are configured under sever groups:

https://kb.swivelsecure.com/w/index.php/Cisco_AnyConnect

upvoted 2 times

majster88 1 year, 3 months ago

Selected Answer: A

The key here is "conjunction with AAA authentication using machine certificates". To use machine certificate as authentication method we need to change Method from AAA to AAA + certificate as a first step. Then we need to create AAA group of type RADIUS/SDI (depends of integration type with Token solution) and change the AAA server group from LOCAL to group we created as the second step. Actually both A and C are correct, but A needs to be first.

upvoted 2 times

webwalker00 1 year, 4 months ago

Selected Answer: A

It is A, the Method dictates what security mechanism to use, aaa server group defines those mechanisms.

upvoted 1 times

YooAndl 1 year, 4 months ago

A. Method - In order to use AAA along with an external token authentication mechanism, set the Method as "Both" in the Authentication. We don't just use AAA in this case.

upvoted 1 times

bmayer 1 year, 7 months ago

Selected Answer: A

The correct answer is A- Method. Select method then from the drop down then select AAA and Certificates option.



upvoted 4 times

Jamesy 1 year, 7 months ago

Hi Guys, appreciate all your answers.

Question says "an administrator would like to utilize an external token authentication mechanism in conjunction with AAA authentication" which is the Method we all know! I think they are asking next in the configuration -> AAA Server Group options. Hope this helps. Thanks

upvoted 1 times

  **psuoh** 1 year, 7 months ago

Selected Answer: A

<https://i.imgur.com/sdfzVeC.png>

<https://www.youtube.com/watch?v=Er5toSsbM8I>

upvoted 5 times

  **Emlia1** 1 year, 9 months ago

Selected Answer: A

It should be A

upvoted 2 times

  **sis_net_sec** 1 year, 10 months ago

Selected Answer: A

<https://www.cisco.com/c/en/us/support/docs/security/anyconnect-secure-mobility-client-v4x/212483-configure-asa-as-the-ssl-gateway-for-any.html>

upvoted 2 times

  **Random000** 1 year, 11 months ago

Selected Answer: A

Must be method based on the documentation.

upvoted 2 times

  **Bortus2022** 1 year, 12 months ago

C is correct:

When configuring a remote access VPN solution terminating on the Cisco ASA, an administrator would like to utilize an external token authentication

upvoted 1 times

An administrator is trying to determine which applications are being used in the network but does not want the network devices to send metadata to Cisco Firepower. Which feature should be used to accomplish this?

- A. Network Discovery
- B. Access Control
- C. Packet Tracer
- D. NetFlow

Correct Answer: D

Community vote distribution

A (100%)

[-] **👤 Raajaa** **Highly Voted** 👍 3 years, 2 months ago

A is the answer as the Q specifies without using metadata
upvoted 8 times

[-] **👤 xziomal9** **Most Recent** 🕒 10 months, 1 week ago

Answer A
upvoted 1 times

[-] **👤 KPzee** 1 year, 5 months ago

It cannot be D as Netflow is concerned with metadata.
upvoted 2 times

[-] **👤 Emlia1** 1 year, 9 months ago

I prefer A
upvoted 1 times

[-] **👤 sis_net_sec** 1 year, 11 months ago

Selected Answer: A

https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Network_Discovery_Policies.html
The network discovery policy has a single default rule in place, configured to discover applications from all observed traffic. The rule does not exclude any networks, zones, or ports, host and user discovery is not configured, and the rule is not configured to monitor a NetFlow exporter. This policy is deployed by default to any managed devices when they are registered to the Firepower Management Center. To begin collecting host or user data, you must add or modify discovery rules and re-deploy the policy to a device.
upvoted 2 times

[-] **👤 francojaraba** 2 years, 1 month ago

Selected Answer: A

As long the questions indicates that no metada is required the answer is A -
<https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/enterprise-network-security/white-paper-c11-736595.html>
Netflow are based on metadata - <https://learning.oreilly.com/library/view/ccna-cyber-ops/9780134608938/ch04.html#ch04lev1sec1>
upvoted 4 times

[-] **👤 networkexpert** 2 years, 4 months ago

Selected Answer: A

I am eliminating D
upvoted 1 times

[-] **👤 semi1750** 2 years, 5 months ago

Selected Answer: A

Opt for A.
Cisco doc says Applications can be discovered by "non-NetFlow discovery rules" without Option D

You can disable detection of application protocols in discovery rules configured to monitor NetFlow exporters, but not in discovery rules configured to monitor Firepower System managed devices. If you enable host or user discovery in non-NetFlow discovery rules, applications are automatically discovered.

https://www.cisco.com/c/en/us/td/docs/security/firepower/630/configuration/guide/fpmc-config-guide-v63/working_with_discovery_events.html
upvoted 3 times

[-] **👤 pohqinan** 2 years, 6 months ago

keyword network devices = switch / router therefore netflow. Network Discover usually is PC client send out
upvoted 2 times

  **NikoNiko** 2 years, 1 month ago

"determine which applications" are running... and "does NOT want the network devices to send metadata to Cisco Firepower"

Correct answer is Network Discovery - a Firepower feature, which fingerprints devices and applications in LAN by their communication parameters.

upvoted 2 times



  **Floki_viking7** 2 years, 6 months ago

An Overview of the NetFlow Protocol:

NetFlow is a protocol used to collect metadata on IP traffic flows traversing a network device.

Developed by Cisco Systems, NetFlow is used to record metadata about IP traffic flows traversing a network device such as a router, switch, or host

upvoted 1 times

  **zheka** 2 years, 9 months ago

Someone below gave an example that Netflow operates with metadata and if we don't want to send them to Cisco FMC then we need to select Netflow as the answer, simple as 123. And yes, you can discover applications by network discoveries by Firepower. Just checked in real production environment

upvoted 1 times

  **zeroC00L** 2 years, 11 months ago

i would go with A here. Because the Network Discovery feature on the FMC/FTD/Firepower stuff works like a passive monitor. The Firewalls are looking into the traffic which is passing through them and use the information they get from there to build up host information you can view from within FMC. So there is no need to send (active do something) metadata the firewalls can get this passively by using network discovery policy.

upvoted 1 times

  **kapplejacks** 2 years, 11 months ago

Correct answer is A:

Question asks for "Firepower", I wish they would specify but I believe they are referring to ASA with firePOWER not FTD. If they say Firepower, cisco usually also includes Threat Defense so its for the ASA.

The ASA does know about are on the network using network discovery and can be view in ASDM without (also a key, the question asks "but does not want to send metadata") so it has to be network discovery

upvoted 2 times

  **kapplejacks** 2 years, 11 months ago

Also its called FireSight, it enables you to see HTTP related info or basically application traffic in a GUI connected to your ASA.

FireSight.

upvoted 1 times

  **Sarbi** 3 years ago

I think the answer is A. As Netflow used metedata to analyse the flow.

Rather than always relying on full packet capture, protocols like NetFlow and IPFIX can generate valuable metadata for less-intensive network monitoring. This metadata is similar to how your phone bill shows your calls, displaying the source, destination and volume rather than showing the actual content of the conversations. With this information, you can gain useful insights at a lower impact on your network management strategy. But which approach or metadata protocol is right for your network monitoring needs?

upvoted 1 times

  **kerniger** 3 years ago

I think A is not true because its based on metadata from firepower by default

With NetFlow you can detect applications without metadata at firepower.

upvoted 1 times

  **zap_pap** 3 years, 1 month ago

- A

"The network discovery policy has a single default rule in place, configured to discover applications from all observed traffic."

https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Network_Discovery_Policies.html

upvoted 3 times

  **Pwned** 2 years, 3 months ago


This is correct!!

upvoted 1 times

  **statikd** 3 years, 2 months ago

The answer is D Netflow. Netflow can be used to see what apps are being used on the network. Network Discovery is used to discover devices on the network.

upvoted 2 times

  **Dinges** 3 years, 2 months ago

NDP is a protocol that discovers devices, but I don't think that's what they are talking about here.

I think they are talking about Firepower Network Discovery function.

https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Network_Discovery_Policies.html

upvoted 1 times

An engineer is implementing NTP authentication within their network and has configured both the client and server devices with the command `ntp authentication-key 1 md5 Cisc392481137`. The server at 1.1.1.1 is attempting to authenticate to the client at 1.1.1.2, however is unable to do so. Which command is required to enable the client to accept the server's authentication key?

- A. `ntp server 1.1.1.2 key 1`
- B. `ntp peer 1.1.1.2 key 1`
- C. `ntp server 1.1.1.1 key 1`
- D. `ntp peer 1.1.1.1 key 1`

Correct Answer: C

Reference:

<https://www.oreilly.com/library/view/cisco-ios-cookbook/0596527225/ch14s13.html>

Community vote distribution

C (71%)

A (29%)

[-] **SulSulEi** 2 years ago

Answer is C according to the below link,

<https://www.oreilly.com/library/view/cisco-ios-cookbook/0596527225/ch14s13.html>

upvoted 4 times

[-] **killbots** 2 years, 4 months ago

Selected Answer: C

server is at 1.1.1.1 so on the client you need to specify the Server IP.

upvoted 4 times

[-] **Kyle1776** 2 years, 6 months ago

Selected Answer: C

For the client to be enabled it needs the server and the key. Answer C would be the command configured on the client to enable NTP to the server.

upvoted 3 times

[-] **u0815** 2 years, 7 months ago

Selected Answer: C

"to enable the client"

upvoted 3 times

[-] **Jetnor** 2 years, 8 months ago

Selected Answer: A

Actually the question says 1.1.1.1 wants to authenticate to 1.1.1.2:

the server at 1.1.1.1 is attempting to authenticate to the client at 1.1.1.2, however is unable to do so. Which command is required to enable the client to accept the server's authentication key?

so config should be done on server side.

Answer is A

upvoted 4 times

[-] **Jetnor** 2 years, 8 months ago

My Bad:

Which command is required to enable the client to accept the server's authentication key?

it says which command on the Client so its C.

upvoted 4 times

[-] **bob511** 2 years, 6 months ago

it actually says "Which command is required to enable the client to accept the server's authentication key?" the important part is "to enable the (client to accept) the (server's authentication)" which indicates the command is coming from the server to the client the answer is A

upvoted 1 times

[-] **Moll** 2 years, 9 months ago

Agree, correct answer is C

upvoted 4 times

Due to a traffic storm on the network, two interfaces were error-disabled, and both interfaces sent SNMP traps. Which two actions must be taken to ensure that interfaces are put back into service? (Choose two.)

- A. Enable the snmp-server enable traps command and wait 300 seconds.
- B. Use EEM to have the ports return to service automatically in less than 300 seconds
- C. Ensure that interfaces are configured with the error-disable detection and recovery feature.
- D. Have Cisco Prime Infrastructure issue an SNMP set command to re-enable the ports after the preconfigured interval.
- E. Enter the shutdown and no shutdown commands on the interfaces.

Correct Answer: CE

Community vote distribution

CE (100%)

LTLnetworker 8 months ago

EEM is a possible method too
upvoted 2 times

Premium_Pils 1 month ago

Yes, I agree. Probably, Cisco want us to select more specific answers. EEM is part of ccnp R&S (encore+enarsi), but not ccnp security.
upvoted 1 times

Felice44 1 year, 6 months ago

Selected Answer: CE

<https://www.cisco.com/c/en/us/support/docs/lan-switching/spanning-tree-protocol/69980-errdisable-recovery.html#anc13>

"After you fix the root problem, the ports are still disabled if you have not configured errdisable recovery on the switch. In this case, you must reenble the ports manually. Issue the shutdown command and then the no shutdown interface mode command on the associated interface in order to manually reenble the ports.

The errdisable recovery command allows you to choose the type of errors that automatically reenble the ports after a specified amount of time. The show errdisable recovery command shows the default error-disable recovery state for all the possible conditions."

upvoted 2 times

Add Device ? X

Host:†

Display Name:

Registration Key:*

Group: ▼

Access Control Policy:* ▼

Smart Licensing

Malware:

Threat:

URL Filtering:

Advanced

Unique NAT ID:†

Transfer Packets:

On Firepower Threat Defense devices version 6.2.1 onwards, AnyConnect VPN licenses can be enabled from [smart license page](#)

Refer to the exhibit. An administrator is adding a new Cisco FTD device to their network and wants to manage it with Cisco FMC. The Cisco FTD uses a registration key of Cisc392481137 and is not behind a NAT device. Which command is needed to enable this on the Cisco FTD?

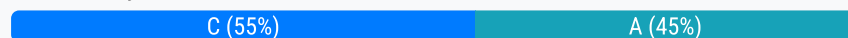
- A. configure manager add <FMC IP address> <registration key> 16
- B. configure manager add DONTRESOLVE <registration key> FTD123
- C. configure manager add <FMC IP address> <registration key>
- D. configure manager add DONTRESOLVE <registration key>

Correct Answer: C

Reference:

https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-config-guide-v62/firepower_command_line_reference.html#ID-2201-000004b4

Community vote distribution



Luc_10 Highly Voted 3 years, 2 months ago

I think the correct answer is C, as this is stated in the Official Cert Guide:

"When you add a managed device to the Cisco FMC, you must provide an IP addresses of the managed device along with a registration key for authentication. The Cisco FMC and the managed device use the registration key and a NAT ID (instead of IP addresses in the case that the device is behind NAT) to authenticate and authorize for initial registration."

But in this case is not behind a NAT, so...C

upvoted 13 times

BennyTheK Highly Voted 3 years, 1 month ago

The answer is C.



A is wrong (would need DONTRESOLVE to work in case on NAT device between FTD and FMC)

B is wrong (would need 16 instead of FTD123, again in case on NAT device between FTD and FMC)

C is correct:)

D is wrong, DONTRESOLVE, KEY & NAT_ID is needed (again in case on NAT device between FTD and FMC)

upvoted 13 times

  **klu16** 3 years ago
Indeed! My vote also for option C ;)
upvoted 4 times

  **XvidalX** Most Recent 6 months, 1 week ago



Selected Answer: A

If you used a NAT ID during device setup, expand in the Advanced section and enter the same NAT ID in the Unique NAT ID field."
upvoted 2 times

  **LTLnetworker** 7 months, 3 weeks ago



Selected Answer: A

FMC 6.6 guide: "If you used a NAT ID during device setup, expand in the Advanced section and enter the same NAT ID in the Unique NAT ID field."
upvoted 3 times

  **MPoels** 6 months, 1 week ago



Correct (A), see https://www.cisco.com/c/en/us/td/docs/security/firepower/660/configuration/guide/fpmc-config-guide-v66/device_management_basics.html#ID-2242-0000069d

upvoted 1 times

  **XvidalX** 6 months, 1 week ago

super agree

upvoted 1 times

  **Ko13** 10 months, 1 week ago

Selected Answer: A



A is correct, I worked with FTDs for a long time, even if there is no Nat device in between, if you use NAT ID on one side then you have to use it on the other side too, the exhibit has nat ID 16 on it so the FTD's command has to match it.

upvoted 4 times

  **KnackerTopf1** 9 months, 1 week ago

i have tried this out in gns3, he's right, when specifying a nat id in the fmc, the nat id has to match on the device as well, otherwise it wont be able to communicate



upvoted 4 times

  **psuoh** 1 year, 7 months ago

Selected Answer: C

Answer is C



upvoted 2 times

  **psuoh** 1 year, 7 months ago

Selected Answer: C

https://w_w_w.youtube.com/watch?v=v_uZ9GbICBk

upvoted 1 times



  **psuoh** 1 year, 7 months ago

Selected Answer: C

<https://i.imgur.com/LdBgjED.png>

https://www.youtube.com/watch?v=v_uZ9GbICBk

upvoted 1 times



  **psuoh** 1 year, 7 months ago

Selected Answer: C

https://www.youtube.com/watch?v=v_uZ9GbICBk


<https://i.imgur.com/LdBgjED.png>

upvoted 1 times

  **harvey227** 2 years, 1 month ago

C is correct answer. You don't need DONOTRESOLVE unless you are behind a NAT device. You need the NATID number.

upvoted 1 times

  **mecacig953** 2 years, 5 months ago

Selected Answer: C

Syntax

configure manager add {hostname | IPv4_address | IPv6_address | DONTRESOLVE} regkey [nat_id]



where {hostname | IPv4_address | IPv6_address | DONTRESOLVE} specifies the DNS host name or IP address (IPv4 or IPv6) of the Firepower Management Center that manages this device. If the Firepower Management Center is not directly addressable, use DONTRESOLVE. If you use DONTRESOLVE, nat_id is required. regkey is the unique alphanumeric registration key required to register a device to the Firepower Management Center. nat_id is an optional alphanumeric string used during the registration process between the Firepower Management Center and the device. It is required if the hostname is set to DONTRESOLVE.

upvoted 1 times

  **brownbear505** 2 years, 6 months ago



Selected Answer: C

Firepower Management Center Configuration Guide, Version 6.1 - Device Management Basics [Cisco Firepower Management Center] - Cisco
upvoted 1 times

  **u0815** 2 years, 7 months ago

Selected Answer: C

100%, did it myself
upvoted 3 times

  **u0815** 2 years, 7 months ago

Selected Answer: C

see Luc and all others
upvoted 1 times

  **NullNull88** 2 years, 9 months ago

C is the correct answer ,...unless your FMC's IP address is "DONTRESOLVE" which makes zero sense at all and the questions says it is not behind NAT
upvoted 1 times

  **Dead_Adriano** 3 years, 1 month ago

The answer is most probably C although it's not clear when NAT ID is specified in FMC options.
Regarding A: IP address + NAT ID can be specified on FTD in 2 cases: when FTD itself is behind NAT or when it's not but this is just another option to register device. But in both those cases IP of the device should be blank in FMC. This is explained here:
<https://www.cisco.com/c/en/us/td/docs/security/firepower/misc/fmc-ftd-mgmt-nw/fmc-ftd-mgmt-nw.html#ID-2242-00000191>
upvoted 1 times

  **Moll** 2 years, 9 months ago

If the FMC is behind a NAT device, enter a unique NAT ID along with the registration key, and specify DONTRESOLVE instead of the hostname, for example:

Example:

```
> configure manager add DONTRESOLVE regk3y78 natid90
```

If the FTD is behind a NAT device, enter a unique NAT ID along with the FMC IP address or hostname, for example:

Example:

```
> configure manager add 10.70.45.5 regk3y78 natid56
```

<https://www.cisco.com/c/en/us/td/docs/security/firepower/misc/fmc-ftd-mgmt-nw/fmc-ftd-mgmt-nw.html#ID-2242-00000191> same link

upvoted 1 times

  **Dead_Adriano** 3 years, 1 month ago

Funny thing is that the question says "F_T_D is not behind NAT", although DONTRESOLVE should be used when F_M_C is NATted.
But anyway DONTRESOLVE must be used with nat_id, and there is no such answer here.

upvoted 3 times

A network administrator needs to find out what assets currently exist on the network. Third-party systems need to be able to feed host data into Cisco Firepower.

What must be configured to accomplish this?

- A. a Network Analysis policy to receive NetFlow data from the host
- B. a File Analysis policy to send file data into Cisco Firepower
- C. a Network Discovery policy to receive data from the host
- D. a Threat Intelligence policy to download the data from the host

Correct Answer: C

  **abdulmalik_mail** Highly Voted 2 years, 8 months ago

It's C, https://www.cisco.com/c/en/us/td/docs/security/firepower/623/configuration/guide/fpmc-config-guide-v623/network_discovery_policies.html
upvoted 5 times

  **NikoNiko** 2 years, 1 month ago

yes, C is correct.

From your link (and from my practice):

"The network discovery policy on the Firepower Management Center controls how the system collects data on your organization's network assets and which network segments and ports are monitored.

...

You can also add sources for host input and NetFlow exporters to monitor." - i. e. data from external devices.

upvoted 2 times

  **iluvmicrosoft** Most Recent 5 months ago

statement 1, statement 2, what must be configured to accomplish this?? not these??



assets on the network = Network Discovery Policy

third party systems feed FMC = Threat Intelligence Director

horrible questions imo..

I do think the answer is C however, because even if we were using Threat Intelligence Director.. the feed wouldn't be from the "host"

upvoted 2 times

  **flejd** 2 years, 8 months ago

its D. Network Discovery is a passive mechanism. You want data from third party ? use TiD

upvoted 2 times

  **pr0fectus** 2 years, 8 months ago

We are looking for "assets" on the network. TID is used for threat feeds not discovering assets on the network.

upvoted 4 times

Which suspicious pattern enables the Cisco Tetration platform to learn the normal behavior of users?

- A. file access from a different user
- B. user login suspicious behavior
- C. privilege escalation
- D. interesting file access

Correct Answer: A

Community vote distribution

A (100%)

dzef13 Highly Voted 3 years, 3 months ago

should be A
upvoted 12 times

networkexpert Highly Voted 2 years, 4 months ago

Please, see Drag and Drop question 110 as well.
so it should be A
upvoted 6 times

Jessie45785 1 year, 4 months ago

Agree as weird that question is , A indeed is a right answer
upvoted 1 times

Jessie45785 Most Recent 1 year, 4 months ago

Selected Answer: A

networkexpert 12 months ago - gets a point:

Please, see Drag and Drop question 110 as well.
so it should be A
upvoted 4 times

MPoels 6 months, 1 week ago

https://web.archive.org/web/20191129023324/https://www.cisco.com/c/en/us/products/collateral/data-center-analytics/tetration-analytics/white-paper-c11-740380.html#_Toc509550184
upvoted 1 times

loser4fun 1 year, 5 months ago

I would go with B. user login suspicious behavior.

The Cisco Tetration platform uses behavior-based anomaly detection to learn the normal behavior of users, applications, and network traffic, and to identify deviations from that normal behavior that may indicate a security threat. One of the behaviors that it looks for is user login suspicious behavior, such as repeated failed login attempts or login attempts from unusual locations or at unusual times.

By analyzing these patterns of behavior, the platform can establish a baseline for normal user behavior and identify deviations that may indicate a potential security threat. Once an anomaly is detected, the platform can take action to mitigate the threat and prevent it from causing damage to the network or applications.

upvoted 3 times

Kyle1776 2 years, 6 months ago

File access from a different user: Cisco Secure Workload platform learns the normal behavior of which file is accessed by which user.

<https://www.cisco.com/c/en/us/products/collateral/data-center-analytics/tetration-analytics/white-paper-c11-740380.html>
upvoted 3 times

jaciro11 2 years, 10 months ago

Should be A no ! Its A !
<https://www.cisco.com/c/en/us/products/collateral/data-center-analytics/tetration-analytics/datasheet-c78-737256.html>
upvoted 5 times

kapplejacks 2 years, 10 months ago

Anwer: A

Table 1. Cisco Tetration platform primary features and benefits
Feature Benefit
Zero-trust model using



microsegmentation

- Cisco Tetration platform allows only the required traffic between application components and users, blocking everything else. This approach prevents a persistent threat from entering or searching for additional vulnerabilities.

Also allows for micro segmentation so you can deny file access from different users.

<https://cdw-prod.adobecqms.net/content/dam/cdw/on-domain-cdw/brands/cisco/data-center-tetration-data-sheet.pdf>

upvoted 5 times

  **Sarbi** 3 years ago

What about b.If a user login from a US location and after 10 min the same user tries to login for Asia.

upvoted 2 times

  **kerniger** 3 years ago

i really dont get the question.

<https://www.cisco.com/c/en/us/products/collateral/data-center-analytics/tetration-analytics/white-paper-c11-740380.html#CiscoSecureWorkloadplatformandapplicationbehaviorallowedlisting>

So SecureWorkload (Tetration) uses all of them but B C and D is not a "learning" mechanism of users behavior while A is?

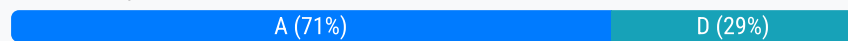
upvoted 1 times

Which attribute has the ability to change during the RADIUS CoA?

- A. authorization
- B. NTP
- C. accessibility
- D. membership

Correct Answer: A

Community vote distribution



Kyle1776 Highly Voted 2 years, 6 months ago

CoA stands for change of Authorization so im gonna go with Authorization
upvoted 10 times

862e76c Most Recent 10 months, 1 week ago

Selected Answer: A

The name CoA (Change of Authorization) explains itself enough.
upvoted 2 times

Cokamaniako 1 year, 2 months ago

Selected Answer: A

The RADIUS Change of Authorization (CoA) feature provides a mechanism to change the attributes of an authentication, authorization, and accounting (AAA) session after it is authenticated
upvoted 3 times

littlewilly 1 year, 3 months ago

Selected Answer: D

It's membership
upvoted 1 times

Terry0987 1 year, 8 months ago

Selected Answer: D

shouldn't it be D ? It's asking about a specific attribute !
upvoted 1 times

SegaMasterSystemAdmin 1 year, 4 months ago

membership? like a gym membership? lol
upvoted 4 times

abdulmalik_mail 2 years, 8 months ago

It's A, Radius CoA provides a mechanism to change the attributes of an authentication, authorization, and accounting (AAA).
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_aaa/configuration/xr-16-10/sec_usr_aaa-xr-16-10-book/sec-rad-coa.pdf
upvoted 4 times

An administrator configures new authorization policies within Cisco ISE and has difficulty profiling the devices. Attributes for the new Cisco IP phones that are profiled based on the RADIUS authentication are seen; however, the attributes for CDP or DHCP are not. What should the administrator do to address this issue?

- A. Configure a service template within the switch to standardize the port configurations so that the correct information is sent to Cisco ISE.
- B. Configure the ip dhcp snooping trust command on the DHCP interfaces to get the information to Cisco ISE.
- C. Configure the authentication port-control auto feature within Cisco ISE to identify the devices that are trying to connect.
- D. Configure the device sensor feature within the switch to send the appropriate protocol information.

Correct Answer: D

Community vote distribution

D (64%)

A (36%)

klu16 Highly Voted 3 years ago

I would choose D..

Device sensor is a feature of access devices. It allows to collect information about connected endpoints. Mostly, information collected by Device Sensor can come from the following protocols:

Cisco Discovery Protocol (CDP)
Link Layer Discovery Protocol (LLDP)
Dynamic Host Configuration Protocol (DHCP)

upvoted 20 times

andrewj511 3 years ago

<https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/200292-Configure-Device-Sensor-for-ISE-Profilin.html>
upvoted 7 times

Premium_Pils Most Recent 1 month ago

Selected Answer: D

D - As others pointed out
upvoted 1 times

Korndal 2 months, 1 week ago

Selected Answer: D

Answer is D. Other answer that should have been there, would be that den ip helper-address hasn't been configured to point to ISE, and therefore ISE does not get copies of the dhcp requests of the clients
upvoted 1 times

4pelos 6 months, 1 week ago

Correct answer D.
Checked with securitytut
upvoted 1 times

nekkrokvlt 12 months ago

It is D. Device sensor sends cdp / lldp attributes as radius accounting data for profiling
upvoted 2 times

gc999 1 year, 3 months ago

Selected Answer: D

I eventually choose "D" after reading this

https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750/software/release/15-0_1_se/device_sensor/guide/sensor_guide.html
upvoted 3 times

Jessie45785 1 year, 5 months ago

Selected Answer: A

D - cannot be correct cause device sensor is configured on ISE, NOT on the switch

<https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/200292-Configure-Device-Sensor-for-ISE-Profilin.html#anc6>

A- service templates can be locally configured on the switch:

<https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/200292-Configure-Device-Sensor-for-ISE-Profilin.html#anc6>
upvoted 4 times

Jessie45785 1 year, 4 months ago

it was really late D- IS CORRECT:

```
switch#show device-sensor cache interface g1/0/13
Device: 20bb.c0de.06ae on port GigabitEthernet1/0/13
-----
Proto Type:Name Len Value
LLDP 6:system-description 40 0C 26 43 69 73 63 6F 20 49 50 20 50 68 6F 6E 65
20 38 39 34 31 2C 20 56 33 2C 20 53 43 43 50 20
39 2D 33 2D 34 2D 31 37
CDP 6:platform-type 24 00 06 00 18 43 69 73 63 6F 20 49 50 20 50 68 6F
6E 65 20 38 39 34 31 20
CDP 28:secondport-status-type 7 00 1C 00 07 00 02 00
    upvoted 4 times
```

  **sis_net_sec** 1 year, 11 months ago

D is correct



Device sensor is a feature of access devices. It allows to collect information about connected endpoints.

Mostly, information collected by Device Sensor can come from the following protocols:

- + Cisco Discovery Protocol (CDP)
- + Link Layer Discovery Protocol (LLDP)
- + Dynamic Host Configuration Protocol (DHCP)

Reference: <https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/200292-ConfigureDevice-Sensor-for-ISE-Profilin.html>

upvoted 2 times

  **JGW** 2 years, 5 months ago

Selected Answer: D

D is correct, use link provided by andrewj511 and coentror.

Answer C is incorrect, as that command needs to be executed on the switch and not on the ISE server

upvoted 1 times

  **jaciro11** 2 years, 6 months ago

Selected Answer: D

Configure the device sensor feature within the switch to send the appropriate protocol information

upvoted 1 times

  **efongvan** 2 years, 8 months ago

I will go with D.

upvoted 1 times

  **coentror** 2 years, 9 months ago

It is D

<https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/200292-Configure-Device-Sensor-for-ISE-Profilin.html>

upvoted 4 times

  **testtaker13** 2 years, 10 months ago

Seems D is the correct one

upvoted 4 times

  **Sarbi** 3 years ago

I will go with D.

upvoted 4 times

  **Sarbi** 3 years ago

Ans is A.

upvoted 2 times

An organization deploys multiple Cisco FTD appliances and wants to manage them using one centralized solution. The organization does not have a local VM but does have existing Cisco ASA that must migrate over to Cisco FTDs. Which solution meets the needs of the organization?

- A. Cisco FMC
- B. CDO
- C. CSM
- D. Cisco FDM

Correct Answer: B

Community vote distribution

B (56%) A (44%)

eazy99 Highly Voted 2 years, 11 months ago

What a tricky question, but I think I just got you the perfect answer and the perfect link from Cisco. The correct answer is A, not B. The reason why, According to Cisco, if you want to migrate your ASA to FTD and want to manage them both through "CDO and FDM" then use (CDO), but if you want to migrate ASA to FTD and manage both in the same time (Centralized) then use FMC" So the answer is absolutely A, and here is the link:
https://www.cisco.com/c/en/us/td/docs/security/firepower/migration-tool/migration-guide-CDO/ASA2FTD_Using_CDO/ASA2FTD_with_FP_Migration_Tool_cdo_chapter_011.html
 upvoted 23 times

loser4fun 1 year, 5 months ago

but there's another tricky part which is the organization doesn't have a local VM which makes the answer is B
 upvoted 4 times

MPoels 6 months, 1 week ago

Answer A seems to be right (with a physical FMC appliance).

Official ASA-2-FTD migration tool exists several years (so CDO built-in migration tool isn't needed):
https://www.cisco.com/c/en/us/td/docs/security/firepower/migration-tool/migration-guide/ASA2FTD-with-FP-Migration-Tool/b_Migration_Guide_ASA2FTD_chapter_00.html

Consideration why not using CDO (in this scenario): When using device credentials to connect CDO to a device, it is a best practice to download and deploy an SDC in your network to manage the communication between CDO and the device. This procedure describes how to install an SDC in your network, using CDO's VM image. This is the preferred, easiest, and most reliable way to create an SDC.
 (see https://docs.defenseorchestrator.com/r_how-it-works_cdo.html#!t_deploy-a-sdc-using-cdos-vm-image.html)
 upvoted 3 times

angry 1 year, 5 months ago

you can have physical FMC deployment. A is correct!
 upvoted 5 times

gc999 1 year, 5 months ago

Just want to confirm that FMC can also support Cloud Deployment. Right?
<https://www.cisco.com/c/en/us/products/collateral/security/firesight-management-center/datasheet-c78-736775.html>
 upvoted 1 times

semi1750 Highly Voted 2 years, 4 months ago

Vote for B

FMC will manage only Firepower images (FTD or Firepower module Services). CDO is able to centrally manage your ASAs, FTD, Meraki security policies and AWS VPC security policies.

For FMC, you need to have a local VM (with some resources like 32G RAM) and need to manage the redundancy as well. CDO is cloud based (could have a local VM with small resources to communicate with the cloud and not expose your devices management). You need to see CDO like the Meraki portal for Cisco Security Firewalls.

<https://community.cisco.com/t5/network-security/a-classic-cdo-vs-fmc/td-p/4070116>
 upvoted 8 times

[Removed] Most Recent 7 months, 2 weeks ago

Selected Answer: B

It is CDO, which can migrate from ASA to FTD. Cisco FMC is a fairly new thing, where Cisco hosts the FMC for you, since that thing is supposed to have around 30GB of memory, even when managing one or two FTD devices. Also, FMC cannot migrate from ASA to FTD, you have to re-enter the entire configuration from scratch.
 upvoted 3 times

Ko13 10 months, 1 week ago

Selected Answer: B

It is B. CDO .

The FMC cannot help with the ASA-to-FTD migration, you do that using the Firepower Migration Tool, then the config is loaded in to the FMC once migrated.

CDO on the other hand does allow you to migrate ASA to FTD (managed using FDM thou), but it also allows you to then manage those FDM FTDs too.

https://www.cisco.com/c/en/us/td/docs/security/firepower/migration-tool/migration-guide-CDO/ASA2FTD_Using_CDO/ASA2FTD_with_FP_Migration_Tool_cdo_chapter_011.html

<https://www.cisco.com/c/en/us/td/docs/security/cdo/managing-ftd-with-cdo/managing-ftd-with-cisco-defense-orchestrator/managing-ftd-with-cdo.html>

upvoted 1 times

DWizard 1 year, 2 months ago

Selected Answer: A

The answer can be A) FMC using an appliance, not a virtual machine, or B) CDO without SDCs... it's a hard one, but I would go for A, has more sense if it must be a "centralized solution"

upvoted 2 times

ffaiz 1 year, 2 months ago

Selected Answer: B

"The organization does not have a local VM"

1-FDM(manage device locally)

2-CDO(cloud based central management no need VM)

3-FMC(VM based central management)

upvoted 2 times

Jessie45785 1 year, 3 months ago

Selected Answer: B

It is Cisco question do not overthink it - if you cannot use VM you are left with CDO

https://www.cisco.com/c/en/us/td/docs/security/firepower/620/asa2ftd-migration/asa2ftd-migration-guide-620/asa2ftd_migration_procedure.pdf

FMC:

Step 1 Download one of the following images from Support:

- Firepower Management Center Virtual for VMware
- Firepower Management Center Virtual for KVM

Step 2 Use the image file to install a dedicated Firepower Management Center Virtual, as described in the appropriate guide:

- Cisco Firepower Management Center Virtual for VMware Deployment Quick Start Guide
- Cisco Firepower Management Center Virtual for KVM Deployment Quick Start Guide

Step 3 Connect to the Firepower Management Center via ssh, using the admin username.

Step 4 Log in to the root shell:

```
sudo su -
```

Step 5 Run the following command:

```
enableMigrationTool.pl
```

After the process completes, refresh any web interface sessions running on the Firepower Management Center to use the migration tool.

upvoted 2 times

littlewilly 1 year, 3 months ago

Selected Answer: B

Answer is CDO

upvoted 1 times

alexyoizat24 1 year, 4 months ago

i came cross this situation for deploying FPR1150 firewalls. basically you will have 3 options

1-FDM(manage device locally)

2-CDO(cloud based central management no need VM)

3-FMC(VM based central management)

so for this question you need to manage them from controller but not from the VM you manage, answer is CDO . so B.

upvoted 3 times

KPzee 1 year, 5 months ago

A is correct. FMC supports both physical and virtual appliances, hence it can be deployed as a virtual machine on an existing server infrastructure or as a physical appliance. also FMC supports the migration of Cisco ASA configurations to Cisco FTD

upvoted 1 times

Tuxinator 1 year, 6 months ago

Selected Answer: A

B is incorrect.

CDO (Cisco Defense Orchestrator) is a cloud-based management solution that can manage multiple Cisco security products, including ASA (Adaptive Security Appliance) and FTD. However, it requires a local VM to be deployed in order to manage on-premises devices.

upvoted 3 times

  **DWizard** 1 year, 2 months ago

No, as long as those on-premises devices have Internet access

<https://www.cisco.com/c/en/us/td/docs/security/cdo/managing-asa-with-cdo/managing-asa-with-cisco-defense-orchestrator/basics-of-cisco-defense-orchestrator.html>



upvoted 1 times

  **Emlia1** 1 year, 9 months ago

Selected Answer: A

A is correct



upvoted 1 times

  **Hereim** 1 year, 10 months ago

I will go with B. Very good comparison between CDO and FMC pros and cons in this link <https://community.cisco.com/t5/network-security/a-classic-cdo-vs-fmc/td-p/4070116>

Main two points here to note: there is no local VM as per the question. FMC needs a local VM. Secondly, the question clearly says the existing ASA must migrate over to FTD - CDO can do that however FMC you need to do separate migration tool.

upvoted 4 times

  **gc999** 1 year, 4 months ago

But here said that FMC can be deployed either physical or virtual, or from the Cloud.

<https://www.cisco.com/c/en/us/products/collateral/security/firesight-management-center/datasheet-c78-736775.html>

upvoted 2 times

  **sis_net_sec** 1 year, 11 months ago

Selected Answer: A



[cisco.com/c/en/us/td/docs/security/firepower/630/configuration/guide/fpmc-config-guide-v63/firepower_threat_defense_logical_devices.html](https://www.cisco.com/c/en/us/td/docs/security/firepower/630/configuration/guide/fpmc-config-guide-v63/firepower_threat_defense_logical_devices.html)

upvoted 1 times

  **xxx_ford** 2 years, 1 month ago

Is B as it states ASA to FTD migration CDO can be used.

upvoted 2 times

  **NikoNiko** 2 years, 1 month ago

It's B - CDO.

"organization deploys multiple Cisco FTD appliances and WANTS TO manage" - i. e. is NOT managing it now but wants to do it (probably) in the future.

"organization does not have a local VM" - i. e. no place for FMC deployment,

"ave existing Cisco ASA that must migrate over to Cisco FTDs" - just another reason for CDO and its migration tool

upvoted 5 times

  **surforlife** 2 years, 2 months ago

Indeed "CDO"

upvoted 4 times

What is a benefit of using telemetry over SNMP to configure new routers for monitoring purposes?

- A. Telemetry uses push and pull, which makes it more secure than SNMP.
- B. Telemetry uses push and pull, which makes it more scalable than SNMP.
- C. Telemetry uses a push method, which makes it faster than SNMP.
- D. Telemetry uses a pull method, which makes it more reliable than SNMP.

Correct Answer: C

Community vote distribution

C (83%)

B (17%)

idto Highly Voted 2 years, 9 months ago

Selected Answer: C

SNMP polling can often be in the order of 5-10 minutes, CLIs are unstructured and prone to change which can often break scripts.

The traditional use of the pull model, where the client requests data from the network does not scale when what you want is near real-time data.

Moreover, in some use cases, there is the need to be notified only when some data changes, like interfaces status, protocol neighbors change etc.

Model-Driven Telemetry is a new approach for network monitoring in which data is streamed from network devices continuously using a push model and provides near real-time access to operational statistics

<https://developer.cisco.com/docs/ios-xe/#!streaming-telemetry-quick-start-guide/streaming-telemetry>
upvoted 10 times

Zatingke 1 year, 6 months ago

The above says, does not scale.

So it should be B then.

upvoted 1 times

MPoels 6 months, 1 week ago

The crucial difference is "uses push method" (not "push and pull"). So answer C seems to be right.

upvoted 2 times

sull3y Most Recent 1 year, 5 months ago

The benefit of using telemetry over SNMP to configure new routers for monitoring purposes is that telemetry uses a push method, which makes it faster than SNMP.

SNMP (Simple Network Management Protocol) is a widely used protocol for network monitoring and management. SNMP uses a pull model where the management system sends a request to the device to retrieve information. The device responds to the request with the requested data. This can result in a delay between when a change occurs and when the monitoring system is made aware of it.

Telemetry, on the other hand, uses a push model where the device sends data to the management system in near real-time. This makes telemetry faster than SNMP and can reduce the time between when a change occurs and when the monitoring system is made aware of it.

Therefore, the answer is C: Telemetry uses a push method, which makes it faster than SNMP.

upvoted 2 times

Zatingke 1 year, 6 months ago

Selected Answer: B

Pull model, such as SNMP, does not scale when what you want is near real-time data.

upvoted 2 times


```
ntp authentication-key 10 md5 cisco123
ntp trusted-key 10
```

Refer to the exhibit. A network engineer is testing NTP authentication and realizes that any device synchronizes time with this router and that NTP authentication is not enforced. What is the cause of this issue?

- A. The hashing algorithm that was used was MD5, which is unsupported.
- B. The key was configured in plain text.
- C. NTP authentication is not enabled.
- D. The router was not rebooted after the NTP configuration updated.

Correct Answer: C

  **Toni_Su91** Highly Voted 1 year, 6 months ago

The following example shows how to configure the system to synchronize only to systems providing authentication keys 1 to 3 in their NTP packets:

```
Router(config)# ntp authenticate
Router(config)# ntp authentication-key 1 md5 key1
Router(config)# ntp authentication-key 2 md5 key2
Router(config)# ntp authentication-key 3 md5 key3
Router(config)# ntp trusted-key 1 - 3
```

<https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/bsm/command/bsm-cr-book/bsm-cr-n1.html#wp2849112306>

ntp authenticate - Enables NTP authentication.
upvoted 7 times

  **abdulmalik_mail** Most Recent 2 years, 8 months ago

It's C, we need put command ntp authentication enable
upvoted 3 times

An engineer has been tasked with configuring a Cisco FTD to analyze protocol fields and detect anomalies in the traffic from industrial systems. What must be done to meet these requirements?

- A. Enable traffic analysis in the Cisco FTD.
- B. Implement pre-filter policies for the CIP preprocessor.
- C. Configure intrusion rules for the DNP3 preprocessor.
- D. Modify the access control policy to trust the industrial traffic.

Correct Answer: C

Community vote distribution

C (100%)

klu16 Highly Voted 3 years ago

I will go with C here... First of all, you need special kind of preprocessors (Modbus/DNP3/CIP) to analyze the industrial system traffic, so enabling "default" traffic analysis in FTD is not enough.

upvoted 11 times

zeroCOOL Highly Voted 3 years ago

i would opt for C. DNP3 is a SCADA Protocol which in turn is widely used in the industrial network world. "The DNP3 preprocessor detects anomalies in DNP3 traffic and decodes the DNP3 protocol for processing by the rules engine, which uses DNP3 keywords to access certain protocol fields." https://www.cisco.com/c/en/us/td/docs/security/firepower/630/configuration/guide/fpmc-config-guide-v63/scada_preprocessors.html

upvoted 8 times

brownb 2 years, 9 months ago

Its definitely not widely used, Id say CIP or Modbus are going to be used 90% of the time or better with CIP likely being dominant in at least the US plus cisco and Rockwell partnered to create the CIP/ethernet Ethernet/IP protocol and it is a cisco exam. Also looking at the preprocessor for CIP, "The CIP preprocessor detects CIP and ENIP traffic running on TCP or UDP and sends it to the intrusion rules engine." So id personally go with CIP preprocessor over intrusion rules with DNP3. But im not yet super familiar with the Firepower processes to be fair.

upvoted 4 times

Premium_Pils Most Recent 1 month ago

Selected Answer: C

Pre-filter policy skips snort engine. C seems to be correct.

upvoted 1 times

Jessie45785 1 year, 5 months ago

Selected Answer: C

definitely C (as mentioned by @zeroCOOL DNP3 is part of SCADA) and SCADA is typical industrial system)

upvoted 2 times

surforlife 2 years, 1 month ago

It does not matter which of the 3 you like the most.

It does not matter which one you choose between Modbus, CIP or DNP3.

What matters is where you set them to be trusted by FTD.

Policies > Access Control, then click Network Analysis Policies or Policies > Access Control > Intrusion, then click Network Analysis Policies.

Note

If your custom user role limits access to the first path listed here, use the second path to access the policy.

Step 2

Click Edit (edit icon) next to the policy you want to edit.

If View (view button) appears instead, the configuration belongs to an ancestor domain, or you do not have permission to modify the configuration.

Step 3

Click Settings in the navigation panel.

"D" is the correct answer.

upvoted 2 times

NikoNiko 2 years, 1 month ago

C is correct - Configure Intrusion Rules... because IR also automatically enable required pre-processors, which handle detection of anomalies (as required in the question).

A - "enable traffic analysis" - means nothing specific

B - Pre-filter policies for CIP -> Pre-filters are used to bypass Snort engine completely, optional first step of access control, rules that match simple values like IP's and ports (like ASA ACL). There is no deep packet inspection nor anomaly detection.[2][3]

[2] <https://www.cisco.com/c/en/us/support/docs/security/firepower-management-center/212700-configuration-and-operation-of-ftd-prefi.html>

[3] <https://networkdirection.net/articles/firewalls/firepowermanagementcentre/prefilterpolicies/>

D - Set Access Control Policy to trust industrial traffic - Action TRUST = allow WITHOUT inspection & anomaly detection.

upvoted 2 times

  **NikoNiko** 2 years, 1 month ago

C - "configure INTRUSION RULES for DNP3" -> Documentation states, that enabling INTRUSION RULES is mandatory for CIP to work + required preprocessors (in Network Access Policy - NAP) will be enabled automatically:

"If you want the CIP preprocessor rules listed in the following table to generate events, you MUST enable them. See Setting Intrusion Rule States for information on enabling rules."

"If the Modbus, DNP3, or CIP preprocessor is disabled, and you enable and deploy an intrusion rule that requires one of these preprocessors, the system automatically uses the required preprocessor, with its current settings, although the preprocessor remains disabled in the web interface for the corresponding network analysis policy."

[1] https://www.cisco.com/c/en/us/td/docs/security/firepower/630/configuration/guide/fpmc-config-guide-v63/scada_preprocessors.html

upvoted 2 times

  **getafix** 2 years, 2 months ago

Selected Answer: C

SCADA: There are two supervisory control and data acquisition (SCADA) protocols for which the Cisco Firepower NGIPS offers preprocessors: DNP3 and Modbus. These protocols monitor and control industrial facilities. The SCADA preprocessors monitor the DNP and Modbus protocols for anomalies and decode their messages for further rule inspection.

From the Cisco Official Cert Guide

upvoted 2 times

  **pr0fectus** 2 years, 8 months ago

Selected Answer: C

Pre-filter policy skips snort engine.

upvoted 5 times

  **Moll** 2 years, 9 months ago

"the system does not inspect blocked or trusted traffic"

https://www.cisco.com/c/en/us/td/docs/security/firepower/610/configuration/guide/fpmc-config-guide-v61/an_overview_of_network_analysis_and_intrusion_policies.html

upvoted 1 times

  **Moll** 2 years, 9 months ago

diagram shows, in a simplified fashion, the order of traffic analysis in an inline, intrusion prevention and AMP for Networks deployment. It illustrates how the access control policy invokes other policies to examine traffic, and in which order those policies are invoked. The network analysis and intrusion policy selection phases are highlighted.

https://www.cisco.com/c/en/us/td/docs/security/firepower/610/configuration/guide/fpmc-config-guide-v61/an_overview_of_network_analysis_and_intrusion_policies.html

In a newly created access control policy, one default network analysis policy governs preprocessing for all traffic for all intrusion policies invoked by the same parent access control policy.

upvoted 1 times

  **andrewj511** 2 years, 11 months ago

https://www.cisco.com/c/en/us/td/docs/security/firepower/630/configuration/guide/fpmc-config-guide-v63/scada_preprocessors.html

If the Modbus, DNP3, or CIP preprocessor is disabled, and you enable and deploy an intrusion rule that requires one of these preprocessors, the system automatically uses the required preprocessor, with its current settings...

upvoted 4 times

  **fabio3wz** 3 years ago

I think the answer should be C. If you're going to detect any kind of anomalies I suppose Intrusion rules is a must.

upvoted 5 times

An organization uses Cisco FMC to centrally manage multiple Cisco FTD devices. The default management port conflicts with other communications on the network and must be changed. What must be done to ensure that all devices can communicate together?

- A. Change the management port on Cisco FMC so that it pushes the change to all managed Cisco FTD devices.
- B. Set the sftunnel port to 8305.
- C. Manually change the management port on Cisco FMC and all managed Cisco FTD devices.
- D. Set the sftunnel to go through the Cisco FTD.

Correct Answer: C

Community vote distribution

C (63%) A (38%)

Moll Highly Voted 2 years, 9 months ago

Answer should be C

https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Security__Internet_Access__and_Communication_Ports.html
8305/tcp

Securely communicate between appliances in a deployment.

" If you change this port, you must change it for all appliances in the deployment. We recommend you keep the default."

upvoted 13 times

eazy99 Highly Voted 2 years, 11 months ago

The answer is C from Cisco website and specifically this paragraph, " In this case you must also change the port on FMC (Configuration > Management Interfaces > Shared Settings). This affects all other devices that are already registered to the same FMC. Cisco strongly recommends that you keep the default settings for the remote management port, but if the management port conflicts with other communications on your network, you can choose a different port. If you change the management port, you must change it for all devices in your deployment that need to communicate together."

And here is the link

<https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/215540-configure-verify-and-troubleshoot-firep.html>

upvoted 9 times

Alizade Most Recent 11 months, 2 weeks ago

Selected Answer: C

C. Manually change the management port on Cisco FMC and all managed Cisco FTD devices.

upvoted 1 times

Tuxinator 1 year, 6 months ago

Selected Answer: C

The answer is C. However if you overthink it it could also be A. however in the form the question is asked it should be C.

Cisco FMC has the ability to push configuration changes to managed Cisco FTD devices automatically, so changing the management port on the FMC can be propagated to all managed FTD devices without the need for manual intervention on each device. This can be done through the use of FlexConfigs or the Configuration Deployments feature in the FMC.

FlexConfigs allow for the execution of custom commands on managed devices, including configuration changes. The FMC can be configured to push a FlexConfig that changes the management port on all managed FTD devices at once.

upvoted 2 times

Emlia1 1 year, 9 months ago

I prefer C

upvoted 1 times

sis_net_sec 1 year, 11 months ago

Selected Answer: A

Cisco strongly recommends that you keep the default settings for the remote management port, but if the management port conflicts with other communications on your network, you can choose a different port. If you change the management port, you must change it for all devices in your deployment that need to communicate with each other.

upvoted 3 times

francojaraba 2 years, 1 month ago

Selected Answer: C

Answer is C. The sftunnel is created once the communication is established - <https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/215540-configure-verify-and-troubleshoot-firep.html>

"Once the registration is done the FTD and the FMC establish a secure tunnel called sftunnel (the name derives from the Sourcefire tunnel)."

upvoted 1 times

  **Laryoul** 2 years, 5 months ago

Selected Answer: C

Answer is C

upvoted 1 times

  **Minion2021** 2 years, 6 months ago

The answer is C

upvoted 2 times

  **klu16** 3 years ago

The answer is C... When you change the default port, you have to change it manually on all FTD devices in the deployment.

upvoted 3 times

  **fabio3wz** 3 years ago

C should be the correct answer; we can change the port manually:

<https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/215540-configure-verify-and-troubleshoot-firep.html#anc7>

upvoted 2 times



Question #138

Topic 1

An administrator is establishing a new site-to-site VPN connection on a Cisco IOS router. The organization needs to ensure that the ISAKMP key on the hub is used only for terminating traffic from the IP address of 172.19.20.24. Which command on the hub will allow the administrator to accomplish this?

- A. `crypto isakmp identity address 172.19.20.24`
- B. `crypto ca identity 172.19.20.24`
- C. `crypto enrollment peer address 172.19.20.24`
- D. `crypto isakmp key Cisco0123456789 172.19.20.24`

Correct Answer: D

  **testtaker13** **Highly Voted**  2 years, 8 months ago

probably D. However the correct command should be `crypto isakmp key <cisco123> address <host ip>`

upvoted 10 times

  **itashraf** **Most Recent**  3 years ago

Ans: D

upvoted 3 times

A Cisco FTD engineer is creating a new IKEv2 policy called s2s00123456789 for their organization to allow additional protocols to terminate network devices with.

They currently only have one policy established and need the new policy to be a backup in case some devices cannot support the stronger algorithms listed in the primary policy. What should be done in order to support this?

- A. Change the encryption to AES* to support all AES algorithms in the primary policy.
- B. Make the priority for the primary policy 10 and the new policy 1.
- C. Change the integrity algorithms to SHA* to support all SHA algorithms in the primary policy.
- D. Make the priority for the new policy 5 and the primary policy 1.

Correct Answer: D

Community vote distribution

D (100%)

sis_net_sec 1 year, 11 months ago

Selected Answer: D

All IKE policies on the device are sent to the remote peer regardless of what is in the selected policy section.

The first IKE Policy matched by the remote peer will be selected for the VPN connection. Choose which policy is sent first using the priority field. Priority 1 will be sent first.

Reference: <https://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/215470-site-to-site-vpn-configuration-on-ftd-ma.html>

upvoted 1 times

Moll 2 years, 9 months ago

Correct answer should be D

The lower the number, the higher the priority.

https://docs.defenseorchestrator.com/Configuration_Guides/Objects/Configuring_the_Global_IKE_Policy/Managing_FTD_IKEv2_Policies
Priority— The relative priority of the IKE policy, from 1 to 65,535. The priority determines the order of the IKE policy compared by the two negotiating peers when attempting to find a common security association (SA). If the remote IPsec peer does not support the parameters selected in your highest priority policy, it tries to use the parameters defined in the next lowest priority. The lower the number, the higher the priority.

upvoted 4 times

What is a functional difference between a Cisco ASA and Cisco IOS router with Zone-Based Policy Firewall?

- A. The Cisco ASA can be configured for high availability, whereas the Cisco IOS router with Zone-Based Policy Firewall cannot.
- B. The Cisco IOS router with Zone-Based Policy Firewall can be configured for high availability, whereas the Cisco ASA cannot.
- C. The Cisco ASA denies all traffic by default, whereas the Cisco IOS router with Zone-Based Policy Firewall starts out by allowing all traffic, even on untrusted interfaces.
- D. The Cisco IOS router with Zone-Based Policy Firewall denies all traffic by default, whereas Cisco ASA starts out by allowing traffic until rules are added.

Correct Answer: C

Community vote distribution

D (62%)

C (38%)

Premium_Pils 1 month ago

Selected Answer: D

Based on my work experience with both ZFW and ASA, by default no traffic is allowed to pass between zones. Whereas ASA allows traffic from high level security interfaces to low level security interfaces by default.

upvoted 1 times

XvidalX 6 months, 1 week ago

Selected Answer: D

D is correct - ASA starts permitting higher security level interface to access any other security level interfaces by default, until a access list applied

upvoted 2 times

red_sparrow_Gr 9 months, 2 weeks ago

Selected Answer: D

correct id D

<https://www.cisco.com/c/en/us/support/docs/security/ios-firewall/98628-zone-design-guide.html#anc11>

search for the following : ZFW default policy between zones is deny all. If no policy is explicitly configured, all traffic that moves between zones is blocked.

upvoted 2 times

XvidalX 6 months, 1 week ago

ZFW default policy between zones is deny all. If no policy is explicitly configured, all traffic that moves between zones is blocked <-----

upvoted 2 times

kylesam2017 9 months, 3 weeks ago

"C" is the correct answer. Here is the link:

"One difference is that the IOS router starts out by allowing all traffic [on your untrusted interfaces], where as the ASA starts by denying all traffic. Consequently you have to configure the actual hardening of your IOS router. "

<https://community.cisco.com/t5/network-security/ios-firewall-vs-asa/td-p/2133822#:~:text=One%20difference%20is%20that%20the,hardening%20of%20your%20IOS%20router.>

upvoted 3 times

red_sparrow_Gr 10 months, 2 weeks ago

Selected Answer: C

Cisco ASA vs IOS Router with Zone-Based Firewall

Some prefer to have a single device do both routing and security, but others opt for dedicated security devices. The ASA denies all traffic by default, while the IOS router starts out by allowing all traffic, even on your untrusted interfaces.

upvoted 1 times

Pakawat 11 months, 3 weeks ago

Selected Answer: C

C

<https://community.cisco.com/t5/network-security/ios-firewall-vs-asa/td-p/2133822>

upvoted 1 times

fdl543 1 year, 1 month ago

Selected Answer: D

D. "even on untrusted" kills alternative C...

upvoted 2 times

[-]  **Cokamaniako** 1 year, 2 months ago

Selected Answer: C

The ASA denies all traffic by default, while the IOS router starts out by allowing all traffic, even on your untrusted interfaces. You can eliminate this disadvantage, however, by hardening your router.

upvoted 1 times

[-]  **zamljo** 1 year, 2 months ago

C

<https://www.linkedin.com/pulse/cisco-zone-based-firewall-reporting-anna-mcelhany/>

upvoted 3 times

[-]  **majster88** 1 year, 3 months ago

Selected Answer: C

Correct is C, why?

On ASA by default all interfaces with ip address and nameif are configured with security level 0. Without "same-security-level inter/intra-traffic" (which is not by default) all traffic through ASA is denied (traffic between interfaces with the same security level). On other hand, with ZBFW by default all interfaces with ip address are not assigned to a zone. Traffic between interfaces not assigned to a zone is allowed.

upvoted 4 times

[-]  **Jessie45785** 1 year, 5 months ago

Selected Answer: D


C - is not correct:

All traffic to and from a given interface is implicitly blocked when the interface is assigned to a zone, except traffic to and from other interfaces in the same zone, and traffic to any interface on the router.

<https://www.cisco.com/c/en/us/support/docs/security/ios-firewall/98628-zone-design-guide.html>

only D make sense

upvoted 3 times


[-]  **KPzee** 1 year, 5 months ago

D "whereas Cisco ASA starts out by allowing traffic until rules are added" proof DMZ to Inside interfaces is blocked by default. and Outside to Inside interface is blocked default.

C "The Cisco ASA denies all traffic by default" wrong, the Inside to DMZ, Inside to Outside is allowed.


bacsically A to D is wrong! the answers needs to be amended

upvoted 2 times

[-]  **KPzee** 1 year, 5 months ago

D is completely wrong. the Cisco ASA does not allow traffic to move from a lower security zone to a higher one by default, and it does start out with a default deny all policy. so "whereas Cisco ASA starts out by allowing traffic until rules are added." is contradictory. They both can be configured for high-availability so A & B is out. now for C & D, I think this question was poorly worded, poor usage of the english language. The default behavior of a Cisco ASA is to block incoming traffic and allow outgoing traffic i.e. from High security zone to a low one, and the reverse is denied whereas the default behavior of a Cisco IOS router with ZFW is to block all traffic though it can be argued that it behaves like the ASA if you consider that it has two default zones i.e. the self-zone other zone

upvoted 3 times

[-]  **psuoh** 1 year, 7 months ago

Selected Answer: D

ZFW default policy between zones is deny all. If no policy is explicitly configured, all traffic that moves between zones is blocked.

By default, ASA allows a flow of traffic from higher security levels to lower security levels. If the traffic is initiated by the devices in higher security levels, then it will be passed to go through the firewall to reach the devices in lower security levels like outside or DMZ.

upvoted 2 times

[-]  **Emlia1** 1 year, 8 months ago

Selected Answer: D

I prefer D

upvoted 1 times

[-]  **amtf8888** 1 year, 8 months ago

Selected Answer: D

ios router deny traffic by default

upvoted 1 times

[-]  **sis_net_sec** 1 year, 11 months ago

Selected Answer: D

<https://www.cisco.com/c/en/us/support/docs/security/ios-firewall/98628-zone-design-guide.html#anc15>

upvoted 2 times

An engineer is configuring their router to send NetFlow data to Stealthwatch which has an IP address of 1.1.1.1 using the flow record Stealthwatch406143794 command. Which additional command is required to complete the flow record?

- A. cache timeout active 60
- B. destination 1.1.1.1
- C. match ipv4 ttl
- D. transport udp 2055

Correct Answer: C

Reference:

<https://www.cisco.com/c/dam/en/us/td/docs/security/stealthwatch/netflow/config-trouble-netflow-stealth.pdf>

Community vote distribution

C (100%)

psuoh 1 year, 7 months ago

Selected Answer: C

<https://www.networkingwithesans.com/cisco-stealthwatch-netflow-configuration>

<https://i.imgur.com/xKO1BYq.png>

FLOW RECORD command allows MATCH

<https://i.imgur.com/eCXKsRm.png>

upvoted 2 times

nomanlands 2 years, 2 months ago

Selected Answer: C

May have a mistype in the answer but flow records are made of match and collect commands

upvoted 3 times

NikoNiko 2 years, 1 month ago

Example shows how to configure version 9 export for Flexible NetFlow.

!

flow exporter EXPORTER-1

destination 172.16.10.2

export-protocol netflow-v9

transport udp 90

exit

!

flow record v4_r1

match ipv4 tos

match ipv4 protocol

match ipv4 source address

match ipv4 destination address

match transport source-port

match transport destination-port

collect counter bytes long

collect counter packets long

!

flow monitor FLOW-MONITOR-1

record v4_r1

exporter EXPORTER-1

!

ip cef

!

interface GigabitEthernet 0/0/0

ip address 172.16.6.2 255.255.255.0

ip flow monitor FLOW-MONITOR-1 input

<https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/fnetflow/configuration/15-mt/fnf-15-mt-book/fnf-v9-export.html>

upvoted 2 times

NikoNiko 2 years, 1 month ago

So C is correct: match ipv4 ttl

Exporter = specifications of NetFlow protocol parameters and dest. IP of Collector.

Record = specifications of information that NetFlow gathers, such as packets in the flow and the types of counters gathered per flow. "match" and "collect" commands tell which fields to include in the outgoing NetFlow PDU.



"match" = key fields used to determine the uniqueness of the flow.

"collect" = extra fields to include for more detail to the collector for reporting and analysis.

Monitor = pairs Record with Exporter and is applied to network interface from which we want to collect NetFlow statistics & data.

https://www.cisco.com/c/dam/en/us/td/docs/security/stealthwatch/netflow/Cisco_NetFlow_Configuration.pdf

upvoted 2 times

  **otzu1** 2 years, 4 months ago

is ttl a legit parameter tho?

upvoted 1 times

  **NikoNiko** 2 years, 1 month ago

yes, it is valid

```
sw3X50(config)# flow record LANCOPE1
sw3X50(config-flow-record)# description NetFlow record for StealthWatch
sw3X50(config-flow-record)# match datalink mac source address input
sw3X50(config-flow-record)# match datalink mac destination address input
sw3X50(config-flow-record)# match ipv4 ttl
```

https://www.cisco.com/c/dam/en/us/td/docs/security/stealthwatch/netflow/Cisco_NetFlow_Configuration.pdf

upvoted 2 times

  **Smilebloke** 2 years, 4 months ago

B

Once the Flow Record has been created you would tie it to a Flow Exporter.

Flow Exporter configuration defines the physical or virtual Flow Collector IP Address to which NetFlow data is sent. It also defines the source interface from which the Flow Exporter device will send NetFlow data, this can be a physical or logical address; it is also worth considering using a Loopback interface to source NetFlow data from as a Loopback typically will remain up even when other interfaces fail therefore enabling continuous transport (where routing permits) This is also where the transport protocol (TCP or UDP) and destination port is defined; the destination port is specific to the NetFlow Collector and in this case refers to the port used by the Stealthwatch Flow Collector.

To define a Flow Exporter, follow these steps:

```
flow exporter Stealthwatch_Exporter
description Stealthwatch Export to Flow Collector
destination [Collector_IP_Address]
source [Physical_Interface | Logical_Interface]
transport udp 2055
```

<https://www.cisco.com/c/dam/en/us/td/docs/security/stealthwatch/netflow/config-trouble-netflow-stealth.pdf>

upvoted 2 times

  **Smilebloke** 2 years, 4 months ago

Ignore previous comment

C:

```
flow record Stealthwatch_FlowRecord
description Flow Record for Export to Stealthwatch (optional)
match ipv4 source address
match ipv4 destination address
match ipv4 protocol
match ipv4 tos
match transport source-port
match transport destination-port
match interface input
match flow direction
collect routing next-hop address ipv4
collect ipv4 dscp
collect ipv4 ttl minimum
collect ipv4 ttl maximum
collect transport tcp flags
collect interface output
collect counter bytes
collect counter packets
collect timestamp sys-uptime first
collect timestamp sys-uptime last
```

upvoted 5 times

  **Smilebloke** 2 years, 4 months ago

<https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/fnetflow/command/fnf-cr-book/fnf-m1.html#wp8173096590>

upvoted 4 times

An engineer is adding a Cisco DUO solution to the current TACACS+ deployment using Cisco ISE. The engineer wants to authenticate users using their account when they log into network devices. Which action accomplishes this task?

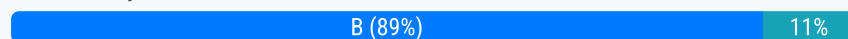
- A. Configure Cisco DUO with the external Active Directory connector and tie it to the policy set within Cisco ISE.
- B. Install and configure the Cisco DUO Authentication Proxy and configure the identity source sequence within Cisco ISE.
- C. Modify the current policy with the condition MFA: SourceSequence:DUO=true in the authorization conditions within Cisco ISE.
- D. Create an identity policy within Cisco ISE to send all authentication requests to Cisco DUO.

Correct Answer: B

Reference:

<https://duo.com/docs/authproxy-reference>

Community vote distribution



nomanlands Highly Voted 2 years, 2 months ago

Selected Answer: B

B is the correct answer. You would have to authenticate first successfully before DUO is triggered for MFA, DUO would not handle authentication directly.

upvoted 5 times

NikoNiko 2 years, 1 month ago

Yes, B is correct.

Scheme & explanation:

<https://community.cisco.com/t5/security-knowledge-base/duo-mfa-integration-with-ise-for-tacacs-device-administration/ta-p/3881767>

DUO scheme:

<https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/214813-configure-duo-two-factor-authentication.html>

A - "configure DUO external Active Directory connector + tie it to the policy set within Cisco ISE" - DUO uses own Authentication Proxy server, which connects to AD (not called "AD connector") and more importantly - it is impossible to configure ISE policy with DUO AD connector. Nonsense. In policy can be used only "AD connector", which is ISE connection to AD (i. e. AD Join Point) but it has nothing to do with DUO.

C - not existing condition in ISE

https://www.cisco.com/c/en/us/td/docs/security/ise/3-0/admin_guide/b_ISE_admin_3_0/b_ISE_admin_30_segmentation.html#ID37

D - nonsense, ISE doesn't have any Identity Policy as I know (I also Googled it for sure)

upvoted 3 times

sis_net_sec Most Recent 1 year, 10 months ago

Selected Answer: B

<https://community.cisco.com/t5/security-documents/duo-mfa-integration-with-ise-for-tacacs-device-administration/ta-p/3881767>

upvoted 3 times

wenorex222 2 years, 3 months ago

Selected Answer: D

The correct answer should be d.


upvoted 1 times

What is the function of the `crypto isakmp key cisc406143794 address 0.0.0.0 0.0.0.0` command when establishing an IPsec VPN tunnel?

- A. It prevents all IP addresses from connecting to the VPN server.
- B. It configures the pre-shared authentication key.
- C. It configures the local address for the VPN server.
- D. It defines what data is going to be encrypted via the VPN.

Correct Answer: B

This command is used to configure pre-shared-key for IPsec remote access users on the Cisco router. Address is mentioned as 0.0.0.0 0.0.0.0 because the users will be connecting from random ip addresses and it is almost impossible to mention all the ip addresses. Hence, 0.0.0.0 0.0.0.0 is used to allow all public ip addresses.

  **Orez1589** 1 year, 8 months ago

They really like to ask this question ^^
upvoted 3 times

An administrator is adding a new switch onto the network and has configured AAA for network access control. When testing the configuration, the RADIUS authenticates to Cisco ISE but is being rejected. Why is the ip radius source-interface command needed for this configuration?

- A. Only requests that originate from a configured NAS IP are accepted by a RADIUS server.
- B. The RADIUS authentication key is transmitted only from the defined RADIUS source interface.
- C. RADIUS requests are generated only by a router if a RADIUS source interface is defined.
- D. Encrypted RADIUS authentication requires the RADIUS source interface be defined.

Correct Answer: A

Reference:

https://www.cisco.com/c/en/us/td/docs/ios/12_2/security/command/reference/srfrad.html#wp1027454

Community vote distribution

A (100%)

loser4fun Highly Voted 1 year, 5 months ago

I would go with A

When configuring AAA for network access control, the ip radius source-interface command is needed to specify the interface that the switch uses to send RADIUS requests to the server. The source interface is important because it determines the IP address that is used as the NAS-IP-Address attribute in the RADIUS packet.

If the RADIUS server is configured to only accept requests that originate from a specific NAS IP address, then the switch must use that address as the source for its requests, or the authentication will fail. This is often the case in enterprise networks where strict access controls are in place.

Therefore, the ip radius source-interface command is needed to ensure that the switch sends RADIUS requests from the correct IP address and that the RADIUS server will accept them. Without this command, the authentication may fail or be rejected by the RADIUS server.

upvoted 5 times

Ko13 Most Recent 10 months, 1 week ago

Selected Answer: A

The RADIUS NAS-IP-Address Attribute Configurability feature allows you to configure an arbitrary IP address to be used as RADIUS attribute 4, NAS-IP-Address, without changing the source IP address in the IP header of the RADIUS packets. This feature may be used for situations in which service providers are using a cluster of small network access servers (NASs) to simulate a large NAS to improve scalability. This feature allows the NASs to behave as a single RADIUS client from the perspective of the RADIUS server.

https://www.cisco.com/c/en/us/td/docs/ios/12_2sb/12_2sba/feature/guide/sbsiara.html

upvoted 2 times

Tutsi 2 years, 2 months ago

Selected Answer: A

When the Radius policy is configured on the radius server, to prevent unauthorised devices from matching the policy, NAS IP can be specified within the policy. I do this configuration very often...

upvoted 2 times

Cyberops 2 years, 3 months ago

I would go with B.

It says Network Access control not Server.

upvoted 1 times

Cyberops 2 years, 3 months ago


Not sure on this one. Couldn't delete my previous comment but i would have if i could.

upvoted 1 times

Which statement about the configuration of Cisco ASA NetFlow v9 Secure Event Logging is true?

- A. To view bandwidth usage for NetFlow records, the QoS feature must be enabled.
- B. A sysopt command can be used to enable NSEL on a specific interface.
- C. NSEL can be used without a collector configured.
- D. A flow-export event type must be defined under a policy.

Correct Answer: D

  **Edy79** 11 months ago

Answer D

Prerequisites for NSEL

NSEL has the following prerequisites:



IP address and hostname assignments must be unique throughout the NetFlow configuration.

You must have at least one configured collector before you can use NSEL.

You must configure NSEL collectors before you can configure filters via Modular Policy Framework.

https://www.cisco.com/c/en/us/td/docs/security/asa/asa84/configuration/guide/asa_84_cli_config/monitor_nsel.html#87790

upvoted 1 times

  **Thusi26** 2 years, 12 months ago

D it is

upvoted 4 times

Which feature requires a network discovery policy on the Cisco Firepower NGIPS?

- A. security intelligence
- B. impact flags
- C. health monitoring
- D. URL filtering

Correct Answer: B

Community vote distribution

B (100%)

yenp Highly Voted 3 years, 2 months ago

B right answer as One of the most valuable analysis tools is the impact flag indicator. You will see impact flag calculated for your intrusion events. To help you evaluate the impact that an event has on your network, the Cisco FMC displays an impact level in the table view of intrusion events. For each event, the system adds an impact level icon, whose color indicates the correlation between intrusion data, network discovery data, and vulnerability information

upvoted 16 times

otzu1 Most Recent 2 years, 4 months ago

You can configure the system to alert you whenever an intrusion event with a specific impact flag occurs. Impact flags help you evaluate the impact an intrusion has on your network by correlating intrusion data, network discovery data, and vulnerability information.

https://www.cisco.com/c/en/us/td/docs/security/firepower/610/configuration/guide/fpmc-config-guide-v61/external_alerting_with_alert_responses.html#ID-2197-00000299

upvoted 1 times

brownbear505 2 years, 6 months ago

Selected Answer: B

Because of the Network Discovery Policy you gain the use of impact flags to evaluate the severity that intrusion events have on your network. That knowledge makes possible the ability to tune intrusion rule states so that they provide maximum protection for your network assets.

upvoted 1 times

NullNull88 2 years, 9 months ago

B is correct for this one

upvoted 1 times

Raajaa 3 years, 2 months ago

B is the answer

upvoted 1 times

bazinga31 3 years, 2 months ago

i believe its B

upvoted 1 times

deathfrom 3 years, 3 months ago

B

<https://www.ciscolive.com/c/dam/r/ciscolive/emea/docs/2019/pdf/BRKSEC-3300.pdf>

upvoted 4 times

Which policy is used to capture host information on the Cisco Firepower Next Generation Intrusion Prevention System?

- A. correlation
- B. intrusion
- C. access control
- D. network discovery

Correct Answer: D

What is a characteristic of traffic storm control behavior?

- A. Traffic storm control drops all broadcast and multicast traffic if the combined traffic exceeds the level within the interval.
- B. Traffic storm control cannot determine if the packet is unicast or broadcast.
- C. Traffic storm control monitors incoming traffic levels over a 10-second traffic storm control interval.
- D. Traffic storm control uses the Individual/Group bit in the packet source address to determine if the packet is unicast or broadcast.

Correct Answer: A

Reference:

<https://www.cisco.com/c/en/us/td/docs/routers/7600/ios/12-1E/configuration/guide/storm.html>

 **NikoNiko** 2 years, 1 month ago

Storm Control behavior:

- If you enable broadcast traffic storm control, and broadcast traffic exceeds the level within a 1-second traffic storm control interval, traffic storm control drops all broadcast traffic until the end of the traffic storm control interval.
- If you enable broadcast and multicast traffic storm control, and the COMBINED BROADCAST and MULTICAST traffic exceeds the level within a 1-second traffic storm control interval, traffic storm control DROPS ALL BROADCAST and MULTICAST traffic until the end of the traffic storm control interval.
- If you enable broadcast and multicast traffic storm control, and broadcast traffic exceeds the level within a 1-second traffic storm control interval, traffic storm control drops all broadcast and multicast traffic until the end of the traffic storm control interval.
- If you enable broadcast and multicast traffic storm control, and multicast traffic exceeds the level within a 1-second traffic storm control interval, traffic storm control drops all broadcast and multicast traffic until the end of the traffic storm control interval.

Default Traffic Storm Control Configuration

https://www.cisco.com/en/US/docs/general/Test/dwverblo/broken_guide/storm.html

upvoted 2 times

 **NikoNiko** 2 years, 1 month ago

So correct is A - Traffic storm control drops all broadcast and multicast traffic if the combined traffic exceeds the level within the interval.

upvoted 3 times

DRAG DROP -

Drag and drop the Firepower Next Generation Intrusion Prevention System detectors from the left onto the correct definitions on the right.

Select and Place:

PortScan Detection	many-to-one PortScan in which multiple hosts query a single host for open ports
Port Sweep	one-to-one PortScan, attacker mixes spoofed source IP addresses with the actual scanning IP address
Decoy PortScan	one-to-many port sweep, an attacker against one or a few hosts to scan a single port on multiple target hosts
Distributed PortScan	one-to-one PortScan, an attacker against one or a few hosts to scan one or multiple ports

Correct Answer:

PortScan Detection	Distributed PortScan
Port Sweep	Decoy PortScan
Decoy PortScan	Port Sweep
Distributed PortScan	PortScan Detection

Reference:

https://www.cisco.com/c/en/us/td/docs/security/firepower/640/configuration/guide/fpmc-config-guide-v64/detecting_specific_threats.html

 **otzu1** Highly Voted 2 years, 4 months ago

PortScan Detection Keyword "portscan"

Port Sweep Keyword "sweep"

Decoy PortScan Keyword "Spoofed"

Distributed PortScan Keyword "many-to-one"

https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Detecting_Specific_Threats.html#ID-2236-000000bb

upvoted 11 times

```
aaa new-model
```

```
radius-server host 10.0.0.12 key secret12
```

Refer to the exhibit. Which statement about the authentication protocol used in the configuration is true?

- A. The authentication request contains only a password
- B. The authentication request contains only a username
- C. The authentication and authorization requests are grouped in a single packet.
- D. There are separate authentication and authorization request packets.

Correct Answer: C

  **testtaker42** Highly Voted  3 years, 8 months ago

C does seem to be the most correct.

"RADIUS combines authentication and authorization. The access-accept packets sent by the RADIUS server to the client contain authorization information. This makes it difficult to decouple authentication and authorization."

Source: <https://www.cisco.com/c/en/us/support/docs/security-vpn/remote-authentication-dial-user-service-radius/13838-10.html>

upvoted 12 times

  **kwong328** Most Recent  1 year, 6 months ago

Correct answer is C, "In RADIUS, authentication and authorization are coupled together"

<https://www.cisco.com/c/en/us/support/docs/security-vpn/remote-authentication-dial-user-service-radius/12433-32.html>

You can find the answer in the "RADIUS Authentication and Authorization Sequence" diagram

upvoted 2 times

  **NikoNiko** 2 years, 1 month ago

RADIUS

open standard protocol

It uses UDP as a transmission protocol

It uses UDP port number 1812 for authentication and authorization and 1813 for accounting.

Authentication and Authorization are COMBINED in RADIUS.



Only the password is encrypted while the other information such as username, accounting information, etc are not encrypted.

No external authorization of commands is supported.

No multiprotocol support.

Used for network access

upvoted 2 times

  **Raajaa** 3 years, 2 months ago

Answer is C

upvoted 4 times

Which deployment model is the most secure when considering risks to cloud adoption?

- A. public cloud
- B. hybrid cloud
- C. community cloud
- D. private cloud

Correct Answer: D


Community vote distribution

D (100%)

  **hdrnzenlaoroljol** 1 year, 4 months ago

Selected Answer: D

D is the answer
upvoted 1 times

  **Raajaa** 3 years, 2 months ago

D is the answer
upvoted 4 times

What does the Cloudlock Apps Firewall do to mitigate security concerns from an application perspective?

- A. It allows the administrator to quarantine malicious files so that the application can function, just not maliciously.
- B. It discovers and controls cloud apps that are connected to a company's corporate environment.
- C. It deletes any application that does not belong in the network.
- D. It sends the application information to an administrator to act on.

Correct Answer: B

Reference:

<https://www.cisco.com/c/en/us/products/security/cloudlock/index.html#~features>

  **abdulmalik_mail** 2 years, 8 months ago

It's B
The Cloudlock Apps Firewall discovers and controls cloud apps connected to your corporate environment
<https://www.cisco.com/c/en/us/products/security/cloudlock/index.html>
upvoted 4 times

Which exfiltration method does an attacker use to hide and encode data inside DNS requests and queries?

- A. DNS tunneling
- B. DNSCrypt
- C. DNS security
- D. DNSSEC

Correct Answer: A

Reference:

<https://learn-umbrella.cisco.com/cloud-security/dns-tunneling>

  **abdulmalik_mail** 2 years, 8 months ago

It's A

DNS tunneling can establish command and control. Or, it can exfiltrate data.

<https://bluecatnetworks.com/blog/four-major-dns-attack-types-and-how-to-mitigate-them/>

upvoted 2 times

Which technology reduces data loss by identifying sensitive information stored in public computing environments?

- A. Cisco SDA
- B. Cisco Firepower
- C. Cisco HyperFlex
- D. Cisco Cloudlock

Correct Answer: D

Reference:

<https://www.cisco.com/c/dam/en/us/products/collateral/security/cloudlock/cisco-cloudlock-cloud-data-security-datasheet.pdf>

  **abdulmalik_mail** 2 years, 8 months ago

It's D

Cloudlock's data loss prevention (DLP) technology continuously monitors cloud environments to detect and secure sensitive information.

<https://www.cisco.com/c/en/us/products/security/cloudlock/index.html#~features>

upvoted 4 times

In which cloud services model is the tenant responsible for virtual machine OS patching?

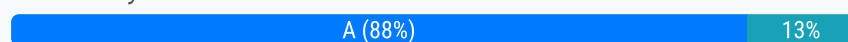
- A. IaaS
- B. UCaaS
- C. PaaS
- D. SaaS

Correct Answer: A

Reference:

<https://www.cmswire.com/cms/information-management/cloud-service-models-iaas-saas-paas-how-microsoft-office-365-azure-fit-in-021672.php>

Community vote distribution



Cokamaniako 1 year, 2 months ago

Selected Answer: A

Infrastructure as a Service (IaaS)

To deploy your applications to the Cloud, you have to install OS images and related application software on the cloud infrastructure. In this model, it's your responsibility to patch/update/maintain the OS and any application software you install.

Answer A

upvoted 1 times

loser4fun 1 year, 6 months ago

I believe the conflict here came from the responsibility

For first sight I thought it's C as in PaaS you own the OS, but in fact vendor handing over OS but you use it for your own application, so you're responsible for Application only

On the other hand IaaS you have the Infra including OS, but you're responsible for everything including OS patching.

If the question was about what model where you have OS then it's PaaS

The correct answer is A

upvoted 2 times

Emlia1 1 year, 8 months ago

Selected Answer: A

A is correct

upvoted 2 times

FortiSherlock 2 years, 1 month ago

IaaS cannot be wrong, because it is the model where you are responsible for most of the things. Only hardware patching is cloud responsibility. So all the people who say PaaS is correct - it might be an ADDITIONAL answer for you, but everything you are responsible for in PaaS you are also responsible for in IaaS.

upvoted 1 times

nomanlands 2 years, 2 months ago

Selected Answer: A

IaaS is the only one where you are responsible for the OS

upvoted 2 times

Jardator 2 years, 4 months ago

tenant is key-word so Cisco again, sorry its A

upvoted 1 times

Jardator 2 years, 4 months ago

Selected Answer: C

IaaS: In this model, it's your responsibility to patch/update/maintain the OS and any application software you install.

upvoted 1 times

asd123123iu 2 years, 3 months ago

So it's A (IaaS), not C.

upvoted 2 times

[-] **Sattm1** 2 years, 4 months ago

Selected Answer: A

This link has a nice diagram showing the difference between infrastructure, platform and software (as a service)
[https://azure.microsoft.com/en-us/overview/what-is-paas/#:~:text=Platform%20as%20a%20service%20\(PaaS,%2C%20cloud%2Denabled%20enterprise%20applications.](https://azure.microsoft.com/en-us/overview/what-is-paas/#:~:text=Platform%20as%20a%20service%20(PaaS,%2C%20cloud%2Denabled%20enterprise%20applications.)
upvoted 2 times

[-] **abdulmalik_mail** 2 years, 8 months ago

It's A
SAAS = Application like SharePoint online, O365
PAAS = Operating system like Windows Azure, Database like SQL Azure
IAAS = Windows Azure Virtual Machine and Network, Storage
<https://www.cmswire.com/cms/information-management/cloud-service-models-iaas-saas-paas-how-microsoft-office-365-azure-fit-in-021672.php>
(same link with admin reference)
upvoted 2 times

Question #156

Topic 1

What is the function of Cisco Cloudlock for data security?

- A. data loss prevention
- B. controls malicious cloud apps
- C. detects anomalies
- D. user and entity behavior analytics

Correct Answer: A

Reference:

<https://umbrella.cisco.com/products/casb>

Community vote distribution

A (100%)

[-] **bobby14** **Highly Voted** 3 years, 7 months ago

Cloudlock use DLP to prevent data exfiltrate to internet.
upvoted 12 times

[-] **Ko13** **Most Recent** 10 months ago

Selected Answer: A

<https://www.cisco.com/c/en/us/products/security/cloudlock/index.html#~features>

Data security
Cloudlock's data loss prevention (DLP) technology continuously monitors cloud environments to detect and secure sensitive information. It provides countless out-of-the-box policies as well as highly tunable custom policies.
upvoted 1 times

[-] **ExamMoney** 3 years, 8 months ago

Such a bad question. Cloudlock can provide all the services mentioned in the question and all of them can offer data security whether directly or indirectly.
upvoted 1 times

[-] **bigdadzzz** 3 years, 8 months ago

In the reference link, under the Data Security section, it specifically states:
"Protect against exposures and a data security breach with highly-configurable data loss prevention engine with automated, policy-driven response actions"

While you're correct (it IS a terrible question), given the specific context of the question, answer "A" is correct.
upvoted 10 times

Which feature is supported when deploying Cisco ASAv within AWS public cloud?

- A. multiple context mode
- B. user deployment of Layer 3 networks
- C. IPv6
- D. clustering

Correct Answer: B

Reference:

<https://www.cisco.com/c/en/us/td/docs/security/asa/asa96/asav/quick-start-book/asav-96-qsg/asav-aws.html>

Community vote distribution

B (100%)

  **abdulmalik_mail** Highly Voted  2 years, 8 months ago

Yes It's B.

The ASAv on AWS supports the following features:

1. Support for Amazon EC2 C5 instances, the next generation of the Amazon EC2 Compute Optimized instance family.
2. Deployment in the Virtual Private Cloud (VPC)
3. Enhanced networking (SR-IOV) where available
4. Deployment from Amazon Marketplace
5. Maximum of four vCPUs per instance
6. User deployment of L3 networks
7. Routed mode (default)

upvoted 7 times

  **DWizard** Most Recent  1 year, 2 months ago

Selected Answer: B

The right option is B, here are listed the unsupported features which include IPv6, clustering and multiple context mode:

https://www.cisco.com/c/en/us/td/docs/security/asa/asa910/asav/quick-start-book/asav-910-qsg/asav_aws.html#id_45810

upvoted 1 times

Which cloud service model offers an environment for cloud consumers to develop and deploy applications without needing to manage or maintain the underlying cloud infrastructure?

- A. PaaS
- B. XaaS
- C. IaaS
- D. SaaS

Correct Answer: A

Community vote distribution

A (100%)

Thusi26 Highly Voted 2 years, 9 months ago

It's PaaS

PaaS

Platform-as-a-service (PaaS) is another step further from full, on-premise infrastructure management. It is where a provider hosts the hardware and software on its own infrastructure and delivers this platform to the user as an integrated solution, solution stack, or service through an internet connection.

upvoted 10 times

Emlia1 Most Recent 1 year, 7 months ago

Selected Answer: A

A is correct

upvoted 1 times

Thusi26 2 years, 9 months ago

SaaS

Software-as-a-service (SaaS), also known as cloud application services, is the most comprehensive form of cloud computing services, delivering an entire application that is managed by a provider, via a web browser

upvoted 1 times

prOfectus 2 years, 8 months ago

PaaS is the correct answer. With SaaS, the customer will only use the application, they won't have to develop nor deploy anything.

upvoted 14 times

Which risk is created when using an Internet browser to access cloud-based service?

- A. misconfiguration of Infra, which allows unauthorized access
- B. intermittent connection to the cloud connectors
- C. vulnerabilities within protocol
- D. insecure implementation of API

Correct Answer: C

Community vote distribution



zheka Highly Voted 2 years, 9 months ago

Disagree with protocol vulnerabilities. The answer is about insecure implementation of API
<https://www.imperva.com/blog/top-10-cloud-security-concerns/>
 upvoted 8 times

dummy 2 years, 7 months ago

API and Internet Browser? Definetly not!
 upvoted 4 times

[Removed] 7 months, 2 weeks ago

REST API and Internet Browser with Javascript and JSON? Definitely yes!
 upvoted 2 times

larn 2 years, 4 months ago

Agreed as stated the user is using a Web browser thus it cannot be API, the correct answer is C
 upvoted 5 times

Premium_Pils Most Recent 1 month ago

Selected Answer: D

I think it is about securing APIs. A web API can be accessed via web browser.
<https://stackoverflow.com/questions/29105007/how-to-make-basic-rest-api-calls-using-a-browser>
 upvoted 1 times

4pelos 6 months, 1 week ago

Correct answer C.
 Checked with securitytut
 upvoted 1 times

xziomal9 10 months, 1 week ago

Answer D
 upvoted 1 times

zamkijo 1 year, 2 months ago

Selected Answer: D

insecure API:
 A malicious user gained access to an organization's database from a cloud-base application programming interface that lacked strong authentication control. (from 350 - 701 practice exam)
 upvoted 2 times

stalkr3 1 year, 5 months ago

another showcase question why Cisco exams are utter garbage.
 upvoted 3 times

Tuxinator 1 year, 6 months ago

Selected Answer: C

Vulnerabilities within protocol:

Cross-site scripting (XSS) vulnerabilities: These allow attackers to inject malicious scripts into web pages viewed by other users.
 upvoted 4 times

Zatingke 1 year, 7 months ago


Selected Answer: D

Should be D.
 A poorly designed or implemented API could allow users accessing confidential data unintentionally, e.g. with a typo in the address box of a

browser.

- A. Wrong. Misconfigured infra, not specifically vulnerable to browsers
- B. Wrong. not that significant, although it is an availability issue in security perspective, but also nothing to do with a browser.
- C. Wrong, vulnerable within protocol? then which protocol? specific to a browser? then should be http or https, however, that also affects non-cloud-based services as well, right?

upvoted 2 times

  **Emlia1** 1 year, 8 months ago

I prefer C

upvoted 1 times

  **FortiSherlock** 2 years, 1 month ago

Selected Answer: A

VM might be publicly reachable and WebUI is weakly protected by a default password like Cisco123.

upvoted 1 times

  **NikoNiko** 2 years, 2 months ago

A - Misconfiguration of Infra, which leads to unauthorized access is CORRECT for me --> it joins 2 most often security issues of public cloud in one answer (see link below)

Question states BROWSER so API is probably not an option (D).

Vulnerabilities within protocol (C) - this is not specific to cloud, PROTOCOLS are being used everywhere and they are years old tuned standards with minimum vulnerabilities.

Option B - connection stability (?) --> means service availability, which is also security aspect but it is not such a big issue as option A and networks are reliable today (risk is DoS / DDoS but they are not asking about it).

A is correct.

<https://www.checkpoint.com/cyber-hub/cloud-security/what-is-cloud-security/top-cloud-security-issues-threats-and-concerns/>

upvoted 3 times

  **FortiSherlock** 2 years, 1 month ago

That is also my answer. You are responsible for configuring users and authentication / authorization for your Cloud, so if you do that in a dumb way it is insecure. Your AWS instances might be publicly reachable for SSL with a Cisco123 password - what do you think ?



upvoted 2 times

  **Sparrsh** 2 years, 5 months ago

Answer is D

Vulnerabilities within protocols that can expose confidential data

upvoted 2 times

  **Iarn** 2 years, 4 months ago

Vulnerabilities within protocols that can expose confidential data. That is C! not D

upvoted 3 times


What is the Cisco API-based broker that helps reduce compromises, application risks, and data breaches in an environment that is not on-premise?

- A. Cisco AppDynamics
- B. Cisco Cloudlock
- C. Cisco Umbrella
- D. Cisco AMP

Correct Answer: B

Community vote distribution

B (100%)


—  **sull3y** Highly Voted 1 year, 7 months ago

Cisco Cloudlock is a cloud-based security platform that helps organizations reduce the risk of data breaches and application risks in an environment that is not on-premise. It is an API-based broker that provides a comprehensive set of security controls and tools to secure data in the cloud. With Cloudlock, organizations can easily monitor and secure data in cloud-based services such as Google Apps, Microsoft Office 365, Salesforce, and more.

Cloudlock uses advanced security analytics and machine learning to identify and prevent threats such as data theft, malicious insider activity, and account takeover attacks. It also provides continuous monitoring and reporting to help organizations understand their security posture and identify potential risks.

By using Cloudlock, organizations can reduce the risk of compromises, application risks, and data breaches, and ensure the security of their data and systems in a cloud-based environment.

upvoted 5 times

—  **sull3y** 1 year, 7 months ago

it is B

upvoted 2 times

—  **FortiSherlock** Most Recent 2 years, 1 month ago

Selected Answer: B

Cloudlock is a CASB - Cloud Access Security BROKER. It is in the name.


upvoted 2 times

—  **abdulmalik_mail** 2 years, 8 months ago

It's B

<https://learn-umbrella.cisco.com/i/781077-cisco-umbrella-and-cloudlock/1?>

upvoted 3 times

—  **Raajaa** 3 years, 2 months ago

B is the answer

upvoted 3 times

Which two aspects of the cloud PaaS model are managed by the customer but not the provider? (Choose two.)

- A. middleware
- B. applications
- C. virtualization
- D. operating systems
- E. data

Correct Answer: *BE*

—  **sull3y** Highly Voted 1 year, 7 months ago

The two aspects of the cloud PaaS model that are managed by the customer but not the provider are:

B. applications: The customer is responsible for developing, deploying, and managing the applications that run on the platform. This can include custom applications or third-party applications that are integrated with the platform.

E. data: The customer is responsible for storing and managing their data, including backups and disaster recovery. This may include data that is stored in databases or file systems, or data that is transmitted between different components of the application.

The provider is responsible for managing the underlying infrastructure and platform components, such as virtualization, operating systems, middleware, and other components that support the applications.


upvoted 5 times

—  **Speckbrot** Most Recent 1 year, 1 month ago

Answer is B and E!

See <https://i0.wp.com/fourweekmba.com/wp-content/uploads/2020/12/what-is-saas.png?resize=1024%2C772&ssl=1>

upvoted 3 times

—  **zheka** 2 years, 9 months ago

Both answers are correct:

<https://www.cmswire.com/cms/information-management/cloud-service-models-iaas-saas-paas-how-microsoft-office-365-azure-fit-in-021672.php>

upvoted 4 times

Which public cloud provider supports the Cisco Next Generation Firewall Virtual?

- A. Google Cloud Platform
- B. Red Hat Enterprise Virtualization
- C. Amazon Web Services
- D. VMware ESXi

Correct Answer: *C*

—  **pr0fectus** Highly Voted 2 years, 8 months ago

As of this writing, GCP is now supported. So if ever the exam changes and asks for 2 answers then A & C would be the correct one.

upvoted 9 times

—  **geppo81** Most Recent 2 years, 2 months ago

If multiple choice are required

Deployment modes: Routed, transparent (inline set — IPS-only), and passive; AWS, Azure, GCP and OCI: routed mode only

<https://www.cisco.com/c/en/us/products/collateral/security/firepower-ngfw-virtual/threat-defense-virtual-ngfwv-ds.html>

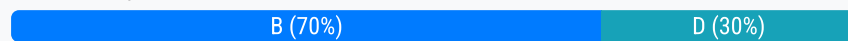
upvoted 2 times

What is an attribute of the DevSecOps process?

- A. security scanning and theoretical vulnerabilities
- B. development security
- C. isolated security team
- D. mandated security controls and check lists

Correct Answer: B

Community vote distribution



Premium_Pils 1 month ago

Selected Answer: B

As sis_net_sec and others wrote, it should be B
upvoted 1 times

Premium_Pils 1 month ago

<https://blogs.cisco.com/developer/flavorsofdevops01>

<https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/devsecops-addressing-security-challenges.html>

upvoted 1 times

MPoels 6 months, 1 week ago

Selected Answer: D

Like statikd about the mentioned DevSecOps manifesto wrote:

"Enabling businesses to address their most critical security requirements over a checklist or security mandates." Which is an attribute listed in the DevSecOps manifesto. Development security is overall what DevSecOps does, it's a given.

<https://blogs.cisco.com/security/devsecops-win-win-for-all>

see also: <https://www.base4sec.com/research/en/DevSecOps-Checklist/> and <https://www.devsecops.org/blog/tag/DevSecOps+Explained>

upvoted 3 times

DWizard 1 year, 2 months ago

Selected Answer: B

I'd go for B, even though it's not written in correct English, it should be security development:

https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/devsecops-infographic.pdf

"Using clearly defined guiding principles to drive security throughout the development process helps establish mutual trust among the Engineering, Operations and Security teams"

upvoted 1 times

sis_net_sec 2 years, 1 month ago

Selected Answer: B

DevSecOps (development, security, and operations) is a concept used in recent years to describe how to move security activities to the start of the development life cycle and have built-in security practices in the continuous integration/continuous deployment (CI/CD) pipeline. Thus minimizing vulnerabilities and bringing security closer to IT and business objectives.

Three key things make a real DevSecOps environment:

+ Security testing is done by the development team.

+ Issues found during that testing is managed by the development team.

+ Fixing those issues stays within the development team.

<https://blogs.cisco.com/security/devsecops-win-win-for-all>

upvoted 3 times

brownbear505 2 years, 6 months ago

Selected Answer: B

The drive toward shorter and more iterative development cycles, with a focus on delivering mission needs, is leading agencies to adopt DevSecOps (development, security, and operations) methodologies that enable development, security, and IT teams to work more closely and collaboratively.

<https://www.cisco.com/c/en/us/solutions/collateral/industries/government/cloud-ready-networks.html>

upvoted 2 times

coentror 2 years, 9 months ago

It is B. D can never be because it goes against the principles of Agile "mandate"

upvoted 2 times

👤 **hulisani** 2 years, 10 months ago

based on this both B and D are correct answers

What is an attribute of the DevSecOps?

What is an attribute of the DevSecOps process? security scanning and theoretical vulnerabilities. development security. isolated security team. mandated security controls and check lists

upvoted 1 times

👤 **kapplejacks** 2 years, 12 months ago

Just from a very basic angle, D is correct. "development security" is not proper grammar and broken English or something. Read the question then the answer, does it flow and sound like a Cisco answer? If i get this on the test and it really does say "development security" I am picking D. If it says "security development" I would pick B.

upvoted 1 times

👤 **itisfakemallo** 3 years, 2 months ago

B. development security

upvoted 2 times

👤 **dzef13** 3 years, 3 months ago

B

DevSecOps (development, security, and operations) is a concept used in recent years to describe how to move security activities to the start of the development life cycle and have built-in security practices in the continuous integration/continuous deployment (CI/CD) pipeline. Thus minimizing vulnerabilities and bringing security closer to IT and business objectives.

Three key things make a real DevSecOps environment:

- + Security testing is done by the development team.
- + Issues found during that testing is managed by the development team.
- + Fixing those issues stays within the development team.

upvoted 2 times

👤 **wfexco** 3 years, 3 months ago

It is a terrible question. I could see it being either B or D. I would go with D though.

DevOps is a deliberate effort to align the application development team with the application operations team, while SecDevOps introduces additional processes within the framework, to mitigate the chances that the Continuous Integration and Continuous Deployment (CI/CD) operational tempo will compromise application security.

upvoted 1 times

👤 **trickbot** 3 years, 4 months ago

If I get this question on the Exam, I will be answering B) Development Security. For reference, search "Cisco's DevSecOps Manifesto, where it explicitly states it's mission is to solve security problems with "Consumable Security Services over Mandated Security Controls" and "Collaboration to Securely enable Business, over Mandates" its a very Agile-ish manifesto. I found it here. <https://blogs.cisco.com/security/devsecops-win-win-for-all>

upvoted 3 times

👤 **statikd** 3 years, 2 months ago

But this same blog states: "Enabling businesses to address their most critical security requirements over a checklist or security mandates." Which is an attribute listed in the DevSecOps manifesto. Development security is overall what DevSecOps does, it's a given. I think the answer is

D

upvoted 8 times

👤 **jaciro11** 2 years, 9 months ago

Man exactly that's the best answer they don't ask about overall work of DevSecops.

They ask about attribute....

Answer D

upvoted 10 times

On which part of the IT environment does DevSecOps focus?


- A. application development
- B. wireless network
- C. data center
- D. perimeter network

Correct Answer: A

—  **sull3y** Highly Voted 1 year, 7 months ago

A. DevSecOps focuses on the application development part of the IT environment. DevSecOps is a software development philosophy that emphasizes collaboration and communication between development, operations, and security teams in order to secure the entire software development life cycle. DevSecOps aims to integrate security into the development process, starting from the design phase, through to deployment and ongoing management. By focusing on the application development environment, DevSecOps aims to improve the security of software applications, reduce the risk of vulnerabilities, and ensure that applications are secure from the start.

upvoted 5 times

—  **Jeeves69** Most Recent 3 years, 6 months ago

Answer: A - Application development

https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/devsecops-infographic.pdf

upvoted 4 times

In a PaaS model, which layer is the tenant responsible for maintaining and patching?

- A. hypervisor
- B. virtual machine
- C. network
- D. application

Correct Answer: D

Reference:

<https://www.bmc.com/blogs/saas-vs-paas-vs-iaas-whats-the-difference-and-how-to-choose/>


Which two deployment model configurations are supported for Cisco FTDv in AWS? (Choose two.)

- A. Cisco FTDv configured in routed mode and managed by an FMCv installed in AWS
- B. Cisco FTDv with one management interface and two traffic interfaces configured
- C. Cisco FTDv configured in routed mode and managed by a physical FMC appliance on premises
- D. Cisco FTDv with two management interfaces and one traffic interface configured
- E. Cisco FTDv configured in routed mode and IPv6 configured

Correct Answer: AC

Reference:

<https://www.cisco.com/c/en/us/products/collateral/security/adaptive-security-virtual-appliance-asav/white-paper-c11-740505.html>

  **micruguy** Highly Voted 2 years, 7 months ago

A & C are correct.
 Management console for NGFW
 Virtual FMC can be deployed on ESXi, KVM and in AWS
 Required for configuration, management & checking events
 NGFWv in cloud can be managed by FMC in AWS or FMC on
 premise (physical or virtual)
 FMC dashboard provides complete visibility

<https://www.ciscolive.com/c/dam/r/ciscolive/emea/docs/2019/pdf/BRKSEC-2064.pdf>
 upvoted 5 times

  **Cokamaniako** 1 year, 2 months ago

A & C
<https://www.ciscolive.com/c/dam/r/ciscolive/emea/docs/2019/pdf/BRKSEC-2064.pdf>
 Page 56
 upvoted 1 times

  **abdulmalik_mail** Most Recent 2 years, 8 months ago

Correct, It's A and C
 Based on reference "Cisco NGFWv in AWS (routed mode), Cisco NGFWv is deployed in routed mode and managed by an on premises FMC or FMC running in AWS"
 upvoted 4 times

  **Thusi26** 2 years, 9 months ago

A and C

Communications paths:

Management interface—Used to connect the ASAv to the ASDM; can't be used for through traffic.

Inside interface (required)—Used to connect the ASAv to inside hosts.


Outside interface (required)—Used to connect the ASAv to the public network.

DMZ interface (optional)—Used to connect the ASAv to the DMZ network when using the c3.xlarge interface.

upvoted 1 times

  **Joseph47** 1 year, 7 months ago

it seems 4 interfaces are required, even to boot, as per video (interface section).
https://www.youtube.com/watch?v=ycjTZhl_acQ&embeds_uri=https%3A%2F%2Fwww.google.com%2F&feature=emb_rel_pause
 upvoted 1 times

  **jccastiyo** 2 years, 10 months ago

I'd say A and B because C states "Physical" on premise and we can do both physical and virtual on premise.

<https://www.cisco.com/c/en/us/products/collateral/security/adaptive-security-virtual-appliance-asav/white-paper-c11-740505.html>



B is closer to right since we have 1 management and 2 data interfaces for FTDv in AWS, ignoring the diagnostic interface(eth0) since it's not mentioned here.

upvoted 1 times

  **duck_hat** 2 years, 9 months ago

https://www.cisco.com/c/en/us/td/docs/security/firepower/quick_start/aws/ftdv-aws-gsg/ftdv-aws-intro.html
 Firepower Threat Defense Virtual Limitations

The c4.xlarge is the recommended instance; the c3.xlarge instance has limited availability across AWS regions. You must have two management interfaces configured during launch. You must have two traffic interfaces and two management interfaces to launch, for a total of four interfaces.
upvoted 2 times

  **Raajaa** 3 years, 2 months ago

A and C

upvoted 2 times

DRAG DROP -

Drag and drop the steps from the left into the correct order on the right to enable Cisco AppDynamics to monitor an EC2 instance in AWS.

Select and Place:

Install monitoring extension for AWS EC2.	step 1
Restart the Machine Agent.	step 2
Update config.yaml.	step 3
Configure a Machine Agent or SIM Agent.	step 4

Correct Answer:

Install monitoring extension for AWS EC2.	Configure a Machine Agent or SIM Agent.
Restart the Machine Agent.	Install monitoring extension for AWS EC2.
Update config.yaml.	Update config.yaml.
Configure a Machine Agent or SIM Agent.	Restart the Machine Agent.

Reece_S Highly Voted 3 years, 1 month ago

Actually the answer is correct. According to this <https://www.appdynamics.com/community/exchange/extension/aws-ec2-monitoring-extension/>

The prerequisites states that you need a Standalone JAVA Machine Agent or SIM Agent; Which means you need to have that configured first before you can install the monitoring extension.

upvoted 14 times

MPoels 6 months, 1 week ago

config
install
update
restart

<https://web.archive.org/web/20200807125050/https://www.appdynamics.com/community/exchange/extension/aws-ec2-monitoring-extension/>

upvoted 1 times

jshow Highly Voted 3 years, 2 months ago

install
config
update
restart

Run 'mvn clean install' from aws-ec2-monitoring-extension

Copy and unzip AWSEC2Monitor-<version>.zip from 'target' directory into <machine_agent_dir>/monitors/

The metricPrefix of the extension has to be configured as specified here. Please make sure that the right metricPrefix is chosen based on your machine agent deployment, otherwise this could lead to metrics not being visible in the controller.

Edit config.yml file in AWSEC2Monitor and provide the required configuration (see Configuration section)

Restart the Machine Agent.

<https://www.appdynamics.com/community/exchange/extension/aws-ec2-monitoring-extension/>

upvoted 10 times

Tuxinator Most Recent 1 year, 6 months ago

it is recommended to install and configure the machine agent or the sim agent before installing the monitoring extension for AWS EC2. This is because the agent is required to run the monitoring extension and collect the necessary data for monitoring

upvoted 3 times

Totosos1 1 year, 5 months ago



So are you saying it should be:

1. Config
2. Install
3. Update
4. Restart

Can someone confirm, the AppDynamics link is a little misleading?



Many thanks,

upvoted 1 times

  **nomanlands** 2 years, 2 months ago

Must configure the agent first as a pre-req.
Install the AWS monitoring extension.
Configure yaml file
Restart

upvoted 1 times

  **otzu1** 2 years, 4 months ago

Makes sense,

you first need a machine to install the AWS EC2. Also Update the Yaml.config so when you restart it can be pushed back if needed.

Config Machine Agent

Install AWS EC2

Update YAML

Restart

upvoted 2 times

  **litespirit** 2 years, 6 months ago

The link below has been mostly misinterpreted. Reece_S is correct...

Config [Pre-requisite]

Install


Update

Restart

PreReq: AppDynamics Monitoring Extensions require either a Server Infrastructure and Monitoring (SIM) Agent or a stand-alone Machine Agent (MA) to report metrics to the AppDynamics Controller.

IMPORTANT | AppDynamics Extensions are only supported if there is a single instance of either a Machine Agent with APM Agents or a SIM Agent on a physical host. Multiple instances of Machine Agent or SIM on a single physical host are not supported for extensions installation.

upvoted 3 times

  **Seawanderer** 3 years, 2 months ago

Install 1, configure 2

upvoted 1 times

What is a required prerequisite to enable malware file scanning for the Secure Internet Gateway?

- A. Enable IP Layer enforcement.
- B. Activate the Cisco AMP license.
- C. Activate SSL decryption.
- D. Enable Intelligent Proxy.

Correct Answer: D

Community vote distribution

D (100%)

MPoels 6 months, 1 week ago

Selected Answer: D

Toggle on Enable Intelligent Proxy. When enabled, you have access to the following options: Inspect Files [...]

<https://docs.umbrella.com/deployment-msp/docs/enable-the-intelligent-proxy>

btw Support for the intelligent proxy is deprecated and only available for legacy deployments of the MSP console. The intelligent proxy is not available for new deployments of the MSP console.

upvoted 1 times

Dorr20 1 year, 5 months ago

This question is bad at so many levels.

The "File Inspection" in SIG is included in all Bundles, so there is no need to activate it, but still there is a warning on Cisco's website and I guess this makes it the correct answer.

My educated answer is B

This is way:

All terms are part of the "Advanced Settings" in the "DNS Policy" (the SIG adds us a "Web Policy" section).

IP Layer enforcement is a protection against malicious servers and it is end of life for over a year now (so A is wrong)

Turning on SSL decryption allows HTTPS URL blocking (so C is wrong).

Intelligent Proxy gains us visibility into threats, content or apps for risky domains (only). If the question was not about SIG, I would go with this answer, BUT It's not a true malware inspection like SIG has to offer (and that is way i think D is wrong).

In order to use File Analysis in SIG you need to make sure you have a license (see link below), enable HTTPS inspection etc.

<https://docs.umbrella.com/umbrella-user-guide/docs/manage-file-analysis>

upvoted 1 times

Tuxinator 1 year, 6 months ago

stop posting umbrella link's. SIG = not umbrella.

upvoted 1 times

Toni_Su91 1 year, 6 months ago

<https://umbrella.cisco.com/trends-threats/secure-internet-gateway>

Cisco Umbrella SIG unifies multiple security capabilities in the cloud to secure cloud adoption and direct internet access

upvoted 2 times

Tuxinator 1 year, 6 months ago

Don't you need a license before it actually works?

upvoted 4 times

sull3y 1 year, 7 months ago

The Secure Internet Gateway is a security solution that helps protect your organization's network and users from online threats such as malware. To enable malware file scanning, it is necessary to have the Intelligent Proxy feature enabled. The Intelligent Proxy provides an additional layer of security by examining and filtering out malicious traffic, including malware files, before they can reach your network. Without this feature, the Secure Internet Gateway may not be able to detect and prevent malware from entering your network.

upvoted 4 times

mecacig953 2 years, 5 months ago

Selected Answer: D

<https://docs.umbrella.com/deployment-umbrella/docs/configure-advanced-settings>

Advanced Settings let you enable various security settings including Umbrella's intelligent proxy, which gives Umbrella the ability to intercept and proxy requests for malicious files embedded within certain so-called "grey" domains. With the intelligent proxy, if a site is considered potentially

suspicious or could host malicious content, we'll return the IP address of the intelligent proxy. The request to that domain is then routed through our cloud-based secure gateway, and malicious content is found and stopped before it's sent to you.

upvoted 1 times

Question #169

Topic 1

A company is experiencing exfiltration of credit card numbers that are not being stored on-premise. The company needs to be able to protect sensitive data throughout the full environment. Which tool should be used to accomplish this goal?

- A. Cisco ISE
- B. Web Security Appliance
- C. Security Manager
- D. Cloudlock

Correct Answer: D

Community vote distribution

D (83%)

B (17%)

— **sull3y** **Highly Voted** 1 year, 7 months ago

The answer is D, Cloudlock. Cisco Cloudlock is an API-based broker that helps reduce compromises, application risks, and data breaches in an environment that is not on-premise. It provides protection of sensitive data throughout the full environment and helps secure cloud-based email, file storage, and web applications. Cloudlock detects and protects sensitive data across all cloud services, including cloud storage and collaboration services such as AWS, Box, Dropbox, Google Drive, Microsoft OneDrive, Salesforce, and more

upvoted 7 times

— **Moe1416** **Most Recent** 1 year, 9 months ago

Selected Answer: D

A company is experiencing exfiltration of credit card numbers that are NOT being stored on-premise.

Its NOT on premise

Answer is D

upvoted 3 times

— **Jariaya1** 1 year, 10 months ago

B = Cisco Cloudlock is a cloud-native cloud access security broker (CASB) that helps you move to the cloud safely. It protects your cloud users, data, and apps. Cisco Cloudlock provides visibility and compliance checks, protects data against misuse and exfiltration, and provides threat protections against malware like ransomware.

upvoted 1 times

— **nomanlands** 2 years, 2 months ago

Selected Answer: D

Cloudlock DLP

upvoted 2 times

— **DarkestHour** 2 years, 2 months ago

It says NOT on premise. So I suspect B is incorrect.

upvoted 3 times

— **wenorex222** 2 years, 3 months ago

Selected Answer: B

Correct answer is B, keyword on premise.

<https://www.cisco.com/c/en/us/products/collateral/security/web-security-appliance/solution-overview-c22-732948.html>

upvoted 1 times

— **GoldFree** 1 year, 3 months ago

No, the key word is said before on premise: "NOT being stored on-premise"

upvoted 1 times

What are the two types of managed Intercloud Fabric deployment models? (Choose two.)

- A. Service Provider managed
- B. User managed
- C. Public managed
- D. Hybrid managed
- E. Enterprise managed

Correct Answer: AE

Community vote distribution

AE (100%)

  **Medusa8** 1 year, 9 months ago

Selected Answer: AE

https://www.cisco.com/c/en/us/td/docs/solutions/Hybrid_Cloud/Intercloud/Intercloud_Fabric/Intercloud_Fabric_1.html#pgfld-2319061
upvoted 3 times

  **cesardgrd** 2 years, 7 months ago

AE
without a doubt
upvoted 1 times

  **abdulmalik_mail** 2 years, 8 months ago

Correct, It's AE
https://www.cisco.com/c/en/us/td/docs/solutions/Hybrid_Cloud/Intercloud/Intercloud_Fabric.pdf, please see on page 8 and 9 on PDF
upvoted 3 times

  **VI_Vershinin** 3 years, 1 month ago

It's a correct answer.
Cisco Intercloud Fabric addresses the cloud deployment requirements appropriate for two hybrid cloud deployment models: Enterprise Managed and Service Provider Managed.
upvoted 3 times

An engineer needs a cloud solution that will monitor traffic, create incidents based on events, and integrate with other cloud solutions via an API. Which solution should be used to accomplish this goal?

- A. CASB
- B. Cisco Cloudlock
- C. Adaptive MFA
- D. SIEM

Correct Answer: B

Community vote distribution

B (100%)

netwuy Highly Voted 3 years, 3 months ago

its clearly B
upvoted 11 times

itisfakemailol Highly Voted 3 years, 2 months ago

It's Cisco exam, so the correct answer is - B. Cisco Cloudlock
upvoted 9 times

cyberwhizzy0 Most Recent 1 year, 1 month ago

Selected Answer: B

The question is the definition of CASB but CASB is just the technology not that solution. Cloudlock, which is a cloud-native CASB, is the solution. Compare with Q184
upvoted 3 times

ddev3737 1 year, 7 months ago

Although Cisco exam, the most correction answer would be D Cisco has SIEM Cisco's Stealthwatch Cloud but that is not an option here. If that were present then it would stealthwatch instead of Cloudlock. I vote for D siem
upvoted 2 times

nomanlands 2 years, 2 months ago

Selected Answer: B

B since this is a Cisco exam. A SIEM could do this if you set it up to do so.
upvoted 1 times

brownbear505 2 years, 6 months ago

Selected Answer: B

Cisco Cloudlock for Google Workspace - Digital Marketplace

<https://www.digitalmarketplace.service.gov.uk/g-cloud/services/468189650542713>

upvoted 2 times

Minion2021 2 years, 6 months ago

It should be B
upvoted 1 times

flejd 2 years, 8 months ago

A and B is the same. I'd pick D
upvoted 1 times

Moll 2 years, 9 months ago

Answer should be B
upvoted 2 times

ZanaHiwa 2 years, 10 months ago

Answer B
upvoted 2 times

Sarbi 3 years ago

It is d.
upvoted 2 times

klu16 3 years ago


Come on guys, it's B...

+ Cisco Cloudlock continuously monitors cloud environments with a cloud Data Loss Prevention (DLP) engine to identify sensitive information stored in cloud environments in violation of policy.

+ Cloudlock is API-based.

+ Incidents are a key resource in the Cisco Cloudlock application. They are triggered by the Cloudlock policy engine when a policy detection criteria result in a match in an object (document, field, folder, post, or file).

upvoted 7 times

  **Dinges** 3 years, 2 months ago

A CASB, for any cloud solution. If the question specified a Cisco cloud solution, then B Cloudlock

upvoted 4 times

  **SirFrates24** 3 years, 2 months ago

SIEM software works by collecting log and event data generated by an organizations applications, security devices and host systems and bringing it together into a single centralized platform. ... In this way it detects threats and creates security alerts.

upvoted 3 times

  **statikd** 3 years, 2 months ago

I think it is D, SIEM (Security information and event management). https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise/design-zone-security-technology-partners/bn_cisco_siem.pdf

"This guide focuses on Cisco products and discusses how those products integrate with any third party SIEM product. "

"Customers need the ability to log, monitor, and report on security incidents in their data infrastructure, and to log, store, and report on large volumes of security event logs."

Cisco Cloudlock is a Cloud-Based Security Broker (CASB). "A CASB provides visibility and compliance checks, protects data against misuse and exfiltration, and provides threat protections against malware like ransomware." So basically Cloudlock is a DLP device.

upvoted 4 times

An organization is using Cisco Firepower and Cisco Meraki MX for network security and needs to centrally manage cloud policies across these platforms. Which software should be used to accomplish this goal?

- A. Cisco Defense Orchestrator
- B. Cisco Configuration Professional
- C. Cisco Secureworks
- D. Cisco DNA Center

Correct Answer: A

Reference:

<https://www.cisco.com/c/en/us/products/collateral/security/defense-orchestrator/datasheet-c78-736847.html>

  **sull3y** Highly Voted 1 year, 7 months ago

it is A

Cloud-based Firewall Management

Cisco Defense Orchestrator is a cloud-based management solution that allows you to manage security policies and device configurations with ease across multiple Cisco and cloud-native security platforms.

Cisco Defense Orchestrator centrally manages elements of policy and configuration across:

- Cisco Secure Firewall ASA, both on-premises and virtual
- Cisco Secure Firewall Threat Defense (FTD), both on-premises and virtual
- Cisco Meraki™ MX
- Cisco IOS devices
- AWS security groups

Cisco Defense Orchestrator also incorporates the cloud-delivered version of Firewall Management Center (FMC), providing a fully unified experience between on-premises and cloud-based firewall management. This expands management of policy and configuration to:

- Cisco Secure Firewall Threat Defense (FTD), both on-premises and virtual
- Cisco Secure IPS (formerly Firepower NGIPS)
- Cisco Firewall Threat Defense for ISR

upvoted 5 times

  **jshow** Most Recent 3 years, 2 months ago

A is correct

upvoted 3 times

Which factor must be considered when choosing the on-premise solution over the cloud-based one?

- A. With an on-premise solution, the provider is responsible for the installation and maintenance of the product, whereas with a cloud-based solution, the customer is responsible for it.
- B. With a cloud-based solution, the provider is responsible for the installation, but the customer is responsible for the maintenance of the product.
- C. With an on-premise solution, the provider is responsible for the installation, but the customer is responsible for the maintenance of the product.
- D. With an on-premise solution, the customer is responsible for the installation and maintenance of the product, whereas with a cloud-based solution, the provider is responsible for it.

Correct Answer: D

An engineer has been tasked with implementing a solution that can be leveraged for securing the cloud users, data, and applications. There is a requirement to use the Cisco cloud-native CASB and cloud cybersecurity platform. What should be used to meet these requirements?

- A. Cisco NGFW
- B. Cisco Cloudlock
- C. Cisco Cloud Email Security
- D. Cisco Umbrella

Correct Answer: B

  **statikd**  3 years, 2 months ago

Cisco Cloudlock is a Cloud-Based Security Broker (CASB). "A CASB provides visibility and compliance checks, protects data against misuse and exfiltration, and provides threat protections against malware like ransomware." So basically Cloudlock is a DLP device.

upvoted 6 times

  **GARBADOUR**  4 months ago

I've learnt that if Cloudlock is one of the possible solutions, the solution is always Cloudlock

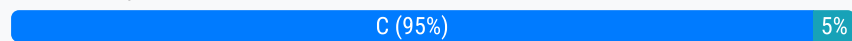
upvoted 2 times

In an IaaS cloud services model, which security function is the provider responsible for managing?

- A. firewalling virtual machines
- B. Internet proxy
- C. hypervisor OS hardening
- D. CASB

Correct Answer: A

Community vote distribution



Dead_Adriano Highly Voted 3 years, 2 months ago

Why A for IaaS? Shouldn't it be C?
upvoted 14 times

itisfakemai101 3 years, 2 months ago

Yes, it must be C
upvoted 17 times

Totosos1 Highly Voted 1 year, 5 months ago

<https://www.bmc.com/blogs/saas-vs-paas-vs-iaas-whats-the-difference-and-how-to-choose/>

According to IaaS, the provider is responsible for:

Virtualization
Servers
Storage
Networking

Hypervisor being the "Virtualisation", therefore C is the correct answer!
upvoted 7 times

Mohammad_h_tarawneh Most Recent 3 months, 1 week ago

I think, option A and C is valid, but regarding Security, I think firewalling is more specific and should be done before O.S hardening..
upvoted 1 times

mhd96far 5 months, 2 weeks ago

Selected Answer: C

C. hypervisor OS hardening Most Voted
upvoted 1 times

xziomal9 10 months, 1 week ago

Answer C
upvoted 1 times

Ko13 10 months, 1 week ago

Selected Answer: C

You have to take on account that there are multiple OSes here, Vendor is responsible for the hypervisor's OS version (currently Hyper-V Server 2022 is the latest as of today) while the VM's software version (Windows 11 for example) is not. <https://comparacloud.com/wp-content/uploads/2019/09/saas-vs-paas-vs-iaas.jpg>
upvoted 2 times

gc999 1 year, 5 months ago

Selected Answer: A

At the first look, I would choose "C". But after a while, "A" maybe more suitable. It is because for the "services" model, Hypervisor would not do "serve" to Cloud users but virtual machine does. For me, even I am running hypervisor, I seldom to take care of it since the management network is isolated to the public access.
upvoted 1 times

Emlia1 1 year, 9 months ago

Selected Answer: C

It's C
upvoted 4 times

tanri04 1 year, 10 months ago


With an IaaS model, the vendor is responsible for security of the physical data centers and other hardware that power the infrastructure -- including VMs, disks and networks. Users must secure their own data, operating systems and software stacks that run their applications. (my answer: C)

upvoted 3 times

  **Totosos1** 1 year, 5 months ago

How can your answer be C then. The question is asking "What is the Vendor responsible for" and your reply is saying that users are responsible for the Operating Systems, that means C is invalid based on your response?

upvoted 1 times

  **Ko13** 10 months, 1 week ago

You have to take on account that there are multiple OSes here, Vendor is responsible for the hypervisor's OS version (currently Hyper-V Server 2022 is the latest as of today) while the VM's software version (Windows 11 for example) is not. <https://comparacloud.com/wp-content/uploads/2019/09/saas-vs-paas-vs-iaas.jpg>

upvoted 1 times

  **sis_net_sec** 1 year, 11 months ago

Selected Answer: C

Infrastructure as a Service (IaaS) in cloud computing is one of the most significant and fastest growing fields. In this service model, cloud providers offer resources to users/machines that include computers as virtual machines, raw (block) storage, firewalls, load balancers, and network devices.

upvoted 1 times

  **FortiSherlock** 2 years, 1 month ago

Selected Answer: C

Clearly C in an IaaS environment.

upvoted 1 times

  **nemeses667** 2 years, 1 month ago

Surely C? [https://www.leanix.net/en/wiki/saas/iaas-vs-paas-vs-saas?](https://www.leanix.net/en/wiki/saas/iaas-vs-paas-vs-saas?utm_term=&utm_source=adwords&utm_medium=ppc&utm_campaign=UK+%7C+SMP+%7C+SaaS+Management+%7C+DSA+%7C+ENG&hsa_ver=3&hsa_cam=15150382310&hsa_grp=133953171750&hsa_acc=9751618594&hsa_kw=&hsa_mt=&hsa_net=adwords&hsa_src=g&hsa_tgt=dsa-1465784135448&hsa_ad=563932871660&gclid=Cj0KCQjw54iXBhCXARIsADWpsG-gPk26BNMvGPKFB34KtX0PVry-x1Wq5mNISFBDBLJkmlhvjUf2caAn2AEALw_wcB)

[utm_term=&utm_source=adwords&utm_medium=ppc&utm_campaign=UK+%7C+SMP+%7C+SaaS+Management+%7C+DSA+%7C+ENG&hsa_ver=3&hsa_cam=15150382310&hsa_grp=133953171750&hsa_acc=9751618594&hsa_kw=&hsa_mt=&hsa_net=adwords&hsa_src=g&hsa_tgt=dsa-1465784135448&hsa_ad=563932871660&gclid=Cj0KCQjw54iXBhCXARIsADWpsG-gPk26BNMvGPKFB34KtX0PVry-x1Wq5mNISFBDBLJkmlhvjUf2caAn2AEALw_wcB](https://www.leanix.net/en/wiki/saas/iaas-vs-paas-vs-saas?utm_term=&utm_source=adwords&utm_medium=ppc&utm_campaign=UK+%7C+SMP+%7C+SaaS+Management+%7C+DSA+%7C+ENG&hsa_ver=3&hsa_cam=15150382310&hsa_grp=133953171750&hsa_acc=9751618594&hsa_kw=&hsa_mt=&hsa_net=adwords&hsa_src=g&hsa_tgt=dsa-1465784135448&hsa_ad=563932871660&gclid=Cj0KCQjw54iXBhCXARIsADWpsG-gPk26BNMvGPKFB34KtX0PVry-x1Wq5mNISFBDBLJkmlhvjUf2caAn2AEALw_wcB)

upvoted 1 times

  **getafix** 2 years, 3 months ago

Selected Answer: C

A. firewalling virtual machines - isn't correct because the virtual machine setup in IaaS belongs to the client and the client is responsible for deploying a firewall and other software as they want

B. Internet proxy - isn't related

C. hypervisor OS hardening - correct answer since the provider is responsible for all security on the baremetal server which runs the hypervisor OS

D. CASB - isn't related as that's only a Cloud Access Security Broker

upvoted 5 times

  **TesterDude** 2 years, 3 months ago

Selected Answer: C

Answer is C

Customer Responsibilities:

Applications

Data

Middleware

OS

People

Runtime Environment

Virtual network and hosts

Security and patching of VMs

Provider Responsibilities

Hypervisors

Servers

Storage devices

Physical Network

upvoted 2 times

  **semi1750** 2 years, 4 months ago



D. is correct

you guys are all wrong.

It is asking which security function is responsible for managing in IaaS...

C is security related task provider is responsible in IaaS environment. but not security function....



upvoted 1 times

  **JGW** 2 years, 5 months ago

Selected Answer: C

in IAAS the service provider is responsible up to the hypervisor. <https://www.cisco.com/c/dam/en/us/solutions/collateral/design-zone/cisco-validated-profiles/safe-secure-cloud-architecture-guide.pdf> page 7

upvoted 4 times

  **Moll** 2 years, 9 months ago

Answer should be C

upvoted 4 times

Question #176

Topic 1



An organization wants to secure users, data, and applications in the cloud. The solution must be API-based and operate as a cloud-native CASB. Which solution must be used for this implementation?

- A. Cisco Cloud Email Security
- B. Cisco Cloudlock
- C. Cisco Umbrella
- D. Cisco Firepower Next-Generation Firewall

Correct Answer: B

Community vote distribution

B (100%)

  **crisip** 4 months, 3 weeks ago

Selected Answer: B

B. Cisco Cloudlock

upvoted 1 times

  **Alizade** 11 months, 2 weeks ago

Selected Answer: B

B. Cisco Cloudlock

upvoted 1 times

DRAG DROP -

Drag and drop the cloud security assessment components from the left onto the definitions on the right.

Select and Place:

user entity behavior assessment	develop a cloud security strategy and roadmap aligned to business priorities
cloud data protection assessment	identify strengths and areas for improvement in the current security architecture during onboarding
cloud security strategy workshop	understand the security posture of the data or activity taking place in public cloud deployments
cloud security architecture assessment	detect potential anomalies in user behavior that suggest malicious behavior in a Software-as-a-Service application

Correct Answer:

user entity behavior assessment	cloud security strategy workshop
cloud data protection assessment	cloud security architecture assessment
cloud security strategy workshop	cloud data protection assessment
cloud security architecture assessment	user entity behavior assessment

Max95 Highly Voted 3 years ago

Answer should be
 cloud security strategy workshop
 cloud security architecture assessment
 cloud data protection assessment
 user entity behaviour assessment

https://www.cisco.com/c/dam/m/en_sg/dc-innovation/assets/pdfs/securing-your-multicloud-journey.pdf
 upvoted 36 times

ZanaHiwa Highly Voted 2 years, 10 months ago

the Answer is:
 cloud security strategy workshop
 cloud security architecture assessment
 cloud data protection assessment
 user entity behavior assessment
 upvoted 5 times

Przemol Most Recent 1 year, 2 months ago

cloud security strategy workshop
 cloud security architecture assessment
 cloud data protection assessment
 user entity behaviour assessment

https://www.cisco.com/c/dam/m/en_sg/dc-innovation/assets/pdfs/securing-your-multicloud-journey.pdf
upvoted 1 times



  **Totosos1** 1 year, 5 months ago

I have the following for the Drag & Drop, as I can't make sense of the below answers from Max95 & ZanaHiwa:

1 > 4 - User Behaviour
2 > 3 - Data Protection
3 > 1 - Strategy
4 > 2 - Security Architecture
upvoted 1 times

  **Leogxn** 1 year, 1 month ago

All of you were basically telling the same thing. They clearly listed the results, you did not move the line in order but gave the movement.
upvoted 1 times

  **eazy99** 2 years, 11 months ago

I agree with you guys, I found a slide that defines each from Cisco and gives the answers.
<https://www.cisco.com/c/dam/en/us/products/security/security-strategy-advisory-aag.pdf>
upvoted 4 times

  **Sarbi** 3 years ago

Agreed with Max 95
upvoted 2 times

An organization wants to secure data in a cloud environment. Its security model requires that all users be authenticated and authorized. Security configuration and posture must be continuously validated before access is granted or maintained to applications and data. There is also a need to allow certain application traffic and deny all other traffic by default. Which technology must be used to implement these requirements?

- A. virtual routing and forwarding
- B. access control policy
- C. virtual LAN
- D. microsegmentation

Correct Answer: D

Community vote distribution

B (69%) D (31%)

jaciro11 Highly Voted 2 years, 6 months ago

Selected Answer: B

Microsegmentation is NOT for posturing checking. All the requirements criteria is met by Access Control Policies where you can define in ISE, Authentication, Authorization (Assign SGT in this part, which is the microsegmentation), then use Access List to deny or allow traffic

Answer is B

upvoted 19 times

Rododendron2 4 months ago

I incline more to microsegmentation. Access control and Identity based access is without doubt necessary part of that, but the whole enforcement technology is microsegmentation.

upvoted 1 times

Smilebloke Highly Voted 2 years, 5 months ago

The key point is all users must be authenticated / authorised (RBAC), using identity based access control, so ISE. Micro segmentation is also part of the solution using SGT. Access policy brings these components together. Answer: B

upvoted 6 times

Premium_Pils Most Recent 4 weeks ago

Selected Answer: B

They meant the broader term, Access Control Policy.

upvoted 1 times

Tthurston1 3 months ago

Selected Answer: D

Have to agree with the others who voted for Option D. The keywords that stood out to me were "...allowing certain application traffic and deny all other traffic by default." This is possible ONLY with microsegmentation. With ACL's - the opposite of that is true - traffic is allowed by default unless explicitly stated otherwise with rules denying certain traffic.

<https://www.cisco.com/c/en/us/products/security/what-is-microsegmentation.html>

upvoted 2 times

gorequill 7 months, 3 weeks ago

https://www.theasciiconstruct.com/post/sda_security_2/

D

upvoted 1 times

Alizade 11 months, 2 weeks ago

Selected Answer: D

The answer is D. microsegmentation.

upvoted 1 times

Jessie45785 1 year, 5 months ago

Selected Answer: B

they asking about the model, access control policy is not a model, microsegmentation is a security deployment model - I am going for B

upvoted 1 times

angry 1 year, 6 months ago

B is correct guys!

upvoted 2 times


  **Tuxzinator** 1 year, 6 months ago

Selected Answer: B

Its security model requires that all users be authenticated and authorized.


How does micro segmentation do this?

upvoted 3 times

  **psuoh** 1 year, 7 months ago

Micro-segmentation software uses network virtualization technology to create increasingly granular secure zones in data centers and cloud deployments, which isolate each individual workload and secure it separately.

upvoted 1 times

  **Anonymous983475** 1 year, 8 months ago

Selected Answer: D

I agree that it's D

upvoted 2 times

  **Emlia1** 1 year, 9 months ago

Selected Answer: D

I prefer D

upvoted 2 times

  **4000000** 1 year, 10 months ago

They r talking about and questioning technology..... Microsegmentation is the technology so D

upvoted 2 times

  **smartcarter** 1 year, 10 months ago

Answer is Microsegmentation. Software defined access provides Microsegmentation capabilities and centralised administration of which the Cisco ISE is part, hence the user part of the question.

<https://www.ciscopress.com/articles/article.asp?p=3100056&seqNum=3>

upvoted 2 times

  **sis_net_sec** 1 year, 11 months ago

Selected Answer: D

<https://www.cisco.com/c/en/us/products/security/what-is-microsegmentation.html>

upvoted 2 times

  **Jamesy** 1 year, 11 months ago

D is my answer guys. Cheers

upvoted 2 times

  **NikoNiko** 2 years, 1 month ago

It's B - Access Control Policy

I think that mentioned "cloud environment" in the question is just catch. Rest of the question is all about USERS, their authentication, authorization, POSTURE (you are not posturing applications or workloads in the cloud but users), deny/allow applications - TrustSec policy - all about ISE.

Microsegmentation is related to APPLICATIONS and WORKLOADS, I haven't found any mention about USERS.

"Micro-segmentation creates secure zones across cloud and data center environments to isolate application workloads from one another and secure them individually. With micro-segmentation, firewall policies limit east-west traffic between workloads based on a zero-trust security approach to reduce attack surfaces, prevent the lateral movement of threats to contain breaches, and strengthen regulatory compliance. Micro-segmentation is also referred to as application segmentation or east-west segmentation in a multicloud data center."

<https://www.cisco.com/c/en/us/products/security/what-is-microsegmentation.html>

upvoted 1 times

  **FortiSherlock** 2 years, 1 month ago

In DNA Center / SD Access the micro segmentation happens via SGTs. So one COULD argue that micro segmentation involves authentication in the Cisco world. You login via 802.1x and you get a role / an SGT assigned via which the segmentation happens via SGACLs.

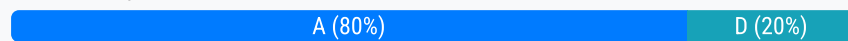
upvoted 3 times

Which cloud model is a collaborative effort where infrastructure is shared and jointly accessed by several organizations from a specific group?

- A. community
- B. private
- C. public
- D. hybrid

Correct Answer: A

Community vote distribution



Premium_Pils 4 weeks ago

Selected Answer: A

community cloud model
upvoted 1 times

Thusi26 2 years, 2 months ago

Selected Answer: A

community cloud model
A community cloud model is a collaborative effort where infrastructure is shared and jointly accessed by several organizations from a specific group that share specific computing concerns such as, security, compliance or jurisdiction considerations.
upvoted 3 times

Thusi26 2 years, 2 months ago

community cloud model
A community cloud model is a collaborative effort where infrastructure is shared and jointly accessed by several organizations from a specific group that share specific computing concerns such as, security, compliance or jurisdiction considerations.
upvoted 2 times

NullNull88 2 years, 9 months ago

Selected Answer: D

This isn't Hybrid? Why not? Community? Isn't this a Cisco exam?
upvoted 1 times

Fragalot 2 years, 9 months ago

It's Community - <https://blogs.cisco.com/datacenter/emerging-cloud-models-community-cloud>
upvoted 5 times

fukumoto0925 1 year, 10 months ago

Hybrid is a mixture of public cloud and private cloud, so it is actually Community
upvoted 4 times

How does Cisco Workload Optimization Manager help mitigate application performance issues?

- A. It automates resource resizing.
- B. It sets up a workload forensic score.
- C. It optimizes a flow path.
- D. It deploys an AWS Lambda system.

Correct Answer: A

Community vote distribution

A (100%)

—  **idto** Highly Voted 2 years, 9 months ago

Selected Answer: A

"Workload Optimization Manager continuously analyzes workload consumption, costs, and compliance constraints and automatically allocates resources in real time."

Source: <https://www.cisco.com/c/dam/en/us/products/collateral/servers-unified-computing/ucs-s-series-storage-servers/whitepaper-c11-741392.pdf>

upvoted 6 times

—  **yong08321** Most Recent 1 year, 4 months ago

Selected Answer: A

A. It automates resource resizing.

Cisco Workload Optimization Manager is designed to automate the management of applications and workloads across hybrid IT environments. It continuously monitors the performance of workloads and applications and makes recommendations for optimizing resources such as compute, storage, and network to improve performance. It can also automatically resize resources based on performance metrics to ensure that the application has the resources it needs to run effectively.

upvoted 1 times

Which DevSecOps implementation process gives a weekly or daily update instead of monthly or quarterly in the applications?

- A. CI/CD pipeline
- B. container
- C. orchestration
- D. security

Correct Answer: A

Reference:

<https://devops.com/how-to-implement-an-effective-ci-cd-pipeline/>

—  **idto** Highly Voted 2 years, 9 months ago

A is correct.

"Unlike the traditional software life cycle, the CI/CD implementation process gives a weekly or daily update instead of monthly or quarterly. The fun part is customers won't even realize the update is in their applications, as they happen on the fly."

Source: <https://devops.com/how-to-implement-an-effective-ci-cd-pipeline/amp/>

upvoted 5 times

Which system facilitates deploying microsegmentation and multi-tenancy services with a policy-based container?

- A. SDLC
- B. Lambda
- C. Contiv
- D. Docker

Correct Answer: D

Reference:

https://www.cisco.com/c/dam/global/es_es/pdfs/Cisco-cloudcenter-architecture-wp-c11-737224.pdf

Community vote distribution

C (100%)

Tuxzinator Highly Voted 1 year, 6 months ago

Selected Answer: C

C. Contiv

With Contiv, cloud architects and IT admin teams can create, manage and consistently enforce operational policies such as multi-tenant traffic isolation, microsegmentation, bandwidth prioritization, latency requirements, and policies

upvoted 6 times

gc999 1 year, 3 months ago

Agree.

<https://blogs.cisco.com/cloud/introducing-contiv-1-0#:~:text=With%20Contiv%2C%20cloud%20architects%2C%20and%20IT%20admin%20teams%20can%20create%2C%20manage%20and%20consistently%20enforce%20operational%20policies%20such%20as%20multi%2Dtenant%20traffic%20isolation%2C%20microsegmentation>

upvoted 2 times

jku2cya Most Recent 1 year, 2 months ago

Selected Answer: C

<https://blogs.cisco.com/cloud/introducing-contiv-1-0>

"create, manage and consistently enforce operational policies such as multi-tenant traffic isolation, microsegmentation..."

upvoted 3 times

yong08321 1 year, 4 months ago

Selected Answer: C

Contiv is an open-source system that provides infrastructure-level virtualization and policy-based networking to facilitate microsegmentation and multi-tenancy services deployment with a policy-based container. It is designed to provide a unified networking fabric across multiple container clusters, hypervisors, and cloud platforms.

upvoted 3 times

sull3y 1 year, 7 months ago

C. Contiv

Contiv is a system that facilitates deploying microsegmentation and multi-tenancy services with a policy-based container. Contiv provides a unified policy model for managing container networks, enabling administrators to easily segment traffic between different tenants and applications. The system allows administrators to define and enforce network security policies, providing a high degree of security and control over network traffic. With its focus on container-based deployment and its support for microsegmentation and multi-tenancy, Contiv provides a powerful solution for organizations looking to secure their containerized environments. By using a policy-based approach, Contiv helps organizations achieve a high level of network security and control, enabling them to securely deploy and manage containers at scale.

upvoted 3 times

Cyberops 2 years, 3 months ago

Selected Answer: C

With Contiv, cloud architects and IT admin teams can create, manage and consistently enforce operational policies such as multi-tenant traffic isolation, microsegmentation, bandwidth prioritization, latency requirements, and policies

upvoted 3 times

HACKERGK 2 years, 3 months ago

Selected Answer: C

its C. contiv

upvoted 2 times

ileri_sec 2 years, 4 months ago

Selected Answer: C

http://contiv.ciscolive.com/pod5/Intro/contiv_intro
upvoted 2 times

  **Yuta1123** 2 years, 4 months ago

Selected Answer: C

Why C ? I think D is answer.

Contive:

Flexible Policy Control

Contiv allows flexible policies to be applied to container networks, including per-application group policy control, bandwidth, QoS, etc.____

upvoted 2 times

  **Yuta1123** 2 years, 4 months ago

Sorry, why D? I think C is answer.

upvoted 1 times

Question #183

Topic 1

An organization is selecting a cloud architecture and does not want to be responsible for patch management of the operating systems. Why should the organization select either Platform as a Service or Infrastructure as a Service for this environment?

- A. Infrastructure as a Service because the customer manages the operating system.
- B. Platform as a Service because the service provider manages the operating system.
- C. Infrastructure as a Service because the service provider manages the operating system.
- D. Platform as a Service because the customer manages the operating system.

Correct Answer: B

Reference:

<https://www.cisco.com/c/en/us/solutions/cloud/what-is-cloud-computing.html#~cloud-computing-services>


How does a cloud access security broker function?

- A. It is an authentication broker to enable single sign-on and multi-factor authentication for a cloud solution.
- B. It scans other cloud solutions being used within the network and identifies vulnerabilities.
- C. It integrates with other cloud solutions via APIs and monitors and creates incidents based on events from the cloud solution.
- D. It acts as a security information and event management solution and receives syslog from other cloud solutions.

Correct Answer: C

Reference:

https://www.cisco.com/c/en_in/products/security/cloudlock/index.html#~stickynav=2

 **sull3y** 1 year, 7 months ago

C. It integrates with other cloud solutions via APIs and monitors and creates incidents based on events from the cloud solution.

A Cloud Access Security Broker (CASB) is a security solution that integrates with cloud solutions such as Software as a Service (SaaS), Infrastructure as a Service (IaaS), and Platform as a Service (PaaS) via APIs. It monitors cloud usage and creates incidents based on events from the cloud solution. This allows organizations to gain visibility into and control over their cloud usage, helping to protect against security threats and ensure compliance with security policies and regulations. CASBs can perform a variety of security-related functions, including identity and access management, data loss prevention, threat protection, and compliance enforcement, among others. By acting as an intermediary between cloud solutions and the organization, CASBs help to bridge the gap between security and cloud adoption, allowing organizations to securely adopt and manage cloud services.

upvoted 2 times

An organization has a requirement to collect full metadata information about the traffic going through their AWS cloud services. They want to use this information for behavior analytics and statistics. Which two actions must be taken to implement this requirement? (Choose two.)

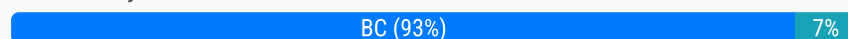
- A. Send syslog from AWS to Cisco Stealthwatch Cloud.
- B. Configure Cisco Stealthwatch Cloud to ingest AWS information.
- C. Send VPC Flow Logs to Cisco Stealthwatch Cloud.
- D. Configure Cisco Thousand Eyes to ingest AWS information.
- E. Configure Cisco ACI to ingest AWS information.

Correct Answer: AC

Reference:

<https://www.cisco.com/c/en/us/products/collateral/security/stealthwatch-cloud/at-a-glance-c45-739850.html>

Community vote distribution



[-] **loser4fun** Highly Voted 1 year, 6 months ago

C. Send VPC Flow Logs to Cisco Stealthwatch Cloud.

VPC Flow Logs are a feature that enables you to capture information about the IP traffic going to and from network interfaces in your VPC. Flow log data is stored using Amazon CloudWatch Logs, which can be easily exported to Cisco Stealthwatch Cloud for analysis and monitoring.

B. Configure Cisco Stealthwatch Cloud to ingest AWS information.

Once the VPC Flow Logs are collected, they can be ingested into Cisco Stealthwatch Cloud for analysis and monitoring. This requires configuring Cisco Stealthwatch Cloud to ingest the AWS information and setting up the appropriate rules and policies for analysis and alerting.

Therefore, options C and B are the correct answers.

upvoted 6 times

[-] **Yuta1123** Highly Voted 2 years, 4 months ago

Selected Answer: BC

I think BC is answer...

upvoted 6 times

[-] **sajoz123** 2 years, 4 months ago

Agree with you

upvoted 2 times

[-] **862e76c** Most Recent 10 months, 1 week ago

Selected Answer: BC

page 36 at: https://www.cisco.com/c/dam/en/us/td/docs/security/stealthwatch/cloud/deployment/Initial_Deployment_Guide_DV_2_3.pdf

upvoted 2 times

[-] **psuoh** 1 year, 7 months ago

Selected Answer: B

Configure AWS s3 bucket to store logs then grant Cisco Stealthwatch to read logs from it

<https://www.youtube.com/watch?v=rBz9jjMFdZc>

upvoted 1 times

[-] **tanri04** 1 year, 8 months ago

Yes correct answer: BC

upvoted 2 times

[-] **FortiSherlock** 2 years, 1 month ago

Selected Answer: BC

Configure StealthWatch Cloud and then send data from AWS to it.

upvoted 2 times

[-] **nomanlands** 2 years, 2 months ago

Selected Answer: BC

Can't syslog out data from AWS. At best you can send logs to an AWS bucket and pick them up from there.

upvoted 1 times

[-] **Cyberops** 2 years, 3 months ago

Selected Answer: BC

B and C

https://www.cisco.com/c/dam/en/us/td/docs/security/stealthwatch/cloud/configuration/Public_Cloud_Monitoring_for_AWS_Quick_Start_Guide_DV_2_0.pdf

upvoted 2 times

Question #186

Topic 1

An organization wants to implement a cloud-delivered and SaaS-based solution to provide visibility and threat detection across the AWS network. The solution must be deployed without software agents and rely on AWS VPC flow logs instead. Which solution meets these requirements?

- A. NetFlow collectors
- B. Cisco Cloudlock
- C. Cisco Stealthwatch Cloud
- D. Cisco Umbrella

Correct Answer: C



Reference:

<https://www.cisco.com/c/en/us/products/security/stealthwatch-cloud/index.html>

  **loser4fun** 1 year, 5 months ago

C. Cisco Stealthwatch Cloud meets these requirements. It is a cloud-delivered and SaaS-based solution that provides visibility and threat detection across AWS networks. It uses AWS VPC flow logs for traffic analysis and does not require software agents to be installed. Cisco Umbrella is a cloud-based security platform for DNS and web traffic protection and does not rely on AWS VPC flow logs for its operation. NetFlow collectors are used for collecting and analyzing network traffic data and are not a complete solution for providing visibility and threat detection across AWS networks. Cisco Cloudlock is a cloud access security broker that provides visibility and control over cloud applications and data but does not provide threat detection across AWS networks.

upvoted 3 times

  **leowulf** 1 year, 11 months ago

C

<https://www.cisco.com/c/en/us/products/security/stealthwatch-cloud/index.html>

upvoted 1 times

Where are individual sites specified to be blacklisted in Cisco Umbrella?

- A. application settings
- B. content categories
- C. security settings
- D. destination lists

Correct Answer: D

—  **idto** Highly Voted 2 years, 9 months ago

D is correct.

"To block a URL, simply enter it into a blocked destination list, or create a new blocked destination list just for URLs. To do this, navigate to Policies > Destination Lists, expand a Destination list, add a URL and then click Save."

Source: <https://support.umbrella.com/hc/en-us/articles/115004518146-Umbrella-Dashboard-New-Features-Custom-blocked-URLs>
upvoted 7 times

—  **[Removed]** Most Recent 2 years, 3 months ago

I worked on Umbrella, D is correct

upvoted 3 times

An engineer configured a new network identity in Cisco Umbrella but must verify that traffic is being routed through the Cisco Umbrella network. Which action tests the routing?

- A. Ensure that the client computers are pointing to the on-premises DNS servers.
- B. Enable the Intelligent Proxy to validate that traffic is being routed correctly.
- C. Add the public IP address that the client computers are behind to a Core Identity.
- D. Browse to <http://welcome.umbrella.com/> to validate that the new identity is working.

Correct Answer: D

Community vote distribution

D (100%)

— **juanlecho** Highly Voted 3 years, 5 months ago

Correct answer is D

<https://docs.umbrella.com/deployment-umbrella/docs/protect-your-network>

upvoted 28 times

— **hisho72** Highly Voted 3 years, 2 months ago

Correct Answer: Browse to <http://welcome.umbrella.com/> to validate that the new identity is working.

According to dump: Enable the Intelligent Proxy to validate that traffic is being routed correctly.

Verify that your DNS connections are routed through Cisco Umbrella's global network by navigating to the following page in your client's browser: <https://welcome.umbrella.com/>.

You should see the Welcome to Umbrella page.

Note: You may need to restart your client's network interface or your computer. <https://docs.umbrella.com/deployment-umbrella/docs/protect-your-network#section-step-4-test-yournetwork>

upvoted 10 times

— **[Removed]** Most Recent 7 months, 2 weeks ago

It says one needs to verify that traffic is routing through umbrella. Redirection is done with the intelligent proxy and the verification site is <http://proxy.opendnstest.com>. Therefore none of the answers are correct.

upvoted 1 times

— **mrimune** 2 years, 3 months ago

Correct is D

upvoted 1 times

— **[Removed]** 2 years, 3 months ago

answer is D. the welcome.umbrella.com is a testing URL that can help to verify that your using umbrella

upvoted 1 times

— **TesterDude** 2 years, 3 months ago

Selected Answer: D

The answer is D to test if Umbrella is protecting your network

upvoted 2 times

— **jaciro11** 2 years, 6 months ago

Selected Answer: D

Correct answer is D

upvoted 3 times

— **Minion2021** 2 years, 6 months ago

Obviously, the answer is D

upvoted 1 times

— **samismayilov** 3 years, 4 months ago

<http://welcome.umbrella.com/>

upvoted 5 times

How does Cisco Umbrella archive logs to an enterprise-owned storage?

- A. by using the Application Programming Interface to fetch the logs
- B. by sending logs via syslog to an on-premises or cloud-based syslog server
- C. by the system administrator downloading the logs from the Cisco Umbrella web portal
- D. by being configured to send logs to a self-managed AWS S3 bucket

Correct Answer: D

Reference:

<https://docs.umbrella.com/deployment-umbrella/docs/log-management>

Community vote distribution

D (100%)

  **Kevbo02** 2 years, 4 months ago

Selected Answer: D

It is D. <https://docs.umbrella.com/deployment-umbrella/docs/log-management> says you can also save your logs to an Amazon S3 Bucket.
upvoted 3 times

Which API is used for Content Security?

- A. NX-OS API
- B. IOS XR API
- C. OpenVuln API
- D. AsyncOS API



Correct Answer: D

Reference:


https://www.cisco.com/c/en/us/td/docs/security/security_management/sma/sma12-0/api/b_SMA_API_12/test_chapter_01.html

Community vote distribution

D (100%)

  **sull3y** 1 year, 5 months ago

The AsyncOS API is used for content security. It is a set of REST APIs provided by Cisco to enable integration and automation of content security features, such as email and web security, into third-party applications or management systems. The AsyncOS API allows developers to interact with the content security platform, retrieve information, and perform actions such as blocking or quarantining emails or URLs based on various criteria.
upvoted 2 times

  **Anonymous983475** 1 year, 8 months ago

Selected Answer: D

https://www.cisco.com/c/en/us/td/docs/security/security_management/sma/sma12-0/api/b_SMA_API_12/test_chapter_01.html
upvoted 2 times

Which Talos reputation center allows you to track the reputation of IP addresses for email and web traffic?

- A. IP Block List Center
- B. File Reputation Center
- C. AMP Reputation Center
- D. IP and Domain Reputation Center

Correct Answer: D

  **Zatingke** 1 year, 7 months ago

Correct

upvoted 1 times

What is the primary role of the Cisco Email Security Appliance?

- A. Mail Submission Agent
- B. Mail Transfer Agent
- C. Mail Delivery Agent
- D. Mail User Agent

Correct Answer: B

  **testtaker42** Highly Voted  3 years, 8 months ago

<https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/Aug2014/CVD-EmailSecurityUsingCiscoESADesignGuide-AUG14.pdf>

Third Paragraph in "Design Overview" section on Page 3.

upvoted 6 times

  **Premium_Pils** 4 weeks ago

"It does this by acting as a Mail Transfer Agent (MTA) within the email-delivery chain. Another name for an MTA is a mail relay."

upvoted 1 times

  **[Removed]** Most Recent  2 years, 3 months ago

ESA is not a mail server but an MTA. So B is correct.

upvoted 3 times

  **testtaker13** 2 years, 10 months ago

B - MTA is correct

upvoted 4 times

Which two services must remain as on-premises equipment when a hybrid email solution is deployed? (Choose two.)

- A. DDoS
- B. antispam
- C. antivirus
- D. encryption
- E. DLP

Correct Answer: DE

Reference:

https://www.cisco.com/c/dam/en/us/td/docs/security/ces/overview_guide/Cisco_Cloud_Hybrid_Email_Security_Overview_Guide.pdf

Community vote distribution

DE (100%)

idto Highly Voted 2 years, 9 months ago

D and E are correct. According to the Cisco doc they shared in the (Reveal Solution)...

"while the on-premises appliances provide granular control—protecting sensitive information with data loss prevention (DLP) and encryption technologies."

upvoted 6 times

gorequill Most Recent 7 months, 3 weeks ago

Selected Answer: DE

The cloud-based infrastructure is typically used for inbound email cleansing, while the on-premises appliances provide granular control—protecting sensitive information with data loss prevention (DLP) and encryption technologies.

upvoted 2 times

NikoNiko 2 years, 1 month ago

Sure, D.

"The cloud-based infrastructure is typically used for inbound email cleansing, while the on-premises appliances provide granular control—protecting sensitive information with data loss prevention (DLP) and encryption technologies."

Source (same as in Q response):

https://www.cisco.com/c/dam/en/us/td/docs/security/ces/overview_guide/Cisco_Cloud_Hybrid_Email_Security_Overview_Guide.pdf

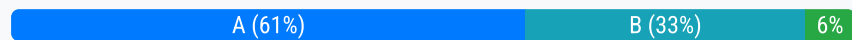
upvoted 2 times

An organization is receiving SPAM emails from a known malicious domain. What must be configured in order to prevent the session during the initial TCP communication?

- A. Configure the Cisco ESA to reset the TCP connection.
- B. Configure policies to stop and reject communication.
- C. Configure the Cisco ESA to drop the malicious emails.
- D. Configure policies to quarantine malicious emails.

Correct Answer: B

Community vote distribution



west33637 Highly Voted 1 year, 8 months ago

Selected Answer: A

A should be correct - TCPREFUSE resets the TCP connection. The question asks for preventing the session during the initial TCP communication. The remaining answers do not specify dropping the communication at TCP level.

upvoted 8 times

kerniger Highly Voted 3 years ago

hm it seems there is no clear valid answer

A - probably the best answer because if you configure as "TCPREFUSE" it will send a "reset" at tcp.

B - the client gets responses at a higher level than tcp

C - its not at tcp layer

D - its not at tcp layer

<https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118179-configure-esa-00.html>

upvoted 6 times

klu16 3 years ago

Based on this, I would go with B...

<https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118007-configure-esa-00.html>

upvoted 2 times

Premium_Pils Most Recent 4 weeks ago

Selected Answer: A

Answer "B", REJECT would be the preferable solution based on this article: <https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118007-configure-esa-00.html>. However, answering with "554 SMTP error" seems to correspond with Layer 7, and not with Layer 4 (TCP). A TCP Reset acts at Layer 4. Thus, for me it is "A".

upvoted 1 times

4pelos 6 months, 1 week ago

Correct answer B.

Checked with securitytut

upvoted 1 times

crisip 8 months, 3 weeks ago

Selected Answer: B

I think it is B

upvoted 1 times

fdl543 1 year, 1 month ago

Selected Answer: A

A is correct. "prevent the session during the initial TCP communication" Only reset the TCP connection does this. B continues to communicate with the reject communication...

upvoted 2 times


jku2cya 1 year, 2 months ago

Selected Answer: B

Typical ambiguous Cisco exam question. However I'd say A corresponds to TCPREFUSE and B corresponds to REJECT. B also mentions the word 'reject' in it.

Also the link provided by multiple people in this thread states "A host that attempts to establish a connection to your ESA and encounters a REJECT will receive a 554 SMTP error (hard bounce)"

upvoted 1 times

  **DWizard** 1 year, 2 months ago

Selected Answer: B

Based on the links already shared, the best answer would be B.

C and D does not work at the TCP level, and option A does not really reset the TCP connection, just ignore it, so the sender will try again to send the email.

Option B will work in a similar way to A, but instead of ignoring the TCP connection, will reject it so the sender won't try again.

It's a difficult one, I don't hope that everybody agrees with me.


upvoted 1 times

  **PeterHasse** 1 year, 2 months ago

I think is A

<https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118214-configure-esa-00.html>

upvoted 1 times

  **Jessie45785** 1 year, 3 months ago

Selected Answer: B

B - its cisco question must be B

<https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118007-configure-esa-00.html>

upvoted 1 times

  **theunnameddemon** 1 year, 4 months ago

To prevent the session during the initial TCP communication with a known malicious domain and stop receiving spam emails, the appropriate action would be:

A. Configure the Cisco ESA to reset the TCP connection.

By configuring the Cisco ESA (Email Security Appliance) to reset the TCP connection, it would terminate the connection attempt during the initial handshake process. This prevents any further communication between the sender and the recipient, effectively blocking the spam emails from that malicious domain.

Options B, C, and D are not specifically related to preventing the TCP session during initial communication:

Option B: Configuring policies to stop and reject communication might be effective in blocking or filtering certain types of traffic or communication, but it doesn't specifically prevent the TCP session from being established.

upvoted 1 times

  **sis_net_sec** 1 year, 11 months ago

Selected Answer: D

<https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118219-configure-esa-00.html>

upvoted 1 times

  **NikoNiko** 2 years, 1 month ago

"You can configure your Email Security Appliance (ESA) to restrict connections by adding any of these items to Sender Groups which use Mail Flow Policies:

IP range

Specific host or domain name

SenderBase Reputation Service (SBRS) "organization" classification

SBRS score range

DNS List query response

Each Mail Flow Policy has an access rule, such as ACCEPT, REJECT, RELAY, CONTINUE, and TCPREFUSE. A host that attempts to establish a connection to your ESA and matches a Sender Group using a TCPREFUSE access rule is not allowed to connect to your ESA."

Source (2014): <https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118007-configure-esa-00.html>

Newer (2021) - the same but TCPREFUSE is replaced by "TCP refuse":

<https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/216842-understand-parameters-related-to-mail-fl.html>

upvoted 2 times

  **lucky2205** 2 years, 2 months ago

Selected Answer: B

its B

Each Mail Flow Policy has an access rule, such as ACCEPT, REJECT, RELAY, CONTINUE, and TCPREFUSE. A host that attempts to establish a connection to your ESA and matches a Sender Group using a TCPREFUSE access rule is not allowed to connect to your ESA. From the standpoint of the sending server, it will appear as if your server is unavailable. Most MTAs will retry frequently in this case, which will create more traffic than answering once with a clear hard bounce, for example, REJECT.


<https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118007-configure-esa-00.html>

upvoted 2 times

  **Dorr20** 1 year, 5 months ago

A "reject" will send an NDR so it's not preventing the session. You also don't want a "known malicious" domain to know you are accepting message from other domains as you are trying to hide your ESA from attackers.

upvoted 2 times

  **[Removed]** 2 years, 3 months ago


I think the answer is A according to the cisco definition:

REJECT. Connection is initially accepted, but the client attempting to connect gets a 4XX or 5XX SMTP status code. No email is accepted.

Note: You can also configure AsyncOS to perform this rejection at the message recipient level (RCPT TO), rather than at the start of the SMTP conversation. Rejecting messages in this way delays the message rejection and bounces the message, allowing AsyncOS to retain more detailed information about the rejected messages. This setting is configured from the CLI listenerconfig > setup command.

TCPREFUSE. Connection is refused at the TCP level.

upvoted 2 times

  **Minion2021** 2 years, 6 months ago

Answer is B.

upvoted 3 times

  **efongvan** 2 years, 8 months ago

I would choose answer A. The question says prevent the session during the "initial TCP" communication.

The explanation from the link below for TCPREFUSE and REJECT.

TCPREFUSE: Connection is refused at the TCP level.

REJECT: Connection is initially accepted, but the client attempting to connect gets a 4XX or 5XX SMTP status code. No email is accepted.

<https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118179-configure-esa-00.html>

upvoted 1 times


```

Gateway of last resort is 1.1.1.1 to network 0.0.0.0

S*  0.0.0.0 0.0.0.0 [1/0] via 1.1.1.1, outside
C   1.1.1.0 255.255.255.0 is directly connect, outside
S   172.16.0.0 255.255.0.0 [1/0] via 192.168.100.1, inside
C   192.168.100.0 255.255.255.0 is directly connected, inside
C   172.16.10.0 255.255.255.0 is directly connected, dmz
S   10.10.10.0 255.255.255.0 [1/0] via 172.16.10.1, dmz

-----

access-list redirect-acl permit ip 192.168.100.0 255.255.255.0 any
access-list redirect-acl permit ip 172.16.0.0 255.255.0.0 any

class-map redirect-class
match access-list redirect-acl

policy-map inside-policy
class redirect-class
sfr fail-open

service-policy inside-policy global

```

Refer to the exhibit. What is a result of the configuration?

- A. Traffic from the DMZ network is redirected.
- B. Traffic from the inside network is redirected.
- C. All TCP traffic is redirected.
- D. Traffic from the inside and DMZ networks is redirected.

Correct Answer: D

Community vote distribution

D (100%)

LynenDutzow Highly Voted 3 years, 9 months ago

The answer is definitely D.

The ACL's match 192.168.100.0 to 192.168.100.255 and 172.16.0.0 to 172.16.255.255. The DMZ and inside network fall in those ranges.
upvoted 14 times

getafix Highly Voted 2 years, 3 months ago

Selected Answer: D

Traffic from both inside and DMZ networks is redirected.
Inside networks are 192.168.100.0/24 and 172.16.0.0/16
DMZ network is 172.16.10.0/24

The redirect acl is permitting 192.168.100.0/24 and 172.16.0.0/16 (which also includes 172.16.10.0/24 --> traffic from DMZ networks)
upvoted 7 times

Alizade Most Recent 11 months, 2 weeks ago

Selected Answer: D

Answer: D

upvoted 1 times

TWu2 2 years, 7 months ago

10.10.10.0/24 (to DMZ) is not in the access-list. So the answer is B only.

upvoted 3 times

Moll 2 years, 9 months ago

Yes, should be D

upvoted 2 times

statikd 3 years, 2 months ago

Answer is D

192.168.100.0 255.255.255.0 is directly connected, inside
172.16.10.0 255.255.255.0 is directly connected, dmz

Both ACLs apply to these networks.

upvoted 3 times

  **oncledave** 3 years, 8 months ago

What about the last static route 10.10.10.0/24 , part of the dmz ?
The inside network, as well as part of the dmz fall in those ranges.

upvoted 1 times

  **netguy** 3 years, 3 months ago



D is correct. Answer D does not state that all networks from inside and DMZ are redirected, just the (some) traffic is redirected.

upvoted 4 times

  **dr4gn00t** 2 years, 7 months ago



correct answer would be: traffic from inside networks and traffic from DMZ DIRECTLY CONNECTED network are redirected. Terribly question as both B and D are can be considered correct answers.

upvoted 2 times

  **Oz3006** 3 years, 11 months ago

forget what is said, answer is D

upvoted 6 times

  **Oz3006** 3 years, 11 months ago

answer is B


If you look at the 172.16.10.0/24 for DMZ does not match the access list 172.16.0.0/16

upvoted 2 times

  **mecacig953** 2 years, 5 months ago

yes to this

upvoted 2 times

  **Initial14** 1 year, 11 months ago



172.16.10.0 matches 172.16.0.0/16... 172.16.0.0 255.255.0.0 has rage of 172.16.0.0 - 172.16.255.255

upvoted 1 times

  **Jimmyluckyone** 3 years, 11 months ago

The access-list also matches the DMZ network 172.16.10.0 so D is correct

upvoted 4 times

  **AZak** 3 years, 11 months ago

Is it D ? Im not 100% sure. Couldn't it maybe B ?

upvoted 1 times


Question #196

Topic 1

An organization received a large amount of SPAM messages over a short time period. In order to take action on the messages, it must be determined how harmful the messages are and this needs to happen dynamically. What must be configured to accomplish this?

- A. Configure the Cisco WSA to modify policies based on the traffic seen.
- B. Configure the Cisco ESA to modify policies based on the traffic seen.
- C. Configure the Cisco WSA to receive real-time updates from Cisco Talos.
- D. Configure the Cisco ESA to receive real-time updates from Cisco Talos.

Correct Answer: D

  **Zatingke** 1 year, 7 months ago

Correct

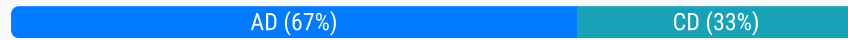
upvoted 2 times

What are two differences between a Cisco WSA that is running in transparent mode and one running in explicit mode? (Choose two.)

- A. The Cisco WSA responds with its own IP address only if it is running in explicit mode.
- B. The Cisco WSA is configured in a web browser only if it is running in transparent mode.
- C. The Cisco WSA responds with its own IP address only if it is running in transparent mode.
- D. The Cisco WSA uses a Layer 3 device to redirect traffic only if it is running in transparent mode.
- E. When the Cisco WSA is running in transparent mode, it uses the WSA's own IP address as the HTTP request destination.

Correct Answer: AD

Community vote distribution



  **wfexco** Highly Voted  3 years, 3 months ago

A and D are correct. - In explicit proxy mode, users are configured to use a web proxy and the web traffic is sent directly to the Cisco WSA. In contrast, in transparent proxy mode the Cisco WSA intercepts user's web traffic redirected from other network devices, such as switches, routers, or firewalls.

upvoted 21 times

  **Sarbi** Highly Voted  3 years ago

A and D is correct. No doubt it.



upvoted 5 times

  **Premium_Pils** Most Recent  4 weeks ago

Selected Answer: AD

I am sure about "D" as a the traffic is redirected on a L3 device with PBR (or similar solution). "A" would be fine without the word "only". The WSA is a full proxy, maintaining separate sessions btw. client - proxy and proxy - webserver. The source IP of the response is surely the ip of the proxy in the client-proxy connection with Explicit mode, when the client directly communicates with the proxy. However, I am not sure the redirected Transparent mode, as again the proxy is sitting in between the client and the webserver. I assume that the client does not get the response directly from the webserver, but rather from the proxy. So the source ip should be from the proxy (or does it spoof the source ip?).



upvoted 1 times

  **squirrelzzz** 5 months, 3 weeks ago

Selected Answer: AD

Transparent means it has no L3 interface

upvoted 1 times

  **Leogxn** 1 year, 1 month ago

Selected Answer: CD

Reference: CCNP And CCIE Security Core SCOR 350-701 Official Cert Guide-> Therefore in Transparent mode, WSA uses its own IP address to initiate a new connection the Web Server

upvoted 1 times

  **Bubu3k** 1 month, 2 weeks ago

The only problem is that that quote is nowhere in the OCG... It's AD: actual quote from the OCG: "When the Cisco WSA (as a web proxy) forwards a request, by default it changes the request source IP address to match its own address."

upvoted 2 times

  **andrewj511** 2 years, 11 months ago

When requests are being redirected to the WSA transparently, the WSA must pretend to be the OCS (origin content server), since the client is unaware of the existence of a proxy. On the contrary, if a request is explicitly sent to the WSA, the WSA will respond with it's own IP information.


upvoted 4 times

  **rad9899** 3 years, 4 months ago

C&E is correct

<https://www.cisco.com/c/en/us/support/docs/security/web-security-appliance/117940-qa-wsa-00.html>

upvoted 1 times

  **entitty** 3 years, 3 months ago

Not C, But A - leaning toward D (wish it stated Layer4)

When requests are being redirected to the WSA transparently, the WSA must pretend to be the OCS (origin content server), since the client is unaware of the existence of a proxy. On the contrary, if a request is explicitly sent to the WSA, the WSA will respond with it's own IP information.

upvoted 4 times

Which technology is used to improve web traffic performance by proxy caching?

- A. WSA
- B. Firepower
- C. FireSIGHT
- D. ASA

Correct Answer: A

  **Zatingke** 1 year, 7 months ago

Correct, WSA can be a proxy cache
upvoted 1 times

Which proxy mode must be used on Cisco WSA to redirect TCP traffic with WCCP?

- A. transparent
- B. redirection
- C. forward
- D. proxy gateway



Correct Answer: A

Reference:

<https://www.cisco.com/c/en/us/support/docs/security/web-security-appliance/117940-qa-wsa-00.html>

Community vote distribution

A (100%)

  **cyberwhizzy0** 1 year, 1 month ago

Selected Answer: A

How the WSA HTTP proxy obtains the client's request can be defined as one of two ways: Transparently or Explicitly.



Deployment: Transparent

Method: WCCP

Description: A WCCP v2 enabled device (typically a router, switch, PIX, or ASA) redirects port 80

<https://www.cisco.com/c/en/us/support/docs/security/web-security-appliance/117940-qa-wsa-00.html>

upvoted 2 times

  **gc999** 1 year, 5 months ago

I guess this question should be rewritten as "Which mode must be used on Cisco WSA to redirect TCP traffic with WCCP?". There is no "transparent proxy mode", there is only "forward proxy mode".

upvoted 1 times

What is the purpose of the Decrypt for Application Detection feature within the WSA Decryption options?

- A. It decrypts HTTPS application traffic for unauthenticated users.
- B. It alerts users when the WSA decrypts their traffic.
- C. It decrypts HTTPS application traffic for authenticated users.
- D. It provides enhanced HTTPS application detection for AsyncOS.

Correct Answer: D

Reference:

https://www.cisco.com/c/en/us/td/docs/security/wsa/wsa11-7/user_guide/b_WSA_UserGuide_11_7/b_WSA_UserGuide_11_7_chapter_01011.html

 **ddev3737** 1 year, 7 months ago

D

Decryption Option

Description

Decrypt for Authentication

For users who have not been authenticated prior to this HTTPS transaction, allow decryption for authentication.

Decrypt for End-User Notification

Allow decryption so that AsyncOS can display the end-user notification.

Note

If the certificate is invalid and invalid certificates are set to drop, when running a policy trace, the first logged action for the transaction will be "decrypt".

Decrypt for End-User Acknowledgment

For users who have not acknowledged the web proxy prior to this HTTPS transaction, allow decryption so that AsyncOS can display the end-user acknowledgment.

Decrypt for Application Detection

Enhances the ability of AsyncOS to detect HTTPS applications.

upvoted 2 times

A network administrator is using the Cisco ESA with AMP to upload files to the cloud for analysis. The network is congested and is affecting communication. How will the Cisco ESA handle any files which need analysis?

- A. The ESA immediately makes another attempt to upload the file.
- B. The file upload is abandoned.
- C. AMP calculates the SHA-256 fingerprint, caches it, and periodically attempts the upload.
- D. The file is queued for upload when connectivity is restored

Correct Answer: B

Community vote distribution

B (67%) C (17%) A (17%)

Seawanderer Highly Voted 3 years, 2 months ago

I'm not really sure about the answer, but it could be B

"The appliance will try once to upload the file; if upload is not successful, for example because of connectivity problems, the file may not be uploaded. If the failure was because the file analysis server was overloaded, the upload will be attempted once more."

<https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118796-technote-esa-00.html>

upvoted 18 times

pohqinan 2 years, 5 months ago

Agree With this.

upvoted 1 times

kerniger Highly Voted 3 years ago

its B

"The appliance will try once to upload the file; if upload is not successful, for example because of connectivity problems, the file may not be uploaded. If the failure was because the file analysis server was overloaded, the upload will be attempted once more."

<https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118796-technote-esa-00.html>

upvoted 12 times

Mulema Most Recent 9 months, 2 weeks ago

The correct answer to me even is D. The first part of the question is just noise to distract.

The emphasis to me is the second half of the question - How will Cisco ESA handle any files which need analysis?

The Cisco ESA will not abandon the file upload. Instead, it will continue to attempt to upload the file until communication is restored. If the file is still not uploaded after a certain period of time, the Cisco ESA will cache the file and continue to attempt to upload it periodically

<https://bard.google.com/chat/e3b8e30fe3160083>

upvoted 3 times

Bandito 1 year, 2 months ago

Selected Answer: B

There is a video from a Cisco engineer.

<https://youtu.be/WD7UD70e2mo?t=453>

I believe the answer is B.

upvoted 2 times

itsklk 1 year, 4 months ago

Selected Answer: A

Read this : <https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118796-technote-esa-00.html#anc5>

Highlighting important notes:

If a file has recently been uploaded from any source, the file will not be uploaded again. For file analysis results for this file, search for the SHA-256 from the File Analysis reporting page.

The appliance will try once to upload the file; if upload is not successful, for example because of connectivity problems, the file may not be uploaded. If the failure was because the file analysis server was overloaded, the upload will be attempted once more.

upvoted 1 times

ddev3737 1 year, 7 months ago

The appliance will try once to upload the file; if upload is not successful, for example because of connectivity problems, the file may not be uploaded. If the failure was because the file analysis server was overloaded, the upload will be attempted once more

upvoted 1 times

Anonymous983475 1 year, 8 months ago

Selected Answer: C

The AMP first tries to compare file's hash to the cloud DB and if there is no such file it tries to upload it. It will retry if the upload fails.
upvoted 2 times

sis_net_sec 1 year, 11 months ago

Selected Answer: A

<https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118796-technote-esa-00.html>
upvoted 1 times

lucky2205 2 years, 2 months ago

Selected Answer: B

its B
the question clearly states that "The network is congested and is affecting communication." & its mentioned in ESA configuration guide "The appliance will try once to upload the file; if upload is not successful, for example because of connectivity problems, the file may not be uploaded."

<https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118796-technote-esa-00.html>
upvoted 6 times

bob511 2 years, 6 months ago

Cisco ESA adds a record of the SHA256 of this file to its internal database, where it is kept for up to 12 hours, and starts periodically querying if the analysis was complete, until it receives a positive response back from the file analysis service

i think C
upvoted 6 times

eazy99 2 years, 11 months ago

I actually believe the answer is D. I got it from Cisco website, here is the paragraph "The appliance will try once to upload the file; if upload is not successful, for example because of connectivity problems, the file may not be uploaded. If the failure was because the file analysis server was overloaded, the upload will be attempted once more."
Please feel free to correct me if you think it's not.

This is the link:

You will find it as the second point where they say Highly Important Notes:

<https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118796-technote-esa-00.html#anc1>
upvoted 3 times

eazy99 2 years, 11 months ago

I apologize, I meant A not D.
upvoted 2 times

psuoh 1 year, 7 months ago

" If the failure was because the file analysis server was overloaded the upload will be attempted once more. " The network is congested as the question points out. The question doesnt mention about the analysis server being overloaded.
upvoted 1 times

kapplejacks 2 years, 12 months ago

There is NO (Zero) file upload, only a hash exchange making answer C the only correct answer.
upvoted 6 times

kapplejacks 2 years, 12 months ago

Cisco likes to do this, do not go down the path they are leading where they want you to over think. They would have said the file analysis server was overloaded if they wanted you to know about periodic upload. This question test your ability to know how AMP communicates about file reputation.

upvoted 5 times

Sarbi 3 years ago

What about A.

Highlighting important notes:

If a file has recently been uploaded from any source, the file will not be uploaded again. For file analysis results for this file, search for the SHA-256 from the File Analysis reporting page.



The appliance will try once to upload the file; if upload is not successful, for example because of connectivity problems, the file may not be uploaded. If the failure was because the file analysis server was overloaded, the upload will be attempted once more.

upvoted 2 times

An engineer is configuring a Cisco ESA and wants to control whether to accept or reject email messages to a recipient address. Which list contains the allowed recipient addresses?

- A. SAT
- B. BAT
- C. HAT
- D. RAT

Correct Answer: D

  **sull3y** 1 year, 5 months ago

The correct answer is D. RAT (Recipient Access Table).

The Cisco ESA (Email Security Appliance) can be used to control whether to accept or reject email messages to a recipient address. The list that contains the allowed recipient addresses is called the Recipient Access Table (RAT).

The Recipient Access Table (RAT) is a list of email addresses that have been authorized to receive emails. When an email is received, the Cisco ESA checks the email address against the list in the RAT to determine whether to accept or reject the email.

upvoted 2 times



  **Kyle1776** 2 years, 6 months ago

Overview of the Recipient Access Table (RAT)

The Recipient Access Table defines which recipients are accepted by a public listener. At a minimum, the table specifies the address and whether to accept or reject it.

The Recipient Access Table (RAT) page shows a listing of the entries in the RAT including the order, default action, and whether or not the entry has been configured to bypass LDAP accept queries.

upvoted 2 times

  **Cock** 2 years, 6 months ago

AsyncOS uses the RAT for each Public Listener for managing acceptance or rejection of recipient addresses. Recipient addresses include these:

Domains

Email addresses

Groups of email addresses

By default, the RAT rejects all recipients to prevent the creation of an open relay.

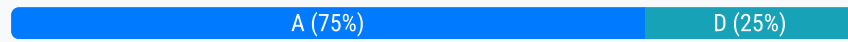
upvoted 1 times

Why would a user choose an on-premises ESA versus the CES solution?

- A. Sensitive data must remain onsite.
- B. Demand is unpredictable.
- C. The server team wants to outsource this service.
- D. ESA is deployed inline.

Correct Answer: A

Community vote distribution



ZappBrannigan 3 months, 1 week ago

Selected Answer: D

D - I think could be correct as well. Not sure how you can deploy a cloud based solution inline.
upvoted 1 times

Cock 2 years, 6 months ago


Selected Answer: A

Cloud Email Security(CES)
upvoted 3 times



Which two features are used to configure Cisco ESA with a multilayer approach to fight viruses and malware? (Choose two.)

- A. Sophos engine
- B. white list
- C. RAT
- D. outbreak filters
- E. DLP



Correct Answer: AD

  **Pakawat** 8 months, 3 weeks ago



Found this one in the exam
upvoted 1 times

  **san111** 2 years, 10 months ago

A , D
CVD-EmailSecurityUsingCiscoESADesignGuide-AUG14.pdf
upvoted 3 times

  **jshow** 3 years, 1 month ago

A and D sophos is av engine
upvoted 1 times

  **jshow** 3 years, 2 months ago

D for sure
Cisco ESA uses a multilayer approach to fight viruses and malware:

- The first layer of defense consists of outbreak filters, which the appliance downloads from Cisco SenderBase. They contain a list of known bad mail servers. These filters are generated by watching global email traffic patterns and looking for anomalies associated with an outbreak. When an email is received from a server on this list, it is kept in quarantine until the antivirus signatures are updated to counter the current threat.
- The second layer of defense is using antivirus signatures to scan quarantined emails, to ensure that they do not carry viruses into the network.
- Cisco ESA also scans outbound emails to provide antivirus protection.

upvoted 3 times

After a recent breach, an organization determined that phishing was used to gain initial access to the network before regaining persistence. The information gained from the phishing attack was a result of users visiting known malicious websites. What must be done in order to prevent this from happening in the future?

- A. Modify web proxy settings.
- B. Modify outbound malware scanning policies.
- C. Modify identification profiles.
- D. Modify an access policy.

Correct Answer: A

Community vote distribution

A (64%) D (36%)

entity Highly Voted 3 years, 3 months ago

A - Configuring Web Proxy Settings - https://www.cisco.com/c/en/us/td/docs/security/wsa/wsa11-0/user_guide/b_WSA_UserGuide/b_WSA_UserGuide_chapter_0100.html
upvoted 15 times

ureis 1 year, 8 months ago

Why Intercepting Web Requests if we can block specific URL in a ACP policy ?
D is the answer imo
upvoted 3 times

larn Highly Voted 2 years, 4 months ago

Selected Answer: A

The Web Security appliance intercepts requests that are forwarded to it by clients or other devices over the network.

The appliance works in conjunction with other network devices to intercept traffic. These may be ordinary switches, transparent redirection devices network taps, and other proxy servers or Web Security appliances.
upvoted 5 times

Premium_Pils Most Recent 4 weeks ago

Selected Answer: A

A - WSA. "Web reputation filtering protects client devices from visiting potentially harmful websites that contain malware or phishing links." + "URLs are checked against a list of known websites in the Cisco URL filtering database of more than 50 million blacklisted sites." <https://studyccnp.com/cisco-secure-web-appliance-cisco-wsa/>, https://www.cisco.com/c/en/us/td/docs/security/esa/esa14-0/user_guide/b_ESA_Admin_Guide_14-0/b_ESA_Admin_Guide_12_1_chapter_010000.html
upvoted 1 times

MPoels 6 months, 1 week ago

Selected Answer: D

Configure URL filters for Access Policy
<https://www.cisco.com/c/en/us/support/docs/security/secure-web-appliance-virtual/220557-configure-custom-url-categories-in-secr.html#toc-hId--1455911870>
upvoted 3 times

bobie 1 year, 3 months ago

Selected Answer: A

I chose A since the term "malicious website" corresponds to the topic WSA.
upvoted 1 times

Dorr20 1 year, 5 months ago

WSA uses access policies to decide what to allow and what to block. "Settings" usually refer to the appliance settings not to a policy. I'll go with - D
upvoted 1 times



Emlia1 1 year, 9 months ago

A or D
upvoted 2 times

pohqinan 2 years, 5 months ago

Answer is D
https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Access_Control_Rules_URL_Filtering.html

upvoted 2 times

  **rbrain** 2 years, 7 months ago

Selected Answer: D

Could it be D, i go for D:

https://www.cisco.com/c/en/us/td/docs/security/firepower/650/configuration/guide/fpmc-config-guide-v65/url_filtering.html

Tricky question.

upvoted 1 times

  **dr4gn00t** 2 years, 7 months ago



Question is not focused on any specific product, therefore I think A is best answer in general, if you consider product can be WSA, Firepower, Umbrella or anything between..

upvoted 1 times

  **bob511** 2 years, 6 months ago

except you would modify an access policy to do this on FTD

upvoted 1 times

  **Cock** 2 years, 8 months ago

The answer is D

upvoted 1 times

  **testtaker13** 2 years, 10 months ago

why not B?

upvoted 1 times

  **NullNull88** 1 year, 11 months ago


B because the issue is with user requests to known malicious websites. Outbound malware scanning sounds more specific to the question.

upvoted 1 times

  **Fazy** 3 years ago

D is the correct answer

upvoted 4 times

  **jshow** 3 years, 1 month ago

i believe its access policy....u can create an ips and attach it to the access policy to prevent

upvoted 3 times

  **trickbot** 3 years, 4 months ago

If I get this question, Im answering "Change an access policy". Seems as this scenario could be prevented by both access policies on a Firepower Device, or policy on a WSA. I think the words "Settings" is the trick answer here. The word "Settings" does not appear in the WSA userguide.

upvoted 3 times

An engineer has enabled LDAP accept queries on a listener. Malicious actors must be prevented from quickly identifying all valid recipients. What must be done on the Cisco ESA to accomplish this goal?

- A. Configure Directory Harvest Attack Prevention
- B. Bypass LDAP access queries in the recipient access table.
- C. Use Bounce Verification.
- D. Configure incoming content filters.

Correct Answer: A

Community vote distribution

A (100%)

kerniger Highly Voted 3 years ago

i would choose A

<https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/117847-technote-esa-00.html>

upvoted 14 times

testtaker13 2 years, 10 months ago

Definitely A

upvoted 2 times

yong08321 Most Recent 1 year, 4 months ago

Selected Answer: A

To prevent malicious actors from quickly identifying all valid recipients, the engineer can use Directory Harvest Attack Prevention (DHAP) on the Cisco ESA. DHAP blocks SMTP messages to invalid recipient addresses and limits the number of messages that can be sent to the server, which helps prevent attackers from obtaining a complete list of valid email addresses. Therefore, option A is the correct answer.

Option B, bypassing LDAP access queries in the recipient access table, does not provide any protection against Directory Harvest Attacks (DHAs).

Option C, using Bounce Verification, is used to prevent backscatter, which is when an email system sends a bounce message to an innocent victim, who did not send the original message and who is not the intended recipient of the bounce message.

Option D, configuring incoming content filters, is used to block unwanted emails based on message content.

upvoted 2 times

sull3y 1 year, 5 months ago

The correct answer is A. Configure Directory Harvest Attack Prevention.

When LDAP (Lightweight Directory Access Protocol) accept queries are enabled on a listener, it is possible for malicious actors to quickly identify all valid recipients on the email server. This is known as a Directory Harvest Attack (DHA), and it can be used by spammers to collect valid email addresses to use for spamming.

To prevent a DHA, the Cisco ESA (Email Security Appliance) must be configured with Directory Harvest Attack Prevention (DHAP). This feature limits the number of invalid queries a sender can make, and it can be used to detect and block DHA attempts.

upvoted 2 times

[Removed] 2 years, 3 months ago

A is correct.

Using LDAP For Directory Harvest Attack Prevention

Directory Harvest Attacks occur when a malicious sender attempts to send messages to recipients with common names, and the email gateway responds by verifying that a recipient has a valid mailbox at that location. When performed on a large scale, malicious senders can determine who to send mail to by "harvesting" these valid addresses for spamming.

The appliance can detect and prevent Directory Harvest Attack (DHA) when using LDAP acceptance validation queries. You can configure LDAP acceptance to prevent directory harvest attacks within the SMTP conversation or within the work queue.

upvoted 2 times

mecacig953 2 years, 5 months ago

Selected Answer: A

The DHAP is a supported feature on the Cisco Content Security Appliances that can be enabled when Lightweight Directory Access Protocol (LDAP) acceptance validation is used. The DHAP feature keeps track of the number of invalid recipient addresses from a given sender.

Once a sender crosses an administrator-defined threshold, the sender is deemed to be untrusted, and mail from that sender is blocked with no Network Design Requirement (NDR) or error code generation. You can configure the threshold based upon the reputation of the sender. For example, untrusted or suspicious senders can have a low DHAP threshold, and trusted or reputable senders can have a high DHAP threshold.

upvoted 1 times

 **nospampls** 3 years, 1 month ago

i choose D

For a read-only state where DLP violations are logged and reported but the messages are not stopped/quarantined or encrypted, the Deliver action is most often used.

Secondary actions include:

- Sending a copy to any custom quarantine or the Policy quarantine.
- Encrypt the message. The appliance only encrypts the message body. It does not encrypt the message headers.
- Altering the Subject header.
- Adding disclaimer text/HTML to the message.
- Sending the message to an alternate destination mailhost.
- Sending bcc copies of the message.
- Sending DLP violation notification to the sender and/or other contacts.

These actions are not mutually exclusive — you can combine some of them within different DLP policies for various processing needs for different user groups.

We are going to implement the following DLP Actions: Encrypt

These actions assume that Encryption is licensed and configured on the ESA and three profiles have been created for High, Medium, and Low security as was done in the earlier sections:

- CRES_HIGH
- CRES_MED
- CRES_LOW

<https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/216086-best-practice-guide-for-data-loss-preven.html#anc1>

upvoted 1 times

 **jshow** 3 years, 1 month ago

i believe its access policy....u can create an ips and attach it to the access policy to prevent

upvoted 1 times

In which two ways does a system administrator send web traffic transparently to the Cisco WSA? (Choose two.)

- A. use Web Cache Communication Protocol
- B. configure AD Group Policies to push proxy settings
- C. configure the proxy IP address in the web-browser settings
- D. configure policy-based routing on the network infrastructure
- E. reference a Proxy Auto Config file

Correct Answer: AD

Community vote distribution

AD (100%)

entity Highly Voted 3 years, 3 months ago

A&D.. transparent
Any configuration on client device is explicit/forward
upvoted 30 times

deathfrom 3 years, 2 months ago

Sticking with A & E
upvoted 3 times

deathfrom 3 years, 2 months ago

Ignore my last comment
upvoted 4 times

sathees_121 Most Recent 2 years, 2 months ago

A & D confirmed
upvoted 2 times

getafix 2 years, 2 months ago

Selected Answer: AD

When the Cisco WSA is in transparent mode, clients do not know there is a proxy deployed. Network infrastructure devices are configured to forward traffic to the Cisco WSA. In transparent mode deployments, network infrastructure devices redirect web traffic to the proxy. Web traffic redirection can be done using policy-based routing (PBR)—available on many routers—or using Cisco's Web Cache Communication Protocol (WCCP) on Cisco ASA, Cisco routers, or switches.

Extract from Cisco OCG
upvoted 3 times

madcloud 2 years, 3 months ago

A&D is the right answer. For Transparent option : use PBR (policy based routing), WCCP or L4-L7 redirection. For explicit forwarding: configure Browser or use .PAC file
upvoted 1 times

[Removed] 2 years, 3 months ago

correct answer A and D
upvoted 1 times

djsonicdh 2 years, 4 months ago

Selected Answer: AD

Pbr a and D
upvoted 1 times

breezer 2 years, 5 months ago

A & D
Using PAC Files is Explicit Mode - <https://www.cisco.com/c/en/us/support/docs/security/web-security-appliance/117940-qa-wsa-00.html>
upvoted 1 times

mecacig953 2 years, 5 months ago

Selected Answer: AD

wccp and routing
upvoted 1 times

flejd 2 years, 8 months ago
PBR and WCCP
upvoted 1 times

Moll 2 years, 9 months ago
I'll go with A and D here
upvoted 2 times

[Removed] 2 years, 11 months ago
A and D
upvoted 2 times

Sarbi 3 years ago
A and D
upvoted 2 times

ferari 3 years, 2 months ago
This question is not direct,direct traffic to WSA is by using explicit mode. The Transparent method is not direct to the WSA.It has to be redirected by a layer 3 device. The question is stating web traffic transparently (Direct). it seems B and C is the right answer.
upvoted 1 times

hisho72 3 years, 2 months ago
Answer E is relatede to explicit mode to configure proxy settings for clients
upvoted 3 times

itisfakemallo 3 years, 2 months ago
A and D
upvoted 2 times

Question #208

Topic 1

What is the function of the Context Directory Agent?

- A. reads the AD logs to map IP addresses to usernames
- B. relays user authentication requests from Cisco WSA to AD
- C. maintains users' group memberships
- D. accepts user authentication requests on behalf of Cisco WSA for user identification

Correct Answer: A

Reference:

https://www.cisco.com/c/en/us/td/docs/security/ibf/cda_10/Install_Config_guide/cda10/cda_oveviw.html

Community vote distribution

A (100%)

mecacig953 2 years, 5 months ago

Selected Answer: A

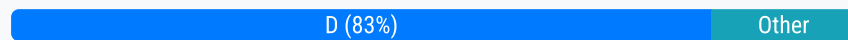
Cisco Context Directory Agent (CDA) is a mechanism that maps IP Addresses to usernames in order to allow security gateways to understand which user is using which IP Address in the network, so those security gateways can now make decisions based on those users (or the groups to which the users belong to).
upvoted 3 times

A network administrator is configuring a rule in an access control policy to block certain URLs and selects the `Chat and Instant Messaging` category. Which reputation score should be selected to accomplish this goal?

- A. 5
- B. 10
- C. 3
- D. 1

Correct Answer: D

Community vote distribution



Kuzi Highly Voted 1 year, 3 months ago

Selected Answer: D

The answer is D. 1.

A reputation score of 1 is the lowest possible score, and it indicates that the URL is considered to be very risky. This means that the network administrator should block all URLs with a reputation score of 1, in order to prevent users from accessing malicious websites.

The other possible answers are incorrect. A reputation score of 5 is considered to be "neutral", while a reputation score of 10 is considered to be "good". This means that URLs with these scores should not be blocked. A reputation score of 3 is considered to be "suspect", and it may be necessary to block some URLs with this score, depending on the organization's specific policies and risk tolerance.

Here is a table that shows the different reputation scores and their corresponding meanings:

Reputation Score | Meaning

----- | -----
 1 | Very risky
 3 | Suspect
 5 | Neutral
 10 | Good
 upvoted 6 times

iratus_umbra Most Recent 1 year, 5 months ago

Selected Answer: D

About URL Filtering with Category and Reputation

With a URL Filtering license, you can control access to websites based on the category and reputation of requested URLs:

Category—A general classification for the URL. For example, ebay.com belongs to the Auctions category, and monster.com belongs to the Job Search category.

A URL can belong to more than one category.

Reputation—How likely the URL is to be used for purposes that might be against your organization's security policy. Reputations range from Unknown risk (level 0) or Untrusted (level 1) to Trusted (level 5).

In the URL Filtering Overview section

https://www.cisco.com/c/en/us/td/docs/security/firepower/650/configuration/guide/fpmc-config-guide-v65/url_filtering.html#Cisco_Reference.dita_72248e9a-706c-4e53-9bf1-de72f87b1beb

upvoted 3 times

jienBoq 1 year, 4 months ago

question is about ESA. Why are you looking at firepower?

upvoted 1 times

stalkr3 1 year, 4 months ago

why do you think the question is from ESA?

upvoted 2 times

seb008 1 year, 2 months ago



Chat and Instant Messaging

upvoted 1 times

[Removed] 7 months, 2 weeks ago

Which is also in Firepower

upvoted 2 times

  **zsrite** 1 year, 5 months ago

Selected Answer: B

The appropriate reputation score to select in an access control policy to block URLs in the "Chat and Instant Messaging" category would depend on the organization's specific policies and risk tolerance. However, generally speaking, a higher reputation score would be more restrictive and block more URLs. Malicious (-10.0 to -6.0), Suspect (-5.9 to 5.9), Clean (6.0 to 10.0)

upvoted 1 times

  **Toni_Su91** 1 year, 5 months ago

Selected Answer: C

In new FMC 7.2 When creating Access Policy Rule, you have a range from 1-5 in Reputation for Chat and Instant Messaging.

3 - Will block Neutral Reputation to Untrusted



1 - Will block Untrusted Reputation

However there is more levels.

In old fmc it seems to be only 1-3 and 3 will block from Untrusted to Neutral.

https://www.cisco.com/c/en/us/td/docs/security/firepower/650/configuration/guide/fpmc-config-guide-v65/url_filtering.html#Cisco_Reference.dita_72248e9a-706c-4e53-9bf1-de72f87b1beb

upvoted 1 times

  **jienBoq** 1 year, 4 months ago

question is about ESA. Why are you looking at firepower?

upvoted 1 times

  **stalkr3** 1 year, 4 months ago

why do you think the question is from ESA?

upvoted 2 times

  **Tuxzinator** 1 year, 6 months ago

Selected Answer: D

I believe it was -10 to +10.

-10 was block.

0 neutral monitor.

Weird question

upvoted 1 times

  **Zatingke** 1 year, 7 months ago

No clue

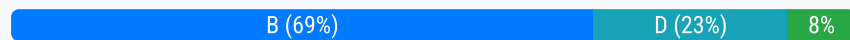
upvoted 1 times

A Cisco ESA network administrator has been tasked to use a newly installed service to help create policy based on the reputation verdict. During testing, it is discovered that the Cisco ESA is not dropping files that have an undetermined verdict. What is causing this issue?

- A. The policy was created to send a message to quarantine instead of drop.
- B. The file has a reputation score that is below the threshold.
- C. The file has a reputation score that is above the threshold.
- D. The policy was created to disable file analysis.

Correct Answer: B

Community vote distribution



Dinges Highly Voted 3 years, 2 months ago

I found B a possibility

Quarantine is only for unrecognised files. When file is undetermined, reputation score is checked. Reputation 1-59: Deliver file / Reputation 60-100: Block file

So B looks correct.

Look at - Figure 1. Advanced Malware Protection Workflow for Public-Cloud File Analysis Deployments

https://www.cisco.com/c/en/us/td/docs/security/esa/esa12-0/user_guide/b_ESA_Admin_Guide_12_0/b_ESA_Admin_Guide_chapter_010000.html

upvoted 20 times

itisfakemalloi Highly Voted 3 years, 2 months ago

I am sure it is D. The policy was created to disable file analysis.

When the reputation is not clear = undetermined, the file should be send for file analysis. It is not happening, so the file is not dropped.

upvoted 6 times

Ozzig Most Recent 4 months, 1 week ago

Selected Answer: B

Check the flow diagram, it's B

https://www.cisco.com/c/en/us/td/docs/security/esa/esa14-2-3/User_Guide/b_ESA_Admin_Guide_14-2-3/b_ESA_Admin_Guide_12_1_chapter_010001.html#con_1809437

upvoted 3 times

rishard 1 year, 1 month ago

The correct answer is B (it took me long to understand that)

There is a difference between "Undetermined" (from the question), and "Unrecognized".

Undetermined - It checks the file score (Which is in the question - Right answer - B).

Unrecognize - Push file for analysis (Answer D - which is wrong in this case).

https://www.cisco.com/c/en/us/td/docs/security/esa/esa12-0/user_guide/b_ESA_Admin_Guide_12_0/b_ESA_Admin_Guide_chapter_010000.html

upvoted 3 times

rishard 1 year, 2 months ago

I would go with D.

When a file's reputation verdict is undetermined, it means that the Cisco ESA's file analysis feature could not determine the reputation of the file. In a typical configuration, the Cisco ESA would have the ability to drop or quarantine files based on their reputation verdicts. However, if the policy is set to disable file analysis, it means that the Cisco ESA is not analyzing the files and therefore cannot drop them based on their reputation.

Therefore, option D is the most likely cause of the issue described in the scenario.

upvoted 1 times

DWizard 1 year, 2 months ago

Selected Answer: B

Option B is correct.

Above figure 1 on the already shared link is the explanation.

upvoted 1 times

achille5 1 year, 6 months ago

Selected Answer: A

In the scenario described in the question, the issue is that the Cisco ESA is not dropping files that have an undetermined verdict. The undetermined verdict means that the reputation service did not have enough information to determine the file's reputation score. When the Cisco ESA

encounters a file with an undetermined verdict, it checks the message filter to determine the action to take. If the message filter is configured to quarantine the message, then the file will be sent to the quarantine area, even if the reputation score is undetermined.

upvoted 1 times

nicklapa 1 year, 8 months ago

If the file is known to the reputation service but there is insufficient information for a definitive verdict, the reputation service returns a reputation score based on characteristics of the file such as threat fingerprint and behavioral analysis. If this score meets or exceeds the configured reputation threshold, the appliance applies the action that you have configured in the mail policy for files that contain malware .

upvoted 1 times

ureis 1 year, 10 months ago

Selected Answer: D

Maybe the "newly installed service" in this Q mentions about Advanced Malware Protection (AMP) which can be used along with ESA. AMP allows superior protection across the attack continuum.

upvoted 1 times

Jamesy 1 year, 11 months ago

C is the correct answer. Cheers

upvoted 1 times

ChrisMT 2 years, 1 month ago

Answer B

guys, please refer to the Figure 1. Advanced Malware Protection Workflow for Public-Cloud File Analysis Deployments

The undetermined verdict with score 1- 59 will delivery the file to user

The undetermined verdict with score 60- 100 will block the file

So answer C, the reputation score is above the threshold is correct !

https://www.cisco.com/c/dam/en/us/td/i/400001-500000/410001-420000/415001-416000/415734.tif/_jcr_content/renditions/415734.jpg

upvoted 4 times

ChrisMT 2 years, 1 month ago

Sorry for the typo, answer is C

upvoted 2 times

ChrisMT 2 years, 1 month ago

Sorry, typo again, final the answer is B Confirmed!

the old version of the doc shown below

https://www.cisco.com/c/en/us/td/docs/security/wsa/wsa11-0/user_guide/b_WSA_UserGuide/b_WSA_UserGuide_chapter_010001.html

upvoted 1 times

Stevens0103 8 months ago

Should be this one:

https://www.cisco.com/c/en/us/td/docs/security/ces/user_guide/esa_user_guide_14-0/b_ESA_Admin_Guide_ces_14-0/b_ESA_Admin_Guide_12_1_chapter_010001.html

upvoted 1 times

Orestesmc 2 years, 3 months ago

it is the reputation of the file that is being inspected, for an indeterminate verdict a score is set from 0 to 100 - C, its correct.

https://www.cisco.com/c/en/us/td/docs/security/ces/user_guide/esa_user_guide/b_ESA_Admin_Guide_ces_11_0/b_ESA_Admin_Guide_chapter_010000.pdf

upvoted 2 times

Iarn 2 years, 4 months ago

Selected Answer: B

How are SenderBase Reputation Scores (SBRS) determined, and what do they mean?

SenderBase scores are assigned to IP addresses based on a combination of factors, including email volume and reputation.

Reputation scores in SenderBase may range from -10 to +10, reflecting the likelihood that a sending IP address is trying to send spam. Highly negative scores indicate senders who are very likely to be sending spam; highly positive scores indicate senders who are unlikely to be sending spam.

upvoted 1 times

semi1750 2 years, 5 months ago

Selected Answer: B

B looks correct.

"undetermined verdict" is located right before scoring within the "Recognized File" process under reputational service.

once a file has undetermind verdict, there are only 2 options below, deliver or drop based on the reputation score.

for D, I am not sure if you can make a policy to disable fily analysis service....you can enable or disable the service optionally....

upvoted 1 times

mecacig953 2 years, 5 months ago

Selected Answer: B

https://www.cisco.com/c/en/us/td/docs/security/esa/esa11-0/user_guide_fs/b_ESA_Admin_Guide_11_0/b_ESA_Admin_Guide_chapter_010000.html

undetermined verdict below threshold on reputation score so delivered

upvoted 1 times

  **Faruzzi1979** 2 years, 6 months ago

Selected Answer: B

Pay attention to "undetermined verdict" (not "unrecognized file"). Policy can not disable File Analysis service (so D can not be the correct answer), but it can send messages with unknown attachments to quarantine while file analysis is performed. After undetermined verdict for known file, reputation score is calculated, and if below threshold (60), message is sent to the recipient (B - correct answer). If file analysis service is enabled (you can not disable file analysis in the policy) and the file is defined as unrecognized (unknown), at the same time policy is set to send unrecognized files to quarantine during file analysis, then potentially this file could be defined as malicious (after sand-boxing) and for that reason not delivered to the recipient.

upvoted 2 times

  **Kyle1776** 2 years, 6 months ago

Alright have to do some process of elimination on this one

A(wrong)- quarantining the files is not the answer because that would be temporarily "dropping" them while talos looks them up and that is not the case. they are getting though. https://www.cisco.com/c/en/us/td/docs/security/esa/esa13-5-1/user_guide/b_ESA_Admin_Guide_13-5-1/b_ESA_Admin_Guide_12_1_chapter_01100.html

B(wrong)- the email has a "undetermined verdict" which means it wouldnt be assigned a threshold to be below

C(Wrong)- the email has a "undetermined verdict" which means it wouldnt be assigned a threshold to be above

D(correct)- only option left

upvoted 1 times

An organization has a Cisco ESA set up with DLP policies and would like to customize the action assigned for violations. The organization wants a copy of the message to be delivered with a message added to flag it as a DLP violation. Which actions must be performed in order to provide this capability?

- A. deliver and add disclaimer text
- B. quarantine and send a DLP violation notification
- C. quarantine and alter the subject header with a DLP violation
- D. deliver and send copies to other recipients

Correct Answer: B

Reference:

<https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/216086-best-practice-guide-for-data-loss-preven.html>

Community vote distribution

A (63%) B (21%) D (16%)

VI_Vershinin Highly Voted 3 years, 1 month ago

It is B.

Read chapter 5. Creating Data Loss Prevention Message Actions

<https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/216086-best-practice-guide-for-data-loss-preven.html>

upvoted 16 times

aalnman 2 years, 11 months ago

Absolutely B. This is from Chapter 5 Vershinin speaks of: About DLP Message Actions

DLP message actions describe what actions that the ESA will take when it detects a DLP violation in an outgoing email. You can specify primary and secondary DLP Actions and different actions can be assigned for different violation types and severities.

Primary actions include:

Deliver

Drop

Quarantine

For a read-only state where DLP violations are logged and reported but the messages are not stopped/quarantined or encrypted, the Deliver action is most often used.

upvoted 3 times

aalnman 2 years, 11 months ago

Here is the rest (can't edit original post)

Secondary actions include:

Sending a copy to any custom quarantine or the 'Policy' quarantine.

Encrypt the message. The appliance only encrypts the message body. It does not encrypt the message headers.

Altering the Subject header.

Adding disclaimer text/HTML to the message.

Sending the message to an alternate destination mailhost.

Sending bcc copies of the message.

Sending DLP violation notification to the sender and/or other contacts.

upvoted 1 times

NikoNiko 2 years, 1 month ago

You meant A, wrote B.

A) deliver and add disclaimer text - exactly as explained above

upvoted 6 times

itisfakemai101 Highly Voted 3 years, 2 months ago

It is definitely A. deliver and add disclaimer text

upvoted 11 times

Premium_Pils Most Recent 4 weeks ago

Selected Answer: A



I would choos A based on this:

<https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/216086-best-practice-guide-for-data-loss-preven.html#:~:text=Adding%20disclaimer%20text/HTML%20to%20the%20message>

-Sending bcc copies of the message.

-Adding disclaimer text/HTML to the message.

upvoted 1 times

  **cbaina** 2 months, 1 week ago

IT is D, look this scenario:

Sending copies (bcc) of messages to other recipients. For example, you could copy messages with critical DLP violations to a compliance officer's mailbox for examination.

Not A, Not B, Because not mentioned about "send a copy of message"

Not B, Although you guys mentioned about the below secondary action in your comments, But in the second option (B) there is not any sign of a copy of message

((Secondary actions include:

Sending a copy to a policy quarantine if you choose to deliver the message. The copy is a perfect clone of the original, including the Message ID. Quarantining a copy allows you to test the DLP system before deployment in addition to providing another way to monitor DLP violations. When you release the copy from the quarantine, the appliance delivers the copy to the recipient, who will have already received the original message.))

upvoted 1 times

  **DaleC78** 3 months, 4 weeks ago

Selected Answer: B

B without a doubt. Emails violating internal DLP policies shouldn't be delivered, otherwise what's the point?


The provided link explains it perfectly:

5. Creating Data Loss Prevention Message Actions

Create DLP Quarantines

If you'd like to keep a copy of messages violating DLP policies you can create individual Policy quarantines for each type of policy violation. This is especially useful when running a 'transparent' POV, where Outbound messages violating DLP policies are logged and delivered but no action is taken on the messages.

upvoted 1 times

  **DaleC78** 3 months, 3 weeks ago

Misreaded that one... Seems that's A

upvoted 1 times

  **red_sparrow_Gr** 10 months, 1 week ago

Selected Answer: A

the question states : ...The organization wants a copy of the message to be delivered...

So B and C are excluded

upvoted 1 times

  **cyberwhizzy0** 1 year, 1 month ago

Selected Answer: B

I think B is correct (not too certain though)

Primary actions include:

Deliver

Drop



Quarantine

Secondary actions include:

Sending a copy to a policy quarantine if you choose to deliver the message. The copy is a perfect clone of the original, including the Message ID. Quarantining a copy allows you to test the DLP system before deployment in addition to providing another way to monitor DLP violations. When you release the copy from the quarantine, the appliance delivers the copy to the recipient, who will have already received the original message.

https://www.cisco.com/c/en/us/td/docs/security/esa/esa12-0/user_guide/b_ESA_Admin_Guide_12_0/b_ESA_Admin_Guide_chapter_010001.html



upvoted 1 times

  **jku2cya** 1 year, 2 months ago

Selected Answer: B

As per the link VI_Vershinin posted and under "Secondary actions include.."

upvoted 1 times

  **gc999** 1 year, 3 months ago

Selected Answer: D

Here I will choose "D". The question said the organization wants a "copy of the message to be delivered". Only option "D" would do "sending copies.

Refer to "[https://www.cisco.com/c/en/us/td/docs/security/esa/esa12-](https://www.cisco.com/c/en/us/td/docs/security/esa/esa12-0/user_guide/b_ESA_Admin_Guide_12_0/b_ESA_Admin_Guide_chapter_010001.html#con_1304495)


0/user_guide/b_ESA_Admin_Guide_12_0/b_ESA_Admin_Guide_chapter_010001.html#con_1304495", only this point can meet - "Sending copies (bcc) of messages to other recipients. (For example, you could copy messages with critical DLP violations to a compliance officer's mailbox for examination.)".

upvoted 2 times

  **gc999** 1 year, 3 months ago

Wrong URL quoted, it should be "<https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/216086-best-practice-guide-for-data-loss-preven.html>"



upvoted 1 times

  **gc999** 1 year, 3 months ago

Sorry, I believe "A" is the answer

<https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/216086-best-practice-guide-for-data-loss-preven.html#:~:text=Adding%20disclaimer%20text/HTML%20to%20the%20message>

upvoted 1 times

  **angry** 1 year, 6 months ago

Absolutely A!

upvoted 2 times

  **achille5** 1 year, 6 months ago

Selected Answer: A

deliver and add disclaimer text

upvoted 1 times

  **jienBoq** 1 year, 6 months ago

Selected Answer: A

as per

<https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/216086-best-practice-guide-for-data-loss-preven.html>

Primary actions include:

Deliver

Drop

Quarantine

For a read-only state where DLP violations are logged and reported but the messages are not stopped/quarantined or encrypted, the Deliver action is most often used.

Secondary actions include:

Sending a copy to any custom quarantine or the 'Policy' quarantine.

Encrypt the message. The appliance only encrypts the message body. It does not encrypt the message headers.

Altering the Subject header.

Adding disclaimer text/HTML to the message.

Sending the message to an alternate destination mailhost.

Sending bcc copies of the message.

Sending DLP violation notification to the sender and/or other contacts.

upvoted 4 times

  **Emlia1** 1 year, 8 months ago

A or B

upvoted 1 times

  **Emlia1** 1 year, 9 months ago

I prefer A


upvoted 1 times

  **sathees_121** 2 years, 2 months ago

It is D

https://www.cisco.com/c/en/us/td/docs/security/esa/esa12-0/user_guide/b_ESA_Admin_Guide_12_0/b_ESA_Admin_Guide_chapter_010001.html

upvoted 1 times


  **sha2** 2 years, 4 months ago

Selected Answer: A

its deliver because the questions says "wants a copy of the message to be delivered" and in the Configuration guide "Note If you select Deliver, you can choose to have a copy of the message sent to a policy quarantine. The copy of the message is a perfect clone, including the Message ID."

then add disclaimer text because the question says "to be delivered with a message added to flag it as a DLP violation" and in configuration guide it says : "To include disclaimer text when delivering messages with DLP violations or suspected violations, specify disclaimer text in Mail Policies" so answer is A

upvoted 5 times

  **Pupu** 2 years, 6 months ago

Selected Answer: D

Answer is D. In the referenced guide, it mentions that you can take two actions for DLP messages, primary and secondary. Here the primary would be "Deliver" and secondary "Sending DLP violation notification to the sender and/or other contacts."

It also says: "For a read-only state where DLP violations are logged and reported but the messages are not stopped/quarantined or encrypted, the Deliver action is most often used."

Since the question clearly states that message needs to be delivered, the answer cannot be B or C. We're left with A and D. I am picking D because the secondary action it specifies is the only that sends violation notifications.

upvoted 1 times

A Cisco ESA administrator has been tasked with configuring the Cisco ESA to ensure there are no viruses before quarantined emails are delivered. In addition, delivery of mail from known bad mail servers must be prevented. Which two actions must be taken in order to meet these requirements? (Choose two.)

- A. Deploy the Cisco ESA in the DMZ.
- B. Use outbreak filters from SenderBase.
- C. Configure a recipient access table.
- D. Enable a message tracking service.
- E. Scan quarantined emails using AntiVirus signatures.

Correct Answer: BE

Community vote distribution

BE (83%)

CE (17%)

ff001 2 years, 2 months ago

Cisco ESA uses a multilayer approach to fight viruses and malware:

- The first layer of defense consists of outbreak filters, which the appliance downloads from Cisco SenderBase. They contain a list of known bad mail servers. These filters are generated by watching global email traffic patterns and looking for anomalies associated with an outbreak. When an email is received from a server on this list, it is kept in quarantine until the antivirus signatures are updated to counter the current threat.
 - The second layer of defense is using antivirus signatures to scan quarantined emails, to ensure that they do not carry viruses into the network.
 - Cisco ESA also scans outbound emails to provide antivirus protection.
- upvoted 4 times

surforlife 2 years, 2 months ago

"B and E"

Cisco ESA uses a multilayer approach to fight viruses and malware:

- The first layer of defense consists of outbreak filters, which the appliance downloads from Cisco SenderBase. They contain a list of known bad mail servers. These filters are generated by watching global email traffic patterns and looking for anomalies associated with an outbreak. When an email is received from a server on this list, it is kept in quarantine until the antivirus signatures are updated to counter the current threat.
 - The second layer of defense is using antivirus signatures to scan quarantined emails, to ensure that they do not carry viruses into the network.
 - Cisco ESA also scans outbound emails to provide antivirus protection.
- upvoted 1 times

nomanlands 2 years, 2 months ago

Selected Answer: BE

BE - C wouldn't stop known bad senders.
upvoted 1 times

semi1750 2 years, 5 months ago

Selected Answer: BE

Picked B & E

Page 6 stated as follow

Fighting Viruses and Malware

Cisco ESA uses a multilayer approach to fight viruses and malware:

- The first layer of defense consists of outbreak filters, which the appliance downloads from Cisco SenderBase. They contain a list of known bad mail servers. These filters are generated by watching global email traffic patterns and looking for anomalies associated with an outbreak. When an email is received from a server on this list, it is kept in quarantine until the antivirus signatures are updated to counter the current threat.
- The second layer of defense is using antivirus signatures to scan quarantined emails, to ensure that they do not carry viruses into the network.
- Cisco ESA also scans outbound emails to provide antivirus protection

<https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/Aug2013/CVD-EmailSecurityUsingCiscoESADesignGuide-AUG13.pdf>

upvoted 1 times

Pupu 2 years, 6 months ago



Selected Answer: BE

I'm going with B and E.

B: https://www.cisco.com/c/en/us/td/docs/security/esa/esa13-0/user_guide/b_ESA_Admin_Guide_13-0/b_ESA_Admin_Guide_12_1_chapter_0101.html

E: https://www.cisco.com/c/en/us/td/docs/security/esa/esa13-0/user_guide/b_ESA_Admin_Guide_13-0/b_ESA_Admin_Guide_12_1_chapter_01101.html

upvoted 3 times

  **Cock** 2 years, 6 months ago

Selected Answer: CE

The answer cannot be A. Either single-armed deployment or dual-armed deployment, Cisco ESA is separate from DMZ. ESA is connected to DMZ, not in the DMZ.

B is not correct as well. What is outbreak filter? An outbreak occurs when messages with attachments containing never-before-seen viruses or variants of existing viruses spread quickly through private networks and the Internet. The question does not specify to new virus.

C is correct. Recipient access table (RAT) acceptance or rejection of recipient addresses.



E is correct.

upvoted 1 times

  **NullNull88** 2 years, 9 months ago

"delivery of mail from known bad mail servers must be prevented" that isn't C. RAT?

upvoted 2 times

  **Moll** 2 years, 9 months ago

Agree with A and B

upvoted 1 times

  **Moll** 2 years, 9 months ago

Sorry I meant B and E

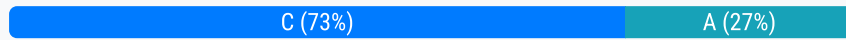
upvoted 2 times

An organization has noticed an increase in malicious content downloads and wants to use Cisco Umbrella to prevent this activity for suspicious domains while allowing normal web traffic. Which action will accomplish this task?

- A. Use destination block lists.
- B. Configure application block lists.
- C. Configure the intelligent proxy.
- D. Set content settings to High.

Correct Answer: C

Community vote distribution



Seawanderer Highly Voted 3 years, 2 months ago

I'd say C, intelligent proxy
upvoted 11 times

sull3y Highly Voted 1 year, 7 months ago

C. Configure the intelligent proxy.

Cisco Umbrella's intelligent proxy allows you to enforce security policies for web traffic based on various criteria, such as destination domain, IP address, or URL category. To prevent malicious content downloads, the organization can configure the intelligent proxy to block access to suspicious domains, while allowing normal web traffic. This can be done by creating a security policy that specifies which domains should be blocked and which should be allowed.

Note: The intelligent proxy is a feature in Cisco Umbrella that can be used to enforce security policies for web traffic. Other Umbrella features, such as destination block lists and application block lists, can also be used to prevent malicious activity. However, the intelligent proxy is the best option for this specific task, as it allows you to enforce security policies based on domain, IP, or URL category

upvoted 6 times

Alizade Most Recent 11 months, 2 weeks ago

Selected Answer: C

C. Configure the intelligent proxy.
upvoted 1 times

F0rtyx40 1 year, 1 month ago

Selected Answer: A

This is a standard destination list category that can be accomplished with simple DNS forwarding.
upvoted 1 times

nomanlands 2 years, 2 months ago

Selected Answer: C

C - it will still allow normal web traffic
upvoted 1 times

TesterDude 2 years, 3 months ago

Selected Answer: A

I'm going with A because it specifies that it only wants to perform that action for malicious domains, which will be identified by a destination list.

Intelligent proxy Inspection of files would apply to all domains

upvoted 2 times

F0rtyx40 1 year, 1 month ago

I agree with this, this is a standard destination list category that can be accomplished with simple DNS forwarding.

upvoted 1 times

Pupu 2 years, 6 months ago

Selected Answer: C

C is the answer.
upvoted 2 times

brownbear505 2 years, 6 months ago

Selected Answer: C

The intelligent proxy is the ability for Umbrella to intercept and proxy requests for malicious files embedded within certain so-called "grey" domains. Some websites, especially those with large user communities or the ability to upload and share files, have content that most users want

to access while also posing a risk because of the possibility of hosting malware. Administrators don't want to block access to the whole "grey" domain for everyone but they also don't want your users to access files that could harm their computers or compromise company data.

upvoted 4 times

  **Minion2021** 2 years, 6 months ago

The Answer is C

upvoted 1 times

  **Floki_viking7** 2 years, 7 months ago

I'd say C

The intelligent proxy is the ability for Umbrella to intercept and proxy requests for malicious files embedded within certain so-called "grey" domains. Some websites, especially those with large user communities or the ability to upload and share files, have content that most users want to access while also posing a risk because of the possibility of hosting malware. Administrators wouldn't want to block access to the whole "grey" domain for everyone but they also don't want your users to access files that could harm their computers, compromise your company data or worse!

upvoted 2 times


  **coentror** 2 years, 9 months ago

I would say C:

How Cisco umbrella will manage traffic to a risky domain?

With the intelligent proxy, if a site is considered potentially suspicious or could host malicious content, Umbrella returns the intelligent proxy's IP address. The request to that domain is then routed through our cloud-based secure gateway, and malicious content is found and stopped before it's sent to you.

upvoted 3 times

  **Moll** 2 years, 9 months ago

I'd go with C here

upvoted 1 times

  **Steve122** 2 years, 10 months ago

Support for the intelligent proxy is deprecated and only available for legacy deployments of the MSP console. The intelligent proxy is not available for new deployments of the MSP console.

upvoted 1 times

  **john_thomas** 2 years, 10 months ago

i Passed and i Used [C. Configure the intelligent proxy.]

upvoted 4 times

  **RockeyMylabathula** 1 year, 11 months ago

hello John , i need your help can you ping me gmail rockydot06523atgmaildotcom

upvoted 1 times

  **Sarbi** 3 years ago

A with Cisco Umbrella there is no intelligent proxy like thing.

upvoted 1 times

  **semi1750** 2 years, 5 months ago

picked C

There is..

<https://docs.umbrella.com/deployment-msp/v2.0/docs/enable-the-intelligent-proxy>

upvoted 1 times

  **BennyTheK** 3 years, 1 month ago

I would choose C:

A. Destination block lists - no (we cannot specify all the suspicious domains on a list)

B. Configure application block lists - obviously not related

C. Configure the intelligent proxy - yes - it is used to decrypt & monitor the traffic for suspicious domains & drop if needed

D. Set content settings to High - no, because it would also block time wasting destinations such as social media, ect

upvoted 3 times

  **aalnman** 3 years, 2 months ago

A = Correct. If you are using Umbrella then you are using DESTINATION BLOCK LISTS. WSA uses "C."

upvoted 3 times

  **F0rtyx40** 1 year, 1 month ago

Umbrella also has a intelligent proxy, it's just not required for core destination and reputation list blocking. I think I am sticking with A, I have deployed many Umbrella instances without intelligent proxy and it offers all security category blocks.

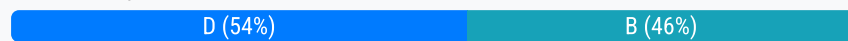
upvoted 1 times

Which attack is preventable by Cisco ESA but not by the Cisco WSA?

- A. SQL injection
- B. phishing
- C. buffer overflow
- D. DoS

Correct Answer: D

Community vote distribution



ddev3737 Highly Voted 1 year, 7 months ago

but also B. Phishing

Cisco ESA (Email Security Appliance) and Cisco WSA (Web Security Appliance) are both security products that provide protection against a variety of network-based threats. However, ESA is designed specifically to protect against email-based threats such as spam, phishing and malware, while WSA is designed to protect against web-based threats such as SQL injection, buffer overflow, and DoS attacks. So, Cisco ESA can prevent phishing but Cisco WSA can't.

upvoted 8 times

Moll Highly Voted 2 years, 9 months ago

I'd go with B because the question is about "Preventable" meaning user should not get the email in the first place, that's ESA's job..

upvoted 7 times

masal Most Recent 2 weeks, 5 days ago

from

<https://www.cisco.com/c/en/us/support/docs/security/web-security-appliance/117952-qanda-wsa-00.html>

WSA can prevent phishing attack. true answer is D.

upvoted 1 times

Premium_Pils 4 weeks ago

D - "Cisco ESA Bounce Verification to avoid the Denial of Service DOS of your email infrastructure." <https://community.cisco.com/t5/security-blogs/cisco-esa-bounce-verification-to-avoid-the-denial-of-service-dos/ba-p/4431574> Not B: WSA - "Web reputation filtering protects client devices from visiting potentially harmful websites that contain malware or phishing links."

upvoted 1 times

Stig_88 4 months ago

b. Phishing.

when an email came in, phishing already happens and WSA did not prevent it. It's the ESA which could prevent it from coming in.

What WSA can prevent is when user clicks the link on the email, but that's not that phishing attack. the phishing attack starts when user received the phishing in his inbox.

upvoted 1 times

Stig_88 4 months ago

Another thing to add here:

Q: but not by the Cisco WSA

When a web server is getting attacked by a DOS, can WSA not prevent it? I think it can.

Maybe we are focusing more on email server and ignoring Web server that we are protecting as well. Nothing on the question states that it only considers email servers.

upvoted 1 times

XvidalX 6 months, 1 week ago

Selected Answer: D

WSA PROTECT against phishing!!

ESA protect againsts DOS because have RATE LIMIT configuration for connections

<https://www.cisco.com/c/en/us/support/docs/security/web-security-appliance/117952-qanda-wsa-00.html> :

Cisco Web Security Appliance (WSA) provides the industry's most comprehensive gateway defense against spyware and web-based malware. This includes everything from Adware (which causes the most supportability issues and consumes significant network resources) to more malicious threats such as Trojans, Browser Hijackers, Browser helper Objects, Phishing, Pharming, System Monitors, Keyloggers, Worms, etc.

upvoted 2 times

mellohello 7 months, 1 week ago


Selected Answer: B

Phishing

upvoted 1 times

[-]  **JavierAcuna** 1 year, 4 months ago

The Answer is the B
upvoted 1 times

[-]  **itsklk** 1 year, 4 months ago

Selected Answer: D

Question

Does the Cisco Web Security Appliance (WSA) provide Malware/Spyware protection?

Cisco Web Security Appliance (WSA) provides the industry's most comprehensive gateway defense against spyware and web-based malware. This includes everything from Adware (which causes the most supportability issues and consumes significant network resources) to more malicious threats such as Trojans, Browser Hijackers, Browser helper Objects, Phishing, Pharming, System Monitors, Keyloggers, Worms, etc.

upvoted 1 times

[-]  **alexvozat24** 1 year, 3 months ago

its asking not by WSA ? so why are we having link for WSA?

upvoted 1 times

[-]  **achille5** 1 year, 5 months ago

Selected Answer: D

<https://www.linkedin.com/pulse/you-using-cisco-wsa-security-appliance-vulnerable-dos-cyber-defence/>

upvoted 1 times

[-]  **rubble291** 1 year, 6 months ago

Selected Answer: D

The ESA is a Transfer Agent therefore will limit mail flow to the actual email server. Therefore stopping a DoS attack.

upvoted 1 times

[-]  **ddev3737** 1 year, 7 months ago

What about answer A A. SQL injection: Cisco ESA can prevent SQL injection attacks by inspecting the payload of the incoming email messages and identifying any SQL injection attempts. However, Cisco WSA is focused on web traffic and may not have the same level of protection against this type of attack.

B. Phishing: Both Cisco ESA and Cisco WSA can prevent phishing attacks by using reputation-based filtering, SSL inspection, and anti-phishing capabilities.

C. Buffer overflow: Cisco ESA can prevent buffer overflow attacks by inspecting the payload of incoming email messages and identifying any buffer overflow attempts. However, Cisco WSA is focused on web traffic and may not have the same level of protection against this type of attack.

D. DoS: Both Cisco ESA and Cisco WSA can prevent DoS attacks by using rate-limiting, access controls, and other security measures to prevent the attack from overwhelming the system.


upvoted 1 times

[-]  **CCNP21** 1 year, 8 months ago

Selected Answer: B

I believe B is the answer.


upvoted 1 times

[-]  **Emlia1** 1 year, 9 months ago

Selected Answer: B

B is correct

upvoted 1 times

[-]  **intirt** 1 year, 9 months ago

B is correct. ESA is email appliance, not firewall.

upvoted 1 times

[-]  **sis_net_sec** 1 year, 11 months ago

Selected Answer: B

The following are the benefits of deploying Cisco Advanced Phishing Protection on the Cisco Email Security Gateway:

Prevents the following:

+ Attacks that use compromised accounts and social engineering.


+ Phishing, ransomware, zero-day attacks and spoofing.

+ BEC with no malicious payload or URL.

Reference: [https://www.cisco.com/c/en/us/td/docs/security/esa/esa13-](https://www.cisco.com/c/en/us/td/docs/security/esa/esa13-5/user_guide/b_ESA_Admin_Guide_13-5/m_advanced_phishing_protection.html)

[5/user_guide/b_ESA_Admin_Guide_13-5/m_advanced_phishing_protection.html](https://www.cisco.com/c/en/us/td/docs/security/esa/esa13-5/user_guide/b_ESA_Admin_Guide_13-5/m_advanced_phishing_protection.html)

upvoted 1 times

[-]  **Jamesy** 1 year, 11 months ago

D is the correct answer. Cheers

upvoted 1 times

An organization recently installed a Cisco WSA and would like to take advantage of the AVC engine to allow the organization to create a policy to control application specific activity. After enabling the AVC engine, what must be done to implement this?

- A. Use security services to configure the traffic monitor.
- B. Use URL categorization to prevent the application traffic.
- C. Use an access policy group to configure application control settings.
- D. Use web security reporting to validate engine functionality.

Correct Answer: C

  **sull3y** Highly Voted  1 year, 7 months ago

C. Use an access policy group to configure application control settings.

The Application Visibility and Control (AVC) engine in Cisco Web Security Appliance (WSA) allows you to control application specific activity by creating policies based on the type of traffic. To implement this, you must use an access policy group to configure the application control settings.

An access policy group defines the set of security rules that the WSA applies to incoming web traffic. The AVC engine in the WSA allows you to categorize applications based on the type of traffic they generate, and then create policies that control how that traffic is handled. This can include allowing or blocking specific applications, controlling the bandwidth used by applications, and setting limits on the amount of data that can be downloaded.

upvoted 5 times

  **NikoNiko** Most Recent  2 years, 1 month ago

C is correct.

"The Application Visibility and Control (AVC) engine lets you create policies to control application activity on the network without having to fully understand the underlying technology of each application. You can configure application control settings in ACCESS POLICY GROUPS. You can block or allow applications individually or according to application type. You can also apply controls to particular application types. "

Source: https://www.cisco.com/c/en/us/td/docs/security/wsa/wsa11-7/user_guide/b_WSA_UserGuide_11_7/b_WSA_UserGuide_11_7_chapter_01111.html

upvoted 4 times

What is the role of Cisco Umbrella Roaming when it is installed on an endpoint?

- A. to establish secure VPN connectivity to the corporate network
- B. to enforce posture compliance and mandatory software
- C. to ensure that assets are secure from malicious links on and off the corporate network
- D. to protect the endpoint against malicious file transfers

Correct Answer: C

Community vote distribution

C (100%)

Steve122 Highly Voted 2 years, 10 months ago

C

Umbrella Roaming is a cloud-delivered security service for Cisco's next-generation firewall. It protects your employees even when they are off the VPN. No additional agents are required. Simply enable the Umbrella functionality in the Cisco AnyConnect client. You'll get seamless protection against malware, phishing, and command-and-control callbacks wherever your users go.

upvoted 5 times

ureis Most Recent 1 year, 10 months ago

Selected Answer: C

Umbrella Roaming is a cloud-delivered security service for Cisco's next-generation firewall. It protects your employees even when they are "off the VPN"

upvoted 2 times

FortiSherlock 2 years, 1 month ago

Selected Answer: C

C - I do agree.

upvoted 1 times

beeker98106 2 years, 10 months ago

Nope, this is confirmed C. (on and off the network is the kicker, Umbrella also works while NOT connected view VPN)

upvoted 2 times

john_thomas 2 years, 10 months ago

Answer: A. to establish secure VPN connectivity to the corporate network

upvoted 1 times

An administrator configures a Cisco WSA to receive redirected traffic over ports 80 and 443. The organization requires that a network device with specific WSA integration capabilities be configured to send the traffic to the WSA to proxy the requests and increase visibility, while making this invisible to the users. What must be done on the Cisco WSA to support these requirements?

- A. Use PAC keys to allow only the required network devices to send the traffic to the Cisco WSA.
- B. Configure transparent traffic redirection using WCCP in the Cisco WSA and on the network device.
- C. Configure active traffic redirection using WPAD in the Cisco WSA and on the network device.
- D. Use the Layer 4 setting in the Cisco WSA to receive explicit forward requests from the network device.

Correct Answer: B

Community vote distribution

B (100%)

  **mikexian** 7 months, 2 weeks ago

Selected Answer: B

client does not have any feeling while use transparent mode
upvoted 1 times

An administrator configures a new destination list in Cisco Umbrella so that the organization can block specific domains for its devices. What should be done to ensure that all subdomains of domain.com are blocked?

- A. Configure the domain.com address in the block list.
- B. Configure the *.domain.com address in the block list.
- C. Configure the *.com address in the block list.
- D. Configure the *domain.com address in the block list.

Correct Answer: A

Community vote distribution

A (100%)

zeroC00L Highly Voted 2 years, 11 months ago

it is actually A -> <https://docs.umbrella.com/deployment-umbrella/docs/wild-cards>
"Every domain in a block or allow destination list has an implied left side and right side wildcard"
upvoted 20 times

aalnman 2 years, 11 months ago

ZeroCool is correct. Same link also states:
It is not possible to use an asterisk to wildcard a different part of the domain. The following will not work:
*.domain.com
subdomain.*.com
sub*.com
domain.*
Adding domain.com to an allow list results in requests to domain.com or its subdomains, such as www.domain.com, being allowed. The result is the same for blocklists.
upvoted 11 times

14LearningStuff Highly Voted 2 years, 12 months ago

I think it is A.
Always add domains in the format "domain.com" rather than www.domain.com to ensure *.domain.com is included (a wildcard is implicit). However, if you only wish to block subdomain.domain.com, then be more specific when you define the entry here.
upvoted 10 times

Pakawat Most Recent 8 months, 3 weeks ago

Selected Answer: A

Found this one in the exam.
upvoted 1 times

loser4fun 1 year, 5 months ago

Answer B is more accurate

To ensure that all subdomains of domain.com are blocked in Cisco Umbrella, the administrator should configure the *.domain.com address in the block list.

The asterisk (*) is a wildcard character that represents any string of characters, including subdomains. By using the wildcard character in the block list, any subdomain of domain.com will be blocked, including subdomains that do not exist yet.

If the administrator only configures the domain.com address in the block list, it will only block traffic to the root domain and not to any of its subdomains. Similarly, configuring the *.com address in the block list will block all traffic to any domain that ends with .com, not just domain.com and its subdomains. Configuring the *domain.com address in the block list will not have any effect, as it does not follow the correct syntax for blocking subdomains.

upvoted 1 times

iratus_umbra 1 year, 5 months ago

You are incorrect. The answer is A.
upvoted 1 times

Dorr20 1 year, 5 months ago

you can't use * in destination list, the system won't allow you. you configure a domain, not a URL so all subdomains are auto included.
upvoted 1 times

Emlia1 1 year, 9 months ago

Selected Answer: A

A is correct
upvoted 1 times

▣ 👤 **ureis** 1 year, 10 months ago

Selected Answer: A

"Adding domain.com to an allow list results in requests to domain.com or its subdomains, such as www.domain.com, being allowed. The result is the same for blocklists."

A

upvoted 1 times

▣ 👤 **Jamesy** 1 year, 11 months ago

B is the correct answer. Cheers

upvoted 2 times

▣ 👤 **madcloud** 2 years, 3 months ago

What you cannot add to a destination list

1. You cannot add wildcards. A wildcard is implicit in the way DNS is structured, so adding a domain covers all of the subdomains and there is no reason to add *.domain.com to cover this.

<https://support.umbrella.com/hc/en-us/articles/115006964927-Understanding-Destination-lists-supported-entries-and-error-messages>

upvoted 1 times

▣ 👤 **jaciro11** 2 years, 10 months ago

The answer is A Guys.

<https://docs.umbrella.com/deployment-umbrella/docs/wild-cards>

upvoted 6 times

▣ 👤 **Moll** 2 years, 9 months ago

Implied Wildcard

upvoted 2 times

▣ 👤 **john_thomas** 2 years, 10 months ago

B. Configure the *.domain.com address in the block list.

upvoted 3 times

▣ 👤 **Sarbi** 3 years ago

The answer is B

upvoted 8 times

An organization wants to use Cisco FTD or Cisco ASA devices. Specific URLs must be blocked from being accessed via the firewall, which requires that the administrator input the bad URL categories that the organization wants blocked into the access policy. Which solution should be used to meet this requirement?

- A. Cisco FTD because it enables URL filtering and blocks malicious URLs by default, whereas Cisco ASA does not.
- B. Cisco ASA because it enables URL filtering and blocks malicious URLs by default, whereas Cisco FTD does not.
- C. Cisco ASA because it includes URL filtering in the access control policy capabilities, whereas Cisco FTD does not.
- D. Cisco FTD because it includes URL filtering in the access control policy capabilities, whereas Cisco ASA does not.

Correct Answer: D

Community vote distribution

D (100%)

  **Pupu** Highly Voted 2 years, 6 months ago

Selected Answer: D

The answer is D.

URL Filtering is not enabled by default on FTD. Adding the license enables the Enable URL Filtering option, which then is required to be enabled by the admin.

https://www.cisco.com/c/en/us/td/docs/security/firepower/630/configuration/guide/fpmc-config-guide-v63/url_filtering.html#id_74537

upvoted 10 times

  **Jamesy** Most Recent 2 years ago

Hi guys, the answer is A please read carefully. I hope I am not confusing anyone. Thanks

upvoted 2 times

  **john_thomas** 2 years, 10 months ago

A. Cisco FTD because it enables URL filtering and blocks malicious URLs by default, whereas Cisco ASA does not.

upvoted 2 times

  **janzeleny** 2 years, 10 months ago

The option for doing URL filtering and blocking malicious URLs is in FTD, but it's not doing it by default, you have to enable it and configure which URLs (categories) should be blocked.

So the correct answer is D.

upvoted 13 times

  **lurker8000** 2 years, 8 months ago

Agree with @janzeleny, correct answer is D, I noticed @john_thomas comments on a lot of the questions but normally gives wrong answers with no explanations. Be careful following his suggestions guys. Just a friendly PSA.

upvoted 16 times

Which component of Cisco Umbrella architecture increases reliability of the service?

- A. BGP route reflector
- B. anycast IP
- C. AMP Threat Grid
- D. Cisco Talos

Correct Answer: B

Community vote distribution

B (100%)

fabio3wz Highly Voted 3 years ago

It should be anycast IP. Why Talos would increase reliability?'
upvoted 14 times

Rabyn Highly Voted 2 years, 11 months ago

Anycast would increase the resiliency of the product. Reliability and resiliency are different. With Cisco Talos, the reliability of Cisco Umbrella threat detection is increased.
upvoted 8 times

Premium_Pils Most Recent 4 weeks ago

Selected Answer: B

anycast ip: "Anycast routing is the key to reliability" - <https://umbrella.cisco.com/blog/why-the-cisco-umbrella-global-network-uses-anycast-routing>
upvoted 1 times

Alizade 11 months, 2 weeks ago

Selected Answer: B

anycast IP
upvoted 1 times

sis_net_sec 1 year, 11 months ago

B is Correct
Anycast would increase the resiliency of the product. Reliability and resiliency are different. With Cisco Talos, the reliability of Cisco Umbrella threat detection is increased.
upvoted 1 times

nomanlands 2 years, 2 months ago

Selected Answer: B

Anycast for sure
upvoted 1 times

jaciro11 2 years, 6 months ago

Selected Answer: B

anycast IP
upvoted 3 times

Pupu 2 years, 6 months ago

Selected Answer: B

The answer is B Anycast.
Check title "Anycast routing is the key to reliability" <https://umbrella.cisco.com/blog/why-the-cisco-umbrella-global-network-uses-anycast-routing>
upvoted 2 times

Minion2021 2 years, 6 months ago

It is B. Anycast IP
upvoted 2 times

lurker8000 2 years, 8 months ago

<https://umbrella.cisco.com/blog/why-the-cisco-umbrella-global-network-uses-anycast-routing#:~:text=Anycast%20routing%20is%20the%20key%20to%20reliability>

B. Anycast IP
upvoted 3 times

[-] 👤 **sysadminshodan** 2 years, 8 months ago

Creator of the question did not know "reliability" could be in a traditional network sense (Anycast) but also reliability in the accuracy of TALOs to accurately classify domains.

upvoted 1 times

[-] 👤 **cyberwhizzy0** 1 year, 2 months ago

Reliability in Networking refers to availabilities, so anycast is correct

upvoted 1 times

[-] 👤 **Moll** 2 years, 9 months ago

Voting fo B here

upvoted 2 times

[-] 👤 **jaciro11** 2 years, 10 months ago

B. anycast IP

upvoted 4 times

[-] 👤 **TonyVi** 2 years, 10 months ago

B is the correct answer

<https://www.ciscolive.com/c/dam/r/ciscolive/emea/docs/2019/pdf/BRKSEC-1980.pdf>

upvoted 3 times

[-] 👤 **beeker98106** 2 years, 10 months ago

It's B.

<https://umbrella.cisco.com/blog/why-the-cisco-umbrella-global-network-uses-anycast-routing>

Above page has this paragraph:

Anycast routing is the key to reliability

upvoted 4 times

[-] 👤 **john_thomas** 2 years, 10 months ago

B. anycast IP

upvoted 3 times

A customer has various external HTTP resources available including Intranet, Extranet, and Internet, with a proxy configuration running in explicit mode. Which method allows the client desktop browsers to be configured to select when to connect direct or when to use proxy?

- A. Bridge mode
- B. Transparent mode
- C. .PAC file
- D. Forward file

Correct Answer: C

  **Jayde** Highly Voted  2 years, 11 months ago

Answer is C

A Proxy Auto-Configuration (PAC) file contains a set of rules coded in JavaScript which allows a web browser to determine whether to send web traffic direct to the Internet or be sent via a proxy server.

PAC files can control how a web browser handles HTTP, HTTPS, and FTP traffic

<http://findproxyforurl.com/pac-file-introduction/>
upvoted 10 times

  **sull3y** Most Recent  1 year, 7 months ago

C. .PAC file

A .PAC (Proxy Auto-Config) file is a JavaScript file that is used to configure proxy settings for client desktop browsers. The .PAC file provides a set of instructions that determine whether a client should connect directly to a target resource or whether it should use a proxy. The .PAC file can be hosted on a web server and can be referenced by the client browser to automatically configure the proxy settings.

In explicit proxy mode, the client desktop browser must be configured to use the proxy for all outbound connections. With a .PAC file, the client desktop browser can be configured to select when to connect directly to a target resource or when to use the proxy based on the destination URL. This provides greater flexibility and control over proxy settings, and allows the client to easily access different types of external HTTP resources, such as Intranet, Extranet, and Internet, with different proxy configurations.

upvoted 1 times

What is a benefit of using Cisco CWS compared to an on-premises Cisco WSA?

- A. Content scanning for SAAS cloud applications is available through Cisco CWS and not available through Cisco WSA.
- B. URL categories are updated more frequently on Cisco CWS than they are on Cisco WSA.
- C. Cisco CWS minimizes the load on the internal network and security infrastructure as compared to Cisco WSA.
- D. Cisco CWS eliminates the need to backhaul traffic through headquarters for remote workers whereas Cisco WSA does not.

Correct Answer: D

Reference:

<https://www.cisco.com/c/en/us/products/collateral/security/web-security-appliance/guide-c07-742373.html>

Community vote distribution

D (100%)

[-] **👤 Rododendron2** 2 months, 3 weeks ago

Cisco Cloud Web Security - Retirement Notification

The Cisco Cloud Web Security has been retired and is no longer supported.

End-of-Sale Date: 2018-10-31

End-of-Support Date: 2019-10-31

upvoted 2 times

[-] **👤 sis_net_sec** 1 year, 10 months ago

Selected Answer: D

Explanation:

<https://www.cisco.com/c/en/us/products/collateral/security/web-security-appliance/guide-c07-742373.html>

upvoted 1 times

[-] **👤 NikoNiko** 2 years, 1 month ago

WSA

- Mobile User Security improves integration with VPN Headend ASA
- Client web traffic must be tunneled back to HQ

CWS

- Remote sites can utilise CWS directly. No VPN Backhaul!
- On-the-Go users are filtered and secured direct to CWS infrastructure
- Consistent policy applied whether in the office or not

<https://www.ciscolive.com/c/dam/r/ciscolive/apjc/docs/2018/pdf/BRKSEC-2042.pdf>

upvoted 1 times

An engineer needs to add protection for data in transit and have headers in the email message. Which configuration is needed to accomplish this goal?

- A. Deploy an encryption appliance.
- B. Provision the email appliance.
- C. Map sender IP addresses to a host interface.
- D. Enable flagged message handling.

Correct Answer: B

Community vote distribution

A (55%) B (45%)

sull3y Highly Voted 1 year, 7 months ago

B. Provision the email appliance

Provisioning the email appliance, also known as an Email Security Gateway or Email Security Appliance, is a solution for protecting data in transit and adding headers to email messages. The email appliance acts as a security layer between the email servers and the Internet, and provides a range of security features such as encryption, anti-virus, anti-spam, and content filtering. These features help to ensure that emails are transmitted securely, and help to prevent unauthorized access to sensitive information. By provisioning the email appliance, the engineer can add protection for data in transit and have headers in the email message.

upvoted 11 times

sull3y 1 year, 7 months ago

A. Deploy an encryption appliance.

Deploying an encryption appliance is the configuration that is needed to add protection for data in transit and have headers in the email message. An encryption appliance encrypts data before it is transmitted over a network, providing protection against eavesdropping and unauthorized access to sensitive information. By deploying an encryption appliance, the engineer can add protection for data in transit and ensure that headers are added to the email message. This solution provides a secure way to transmit data and helps to prevent unauthorized access to sensitive information.

upvoted 4 times

crisip Most Recent 8 months, 2 weeks ago

Selected Answer: A

I Think it is A

upvoted 1 times

jku2cya 1 year, 2 months ago

Selected Answer: B

I'd say B more than A, but who knows. Again another ambiguous exam question, to prove one knows Cisco Security knowledge..

upvoted 1 times

jku2cya 1 year, 2 months ago

Just looked at this again. I'd stick with B. Question says "Which configuration is needed".

The verb 'deploy' corresponds to adding in something new, like a new device.

The verb 'configure' corresponds to changing something that already exists.

upvoted 1 times

Kromwall 1 year, 3 months ago

Selected Answer: A

After doing more research I will change my answer to A.

To add protection for data in transit and have headers in the email message, an engineer needs to deploy an encryption appliance. This is discussed on page 1 of the Cisco Email Encryption PDF guide under the section "How to Encrypt Messages with a Local Key Server" and on page 11 under "Inserting Encryption Headers into Messages". Therefore, the correct answer is A. Deploy an encryption appliance.

https://www.cisco.com/c/en/us/td/docs/security/esa/esa11-0/user_guide_fs/b_ESA_Admin_Guide_11_0/b_ESA_Admin_Guide_chapter_010010.pdf

upvoted 4 times

Kromwall 1 year, 4 months ago



Selected Answer: B

It's B.

To add protection for data in transit and have headers in the email message, you need to insert encryption headers into messages using either a content filter or a message filter. The encryption header can override the encryption settings defined in the associated encryption profile, and it can apply specified encryption features to messages. Therefore, option B (provision the email appliance) is needed to accomplish this goal. Option A

(deploy an encryption appliance) may also be necessary depending on your organization's needs. Options C (map sender IP addresses to a host interface) and D (enable flagged message handling) are not directly related to this goal.

upvoted 2 times

  **achille5** 1 year, 6 months ago

Selected Answer: B

Correct B

upvoted 2 times

  **achille5** 1 year, 5 months ago

option A

upvoted 2 times

  **stalkr3** 1 year, 5 months ago

option C

upvoted 1 times

  **stalkr3** 1 year, 5 months ago

option D

upvoted 1 times

  **CCNP21** 1 year, 8 months ago

Selected Answer: A


The encryption header can override the encryption settings defined in the associated encryption profile, and it can apply specified encryption features to messages.

upvoted 1 times

  **Emlia1** 1 year, 9 months ago

I prefer A

upvoted 1 times

  **4000000** 1 year, 10 months ago

AsyncOS supports using encryption to secure inbound and outbound email. To use this feature, you create an encryption profile that specifies characteristics of the encrypted message and connectivity information for the key server. The key server may either be:

The Cisco Registered Envelope Service (managed service), or

An Cisco Encryption appliance (locally managed server)

😬 it should b (A) as to locally manage one must first deploy it.

upvoted 1 times

  **NikoNiko** 2 years, 1 month ago

A is correct.

WSA: " AsyncOS enables you to add encryption settings to a message by inserting an SMTP HEADER into a message using either a content filter or a message filter. The encryption header can override the encryption settings defined in the associated encryption profile, and it can apply specified encryption features to messages.

NOTE: The Cisco Ironport ENCRYPTION APPLIANCE must be set up to handle flagged messages."

As question states that headers are already in the email messages, we need only Encryption Appliance to do its work.

[https://www.cisco.com/c/en/us/td/docs/security/esa/esa11-](https://www.cisco.com/c/en/us/td/docs/security/esa/esa11-0/user_guide_fs/b_ESA_Admin_Guide_11_0/b_ESA_Admin_Guide_chapter_010010.html#task_1146822)

[0/user_guide_fs/b_ESA_Admin_Guide_11_0/b_ESA_Admin_Guide_chapter_010010.html#task_1146822](https://www.cisco.com/c/en/us/td/docs/security/esa/esa11-0/user_guide_fs/b_ESA_Admin_Guide_11_0/b_ESA_Admin_Guide_chapter_010010.html#task_1146822)

upvoted 3 times

  **FortiSherlock** 2 years, 1 month ago

The Cisco IronPort Encryption Appliance is now obsolete (past End-of-Life and End-of-Support status).

End-of-Sale Date: 2012-07-19

End-of-Support Date: 2015-07-31

=> Either this question is outdated since almost 10 years or this functionality is somehow merged in the ESA itself.

upvoted 3 times

Which Cisco platform processes behavior baselines, monitors for deviations, and reviews for malicious processes in data center traffic and servers while performing software vulnerability detection?

- A. Cisco Tetration
- B. Cisco ISE
- C. Cisco AnyConnect
- D. Cisco AMP for Network

Correct Answer: A

Reference:

https://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/white_papers/Cisco-IT-Tetration-Deployment-Part-2-of-2.html

Community vote distribution



[-]  **Felice44** 1 year, 5 months ago

Selected Answer: A

Cisco Secure Workload (formerly Tetration) seamlessly delivers a zero-trust approach to securing your application workloads across any cloud and on-premises data center environments by reducing the attack surface, preventing lateral movement, identifying workload behavior anomalies, and remediating threats quickly.

upvoted 3 times

[-]  **azertyu** 1 year, 7 months ago

https://www.cisco.com/c/en_sg/products/data-center-analytics/tetration-analytics/index.html

upvoted 1 times

A network engineer must configure a Cisco ESA to prompt users to enter two forms of information before gaining access. The Cisco ESA must also join a cluster machine using preshared keys. What must be configured to meet these requirements?

- A. Enable two-factor authentication through a RADIUS server and then join the cluster by using the Cisco ESA GUI.
- B. Enable two-factor authentication through a TACACS+ server and then join the cluster by using the Cisco ESA CLI.
- C. Enable two-factor authentication through a TACACS+ server and then join the cluster by using the Cisco ESA GUI.
- D. Enable two-factor authentication through a RADIUS server and then join the cluster by using the Cisco ESA CLI.

Correct Answer: A

Community vote distribution

D (100%)

Yuta1123 Highly Voted 2 years, 4 months ago

Selected Answer: D

I think D is the answer.

Sorce:https://www.cisco.com/c/ja_jp/td/docs/security/esa/esa11-0/user_guide_fs/b_ESA_Admin_Guide_fs/b_ESA_Admin_Guide_fs_chapter_0101000.html
upvoted 7 times

Toni_Su91 Highly Voted 1 year, 5 months ago

Document Updated on March6, 2023

<https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/200885-ESA-Cluster-Requirements-and-Setup.html>

Cluster configuration options must be done via the CLI on the ESA and cannot be created or joined in the GUI.

Note: If you run the PREPJOIN option, you need to commit your changes to the primary ESA before you run clusterconfig on the secondary ESA and join that appliance to your newly configured cluster. This is noted from the output throughout the operation: to join this appliance to a cluster with pre-shared keys, log in to the cluster machine, run the clusterconfig > prepjoin > new command , enter the next details, and commit your changes.

So I believe it is D
upvoted 5 times

Jessie45785 Most Recent 1 year, 3 months ago

Selected Answer: D

Check ans from q412

---> Enable two-factor authentication through a RADIUS server, and then join the cluster via the SEG CLI

D - is correct
upvoted 1 times

Tuxinator 1 year, 6 months ago

Selected Answer: D

horrible question.

The ability to join a cluster using the Cisco ESA GUI was introduced in version 13.5.
upvoted 2 times

ross123 1 year, 8 months ago

Answer is D. See: <https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/200885-ESA-Cluster-Requirements-and-Setup.html> under "Requirements" section.
upvoted 1 times

a7mad150 1 year, 10 months ago

joining the cluster-only can be only CLI
and ESA only supports radius
upvoted 1 times

sis_net_sec 1 year, 10 months ago

Selected Answer: D

https://www.cisco.com/c/ja_jp/td/docs/security/esa/esa11-0/user_guide_fs/b_ESA_Admin_Guide_fs/b_ESA_Admin_Guide_fs_chapter_0101000.html
upvoted 1 times

  **NikoNiko** 2 years, 2 months ago

"You cannot create or join a cluster from the Graphical User Interface (GUI). You must use the Command Line Interface (CLI) to create, join, or configure clusters of machines. Once you have created a cluster, you can change configuration settings from either the GUI or the CLI.

...

Although you cannot create or join clusters or administer cluster specific settings from the GUI (the equivalent of the clusterconfig command), you can browse machines in the cluster, create, delete, copy, and move settings among the cluster, groups, and machines (that is, perform the equivalent of the clustermode and clusterset commands) from within the GUI."

<https://www.cisco.com/c/en/us/td/docs/security/esa/esa11->

[1/user_guide/b_ESA_Admin_Guide_11_1/b_ESA_Admin_Guide_11_1_chapter_0101000.html#con_1122438](https://www.cisco.com/c/en/us/td/docs/security/esa/esa11-0/user_guide/b_ESA_Admin_Guide_11_1/b_ESA_Admin_Guide_11_1_chapter_0101000.html#con_1122438)

upvoted 2 times

  **geppo81** 2 years, 2 months ago

Selected Answer: D

I found also these links:

https://www.cisco.com/c/en/us/td/docs/security/esa/esa11-0/user_guide_fs/b_ESA_Admin_Guide_11_0/b_ESA_Admin_Guide_chapter_0100000.html

[https://www.cisco.com/c/en/us/td/docs/security/esa/esa11-](https://www.cisco.com/c/en/us/td/docs/security/esa/esa11-0/user_guide_fs/b_ESA_Admin_Guide_11_0/b_ESA_Admin_Guide_chapter_0100000.html#id_50726)

[0/user_guide_fs/b_ESA_Admin_Guide_11_0/b_ESA_Admin_Guide_chapter_0100000.html#id_50726](https://www.cisco.com/c/en/us/td/docs/security/esa/esa11-0/user_guide_fs/b_ESA_Admin_Guide_11_0/b_ESA_Admin_Guide_chapter_0100000.html#id_50726)

upvoted 3 times

  **Jardator** 2 years, 4 months ago

initial joining the cluster-only CLI can be used

upvoted 4 times

ACME Policy

Applied To
2 Identities

Contains
4 Policy Settings

Last Modified
May 6, 2020

Policy Name

2 Identities Affected

2 Networks

[Edit Identity](#)

3 Destination Lists Enforced

1 Block List

1 Allow Lists

[Edit](#)

Security Setting Applied: ACME-Security-Settings-Trial

Command and Control Callbacks, Malware, and Phishing Attacks will be blocked.

No integration is enabled

[Edit](#) [Disable](#)

File Analysis Enabled

File Inspection Enabled

[Edit](#)

Content Setting Applied: ACME-Content-Settings-Trial

Pornography and German Youth Protection will be blocked

[Edit](#) [Disable](#)

Umbrella Default Block Page Applied

[Edit](#)

No Application Settings Applied

[Enable](#)

[▶ Advanced Settings](#)

[DELETE POLICY](#)

[CANCEL](#)

[SAVE](#)

Refer to the exhibit. How does Cisco Umbrella manage traffic that is directed toward risky domains?

- A. Traffic is managed by the application settings, unhandled and allowed.
- B. Traffic is managed by the security settings and blocked.
- C. Traffic is proxied through the intelligent proxy.
- D. Traffic is allowed but logged.

Correct Answer: B

Community vote distribution

Option	Percentage
B	53%
C	47%

PIX2 Highly Voted 1 year, 6 months ago

Selected Answer: B

Output clearly shows that risky domains (C&C, Malware, Phishing) will be blocked by "Security Settings". Intelligent Proxy (answer C) is configured under the "Advanced settings", which is not visible on the output.
upvoted 11 times

Premium_Pils 4 weeks ago

I agree. it is security settings and blocked based on the picture.
upvoted 1 times

haiderzaid 1 year, 5 months ago

File analyzer require intelligent proxy to be enabled
upvoted 3 times

RemiK Most Recent 2 months, 4 weeks ago

Selected Answer: C

File analysis enable = intelligent proxy
Should be C
upvoted 2 times

mhd96far 5 months, 1 week ago

check out question 230

upvoted 1 times

XvidalX 6 months, 1 week ago

C is CORRECT - File analysis only is enabled when intelligent proxy is enabled, even not seeing proxy configuration, we can assume that is enabled...

upvoted 3 times

LTLnetworker 7 months, 3 weeks ago

Selected Answer: C

'Risky domain' is a term the documentation uses for grey list / Intelligent Proxy.

The IP cannot be seen but should be enabled in Advanced Settings.

upvoted 1 times

fdl543 1 year, 1 month ago

Selected Answer: B

"Refer to the Exhibit" We can not even see if Intelligent Proxy is enabled. So, it's B.

upvoted 1 times

jku2cya 1 year, 2 months ago

Selected Answer: B

Don't overthink it. The question first states "Refer to the exhibit".

upvoted 1 times

ffaiz 1 year, 2 months ago

Selected Answer: C

<https://docs.umbrella.com/deployment-umbrella/docs/manage-intelligent-proxy#:~:text=it%27s%20simple%3A%20Umbrella%20blocks%20those,again%2C%20no%20proxy%20is%20required.>

On this link Read this whole para: Which clearly states how Umbrella will handle "risky domains"

Umbrella's intelligent proxy intercepts and proxies requests for URLs, potentially malicious files, and domain names associated with certain uncategorized or unknown domains. Some websites, especially those with large user communities or the ability to upload and share files, have content that most users want to access but also pose a risk because of the possibility of hosting malware. Administrators don't want to block access to an unknown domain for all users, but they also don't want your users to access files that could harm their computers or compromise company data.

upvoted 2 times

gc999 1 year, 3 months ago

Selected Answer: C

After going through the document, I change to "C". It is because File Inspection is enabled, and it is an extension of the Intelligent Proxy.

<https://docs.umbrella.com/deployment-umbrella/docs/file-inspection#:~:text=File%20inspection%20is%20an%20extension%20of%20the%20intelligent%20proxy%E2%80%99s%20scope%20and%20functionality>

ality

upvoted 2 times

gc999 1 year, 3 months ago

Selected Answer: B

The question is "Refer to the exhibit". Refer to the exhibit, we do not see any hints for Intelligent Proxy. So the answer should be "B", which the exhibit already mentioned it.

upvoted 1 times

Jessie45785 1 year, 4 months ago

Selected Answer: B

Even though from logical point of view C makes more sense,... look at the Question 230

... hence against myself I am voting for B

230. When web policies are configured in Cisco Umbrella, what provides the ability to ensure that domains are blocked when they host malware, command and control, phishing, and more threats?

- A. Application Control
- B. Security Category Blocking
- C. Content Category Blocking
- D. File Analysis

Correct Answer: B

upvoted 2 times

gc999 1 year, 3 months ago

I got the same answer as you, but after reviewing the word clearly, question 230 said "when the domain host malware, command and control ...", those domains are already confirmed "bad", so it can use Security Category Blocking. But in here, the File Inspection is enabled AND the question said "risky", which is the grey list. So I believe answer here is C.

upvoted 3 times

  **cyberwhizzy0** 1 year, 2 months ago

I agree with you that we are talking about the grey list so intelligent proxy is needed
upvoted 2 times

  **davezz** 1 year, 6 months ago

C

It seems the "File Analysis Enabled, File Inspection Enabled" indicates the Intelligent Proxy is enabled, as in order to do file inspection, web traffic needs to be pulled to the proxy server for inspection. Below link shows file inspection is a sub option after Intelligent Proxy is enabled:
<https://docs.umbrella.com/umbrella-user-guide/docs/enable-the-intelligent-proxy>

upvoted 3 times

  **achille5** 1 year, 7 months ago

C

<https://docs.umbrella.com/deployment-umbrella/docs/manage-intelligent-proxy>

upvoted 1 times

  **DaelsBae** 1 year, 7 months ago

Selected Answer: C

Answer is C, as Umbrella Security Settings blocks the URL and protects against phishing while Intelligent Proxy proxies the website and filters the malicious traffic

<https://docs.umbrella.com/deployment-umbrella/docs/dns-security-categories>


upvoted 1 times

  **CCNP21** 1 year, 7 months ago

Selected Answer: C

I believe the answer is C. Umbrella uses intelligent proxy for risky domains.

upvoted 1 times

  **amtf8888** 1 year, 8 months ago

Selected Answer: C

C IS Right

The list of unknown domains is comprised of domains that host both malicious and safe content—we consider these “risky” domains. These sites often allow users to upload and share content—making them difficult to police, even for site administrators.

There's no reason to proxy requests to domains that are already known to be safe or bad. Umbrella's intelligent proxy only routes the requests for risky domains for deeper inspection.

Note: Umbrella does not proxy traffic on non-standard ports for web traffic.

upvoted 2 times

  **Emlia1** 1 year, 9 months ago

Selected Answer: B

B is correct

upvoted 1 times

An organization wants to improve its cybersecurity processes and to add intelligence to its data. The organization wants to utilize the most current intelligence data for URL filtering, reputations, and vulnerability information that can be integrated with the Cisco FTD and Cisco WSA. What must be done to accomplish these objectives?

- A. Configure the integrations with Talos intelligence to take advantage of the threat intelligence that it provides.
- B. Download the threat intelligence feed from the IETF and import it into the Cisco FTD and Cisco WSA databases.
- C. Create an automated download of the Internet Storm Center intelligence feed into the Cisco FTD and Cisco WSA databases to tie to the dynamic access control policies.
- D. Create a Cisco pxGrid connection to NIST to import this information into the security products for policy use.

Correct Answer: A

Community vote distribution

A (100%)

iluvmicrosoft 5 months ago

I also agree its A

I think the point here is current intelligence that can be ingested into FTD and WSA

we know that FMC can use talos AND/OR 3rd party feeds.. (and then push the data to FTD)

I found a post somewhere (wish i could find it) that stated FDM can only use talos

also if you read up on how WSA gets its intelligence data, it states talos and i cannot find anything that says it can get 3rd party feeds - if these are both true then answer is not B NOR C as they can only use talos..

upvoted 1 times

Alizade 11 months, 2 weeks ago

Selected Answer: A

Therefore, the answer is A.

upvoted 3 times

surforlife 2 years, 1 month ago

Why not use pxGrid?

upvoted 1 times

haiderzaid 1 year, 5 months ago

pxGrid enables third party platforms to share threat intelligence ,

in another word ,pxGrid can be used for integration, it is not specifically related to importing information from NIST.

upvoted 1 times

An organization is implementing URL blocking using Cisco Umbrella. The users are able to go to some sites but other sites are not accessible due to an error.

Why is the error occurring?

- A. Client computers do not have an SSL certificate deployed from an internal CA server.
- B. Client computers do not have the Cisco Umbrella Root CA certificate installed.
- C. IP-Layer Enforcement is not configured.
- D. Intelligent proxy and SSL decryption is disabled in the policy.

Correct Answer: A

Community vote distribution

B (100%)

screech Highly Voted 3 years, 4 months ago

Should be B.

<https://support.umbrella.com/hc/en-us/articles/115004564126-SSL-Decryption-in-the-Intelligent-Proxy>

Requirements and Implementation

Although only SSL sites on our 'grey' list will be proxied, it's required that the root certificate be installed on the computers that are using SSL Decryption for the Intelligent Proxy in their policy.

Without the root certificate, when your users go to that service, they will receive errors in the browser and the site will not be accessible. The browser, correctly, will believe the traffic is being intercepted (and proxied!) by a 'man in the middle', which is our service in this case. The traffic won't be decrypted and inspected; instead, the entire website won't be available.

upvoted 18 times

samismayilov Highly Voted 3 years, 4 months ago

Answer is B

upvoted 16 times

RemiK Most Recent 3 months ago

Selected Answer: B

<https://docs.umbrella.com/deployment-umbrella/docs/rebrand-cisco-certificate-import-information>
then

<https://docs.umbrella.com/deployment-umbrella/docs/install-cisco-umbrella-root-certificate>
all

No advice for pushing the Root CA Umbrella into an internal CA. Only via Windows GPO.

Cisco wants you to answer B.

upvoted 1 times

Mohammad_h_tarawneh 3 months, 1 week ago

you can deploy certificate from internal CA server on cisco umbrella and users pc ,
so why answer A is wrong ?

upvoted 1 times

Jessie45785 1 year, 5 months ago

Selected Answer: B

Definitely B, was doing it myself

<https://docs.umbrella.com/deployment-umbrella/docs/install-cisco-umbrella-root-certificate>

upvoted 1 times

Webster21 1 year, 9 months ago

Selected Answer: B

Should be B

upvoted 2 times

sis_net_sec 1 year, 11 months ago

Selected Answer: B

root certificate be installed on the computers that are using ssl Decryption for the intelligent proxy in their policy

<https://docs.umbrella.com/deployment-umbrella/docs/manage-intelligent-proxy>

upvoted 1 times

mrimune 2 years, 3 months ago

Should be B

upvoted 2 times

  **jaciro11** 2 years, 6 months ago

Selected Answer: B

Client computers do not have the Cisco Umbrella Root CA certificate installed.

upvoted 3 times

  **Minion2021** 2 years, 6 months ago

Answer is B

upvoted 2 times

  **Moll** 2 years, 9 months ago

Answer should be B



upvoted 2 times

  **ZanaHiwa** 2 years, 10 months ago

Answer is B:

B. Client computers do not have the Cisco Umbrella Root CA certificate installed.

upvoted 3 times

  **eazy99** 2 years, 11 months ago

The answer is absolutely B, you will find it on the first paragraph in the link I included.

<https://support.opendns.com/hc/en-us/articles/227987007-Block-Page-Errors-Installing-the-Cisco-Umbrella-Root-CA>

upvoted 2 times

  **trickbot** 3 years, 4 months ago

Well it's a good thing I paid examtopics to see all the wrong answers on the rest of the questions. This is a missing certificate problem, but the missing certificate is a CA certificate. SSL certificates issued by internal CAs would prove the user's host machine's identity to the website, which is clearly not how web browsing works.

upvoted 6 times


Question #229

Topic 1

Which feature within Cisco Umbrella allows for the ability to inspect secure HTTP traffic?

- A. File Analysis
- B. SafeSearch
- C. SSL Decryption
- D. Destination Lists

Correct Answer: C

  **idto** 2 years, 9 months ago

Correct answer is C

"As well, the intelligent proxy's SSL decryption feature is required in order to scan files on secure—HTTPS—sites."

Source: <https://docs.umbrella.com/umbrella-user-guide/docs/enable-file-analysis>

upvoted 4 times



When web policies are configured in Cisco Umbrella, what provides the ability to ensure that domains are blocked when they host malware, command and control, phishing, and more threats?

- A. Application Control
- B. Security Category Blocking
- C. Content Category Blocking
- D. File Analysis

Correct Answer: B



Reference:

<https://support.umbrella.com/hc/en-us/articles/115004563666-Understanding-Security-Categories>

  **Arris9** 1 year, 8 months ago

<https://docs.umbrella.com/deployment-umbrella/docs/dns-security-categories>

upvoted 2 times

  **ureis** 1 year, 8 months ago

I have this options in the proper Umbrella Dashboard:
"Add New Security Setting"

Options:

- Malware *****
- Newly Seen Domains
- Command and Control Callbacks *****
- Phishing Attacks *****
- Dynamic DNS
- Potentially Harmful Domains
- DNS Tunneling VPN
- Cryptomining

upvoted 2 times

  **abdulmalik_mail** 2 years, 8 months ago

correct, Its B

on reference "the security setting categories are, at a minimum, the ones listed below :

1. Malware
2. Command and Control Callbacks
3. Phishing Attack

upvoted 3 times

How is Cisco Umbrella configured to log only security events?

- A. per policy
- B. in the Reporting settings
- C. in the Security Settings section
- D. per network in the Deployments section

Correct Answer: A

Reference:

<https://docs.umbrella.com/deployment-umbrella/docs/log-management>

  **abdulmalik_mail** 2 years, 8 months ago

correct, It's A

upvoted 4 times

Which Cisco solution does Cisco Umbrella integrate with to determine if a URL is malicious?

- A. Cisco AMP
- B. Cisco AnyConnect
- C. Cisco Dynamic DNS
- D. Cisco Talos

Correct Answer: D

  **abdulmalik_mail** 2 years, 8 months ago

Correct, It's D

<https://www.insight.com/content/dam/insight-web/Canada/PDF/partner/cisco/cisco-umbrella-at-a-glance.pdf>

"The Umbrella proxy

uses Cisco Talos web reputation and other third-party feeds to determine if a URL is malicious"

upvoted 1 times

What are two list types within Cisco AMP for Endpoints Outbreak Control? (Choose two.)

- A. blocked ports
- B. simple custom detections
- C. command and control
- D. allowed applications
- E. URL

Correct Answer: BD

Reference:

<https://docs.amp.cisco.com/en/A4E/AMP%20for%20Endpoints%20User%20Guide.pdf> chapter 2

Community vote distribution

BD (100%)

  **nospampls** Highly Voted  3 years, 1 month ago

B and D

<https://docs.amp.cisco.com/AMPPrivateCloudConsoleUserGuide-latest.pdf>

upvoted 10 times

  **aalnman** 2 years, 11 months ago

B and D is CORRECT

upvoted 3 times

  **Tuxzinator** Most Recent  1 year, 6 months ago

Selected Answer: BD

bd correct

upvoted 1 times

  **Moll** 2 years, 9 months ago

Voting for B and D here

upvoted 1 times

For which two conditions can an endpoint be checked using ISE posture assessment? (Choose two.)

- A. computer identity
- B. Windows service
- C. user identity
- D. Windows firewall
- E. default browser

Correct Answer: BD

Community vote distribution

BD (100%)

Vic25H Highly Voted 4 years, 2 months ago

Agree B&D

https://www.cisco.com/c/en/us/td/docs/security/ise/2-2/admin_guide/b_ise_admin_guide_22/b_ise_admin_guide_22_chapter_010111.html

upvoted 27 times

bigdadzzz 3 years, 8 months ago

Specifically: Table 2. Posture Assessment Options - Windows Service status/config can be assessed, Windows Firewall can be assessed by assessing the registry entry.

upvoted 7 times

kudlaaaty Highly Voted 4 years, 2 months ago

IMHO: B & D

upvoted 11 times

getafix Most Recent 2 years, 3 months ago

Selected Answer: BD

i have implemented this myself. Posture checks for firewall enablement and also checks for Windows updates enabled.

upvoted 1 times

larn 2 years, 4 months ago

Selected Answer: BD

A posture condition can be any one of the following simple conditions: a file, a registry, an application, a service, or a dictionary condition. One or more conditions from these simple conditions form a compound condition, which can be associated to a posture requirement.

upvoted 1 times

Moll 2 years, 9 months ago

I agree with B and D

upvoted 2 times

pfunkylol 2 years, 9 months ago

b and c are correct

upvoted 1 times

itisfakemallo 3 years, 2 months ago

B and D

upvoted 5 times

fr3dastik 3 years, 7 months ago

Correct answer : B & D

upvoted 8 times

Which Cisco product provides proactive endpoint protection and allows administrators to centrally manage the deployment?

- A. NGFW
- B. AMP
- C. WSA
- D. ESA

Correct Answer: B

CCNP21 **Highly Voted** 1 year, 7 months ago

Now called Secure Endpoint.
upvoted 5 times

Ferdaush **Most Recent** 8 months, 2 weeks ago

Cisco Advanced Malware Protection (AMP) for Endpoints is a cloud-managed endpoint security solution that provides advanced protection against viruses, malware, and other cyber-threats by detecting, preventing, and responding to threats.
upvoted 1 times

Which two endpoint measures are used to minimize the chances of falling victim to phishing and social engineering attacks? (Choose two.)

- A. Patch for cross-site scripting.
- B. Perform backups to the private cloud.
- C. Protect against input validation and character escapes in the endpoint.
- D. Install a spam and virus email filter.
- E. Protect systems with an up-to-date antimalware program.

Correct Answer: DE

Community vote distribution

DE (100%)

bigdadzzz Highly Voted 3 years, 8 months ago
<https://us-cert.cisa.gov/ncas/tips/ST04-014>

How do you avoid being a victim?

"Install and maintain anti-virus software, firewalls, and email filters to reduce some of this traffic. (See Understanding Firewalls for Home and Small Office Use, Protecting Against Malicious Code, and Reducing Spam for more information.) "

"Less correct" answers than D/E

A - Indirectly, yes.

B - Defence against Ransomware

C - Defence against SQLi

upvoted 15 times

NikoNiko 2 years, 1 month ago

...where:

A. Patch for cross-site scripting

&

C. Protect against input validation and character escapes in the endpoint

= BOTH ARE SERVER SIDE MEASURES, NOT ENDPOINT

("server side" in this case means WHO IS RESPONSIBLE for code security, NOT WHERE the code is running - XSS will run in user's browser at client side but responsible for that is vulnerable server)

If some well known TRUSTED server (for example your own company's web) is vulnerable to XSS or another attack based on poor input validation, protection from user's side is mostly NOT possible - because you TRUST that server, you (and your security tools - for example NoScript) allow to run scripts from the server, you contentedly insert sensitive information to the page from the server, etc...

Endpoint protection is anti-spam, anti-virus, anti-malware - i. e. options D & E

upvoted 3 times

Oz3006 Highly Voted 3 years, 11 months ago

i think is D-E

C is used for cross site scripting.

upvoted 6 times

Ferdaush Most Recent 8 months, 2 weeks ago

Cisco Advanced Malware Protection (AMP) for Endpoints is a cloud-managed endpoint security solution that provides advanced protection against viruses, malware, and other cyber-threats by detecting, preventing, and responding to threats.

upvoted 1 times

Mulema 9 months, 2 weeks ago

A and C are correct assuming the following question that I asked Bard AI:

Can Cisco ISE install patches on an endpoint like a pc after identifying that the pc lacks up-to-date patches?

Yes, Cisco ISE can install patches on an endpoint like a PC after identifying that the PC lacks up-to-date patches. This is done using the Cisco Endpoint Security Agent (ESA), which is a software agent that is installed on the endpoint. The ESA communicates with Cisco ISE to determine which patches are needed and then downloads and installs them on the endpoint.

<https://bard.google.com/chat/24ec2765faf58266>

upvoted 1 times


somaao 2 years, 6 months ago

Selected Answer: DE

D,E

C for XSS

upvoted 3 times

[-]  **Moll** 2 years, 9 months ago

Voting for D and E here
upvoted 1 times

[-]  **jaciro11** 2 years, 10 months ago

D and E:

Little cathedra:

Okay many people put C " Protect against input validation and character escapes in the endpoint."
well how you protect about that "E. Protect systems with an up-to-date antimalware program."

So the answer is D and E

upvoted 5 times

[-]  **Reece_S** 3 years, 1 month ago


The question is specifically for mitigation on endpoints, so D&E.

upvoted 5 times

[-]  **thegreek1** 3 years, 10 months ago


phising is when someone tries to send you an email to lure you into a dummy website so D & E are both valid

upvoted 6 times

[-]  **naddaf** 4 years, 1 month ago


i believe C & E

upvoted 1 times

[-]  **naddaf** 4 years, 1 month ago

i believe C & E

upvoted 1 times

[-]  **Alexis182b** 4 years, 1 month ago

I think it is CD

upvoted 1 times

An engineer used a posture check on a Microsoft Windows endpoint and discovered that the MS17-010 patch was not installed, which left the endpoint vulnerable to WannaCry ransomware.

Which two solutions mitigate the risk of this ransomware infection? (Choose two.)

- A. Configure a posture policy in Cisco Identity Services Engine to install the MS17-010 patch before allowing access on the network.
- B. Set up a profiling policy in Cisco Identity Services Engine to check an endpoint patch level before allowing access on the network.
- C. Configure a posture policy in Cisco Identity Services Engine to check that an endpoint patch level is met before allowing access on the network.
- D. Configure endpoint firewall policies to stop the exploit traffic from being allowed to run and replicate throughout the network.
- E. Set up a well-defined endpoint patching strategy to ensure that endpoints have critical vulnerabilities patched in a timely fashion.

Correct Answer: AC

Community vote distribution



Sorel Highly Voted 4 years ago

I'm struggling to find a good link on this, but seems to me that ISE will not patch an endpoint by himself, instead it relies on WSUS for this. So, A is probably incorrect, and the right answer is CE. Anyone else?

upvoted 26 times

bigdadzzz 3 years, 8 months ago

https://www.cisco.com/c/en/us/td/docs/security/ise/2-1/admin_guide/b_ise_admin_guide_21/b_ise_admin_guide_20_chapter_010110.html

upvoted 2 times

Monnezzo Highly Voted 3 years, 9 months ago

It's A and C

source: <https://community.cisco.com/t5/security-documents/how-to-integrate-cisco-ise-with-microsoft-sccm-for-patch/ta-p/3725035#toc-hld-2070782007>

upvoted 10 times

nep1019 1 year, 1 month ago

Disagree. Your link says that ISE only sees that SCCM shows that there are patches needed. It then uses AnyConnect to trigger SCCM to install the patch. Answer A specifically states that ISE installs the patch. There is nowhere in any guide that says ISE installs a patch. Further if you look at the posture policy section of the admin guide, it says nothing about pushing patches. Answer A mentions the configuring a posture policy.

upvoted 1 times

iluvmicrosoft Most Recent 5 months ago

anyone consider D? if your a client w tcp 445 open?? you could have been vulnerable.. file servers w tcp 445 ok.. but clients??

upvoted 1 times

XvidalX 6 months, 1 week ago

Selected Answer: CE

ISE does not intall patches , remediation policies does not install patches , Remediation policies does trigger installations by third party systems... A is malformed answer , C and E are totally correct

upvoted 2 times

Premium_Pils 4 weeks ago

E seems to be more logical

upvoted 1 times

nep1019 1 year, 1 month ago

If you go look at the posture policy section of the admin guide (https://www.cisco.com/c/en/us/td/docs/security/ise/2-4/admin_guide/b_ISE_admin_guide_24/m_client_posture_policies.html#task_DBFD37F536134843BC81C4DFEF34A8EC) you see that there is nothing in there that allows ISE to INSTALL a patch which is what it says for answer A). Can it be integrated with SCCM to invoke an action in SCCM to update with a patch? Yes. Can ISE itself install that patch? No. Answer is C and E.

upvoted 2 times



Tuxinator 1 year, 6 months ago

Selected Answer: AC

Option C specifically addresses the vulnerability that was exploited by the WannaCry ransomware, which is the MS17-010 patch that was not installed on the endpoint. By configuring a posture policy to check that the endpoint patch level is met before allowing access to the network, the organization can ensure that all endpoints have the necessary patches installed to mitigate the risk of this ransomware.

Option E is still a good solution in general to ensure that endpoints are patched in a timely fashion, but it does not specifically address the vulnerability that was exploited by the WannaCry ransomware.



upvoted 3 times

  **psuoh** 1 year, 7 months ago

Selected Answer: CE



<https://community.cisco.com/t5/network-access-control/ise-posture-windows-updates/td-p/3575621>

upvoted 2 times

  **psuoh** 1 year, 7 months ago

ISE wouldn't know how to patch an Windows OS. It needs integration with some patching system.

upvoted 1 times

  **Anonymous983475** 1 year, 8 months ago

Selected Answer: CE

ICE can check for patches not install them in the end user's OS

upvoted 2 times

  **nomanlands** 2 years, 2 months ago


A and C is correct. SCCM will integrate to do the patching as others mentioned and E is only not an option as it asks what can be done to mitigate THIS ransomware infection and not best practices overall.

upvoted 1 times

  **west33637** 1 year, 8 months ago

it asks what can be done to mitigate 'THE RISK' of this ransomware infection. Not to mitigate the ransomware itself. C and E mitigate the risk. ISE itself does not patch systems.

upvoted 1 times

  **larn** 2 years, 4 months ago

Selected Answer: AC



People are saying patching isnt possible from ISE but the doco show it is configurable.

<https://community.cisco.com/t5/security-documents/how-to-integrate-cisco-ise-with-microsoft-sccm-for-patch/ta-p/3725035#toc-hld-2070782007>

Step 1



Go to Workcentre-> Posture-> Policy Elements-> Condition-> Patch management. Add a patch management condition to check for up-to-date patch status. This conditions checks if there are any pending patches to be installed in the SCCM client.

upvoted 3 times

  **Moll** 2 years, 9 months ago

I'd go with A and C here.

upvoted 2 times

  **jaciro11** 2 years, 10 months ago

Hello TEAM,

Well you want to check if a specified KB its patched in your system, okay nice the Answer is:

A. Configure a posture policy in Cisco Identity Services Engine to install the MS17-010 patch before allowing access on the network. but I think the appropriate answer for this is C. Configure a posture policy in Cisco Identity Services Engine to check that an endpoint patch level is met before allowing access on the network.

Well that's means A and C its the same but C its more completed answer.

So the answer is C and E

upvoted 3 times

  **Steve122** 2 years, 10 months ago

A: Patch will be installed by ISE NAC agent on endpoint

C: ISE checks the endpoint first if that is compliant (NAC agent)


B: Make no sense "profiling policy"

upvoted 2 times

  **beeker98106** 2 years, 10 months ago


A+C is correct, just confirmed

upvoted 4 times

  **stalkr3** 1 year, 5 months ago



confirmed by who?

upvoted 4 times

  **jshow** 3 years, 1 month ago

A and C for mequestion states for THIS exploit

upvoted 2 times

  **deathfrom** 3 years, 2 months ago

C & E for me, why would you protect against one threat when you can protect yourself from all threats?
upvoted 3 times

Question #238

Topic 1

What is the primary difference between an Endpoint Protection Platform and an Endpoint Detection and Response?

- A. EPP focuses on prevention, and EDR focuses on advanced threats that evade perimeter defenses.
- B. EDR focuses on prevention, and EPP focuses on advanced threats that evade perimeter defenses.
- C. EPP focuses on network security, and EDR focuses on device security.
- D. EDR focuses on network security, and EPP focuses on device security.



Correct Answer: A

Reference:

<https://www.cisco.com/c/en/us/products/security/endpoint-security/what-is-endpoint-detection-response-edr.html>

Community vote distribution

A (100%)

  **MPoels** 6 months, 1 week ago

Selected Answer: A

Prevention capabilities provided by EPPs, and detection and response capabilities (if something evades preventative measures) provided by EDRs.
<https://blogs.cisco.com/security/epp-edr-cisco-amp-for-endpoints-is-next-generation-endpoint-security>
upvoted 3 times

  **NikoNiko** 2 years, 1 month ago

A) is correct

<https://www.cynet.com/endpoint-protection-and-edr/epp-vs-edr-what-matters-more-prevention-or-response/>
upvoted 2 times

An engineer is configuring AMP for endpoints and wants to block certain files from executing.

Which outbreak control method is used to accomplish this task?

- A. device flow correlation
- B. simple detections
- C. application blocking list
- D. advanced custom detections

Correct Answer: C

Community vote distribution

C (100%)

klu16 Highly Voted 3 years ago

I thought it's B like some guys said, but it's C for sure...

From AMP for Endpoints User Guide, chapter 2: Outbreak Control:

An application blocking list is composed of files that you do not want to allow users to execute but do not want to quarantine. You may want to use this for files you are not sure are malware, unauthorized applications, or you may want to use this to stop applications with vulnerabilities from executing until a patch has been released.

B also is incorrect, because it says "simple detections" but actually it's called simple custom detections (like in answer D, but it's another function which allows the customer to write his own antivirus definitions...).

I am 100% sure it's an answer C here :)

upvoted 15 times

aalnman 2 years, 11 months ago

C = Correct as Klu16 pointed out. Also "B" does not block, it quarantines. This is from same doc klu mentioned regarding "B": A Simple Custom Detection list is similar to a blocked list. These are files that you want to detect and quarantine. Not only will an entry in a Simple Custom Detection list quarantine future files, but through Retrospective it will quarantine instances of the file on any endpoints in your organization that the service has already seen it on.

upvoted 4 times

Alizade Most Recent 11 months, 2 weeks ago

Selected Answer: C

C. Application Blocking List

upvoted 2 times

Emlia1 1 year, 9 months ago

It's C

upvoted 2 times

denverfly 2 years, 6 months ago

C is good.

Outbreak control: Achieve control over suspicious files or outbreaks and remediate an infection without waiting for a content update. Within the outbreak control feature:

- Simple custom detections can quickly block a specific file across all or selected systems
- Advanced custom signatures can block families of polymorphic malware
- Application blocking lists can enforce application policies or contain a compromised application being used as a malware gateway and stop the reinfection cycle
- Custom whitelists will help ensure that safe, custom, or mission-critical applications continue to run no matter what
- Device flow correlation will stop malware call-back communications at the source, especially for remote endpoints outside the corporate network

upvoted 2 times

Moll 2 years, 9 months ago

Would go with C here.

upvoted 2 times

Steve122 2 years, 10 months ago

Would go with C

Application Block Lists are only applicable to binaries. When the SHA-256 of a binary is added to the Application Block List, AMP will prevent that file from being executed.

upvoted 2 times

[-] 👤 **beeker98106** 2 years, 10 months ago

C. it is
upvoted 3 times

[-] 👤 **ferari** 3 years, 2 months ago

The correct answer is B.
<https://www.connection.com/~media/pdfs/brands/c/cisco/cisco-security-amp-solution-overview.pdf?la=en>
upvoted 2 times

[-] 👤 **itisfakemallo** 3 years, 2 months ago

For me the answer is B

A Simple Custom Detection list is similar to a blocked list. These are files that you want to detect and quarantine. Not only will an entry in a Simple Custom Detection list quarantine future files, but through Retrospective it will quarantine instances of the file on any endpoints in your organization that the service has already seen it on.

upvoted 3 times

[-] 👤 **Luc_10** 3 years, 2 months ago

I would answer D in this case, as custom detection blocks specific files, while application control is used to block application
upvoted 1 times

[-] 👤 **Seawanderer** 3 years, 2 months ago

It's tricky, as for example we don't execute an excel file but we run instead excel program that opens the excel file itself.
upvoted 2 times

Question #240

Topic 1

An engineer must force an endpoint to re-authenticate an already authenticated session without disrupting the endpoint to apply a new or updated policy from ISE.

Which CoA type achieves this goal?

- A. Port Bounce
- B. CoA Terminate
- C. CoA Reauth
- D. CoA Session Query

Correct Answer: C

[-] 👤 **NikoNiko** 2 years, 1 month ago

C is correct:

"CoA Session Reauthenticate Command

To initiate session authentication, the AAA server sends a standard CoA-Request message containing the following VSAs:

Cisco:Avpair="subscriber:command=reauthenticate" ...

The following rules apply:

- "subscriber:command=reauthenticate" must be present to trigger a reauthentication.
- If "subscriber:reauthenticate-type" is not specified, the default behavior is to rerun the last successful authentication method for the session. If the method reauthenticates successfully, all old authorization data is replaced with the new reauthenticated authorization data"

A - Bounce = session disrupted by disabling & enabling port

B - Terminate = session discarded

D - Session Query = ISE getting info about auth. session

"CoA Session Query Command

The CoA session query command requests service information about a subscriber session"

Source: <https://www.cisco.com/en/US/docs/ios-xml/ios/san/configuration/xe-3se/3850/san-coa-supp.pdf>

upvoted 1 times

Which two risks is a company vulnerable to if it does not have a well-established patching solution for endpoints? (Choose two.)

- A. malware
- B. denial-of-service attacks
- C. ARP spoofing
- D. exploits
- E. eavesdropping

Correct Answer: AD

  **dr4gn00t** Highly Voted  2 years, 8 months ago

D (Exploits) for sure. B (DDoS) would be suitable if the questions was about servers but since it is about endpoints, I would go with A&D.
upvoted 7 times

  **FortiSherlock** 2 years, 1 month ago

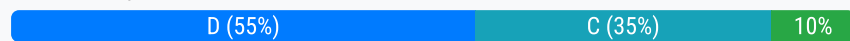
Even with current patches a DDoS attack could not really be prevented on servers or clients. You could just bomb them with illegitimate traffic and they could not do anything.
It is for sure A & D.
upvoted 3 times

Which benefit is provided by ensuring that an endpoint is compliant with a posture policy configured in Cisco ISE?

- A. It adds endpoints to identity groups dynamically
- B. It allows the endpoint to authenticate with 802.1x or MAB
- C. It allows CoA to be applied if the endpoint status is compliant
- D. It verifies that the endpoint has the latest Microsoft security patches installed

Correct Answer: D

Community vote distribution



Jeeves69 Highly Voted 3 years, 6 months ago

Correct answer should be D
upvoted 27 times

klu16 3 years ago

But "by ensuring that the endpoint is compliant", then you can authenticate afterwards. So might be a B also...
I agree that with posture policy you verify the latest patches are installed, but when you ensure that, you can then authenticate. Or is my interpretation incorrect? ;)

upvoted 3 times

Smileebloke 2 years, 5 months ago

Depends what the policy requirements are, if the requirements on the policy don't include the latest patches, then D is incorrect.

upvoted 2 times

Moll Highly Voted 2 years, 10 months ago

Answer should be C
<https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/215419-ise-session-management-and-posture.html>
step 3. Posture assessment happens.
step 4. Session marked as Compliant.
step 5. Change of Authorization (COA) triggered by posture status change leads to re-authentication of the endpoint to apply the next access level.

upvoted 19 times

klu16 Most Recent 2 months ago

Option C remains the most appropriate answer because it directly addresses the capability of applying CoA based on endpoint compliance status, which is a key benefit of posture assessment and enforcement in Cisco ISE. Therefore, while option D is a valuable functionality, option C offers a more comprehensive and overarching benefit of posture compliance in Cisco ISE. It highlights the dynamic access control and policy enforcement capabilities enabled by CoA based on the endpoint's security posture.

In conclusion, while option D reflects a significant aspect of posture policies, option C provides a more encompassing benefit by emphasizing the dynamic access control and policy enforcement possibilities through CoA based on the endpoint's overall security posture.

upvoted 1 times

Rododendron2 3 months, 1 week ago

Selected Answer: D

CoA is not a benefit, it is mechanism
upvoted 1 times

Rododendron2 2 months, 2 weeks ago

mechanism that brings desired result = benefit
upvoted 1 times

abdul9621 7 months, 1 week ago

Selected Answer: D

D is correct
upvoted 1 times

Mulema 9 months, 2 weeks ago

C is the correct answer for me.
An endpoint (PC) having the latest Microsoft security patches installed, is part of the compliant posture policy defined in ISE. So, an endpoint cannot be said to be compliant without this Microsoft patch and the other necessary patches for the other applications running on that pc. The patches are determined by the company in function of its business applications.

upvoted 1 times

Edy79 10 months, 3 weeks ago

It must be D. It cannot be C because CoA also happens if the endpoint is not compliant.

" Validating a Posture Requirement Request

Once the client (an endpoint) is authenticated on the network, the client can be granted limited access on the network. For example, the client can access remediation-only resources on the network. The NAC Agent that is installed on the client validates the requirements for an endpoint and the endpoint is moved to a compliant state upon successful validation of the requirements. If the endpoint satisfies the requirement, a compliance report will be sent to the Cisco ISE node that assumes the Policy Service persona and the run-time services triggers a Change of Authorization (CoA) for the posture compliant status. If the endpoint fails to satisfy the requirement, a noncompliance report will be sent to the Cisco ISE node that assumes the Policy Service persona and the run-time services triggers a CoA for the posture noncompliant status."

source: https://www.cisco.com/en/US/docs/security/ise/1.0/user_guide/ise10_pos_pol.html#wp1496783

upvoted 2 times

  **cyberwhizzy0** 1 year, 1 month ago

This is what I have been thinking about too but I am not sure...I'm tilting towards "C"

5. Change of Authorization (COA) triggered by posture status change leads to re-authentication of the endpoint to apply the next access level.

<https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/215419-ise-session-management-and-posture.html>

upvoted 3 times

  **SegaMasterSystemAdmin** 1 year, 3 months ago

Selected Answer: D

Please stop voting for C, it is not the right answer. CoA is not a benefit, it's just the action as result of the compliance status whether it is compliant, noncompliant, or unknown. If you read the question carefully "Which benefit is provided by ensuring that an endpoint is compliant.." if checking for the latest MS security patches is what the posture policy is looking for, then that would be the benefit, answer is D.

upvoted 4 times

  **stalkr3** 1 year, 5 months ago

The key here, is allowing COA is not a "benefit", rather the expected behaviour once the endpoint is compliant, to grant full access.

upvoted 2 times

  **tramollaaaa** 1 year, 5 months ago

Selected Answer: D

for me it is D, why ask about benefits

upvoted 2 times

  **loser4fun** 1 year, 5 months ago

The correct answer is B, i.e., ensuring that an endpoint is compliant with a posture policy configured in Cisco ISE allows the endpoint to authenticate with 802.1x or MAB (MAC Authentication Bypass).

Posture assessment is a feature in Cisco ISE that checks the security status of endpoints before allowing them access to the network. The posture assessment can check various aspects of the endpoint's security status, such as antivirus status, patch level, and software versions. If the endpoint is found to be non-compliant, it can be redirected to a remediation server to update its security status.

Once the endpoint is found to be compliant with the posture policy, it can be granted access to the network. Depending on the configuration, the endpoint may be required to authenticate using 802.1x or MAB. This authentication process ensures that only authorized devices are allowed access to the network.

upvoted 1 times

  **loser4fun** 1 year, 6 months ago

The correct answer is option C: It allows CoA to be applied if the endpoint status is compliant.

Posture policies in Cisco ISE provide the ability to check the compliance of endpoints with regard to specific security settings or configurations, such as antivirus software or the latest security patches. This allows network administrators to ensure that all endpoints on the network meet the required security standards and are not a risk to the network.

When an endpoint is found to be noncompliant with a posture policy, the Cisco ISE can initiate remediation actions, such as quarantining the endpoint or restricting its network access until it meets the policy requirements. Once an endpoint is compliant, a Change of Authorization (CoA) can be sent to allow the endpoint full network access.

upvoted 2 times

  **Tuxinator** 1 year, 6 months ago

Selected Answer: C

Ensuring that an endpoint is compliant with a posture policy configured in Cisco ISE allows CoA (Change of Authorization) to be applied if the endpoint status is compliant. CoA can be used to reapply network access policies based on endpoint compliance status, such as updating VLAN assignments or implementing ACLs, ensuring that the endpoint has appropriate network access.



upvoted 3 times

  **amtf8888** 1 year, 8 months ago

Selected Answer: C

C IS right

upvoted 2 times

  **Emlia1** 1 year, 9 months ago

Selected Answer: B

It's B

upvoted 1 times

  **Enlia1** 1 year, 9 months ago

Selected Answer: B

seems B

upvoted 1 times

An engineer wants to automatically assign endpoints that have a specific OUI into a new endpoint group. Which probe must be enabled for this type of profiling to work?

- A. SNMP
- B. NMAP
- C. DHCP
- D. NetFlow

Correct Answer: C

Community vote distribution



Jeeves69 Highly Voted 3 years, 6 months ago

The answer is C, through DHCP Profiling.

The OUI is part of the MAC address, which can be learned from the dhcp-client-identifier option 61.

upvoted 34 times

semi1750 2 years, 5 months ago

I agree. NMAP scan is based on IP, any information collected during scan will be discarded if MAC-IP binding doesn't exist

According to ISE profile design guide, "The dhcp-client-identifier typically provides the MAC address, which in turn provides the vendor OUI information through correlation from the MAC Address-OUI mapping table." under Procedure 25 Verify DHCP Probe Data

<https://community.cisco.com/t5/security-documents/ise-profiling-design-guide/ta-p/3739456#toc-hId-2096149162>

upvoted 7 times

semi1750 2 years, 4 months ago

in addition to Jeeves69, It is option 60, not 61

<https://www.ciscolive.com/c/dam/r/ciscolive/apjc/docs/2019/pdf/BRKSEC-2725.pdf>

Vendor / OS information can be gathered from dhcp-class-identifier (60)

DHCP parameter request list and DHCP class ID can be used for platform and model.

upvoted 3 times

Premium_Pils 4 weeks ago

The dhcp-client-identifier typically provides the MAC address, which in turn provides the vendor OUI information through correlation from the MAC Address-OUI mapping table.

The dhcp-class-identifier often provides a unique platform-specific attribute and in some cases provides a detailed description of the connected endpoint - in this example, MSFT 5.0 which is the value assigned to Microsoft Windows workstations.

<https://community.cisco.com/t5/security-knowledge-base/ise-profiling-design-guide/ta-p/3739456>

upvoted 1 times

044f2fc 5 months, 1 week ago

And check Nmap probe to access mac ...it is done on manual scan

upvoted 1 times

044f2fc 5 months, 1 week ago

[https://www.cisco.com/c/en/us/td/docs/security/ise/2-](https://www.cisco.com/c/en/us/td/docs/security/ise/2-4/admin_guide/Workflow/b_endpoint_profiling_2_4.html#reference_FD15BD65A25A4390B2A865450F938ADF)

[4/admin_guide/Workflow/b_endpoint_profiling_2_4.html#reference_FD15BD65A25A4390B2A865450F938ADF](https://www.cisco.com/c/en/us/td/docs/security/ise/2-4/admin_guide/Workflow/b_endpoint_profiling_2_4.html#reference_FD15BD65A25A4390B2A865450F938ADF)

upvoted 1 times

nomanlands Highly Voted 2 years, 2 months ago

Selected Answer: A

The answer is SNMP. It will work and can pull ARP tables from the network devices. In fact, page 28 in the ISE Profiling guide recommends it if Radius or DHCP probes can't be effective.

An NMAP scan cannot get a MAC address. If it is on the same subnet, then it would pull the MAC from the ARP table which would then be effective. That's a big IF

DHCP would miss static devices as mentioned.

A Netflow probe with additional attributes of SRC_MAC and DST_MAC should also be able to work for this situation if placed properly within the networks but I'm going with SNMP as that is what is recommended in the guide.

upvoted 5 times

Premium_Pils Most Recent 4 weeks ago

Selected Answer: C

<https://community.cisco.com/t5/security-knowledge-base/ise-profiling-design-guide/ta-p/3739456>

upvoted 1 times

  **Korndal** 2 months, 1 week ago

Selected Answer: C

DHCP. This is the most used function for ISE to learn about endpoints. Since it can learn about them even if the endpoints are not in a 802.1x enabled port. NMAP is a manually/triggered. Its teoretic that some clients use static IP. Most devices use dhcp

upvoted 1 times

  **RemiK** 2 months, 4 weeks ago

Selected Answer: C

More relevant about OUI stil "probe DHCP". Answer C.

upvoted 1 times

  **Rododendron2** 3 months, 1 week ago

Selected Answer: C

A and C will work, C for dynamic only. I just like it more. NMAP looks to me as and absolute nonsense , would work only scanning on same subnet

upvoted 2 times

  **c66bc39** 3 months, 1 week ago

SNMP

<https://community.cisco.com/t5/tkb/articleprintpage/tkb-id/4561-docs-security/article-id/6096>

Procedure 11

upvoted 1 times

  **044f2fc** 5 months, 1 week ago

Selected Answer: D



Why not D? Check profiling probe using net flow v9 ... also dhcp on security perspective uses ip to mac binding doesn't mean it is used as a probe to get mac details..

upvoted 1 times

  **044f2fc** 5 months, 1 week ago

And check Nmap probe to access mac ...it is done on manual scan


upvoted 1 times

  **044f2fc** 5 months, 1 week ago

[https://www.cisco.com/c/en/us/td/docs/security/ise/2-](https://www.cisco.com/c/en/us/td/docs/security/ise/2-4/admin_guide/Workflow/b_endpoint_profiling_2_4.html#reference_FD15BD65A25A4390B2A865450F938ADF)

[4/admin_guide/Workflow/b_endpoint_profiling_2_4.html#reference_FD15BD65A25A4390B2A865450F938ADF](https://www.cisco.com/c/en/us/td/docs/security/ise/2-4/admin_guide/Workflow/b_endpoint_profiling_2_4.html#reference_FD15BD65A25A4390B2A865450F938ADF)

upvoted 1 times

  **squirrelzzz** 5 months, 3 weeks ago

Selected Answer: C

OUI is part of MAC Address

upvoted 1 times

  **nekkrokvlt** 11 months, 2 weeks ago

Selected Answer: C

I vote for C As well, NMAP is layer 3.

upvoted 1 times

  **GoldFree** 1 year ago

Selected Answer: A

Probe SNMP:

Key profiling attributes:

- MAC Address/OUI
- CDP/LLDP
- ARP tables

Common Endpoint Profiling Use Cases

See RADIUS probe for MAC info.

Valuable for any vendor that uses CDP/LLDP. For example,

Cisco IP phones, cameras, access points, appliances.

Polling of device ARP tables populates ISE MAC-to-IP bindings.

<https://community.cisco.com/t5/security-knowledge-base/ise-profiling-design-guide/ta-p/3739456>

CTRL + F to the setion: "Probe Selection Best Practices"

upvoted 2 times

  **F0rtyx40** 1 year, 1 month ago

Selected Answer: A

NMAP scans for open ports and OS detection, how do you get MAC address in NMAP scans over L3? you can configure SNMP probes to start profiling and populating endpoints before enforcing MAB/802.1X IN ISE. I have done this a few times.


upvoted 2 times

  **GCalvo** 1 year, 4 months ago

C. DHCP

DHCP stands for Dynamic Host Configuration Protocol, and it's a network protocol used on IP networks to dynamically assign IP addresses and other network configuration parameters to devices on a network. The DHCP probe can capture the DHCP request packets, which contain the MAC address of the device. The first half of a MAC address is the Organizationally Unique Identifier (OUI), which is specific to a manufacturer.

upvoted 1 times

  **Carlis** 1 year, 5 months ago

Selected Answer: B

most correct answer is SNMP probe. DHCP probe can also pull Unique vendor IDs for hardware, but not for endpoints with static IPs.

When determining which probes to enable in the network, it is helpful to understand which attributes can be collected by each probe:

RADIUS - MAC Address (OUI), IP Address, NDG values

RADIUS w/Device Sensor - CDP/LLDP, DHCP, User-Agent, mDNS, H323/SIP

RADIUS w/ACIDex - MAC Address, UDID, Operating System, Platform/Device Type

SNMP - MAC Address/OUI, CDP/LLDP, ARP tables

DHCP - DHCP [also OUI]

DNS - FQDN

HTTP - User-Agent

NetFlow - Protocol, Source/Dest IP, Source/Dest/Ports



NMAP - Operating System, Common and custom ports, Service Version Info, SMB data, Endpoint SNMP data

AD - Exists in AD, Operating System and Version, AD Domain

pxGrid - IoT Asset, Custom Attributes

<https://community.cisco.com/t5/security-knowledge-base/ise-profiling-design-guide/ta-p/3739456#toc-h1d--2031470585> --> Table 13. Probe Attributes

upvoted 2 times

  **Carlis** 1 year, 5 months ago

SNMP is A, of course

upvoted 1 times

  **Toni_Su91** 1 year, 5 months ago

<https://www.ciscolive.com/c/dam/r/ciscolive/apjc/docs/2019/pdf/BRKSEC-2725.pdf>

Interesting debate. I would go for DHCP based on above.

DHCP can certainly gather OUI and it is dynamic a well. Nmap would have to be manually initiated or scheduled.



upvoted 2 times

  **Brumik** 1 year, 6 months ago

Selected Answer: C

Answer is C

upvoted 2 times

  **jienBoq** 1 year, 6 months ago

Selected Answer: B

<http://www.network-node.com/blog/2016/1/2/ise-20-profiling#:~:text=ISE%20can%20check%20the%20vendor,troubleshooting%20if%20the%20session%20terminates.&text=SNMP%20Trap%3A,or%20Odisconnecting%20from%20the%20network>.

NMAP Scan Probe:

After a scan is run, there are new attributes you can see about this host:

EndPointPolicy

LastNmapScanCount

NmapScanCount

OUI

operating-system

upvoted 1 times

What is the benefit of installing Cisco AMP for Endpoints on a network?

- A. It enables behavioral analysis to be used for the endpoints
- B. It provides flow-based visibility for the endpoints' network connections.
- C. It protects endpoint systems through application control and real-time scanning.
- D. It provides operating system patches on the endpoints for security.

Correct Answer: C

Community vote distribution

A (50%) C (33%) B (17%)

jaciro11 Highly Voted 2 years, 9 months ago

I use AMP for many years Like partner.
But now I have this questions Obviously its A Or C.
A Behavioral analysis its an amazing plus which this EDR doing.
C Real time and App block : This is something which all the antivirus or EPP use.

Im confused here because AMP can do the both but which answer is the more accurate answer.

How I hate this CISCO EXAMS, never have a good sense to make a real question and not a stupid tricky question like this... let me know guys what you think about it
upvoted 18 times

NikoNiko 2 years, 1 month ago

As they are asking about AMP BENEFITS, it will be probably A - behavioral analysis - because it is greater benefit than real-time scanning, which can be also done by standard AV solution.

"Behavioral protection: Secure Endpoint's enhanced behavioral analysis continually monitors all user and endpoint activity to protect against malicious behavior in real-time by matching a stream of activity records against a set of attack activity patterns which are dynamically updated as threats evolve. For example, this enables granular control and protection from the malicious use of living-off-the-land tools."

<https://www.cisco.com/c/en/us/products/collateral/security/fireamp-endpoints/datasheet-c78-733181.html>

upvoted 4 times

NikoNiko 2 years, 1 month ago

Moreover, traditional AV scanning in AMP - TETRA engine - is disabled by default (but there is still real-time protection "through application control and real-time scanning", so this is just for info):

"There are three detection and protection "engines" in AMP for Endpoints:

- TETRA: A full client-side antivirus solution. Do not enable the use of TETRA if there is an existing antivirus product in place. The default AMP setting is to leave TETRA disabled, as it changes the nature of the AMP connector from being a very lightweight agent to being a "thicker" software client that consumes more disk space for signature storage + BW for updates.
- Spero: A machine learning-based technology that proactively identifies threats that were previously unknown. It uses active heuristics to gather execution attributes, and because the underlying algorithms come up with generic models, they can identify malicious software based on its general appearance rather than basing identity on specific patterns or signatures.
- Ethos: A "fuzzy fingerprinting" engine that uses static or passive heuristics."

Source: CCNP / CCIE SCOR official cert guide by Omar Santos

upvoted 2 times

bob511 2 years, 6 months ago

im convinced they ask to choose one but have 2 correct answers and if you choose either they will mark it as correct.

upvoted 2 times

Premium_Pils Most Recent 4 weeks ago

Selected Answer: A

"Behavior-based malware detection, which builds a full context around every process execution path in real time"



<https://www.cisco.com/c/en/us/products/security/advanced-malware-protection/index.html>

upvoted 1 times

4pelos 6 months, 1 week ago

Correct answer C
Checked with securitytut

upvoted 1 times

  **gc999** 1 year, 3 months ago

Selected Answer: C

For A and C, I will choose C.

For A, it said "It enables behavioral analysis to be used for the endpoints", it didn't tell the benefit, how to use and what does it use for? Does it mean the endpoint use it?

For C, it can help for the protection.

upvoted 2 times

  **loser4fun** 1 year, 6 months ago

The correct answer is C: It protects endpoint systems through application control and real-time scanning.


Cisco AMP for Endpoints is an advanced endpoint security solution that provides protection for endpoints such as desktops, laptops, servers, and mobile devices. It provides multiple layers of protection against various types of cyber threats, such as malware, viruses, spyware, and ransomware.

Option A, behavioral analysis, is a feature of Cisco AMP for Endpoints that enables the detection of malicious activity on an endpoint by analyzing its behavior. It is a part of the real-time scanning and advanced threat intelligence capabilities of the solution.

Option B, flow-based visibility, is a feature of Cisco Firepower that provides visibility into the network connections of endpoints, but it is not a feature of Cisco AMP for Endpoints.

Option D, operating system patches, is not a feature of Cisco AMP for Endpoints. However, it is important to keep endpoint systems updated with the latest security patches to protect against vulnerabilities.



upvoted 2 times

  **achille5** 1 year, 6 months ago

Selected Answer: C

Both A and C are important benefits, however to protect endpoint systems through application control and real-time scanning," as it is the primary benefit of using Cisco AMP for Endpoints.

upvoted 1 times

  **psuoh** 1 year, 7 months ago

i think the best Cisco answer is A. IT makes there app stand out from other AV apps.

upvoted 1 times

  **Emlia1** 1 year, 9 months ago

Selected Answer: C

it should be C

upvoted 1 times

  **minous123** 2 years, 1 month ago

Selected Answer: B

Question is tricky.. but it is asking about BENEFIT of installing AMP for endpoints on a NETWORK. Based on that I choose B because it can monitor network connection and block malicious. A and C seems also valid but B seems to be the best option based on question.

Explanation:

You can enable Device Flow Correlation. It allows you to monitor network activity and determine which action the connector should take when connections to malicious hosts are detected.

<https://docs.amp.cisco.com/en/SecureEndpoint/Secure%20Endpoint%20User%20Guide.pdf>

upvoted 2 times

  **semi1750** 2 years, 4 months ago

Vote for A

AMP for Endpoints Malicious Activity Protection (MAP) engine included in the AMP Connector Version 6.1.5 for Windows defends your endpoints by monitoring the system and identifying processes that exhibit malicious activities when they execute and stops them from running. Because the MAP engine detects threats by observing the behavior of the process at run time, it can generically determine if a system is under attack by a new variant of ransomware or malware that may have eluded other security products and detection technology, such as legacy signature-based malware detection. The first release of the MAP engine targets identification, blocking, and quarantine of ransomware attacks on the endpoint.



upvoted 1 times

  **dr4gn00t** 2 years, 7 months ago

Selected Answer: A

C is not wrong but it is something that every AV does. A is better answer for AMP.

upvoted 1 times

  **Jetnor** 2 years, 8 months ago

Voting for C



<https://www.cisco.com/c/en/us/products/collateral/security/fireamp-endpoints/datasheet-c78-733181.html>

check section:

Benefits


In the rapidly evolving world of malware, threats are becoming harder and harder to detect. The most advanced 1% of these threats, those that will eventually enter and wreak havoc in your network, could potentially go undetected. However, Secure Endpoint provides comprehensive protection against that 1%. This security software prevents breaches, blocks malware at the point of entry, and continuously monitors and analyzes file and process activity to rapidly detect, contain, and remediate threats that can evade front-line defenses.

upvoted 2 times

  **Moll** 2 years, 9 months ago

Voting for C here

upvoted 2 times

  **jaciro11** 2 years, 9 months ago

Selected Answer: A

The answer is A

<https://www.cisco.com/c/en/us/products/collateral/security/fireamp-endpoints/datasheet-c78-733181.html>

Behavioral protection: Secure Endpoint's enhanced behavioral analysis continually monitors all user and endpoint activity to protect against malicious behavior in real-time by matching a stream of activity records against a set of attack activity patterns which are dynamically updated as threats evolve. For example, this enables granular control and protection from the malicious use of living-off-the-land tools.

upvoted 4 times

Question #245

Topic 1

Why is it important to have logical security controls on endpoints even though the users are trained to spot security threats and the network devices already help prevent them?

- A. because defense-in-depth stops at the network
- B. because human error or insider threats will still exist
- C. to prevent theft of the endpoints
- D. to expose the endpoint to more threats

Correct Answer: B

What must be configured in Cisco ISE to enforce reauthentication of an endpoint session when an endpoint is deleted from an identity group?

- A. SNMP probe
- B. CoA
- C. external identity source
- D. posture assessment

Correct Answer: B

Community vote distribution

B (100%)

- entitty** Highly Voted 3 years, 3 months ago

b - COA See -https://www.cisco.com/c/en/us/td/docs/security/ise/2-1/admin_guide/b_ise_admin_guide_21/b_ise_admin_guide_20_chapter_010100.html - search for Endpoint deleted: When an endpoint is deleted from the Endpoints page and the endpoint is disconnected or removed from the network

upvoted 20 times
- Minipaf** Highly Voted 3 years, 4 months ago

Answer is B CoA.

upvoted 10 times
- sull3y** Most Recent 1 year, 7 months ago

B. CoA (Change of Authorization)

Cisco ISE (Identity Services Engine) is a policy control platform that provides secure access control and BYOD (Bring Your Own Device) support. To enforce reauthentication of an endpoint session when an endpoint is deleted from an identity group, a Change of Authorization (CoA) must be configured in ISE. CoA allows for dynamic changes to the authorization level of an endpoint, and can be used to trigger reauthentication when an endpoint is deleted from an identity group. This helps to ensure that the endpoint remains compliant with security policies and that any potential security risks are addressed in real-time.

upvoted 2 times
- nomanlands** 2 years, 2 months ago

Selected Answer: B

B, deleting causes a CoA to occur

upvoted 1 times
- Moll** 2 years, 9 months ago

Would go with Answer: A here

upvoted 1 times
- Moll** 2 years, 9 months ago

<https://community.cisco.com/t5/network-access-control/do-i-really-need-the-snmp-query-probe/td-p/2915326>

upvoted 1 times
- Steve122** 2 years, 10 months ago

C

The profiling service issues the change of authorization in the following cases:

 - Endpoint deleted: When an endpoint is deleted from the Endpoints page and the endpoint is disconnected or removed from the network.

upvoted 1 times
- Steve122** 2 years, 10 months ago

not C, B

upvoted 1 times
- Moll** 2 years, 10 months ago

Answer: A makes sense

https://www.cisco.com/c/en/us/td/docs/security/ise/2-1/admin_guide/b_ise_admin_guide_21/b_ise_admin_guide_20_chapter_010100.html


Cisco ISE does not issue a CoA for the following reasons:

 - An Endpoint disconnected from the network

upvoted 2 times
- killbots** 2 years, 4 months ago

its not disconnecting. its being deleted from the policy. 2 different things. Its a definite B.

upvoted 1 times

  **klu16** 3 years ago

Yeah, B...

upvoted 4 times

  **acc2326** 3 years, 4 months ago

CoA for sure

upvoted 5 times

  **kakakayaya** 3 years, 4 months ago

SNMP probe - no use for CoA

upvoted 4 times

In which situation should an Endpoint Detection and Response solution be chosen versus an Endpoint Protection Platform?

- A. when there is a need to have more advanced detection capabilities
- B. when there is no firewall on the network
- C. when there is a need for traditional anti-malware detection
- D. when there is no need to have the solution centrally managed

Correct Answer: A

Community vote distribution

A (100%)

jccastiyo Highly Voted 2 years, 9 months ago

Selected Answer: A

It's so obvious if you know the difference between EDR and EPP.
upvoted 10 times

itisfakemailol Highly Voted 3 years, 2 months ago

A. when there is a need to have more advanced detection capabilities
upvoted 6 times

sis_net_sec Most Recent 2 years, 1 month ago

Selected Answer:A

What is the difference between an endpoint protection platform (EPP) and endpoint detection and response (EDR)?

EDR focuses primarily on advanced threats that are designed to evade front-line defenses and have successfully entered into the environment. An EPP focuses solely on prevention at the perimeter. It is difficult, if not impossible, for an EPP to block 100 percent of threats. So in the ideal case, an endpoint security solution deploys both EPP and EDR capabilities.

<https://www.cisco.com/c/en/us/products/security/endpoint-security/what-is-endpoint-detection-response-edr.html#:~:text=What%20is%20the%20difference%20between,on%20prevention%20at%20the>

%20perimeter.
upvoted 2 times

killbots 2 years, 4 months ago

Selected Answer: A

Its A. EDR provide advanced capabilities as EPP provide your traditional protections.
upvoted 3 times

Moll 2 years, 9 months ago

Answer should be A
upvoted 5 times

Steve122 2 years, 10 months ago

A

EDR focuses primarily on advanced threats that are designed to evade front-line defenses and have successfully entered into the environment.

An EPP focuses solely on prevention at the perimeter.
upvoted 5 times

trickbot 3 years, 4 months ago

Endpoint Detection and Response (EDR) is the next gen replacement of traditional anti-malware which was primarily signature based. EDR is centrally managed because it is practically run by crowd sourced AI. Having a firewall on the network wouldnt influence a decision between the two. Signature based Anti-malware is going bye-bye.

upvoted 6 times

kakakayaya 3 years, 4 months ago

Traditional EPP
Advanced EDR
So A fits better
upvoted 6 times

Minipaf 3 years, 4 months ago

Correct answer is A: when there is a need to have more advanced detection capabilities.

[https://www.esecurityplanet.com/endpoint/antivirus-vs-epp-vs-edr/#:~:text=Endpoint%20detection%20and%20response%20\(EDR\)%20represents%20the%20newest%20and%20most,advanced%20layer%20of%20endpoint%20protection.&text=Whereas%20EPP%20is%20a%20first,they%20can%20cause%20significant%20damage.](https://www.esecurityplanet.com/endpoint/antivirus-vs-epp-vs-edr/#:~:text=Endpoint%20detection%20and%20response%20(EDR)%20represents%20the%20newest%20and%20most,advanced%20layer%20of%20endpoint%20protection.&text=Whereas%20EPP%20is%20a%20first,they%20can%20cause%20significant%20damage.)

upvoted 5 times

Question #248

Topic 1

Which two probes are configured to gather attributes of connected endpoints using Cisco Identity Services Engine? (Choose two.)

- A. RADIUS
- B. TACACS+
- C. DHCP
- D. sFlow
- E. SMTP

Correct Answer: AC

Reference:

https://www.cisco.com/en/US/docs/security/ise/1.0/user_guide/ise10_prof_pol.html

Community vote distribution



loser4fun 1 year, 6 months ago

The correct answers are A. RADIUS and C. DHCP.

Cisco Identity Services Engine (ISE) uses different probes to gather information about network endpoints for device profiling and authentication. Two of the probes used to gather attributes of connected endpoints are:

A. RADIUS: Remote Authentication Dial-In User Service (RADIUS) is a network protocol that provides centralized authentication, authorization, and accounting (AAA) management for devices that connect and use a network service. ISE can use RADIUS probes to gather endpoint attributes such as device type, operating system, and installed applications.

C. DHCP: Dynamic Host Configuration Protocol (DHCP) is a network protocol that enables devices to automatically obtain an IP address and network configuration settings from a DHCP server. ISE can use DHCP probes to gather endpoint attributes such as MAC address, hostname, and IP address.

upvoted 1 times

killbots 2 years, 4 months ago

Selected Answer: AC

The selected answer is correct.

upvoted 1 times

What are two reasons for implementing a multifactor authentication solution such as Cisco Duo Security provide to an organization? (Choose two.)

- A. single sign-on access to on-premises and cloud applications
- B. identification and correction of application vulnerabilities before allowing access to resources
- C. secure access to on-premises and cloud applications
- D. integration with 802.1x security using native Microsoft Windows supplicant
- E. flexibility of different methods of 2FA such as phone callbacks, SMS passcodes, and push notifications

Correct Answer: CE

Community vote distribution



aalnman Highly Voted 2 years, 11 months ago

C & E - I agree with. BUT this is also on DUOs page: Simple, Secure Single Sign-On Single sign-on (SSO) from Duo provides users with an easy and consistent login experience for any and every application, whether it's on-premises or cloud-based. Cloud-based and hosted by Duo, it's easy to set up and manage. <https://duo.com/product/single-sign-on-ss0>
upvoted 11 times

west33637 Highly Voted 1 year, 8 months ago

Selected Answer: AC

A,C are the correct answers. The question is what are the reasons? In other words, why would you deploy DUO? for single sign on access to apps and for secure access to apps, whether onprem or cloud. I have never heard a CISO say we want to buy a DUO solution because it has many different authentication methods.
upvoted 6 times

Premium_Pils Most Recent 4 weeks ago

Selected Answer: AC

AC based on these articles: <https://www.cisco.com/c/en/us/products/security/duo/what-is-duo.html>
<https://www.cisco.com/c/en/us/products/security/what-is-two-factor-authentication.html#~related-solutions>
upvoted 1 times

XvidalX 6 months, 1 week ago

Selected Answer: CE

DUO support SSO, but not provide, SAML or AD provide SSO.
A is incorrect
upvoted 1 times

mikexian 8 months ago

Selected Answer: AC

A C focus on why we should choose Multifactor authentication
upvoted 1 times

Przemol 1 year ago

I go for C and E

Cisco Duo as MFA solution provides Duo Push, Call me and passcode:
<https://guide.duo.com/prompt#:~:text=Authenticate%20via%20phone%20callback.&text=Log%20in%20using%20a%20passcode,%2Dtouch%20hardware%2Dbacked%20authentication.>

Also provides secure access to on-premises and cloud applications.

I am not going for A, because SSO is one of the features Cisco Duo provides besides MFA. And in this question they ask for reasons for implementing a multifactor authentication solution such as Cisco Duo.

upvoted 2 times

gc999 1 year, 5 months ago

I don't think "C" is the reason.
upvoted 1 times

gc999 1 year, 5 months ago

Sorry for the typo. I wanted to say "E" is not a reason.
upvoted 1 times

  **stalkr3** 1 year, 5 months ago

There is a Cisco reason. This is also a marketing question
upvoted 1 times

  **Toni_Su91** 1 year, 5 months ago

<https://duo.com/product/multi-factor-authentication-mfa/authentication-methods>

I don't see voice call-backs in the guide. Is this the clue? :)
upvoted 1 times

  **achille5** 1 year, 6 months ago

Why i can't access this exam? I paid for 1 yr contributor access.
upvoted 2 times



  **jerac58653** 1 year, 6 months ago

Selected Answer: CE

C+E

Read Carefully, they are asking about the reason to implement MFA (DUO is just an example), not to implement DUO specifically. SSO is another separate feature that is not asked about here.

upvoted 5 times

  **zimmer54** 1 year, 7 months ago

CE

<https://duo.com/docs/ss0>

upvoted 1 times

  **Emlia1** 1 year, 9 months ago

Selected Answer: AE



finally I prefer A, E

upvoted 1 times

  **Emlia1** 1 year, 9 months ago


AE or CE

upvoted 1 times

  **4000000** 1 year, 10 months ago

I think, A, c and e seems to be all correct combinations..... Just to be smart enough to have the choices 😂😂

upvoted 1 times

  **sis_net_sec** 1 year, 11 months ago

Selected Answer: AE

Trust Every User With Single Sign-On and 2FA

Verify the identity of your users with two-factor authentication and give them easy access to work applications with single sign- on. Customized policies and controls on a per-application basis will secure your organization from risky users and devices.

upvoted 1 times

  **Jamesy** 2 years ago

A and E guys, I have looked everywhere.

Single sign on Access to On premises and cloud applications is a better option.

If we have to choose C, the answer should be "secure access to remote users not on-premises and cloud applications."

I hope this helps. Good luck.

upvoted 1 times

  **sis_net_sec** 2 years, 1 month ago

A and E

Trust Every User With Single Sign-On and 2FA

Verify the identity of your users with two-factor authentication and give them easy access to work applications with single sign- on. Customized policies and controls on a per-application basis will secure your organization from risky users and devices.

<https://duo.com/single-sign-on>

upvoted 1 times

What are the two most commonly used authentication factors in multifactor authentication? (Choose two.)

- A. biometric factor
- B. time factor
- C. confidentiality factor
- D. knowledge factor
- E. encryption factor

Correct Answer: AD

Community vote distribution

AD (57%)

BD (43%)

NikoNiko Highly Voted 2 years, 1 month ago

"Authentication credentials are called factors. There are three categories of factors:

- Knowledge (something the user knows)
--> authentication by knowledge would be a user providing a password, a personal identification number (PIN) code, or answering security questions.
- Possession (something a user has)
--> authentication by ownership or possession include the following: a one-time passcode, memory card, smartcard, and out-of-band communication.
The most common of the four is the one-time passcode sent to a device in the user's possession.
- Inherence (something the user is)"
--> authentication by characteristic authenticates the user based on some physical or behavioral characteristic, sometimes referred to as a biometric attribute. The most used physical or physiological characteristics are as follows:
 - Fingerprints
 - Face recognition
 - Retina and iris
 - Palm and hand geometry
 - Blood and vascular information
 - Voice recognition

CCNP / CCIE SCOR official cert guide by Omar Santos

upvoted 8 times

RemiK Most Recent 2 months, 4 weeks ago

Selected Answer: AD

agree with A & D

upvoted 1 times

SegaMasterSystemAdmin 1 year, 3 months ago

Selected Answer: AD

A and D are correct. B is not correct, time is not a factor in MFA

upvoted 1 times

bobie 1 year, 3 months ago

Selected Answer: AD

I'll go for biometric and knowledge factor :

Something you know - (Knowledge - password)

Something you have - (No choices)

Something you are - (Biometric - fingerprint scanning or facial recognition or voice biometry)

upvoted 1 times

stalkr3 1 year, 5 months ago

people please stop voting for answer A - how many times have you used 2FA that relies on biometric data?

upvoted 1 times

Jessie45785 1 year, 4 months ago

Daily, and not only biometric but live GPS position as well - time based tokens are so outdated

upvoted 1 times

SegaMasterSystemAdmin 1 year, 3 months ago

Go hit the books kiddo

upvoted 1 times

  **nep1019** 1 year, 1 month ago

Every. Single. Day.

upvoted 2 times

  **Jessie45785** 1 year, 5 months ago

Selected Answer: AD

B- is not a factor - we can have time based hashed function but it is not a factor - in this case it would be possession factor which is not listed

upvoted 1 times

  **stalkr3** 1 year, 5 months ago

it IS a factor, hence the inherent security of using OTPs that expire after a very short time. And it is used very frequently, so B should be correct

upvoted 2 times

  **Emlia1** 1 year, 9 months ago

Selected Answer: BD

BD - should be the correct answer

upvoted 1 times

  **Jessie45785** 1 year, 5 months ago

B- is not a factor - you can have time based hashed function but it is not a factor - in this case it would be possession factor listed not time

upvoted 1 times

  **NikoNiko** 2 years, 1 month ago

Currently: "Duo Push is our most commonly-used second factor of authentication, thanks to its simplicity and reliability. Users just download the Duo Mobile app and are automatically prompted to confirm each login attempt "

--> Questio: Push is knowledge-based or time-based or both? - I think both.

<https://duo.com/product/multi-factor-authentication-mfa/authentication-methods/tokens-and-passcodes>

2019 DUO: "Passcodes. Passcodes are the most common form of 2FA, and usually consist of a short string of numbers sent to a smartphone. Passcodes definitely count as 2FA. Since they rely on phone lines, however — which can be compromised — they represent the least secure method. Passcodes aren't a real hit with users, either: each code must be manually entered, which can be a nuisance"

<https://duo.com/blog/two-factor-authentication-the-basics>

upvoted 1 times

  **NikoNiko** 2 years, 1 month ago

UPDATE: Push / one-time passcode is POSSESSION BASED (something a user has), but also time-based according to Cisco DUO:

"

Time-Based One-Time Passcodes

Some websites and online services let users protect their accounts with a mobile-generated passcode that must be manually entered and only works for a certain amount of time — typically 30-60 seconds. Duo Mobile can generate these time-based one-time passcodes (TOTP) for all third-party sites, letting users keep all of their accounts in one app."

<https://duo.com/product/multi-factor-authentication-mfa/authentication-methods/tokens-and-passcodes>

upvoted 1 times

  **nomanlands** 2 years, 2 months ago

Selected Answer: BD

D is a given.

This page mentions Time-based is currently widely used while biometric is still up and coming.

<https://www.cisco.com/c/en/us/products/security/what-is-multi-factor-authentication.html#~methods>

upvoted 1 times

  **Thusi26** 2 years, 2 months ago

A, B and D all are good according to Cisco.

From Cisco Site:

Knowledge

Knowledge--usually a password--is the most commonly used tool in MFA solutions. However, despite their simplicity, passwords have become a security problem and slow down productivity.

Inherent

This category includes biometrics like fingerprint, face, and retina scans.

And.....

Location-based and time-based

Authentication systems can use GPS coordinates, network parameters, and metadata for the network in use, and device recognition for MFA. Adaptive authentication combines these data points with historical or contextual user data.

Cisco needs to get their stuff together...

upvoted 1 times

  **pohqinan** 2 years, 5 months ago

Reference: <https://www.cisco.com/c/en/us/products/security/what-is-multi-factor-authentication.html>
The two most popular authentication factors are knowledge and inherent (including biometrics like fingerprint, face, and retina scans. Biometrics is used commonly in mobile devices).

A and D is correct

upvoted 1 times

  **Sun2sun** 2 years, 7 months ago

Selected Answer: BD

Its B and D. time factor , knowledge factor

upvoted 1 times

  **lurker8000** 2 years, 8 months ago

I'd go with AD here, here's a reference where "Biometric Factor" is mentioned on a cisco documentation:
<https://www.cisco.com/c/en/us/products/security/what-is-multi-factor-authentication.html#~how-mfa-works>.

D is a no brainer in my mind, that's the most common, although not the most secure...

upvoted 4 times

  **coentror** 2 years, 9 months ago

There not much here. A and D are the correct one. Do no complicate what is easy.



:)

upvoted 1 times

  **coentror** 2 years, 9 months ago

Sorry B and D are correct.

upvoted 1 times

  **Moll** 2 years, 9 months ago

Agree with B and D

upvoted 1 times

  **jaciro11** 2 years, 10 months ago

Ey people stop discuss it

Its B and D.



<https://www.cisco.com/c/en/us/products/security/what-is-multi-factor-authentication.html>

upvoted 2 times

  **abdulmalik_mail** 2 years, 8 months ago

AD, on that URL writted, inherent... This category includes biometrics like fingerprint, face, and retina scans.

upvoted 1 times

  **eazy99** 2 years, 11 months ago

Something you are.

Something you know.

Correct, A and D.

upvoted 3 times

  **NullNull88** 2 years, 9 months ago

Uh em, .."something you "have" something you "know".

upvoted 2 times

An MDM provides which two advantages to an organization with regards to device management? (Choose two.)

- A. asset inventory management
- B. allowed application management
- C. AD group policy management
- D. network device management
- E. critical device management

Correct Answer: AB

—  **bigdadzzz** Highly Voted 3 years, 8 months ago

I'm going to chime in with A&B as correct answers.

I've administered Mobile Device Management systems for several years, and never managed a network device or critical device (ie server) with them. While I suppose it's technically POSSIBLE, it's just not the purpose of the solution. MDMs will use the term groups/policies/Group Policy, but it's never going to allow you to manage ADDS GPOs.

What I HAVE done though, is use it to remotely manage a fleet of mobile devices and add/remove/monitor those assets, and control the applications on the device.

upvoted 25 times

—  **j0ej0e** Highly Voted 3 years, 9 months ago

A an B are correct.

upvoted 12 times

—  **sull3y** Most Recent 1 year, 7 months ago

A. Asset inventory management: A Mobile Device Management (MDM) solution provides an organization with the ability to maintain an inventory of all the mobile devices that are being used within the organization. This includes tracking information such as device type, operating system, serial number, and other relevant details. This information helps organizations to manage their mobile device fleet effectively, keep track of devices and ensure they are properly configured and secure.

B. Allowed application management: An MDM solution also enables organizations to control and manage the applications that are installed on the mobile devices being used within the organization. This includes the ability to allow or disallow specific applications, manage updates and upgrades, and enforce security policies around application usage. This helps organizations to maintain a secure and controlled environment for mobile devices and ensure that only approved applications are being used within the network.

upvoted 6 times

—  **Moll** 2 years, 9 months ago

Agree with A and B

upvoted 1 times

—  **thegreek1** 3 years, 10 months ago

I would not call a mobile phone to be a 'critical device management'

https://en.wikipedia.org/wiki/Mobile_device_management

Some of the core functions of MDM include:

Ensuring that diverse user equipment is configured to a consistent standard / supported set of applications, functions, or corporate policies

Updating equipment, applications, functions, or policies in a scalable manner

Ensuring that users use applications in a consistent and supportable manner

Ensuring that equipment performs consistently

Monitoring and tracking equipment (e.g. location, status, ownership, activity)


Being able to efficiently diagnose and troubleshoot equipment remotely

upvoted 3 times

—  **Smilebloke** 2 years, 5 months ago

Completely agree with A/B, however, have you dealt with a sales bod / A/B/C level exec whos mobile isn't working - Their world has come to an end.....

upvoted 1 times

—  **FilipNel** 3 years, 11 months ago

The answer is B, E

upvoted 2 times

 **naddaf** 4 years, 1 month ago

i think the correct Answer is B & E

upvoted 2 times

What is the purpose of the My Devices Portal in a Cisco ISE environment?

- A. to register new laptops and mobile devices
- B. to manage and deploy antivirus definitions and patches on systems owned by the end user
- C. to provision userless and agentless systems
- D. to request a newly provisioned mobile device

Correct Answer: A

Community vote distribution

A (67%)

C (33%)

karmaomar Highly Voted 3 years, 3 months ago

A is a correct answer
My Devices Portal

Q. Why do I need to use the My Devices Portal?

A. Depending on your company policy, you might be able to use your mobile phones, tablets, printers, Internet radios, and other network devices on your company's network. You can use the My Devices portal to register and manage these devices on your company's network. When you use a laptop computer, mobile phone, or tablet to access the Internet, you typically use a web browser on the device itself.

upvoted 18 times

sull3y Most Recent 1 year, 7 months ago

A. to register new laptops and mobile devices.

The My Devices Portal in a Cisco ISE environment is a self-service portal that allows end users to register and manage their personal devices, such as laptops and mobile devices, within the ISE network. This portal enables users to enroll their devices, update device information, and manage device settings, such as certificates and Wi-Fi profiles. This can help streamline the process of onboarding new devices and improve the overall security posture of the network by ensuring that all devices are properly registered and managed.

upvoted 3 times

Emlia1 1 year, 9 months ago

Selected Answer: A

Employees can use MDP to register and manage their personal devices.
upvoted 2 times

Webster21 1 year, 9 months ago

Selected Answer: C

Depending on your company policy, you might be able to use your mobile phones, tablets, printers, Internet radios, and other network devices on your company's network. You can use the My Devices portal to register and manage these devices on your company's network.

When you use a laptop computer, mobile phone, or tablet to access the Internet, you typically use a web browser on the device itself. The first time you try to do so using your company's network, the system will automatically guide you through registering and installing the required software. You may not need to use the My Devices Portal to register those types of devices. However, once you register them, you can use the My Devices Portal to perform operations such as remove them, mark them as lost, or reinstate devices that were marked as lost, once they are found.

Other network devices do not have web browsers on them because they need access to the network only to allow you to perform activities such as listen to music, print documents, and watch videos. If you want to add these types of devices to your company's network, you need to use the My Devices portal.

upvoted 1 times

beeker98106 2 years, 10 months ago

It should be C.

The FAQ section explains the use of the portal for radios or other funny devices that don't have users or even browsers
https://www.cisco.com/c/en/us/td/docs/security/ise/2-4/mydevices/b_mydevices_2x.html

upvoted 3 times

PeterHasse 1 year, 2 months ago

KEY WORD is register not provision
upvoted 1 times

Darealis 3 years, 3 months ago

Answer is D
upvoted 1 times

Seawanderer 3 years, 2 months ago

So when I need a new phone, I can go to My Devices Portal and get a new one? :-)

upvoted 7 times

  **NikoNiko** 2 years, 1 month ago

I wish so :D Good one! :D

upvoted 3 times

Question #253

Topic 1

Which Cisco platform ensures that machines that connect to organizational networks have the recommended antivirus definitions and patches to help prevent an organizational malware outbreak?

- A. Cisco Prime Infrastructure
- B. Cisco ESA
- C. Cisco WiSM
- D. Cisco ISE

Correct Answer: D

Community vote distribution



  **Felice44** 1 year, 5 months ago

Selected Answer: D

Posture Assessment with ISE

upvoted 1 times

In which two ways does Easy Connect help control network access when used with Cisco TrustSec? (Choose two.)

- A. It integrates with third-party products to provide better visibility throughout the network.
- B. It allows for the assignment of Security Group Tags and does not require 802.1x to be configured on the switch or the endpoint.
- C. It creates a dashboard in Cisco ISE that provides full visibility of all connected endpoints.
- D. It allows for managed endpoints that authenticate to AD to be mapped to Security Groups (PassiveID).
- E. It allows multiple security products to share information and work together to enhance security posture in the network.

Correct Answer: BD

Reference:

<https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/trustsec/trustsec-with-easy-connect-configuration-guide.pdf>

Community vote distribution

AD (80%)

BD (20%)

Sarbi Highly Voted 3 years ago

Easy Connect simplifies network access control and segmentation by allowing the assignment of Security Group Tags to endpoints without requiring 802.1X on those endpoints, whether using wired or wireless connectivity.

Active Directory logins are used to map user information onto network connections, which are then used for authorizing users on the network even when the Identity Services Engine (ISE) is not involved in the authentication process. Consequently, this authorization method only supports devices that authenticate with a Domain Controller. Easy Connect can also be used as a backup authentication method to 802.1X, to ensure that managed assets are classified even when an 802.1X supplicant is not correctly configured. This can dramatically reduce help desk calls

upvoted 10 times

Rododendron2 Most Recent 4 months ago

Selected Answer: AD

switch needs to have dot1x setup, end point does not

upvoted 2 times

Rododendron2 2 months, 3 weeks ago

After I again reviewed documentation, BD is right, Easyconnect does not required dot1x on switch and integrates with TrustSec on ISE as Passive ID

upvoted 1 times

iluvmicrosoft 5 months, 2 weeks ago

<https://community.cisco.com/t5/security-knowledge-base/ise-easy-connect/ta-p/3638861>
MAB or 802.1X (required for ISE to stitch RADIUS session with PassiveID info)

You can configure NAD w MAB, so technically 802.1x is not a requirement??

upvoted 2 times

XvidalX 6 months, 1 week ago

Selected Answer: AD

A CORRECT - EASYconenct integrate with AD to gaing visibility
B- incorrect - SWITCHES NEED 802.1x configuration , Endpoints DOES not
C- Does not create dashboards
D - its correct - it is the main purpose
E - incorrect - it is not about posture needs

upvoted 2 times

haiderzaid 1 year, 5 months ago

why not B C
since PassiveID can be used independently without easy connect feature??

upvoted 1 times

haiderzaid 1 year, 5 months ago

im wrong C does not describe the way in which Easy Connect helps control network access

so I will go for BD

upvoted 1 times

sull3y 1 year, 7 months ago

B. It allows for the assignment of Security Group Tags and does not require 802.1x to be configured on the switch or the endpoint.

D. It allows for managed endpoints that authenticate to AD to be mapped to Security Groups (PassiveID).

Easy Connect helps control network access by allowing for the assignment of Security Group Tags (SGTs) and mapping managed endpoints that authenticate to AD to Security Groups (PassiveID). This enables organizations to enforce granular access policies based on the endpoint's identity and role, rather than just its IP address or MAC address. The use of SGTs and PassiveID helps simplify the deployment of TrustSec and reduces the complexity of network access control, as it does not require the configuration of 802.1x on the switch or endpoint.

upvoted 4 times

  **Emlia1** 1 year, 8 months ago

Selected Answer: BD

I prefer B, D

Easy Connect simplifies network access control and segmentation by allowing the assignment of Security Group Tags to endpoints without requiring 802.1X on those endpoints, whether using wired or wireless connectivity.

Reference: [https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/trustsec/trustsecwith-easy-connect-configuration-guide.p](https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/trustsec/trustsecwith-easy-connect-configuration-guide.pdf)

upvoted 1 times

  **Jamesy** 1 year, 11 months ago

D & E in my opinion. Cheers

upvoted 1 times

What does Cisco AMP for Endpoints use to help an organization detect different families of malware?

- A. Tetra Engine to detect malware when the endpoint is connected to the cloud
- B. ClamAV Engine to perform email scanning
- C. Spero Engine with machine learning to perform dynamic analysis
- D. Ethos Engine to perform fuzzy fingerprinting

Correct Answer: D

Reference:

<https://www.ciscolive.com/c/dam/r/ciscolive/emea/docs/2016/pdf/BRKSEC-2139.pdf>

Community vote distribution

D (100%)

Ampersand Highly Voted 3 years, 3 months ago

It should be Ethos

Spero: A machine-learning based technology that proactively identifies threats that were previously unknown.
Uses active heuristics to gather execution attributes
Needs good data in large sets to tune
Built to identify new malware

Ethos: A generic signature capability, again ostensibly similar to the generic detection capabilities that some vendors provide.
Directed at families of malware
Can have more false-positives than 1-to-1 signatures
upvoted 20 times

wfexco 3 years, 3 months ago

agreed - Ethos is a generic signature capability that provides a way to help with the reality that one-to-one signatures are easily evaded. With Ethos, you can detect families of malware.
upvoted 6 times

NikoNiko Most Recent 2 years, 2 months ago

"detect different families of malware" = ETHOS
See line diagram at page 109 in this PDF (page 120 according to page numbers) - it depicts sequence of AMP operations and their functions:
<https://www.ciscolive.com/c/dam/r/ciscolive/emea/docs/2020/pdf/R6BGArNQ/TECSEC-2599.pdf>
upvoted 1 times

Sparrsh 2 years, 5 months ago

Answer is D

ETHOS is the Cisco file grouping engine. It allows us to group families of files together so if we see variants of a malware, we mark the ETHOS hash as malicious and whole families of malware are instantly detected.
upvoted 1 times

iceman24ccs 2 years, 7 months ago

Selected Answer: D

ETHOS and SPERO are both considered generic engines. Because of this, the user has the ability to control how false positive-prone an ETHOS or SPERO hash is.
ETHOS is the Cisco file grouping engine. It allows us to group families of files together so if we see variants of a malware, we mark the ETHOS hash as malicious and whole families of malware are instantly detected
SPERO is the Cisco machine-based learning system. We use hundreds of features of a file, which we call a SPERO fingerprint. This is sent to the cloud and SPERO trees determine whether a file is malicious.
upvoted 2 times

idto 2 years, 9 months ago

Selected Answer: D

"ETHOS is the Cisco file grouping engine. It allows us to group families of files together so if we see variants of a malware, we mark the ETHOS hash as malicious and whole families of malware are instantly detected."

Source: <https://docs.amp.cisco.com/en/SecureEndpoint/Secure%20Endpoint%20User%20Guide.pdf>
upvoted 2 times

  **jaciro11** 2 years, 9 months ago

Selected Answer: D

The correct answer is D

<http://www.download.safeplus.pl/Prezentacje/Cisco%20Live%20San%20Diego%202015/BRKSEC-2139.pdf>


upvoted 1 times

  **jaciro11** 2 years, 10 months ago

The correct answer is D

<http://www.download.safeplus.pl/Prezentacje/Cisco%20Live%20San%20Diego%202015/BRKSEC-2139.pdf>

upvoted 3 times



  **Moll** 2 years, 10 months ago

Dynamic analysis is a sandboxing technique.

Answer should be D

https://www.cisco.com/web/KR/events/CiscoConnect/2014/downloads/Day2_Track5-1.pdf

upvoted 1 times

  **Stardec** 2 years, 10 months ago

C is correct.

https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Reference_a_wrapper_Chapter_topic_here.html#ID-2199-000005d8

upvoted 1 times

What is a benefit of conducting device compliance checks?

- A. It validates if anti-virus software is installed.
- B. It scans endpoints to determine if malicious activity is taking place.
- C. It indicates what type of operating system is connecting to the network.
- D. It detects email phishing attacks.

Correct Answer: A

Community vote distribution

A (100%)

klu16 Highly Voted 3 years ago

A of course.

upvoted 16 times

jccastiyo Highly Voted 2 years, 9 months ago

Selected Answer: A

Based on https://www.cisco.com/c/en/us/td/docs/security/ise/3-0/admin_guide/b_ISE_admin_3_0/b_ISE_admin_30_compliance.html?bookSearch=true#id_17065

It helps AnyConnect agent to support newer additions. Once the AnyConnect agents retrieve this support information, they check the latest definition information from the periodically updated se-checks.xml file (which is published along with the se-rules.xml file in the se-templates.tar.gz archive), and determine whether clients are compliant with the posture policies. Depending upon what is supported by the library for a particular antivirus, antispymware, antimalware, disk encryption, or patch management product, the appropriate requirements will be sent to the AnyConnect agents for validating their existence, and the status of the particular products on the clients during posture validation.

upvoted 6 times

djsonicdh Most Recent 2 years, 4 months ago

Are two types of compliance, with posture (ise) or compliance for organization Security agreements

upvoted 1 times

jaciro11 2 years, 9 months ago

Selected Answer: A

Its A.

The compliance check what thing is missing in the endpoint and if something is missing this not will permit the access to the network.

Answer A its the only one answer possible here, no tricky answers

upvoted 4 times

Moll 2 years, 9 months ago

I vote for A as well

upvoted 2 times

eazy99 2 years, 11 months ago

I will go with B.

When you do the compliance checks on device, you will know if you had any malicious activity in the device, you are doing deep inspections, you are not doing a checklist of what software the device has.

upvoted 2 times

Dinges 3 years, 2 months ago

My bad, I didnt read B answer right. It talks about endpoints, but the DNA compliance check is for network devices, while ISe compliance check is for endpoints. ISE does not check for malicious activities, it checks for posture compliance: A is correct.

upvoted 3 times

Dinges 3 years, 2 months ago

A for compliance check on ISE (posture of one device - end devices), B for compliance check of all devices on the network (DNA - network devices) I hope the exam will be more clear about this.

upvoted 3 times

itisfakemallo 3 years, 2 months ago

It is A. It validates if anti-virus software is installed.



upvoted 3 times

statikd 3 years, 2 months ago

B seems like the write answer to me.

https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/2-1-2/user_guide/b_cisco_dna_center_ug_2_1_2/m-compliance-audit-for-network-devices.html

upvoted 2 times

  **eddy12345** 2 years, 11 months ago

GREAT LINK. The problem is the question says "Compliance Check" - DNA center does compliance checks, ISE does Profiling and Posture - not "Compliance Checks" Now here is the RUB. None of the answers are correct for "DNA Center Compliance Checks" All the answers seem to be written for ISE, in which case Answer A is the best answer. Its just a bad question in general.

upvoted 1 times

  **itisfakemaiol** 3 years, 3 months ago

I think the correct answer is A

upvoted 3 times

Question #257

Topic 1



A network administrator is configuring a switch to use Cisco ISE for 802.1X. An endpoint is failing authentication and is unable to access the network. Where should the administrator begin troubleshooting to verify the authentication details?

- A. Context Visibility
- B. Accounting Reports
- C. Adaptive Network Control Policy List
- D. RADIUS Live Logs

Correct Answer: D

Community vote distribution

D (100%)

  **gc999** 1 year, 3 months ago

Selected Answer: D

<https://community.cisco.com/t5/security-knowledge-base/how-to-troubleshoot-ise-failed-authentications-amp/ta-p/3630960#toc-hld-720407544:~:text=troubleshoot%20authentication%20failures.-,RADIUS%20Live%20Logs,-The%20RADIUS%20Live>

upvoted 2 times

  **Zatingke** 1 year, 7 months ago

Sounds correct to me

upvoted 1 times

What is the role of an endpoint in protecting a user from a phishing attack?

- A. Ensure that antivirus and antimalware software is up-to-date.
- B. Use machine learning models to help identify anomalies and determine expected sending behavior.
- C. Use Cisco Stealthwatch and Cisco ISE Integration.
- D. Utilize 802.1X network security to ensure unauthorized access to resources.

Correct Answer: A

Community vote distribution

B (67%) A (33%)

Premium_Pils 4 weeks ago

Selected Answer: A

Endpoint protection and machine learning would be AMP, but I can't find any corresponding information about phishing protection on endpoints and AMP. So the only answer left is A.

upvoted 1 times

Rododendron2 3 months, 1 week ago

Selected Answer: A

If question really is like this - about endpoint, then A

upvoted 1 times

Ko13 10 months, 1 week ago

Ok so, the Secure Endpoint Datasheet does speak about machine learning but it seems to be for malware only.

<https://www.cisco.com/c/en/us/products/collateral/security/fireamp-endpoints/datasheet-c78-733181.html>

At no point it speaks about phishing, so it seems the only option would be A...

upvoted 2 times

jku2cya 1 year, 2 months ago

Selected Answer: B

Not sure between A and B, but leaning toward B. A is signatures based.

upvoted 1 times

zamkljo 1 year, 3 months ago

Selected Answer: A

Machine Learning & Endpoint??? would be correct for Machine Learning & ESA.

upvoted 2 times

SegaMasterSystemAdmin 1 year, 3 months ago

Antivirus and antimalware software does not protect from phishing attacks

upvoted 1 times

itsklk 1 year, 4 months ago

Selected Answer: B

Machine Learning :)

upvoted 1 times

tanri04 1 year, 8 months ago

my answer: B

upvoted 1 times

Emlia1 1 year, 9 months ago

Selected Answer: B

It should be B

upvoted 1 times

kjubo 1 year, 10 months ago

Selected Answer: B

I agree with B

upvoted 1 times

FortiSherlock 2 years, 1 month ago

Selected Answer: B

I agree with B, it is the only thing that makes sense. Machine Learning can be used to detect patterns of Phishing Mails, while Anti-Virus tools will not prevent this. How can an anti-virus tool stop you from inserting your credentials into a malicious website for example ? Machine learning tools could detect this by checking URLs and detect something like am4zon.com.

upvoted 4 times

  **djsonicdh** 2 years, 4 months ago

The Q Say the rol of the endpoint, but the answers don't Match with the Question

upvoted 1 times

  **semi1750** 2 years, 5 months ago

Picked A.

The question is asking EPP, not EDR

<https://www.cisco.com/c/en/us/products/security/what-is-endpoint-protection-platform.html#~how-an-epp-works>

upvoted 4 times

  **stalkr3** 1 year, 5 months ago

How do you if it is asking EPP?

upvoted 1 times

  **coentror** 2 years, 9 months ago

It is B:



Cisco Advanced Phishing Protection provides unprecedented insight into the email coming in to your organization, flowing out of your organization, and within your organization. Powered by Cisco Identity Intelligence – Cisco's unique machine learning techniques based on historical email traffic to your organization – Advanced Phishing Protection models the unique behavior of all legitimate email senders and allows you to quickly distinguish good messages from potentially bad messages. Coupled with Identity Intelligence, Cisco's platform of data – built from analyzing billions of email messages worldwide – provides you a risk overview of all messages in your organization and senders who send email into your organization.

upvoted 4 times

  **dr4gn00t** 2 years, 7 months ago



Q was about endpoints, not ESA

upvoted 6 times

  **Moll** 2 years, 9 months ago

I'd go with B here

upvoted 1 times

  **Moll** 2 years, 9 months ago

Sorry about that, I'll go for A instead since I belive B belongs to Cisco Secure Email Phishing Defense:

<https://www.cisco.com/c/dam/en/us/products/collateral/security/cloud-email-security/at-a-glance-c45-740894.pdf>

The only remianing valid option would be A

upvoted 3 times

  **jccastiyo** 2 years, 9 months ago

The answer is right but the question looks wrong. Should be "the role of AMP for Endpoints" and not "the role of an endpoint". Endpoints do not have any role in protecting the user. Admins, appliances and the user himself do.

upvoted 3 times

  **MUKD** 3 years ago

answer is A

upvoted 2 times

  **Sarbi** 3 years ago

Should be A

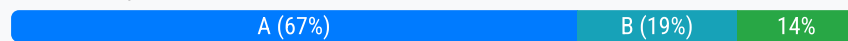
upvoted 1 times

Why is it important to implement MFA inside of an organization?

- A. To prevent brute force attacks from being successful.
- B. To prevent phishing attacks from being successful.
- C. To prevent DoS attacks from being successful.
- D. To prevent man-in-the-middle attacks from being successful.

Correct Answer: A

Community vote distribution



cesar1106 Highly Voted 3 years, 2 months ago

Its A, A brute force or a man-in-the-middle attack also happen inside an organization
upvoted 14 times

Premium_Pils Most Recent 4 weeks ago

Selected Answer: A

<https://blogs.cisco.com/security/akira-ransomware-targeting-vpns-without-multi-factor-authentication>
upvoted 1 times

Rododendron2 4 months ago

Cisco WTF, this is crazy
But what types of cyberattacks does MFA protect against?

Phishing
Spear phishing
Keyloggers
Credential stuffing
Brute force and reverse brute force attacks
Man-in-the-middle (MITM) attacks
You can pick the one you like forever
upvoted 2 times

cyberwhizzy0 1 year, 2 months ago

I strongly believe that MFA should not be the primary tool to stop brute force attack. This should be handled by a perimeter device
upvoted 1 times

ums008 1 year, 2 months ago

Selected Answer: D

The question is focused on attacks from INSIDE the organisation, I believe D Man In Middle attacks is the more relevant answer

While implementing Multi-Factor Authentication (MFA) offers several security benefits, the primary reason for its implementation is to prevent man-in-the-middle (MitM) attacks. A MitM attack occurs when an attacker intercepts the communication between two parties and can potentially eavesdrop, modify, or manipulate the information exchanged.

By implementing MFA, organizations add an extra layer of security to the authentication process. MFA requires users to provide multiple factors of authentication, typically something they know (such as a password), something they have (such as a physical token or mobile device), or something they are (such as a fingerprint or biometric scan). This significantly reduces the risk of an attacker successfully impersonating a legitimate user and carrying out a MitM attack.

upvoted 3 times

Premium_Pils 4 weeks ago

I agree
upvoted 1 times

BoxX 1 year, 2 months ago

Selected Answer: B

Vote for B

Multifactor authentication (MFA) is a useful security feature, providing an additional security barrier that can slow down hackers, who use techniques, such as social engineering, phishing attacks, and other tactics to steal data and identities.



upvoted 1 times

gc999 1 year, 3 months ago

Selected Answer: B

<https://duo.com/solutions/phishing-prevention>

upvoted 1 times

  **Jamesy** 1 year, 11 months ago

B in my opinion. To prevent Phishing attacks from being successful. Cheers

upvoted 1 times

  **nomanlands** 2 years, 2 months ago

Selected Answer: A

A is the most correct, it could also help with B and D

upvoted 2 times

  **getafix** 2 years, 3 months ago

Selected Answer: A

Brute force attacks target getting user credentials by sending authentication requests overwhelmingly. If no password failure policies are implemented this can result in credential theft. MFA is used to protect user credentials following the principle of what you have (MFA token) complemented by what you know (password). Brute force attack cannot be successful if MFA is enabled

upvoted 2 times

  **semi1750** 2 years, 5 months ago

Selected Answer: A

It looks A.

<https://www.cisco.com/c/en/us/solutions/collateral/enterprise/design-zone-security/breach-defense-design-guide.html>

Cisco Breach Defense Design Guide

Multi-Factor Authentication (MFA) and Posture Assessment

Integrating MFA (M1032) as part of *organizational policy can greatly reduce the risk of an adversary gaining control of valid credentials that may be used for additional tactics such as initial access, lateral movement, and collecting information. MFA can also be used to restrict access to cloud resources and APIs. If a password is hacked, guessed, or even phished, that's no longer enough to give an intruder access. Without approval at the second factor, a password alone is useless. Secure Access by Duo provides modern, effective MFA that helps eliminate the problem of *brute force attacks (T1110)

upvoted 4 times

  **SanchezEldorado** 2 years, 5 months ago

The answer is A. Most of the people voting for B are assuming that the only purpose of Phishing is to harvest credentials. The definition of Phishing includes things like giving up personal information. This could be credit cards, SSN, or wire transfers. MFA has nothing to do with that.


From the official cert guide page 33 under the Credential Brute Force Attacks and Password Cracking section: "The strength of user and application credentials has a direct effect on the success of brute-force attacks. Weak credentials are one of the major causes of credential compromise. The more complex and the longer a password (credential), the better. An even better approach is to use multifactor authentication (MFA). The use of MFA significantly reduces the probability of success for these types of attacks."

upvoted 3 times

  **SegaMasterSystemAdmin** 2 years, 7 months ago

Its B. MFA is the best solution against phishing attacks. In order to prevent brute force attacks you have to have password policies in place like timed lock outs. If someone knows your password because of a successful phishing attack, they will be able to use this password unless you have some sort of MFA.

upvoted 3 times

  **Cock** 2 years, 8 months ago

Selected Answer: A

I prefer A

upvoted 3 times

  **jaciro11** 2 years, 9 months ago

Selected Answer: B

Its B in the documents of cisco all the time its motioned this about phishing

upvoted 2 times

  **coentror** 2 years, 9 months ago

From Cisco page:

Benefits of multi-factor authentication

Improved trust

The costs of hacking and phishing attacks can be high. Because MFA helps secure systems against unauthorized users--and their associated threats--the organization is more secure overall.



B is the correct one

upvoted 2 times

  **pohqinan** 2 years, 5 months ago

Answer is A, Cisco Page state that MFA = High Cost of Hacking and phishing but it did not state preventable, if blackhat want break in willing to pay the cost it is hackable or phishing.

upvoted 1 times

  **Moll** 2 years, 9 months ago

Among all the attack types in the question, only Phishing attacks are supposed to have the highest probability of reaching/happening "inside" an organization

I'll go with B here

upvoted 3 times

  **cyberwhizzy0** 1 year, 2 months ago

My exact thought

upvoted 1 times

Which posture assessment requirement provides options to the client for remediation within a certain timeframe?

- A. audit
- B. mandatory
- C. visibility
- D. optional

Correct Answer: B

Reference:

https://www.cisco.com/c/en/us/td/docs/security/ise/2-2/admin_guide/b_ise_admin_guide_22/b_ise_admin_guide_22_chapter_010111.html

Community vote distribution

B (71%)

D (29%)

rishard 1 year, 1 month ago

B is the correct answer.
Mandatory Requirements

During policy evaluation, the agent provides remediation options to clients who fail to meet the mandatory requirements defined in the posture policy. End users must remediate to meet the requirements within the time specified in the remediation timer settings.

https://www.cisco.com/c/en/us/td/docs/security/ise/2-2/admin_guide/b_ise_admin_guide_22/b_ise_admin_guide_22_chapter_010111.html#ID873
upvoted 2 times

cyberwhizzy0 1 year, 2 months ago

Selected Answer: B

Mandatory Requirements

During policy evaluation, the agent provides remediation options to clients who fail to meet the mandatory requirements defined in the posture policy. End users must remediate to meet the requirements within the time specified in the remediation timer settings.

https://www.cisco.com/c/en/us/td/docs/security/ise/2-2/admin_guide/b_ise_admin_guide_22/b_ise_admin_guide_22_chapter_010111.html
upvoted 2 times

cyberwhizzy0 1 year, 2 months ago

B is the correct answer
upvoted 2 times

kakabk 1 year, 2 months ago

Selected Answer: B

Mandatory Requirements

During policy evaluation, the agent provides remediation options to clients who fail to meet the mandatory requirements defined in the posture policy. End users must remediate to meet the requirements within the time specified in the remediation timer settings.

Optional Requirements

During policy evaluation, the agent provides an option to clients to continue, when they fail to meet the optional requirements specified in the posture policy. End users are allowed to skip the specified optional requirements.

upvoted 4 times

ffaiz 1 year, 2 months ago

Selected Answer: B

The question is specifically asking "remediation within a certain timeframe?"
And as per the mentioned Link

https://www.cisco.com/c/en/us/td/docs/security/ise/2-2/admin_guide/b_ise_admin_guide_22/b_ise_admin_guide_22_chapter_010111.html#ID155:~:text=Policy%20Requirement%20Types-,Mandatory%20Requirements,-During%20policy%20evaluation

It is clearly stating:

"During policy evaluation, the agent provides remediation options to clients who fail to meet the mandatory requirements defined in the posture policy. End users must remediate to meet the requirements within the time specified in the remediation timer settings."

upvoted 3 times

gc999 1 year, 3 months ago

Selected Answer: D

The question asks which posture assessment requirement provides "options" to the client. It is an option, that is even fail to meet, the user is still allowed to pass.

https://www.cisco.com/c/en/us/td/docs/security/ise/2-2/admin_guide/b_ise_admin_guide_22/b_ise_admin_guide_22_chapter_010111.html#ID155:~:text=Non%2DCompliant%20state,-,Optional%20Requirements,-During%20policy%20evaluation

upvoted 1 times

  **GoldFree** 1 year, 3 months ago

Selected Answer: B

Should be B

upvoted 1 times

  **GCalvo** 1 year, 4 months ago

Selected Answer: D

D. optional

In the context of posture assessment, an optional requirement allows clients to remediate any issues within a certain timeframe. This approach provides more flexibility for clients to resolve non-compliant states, ensuring that they have the opportunity to meet the necessary security standards without being immediately restricted from accessing the network.

upvoted 2 times

  **theodosis** 1 year, 6 months ago



Selected Answer: D

Optional Requirements

During policy evaluation, the agent provides an option to clients to continue, when they fail to meet the optional requirements specified in the posture policy. End users are allowed to skip the specified optional requirements.

When this requirement is used in a posture policy, endpoints that fail the assessment are presented with remediation options and given a specified timeframe to complete the necessary actions. If the remediation is completed within the specified timeframe, the endpoint is marked as compliant. If the endpoint fails to complete the remediation or the timeframe expires, the endpoint is marked as noncompliant.

upvoted 2 times

  **getafix** 2 years, 3 months ago

Selected Answer: B

Mandatory policies enforce the posture check and if the posture check fails notify the user about the remediation time set in the remediation timer. Once the remediation timer is up, the user is denied access to the environment if he hasn't fulfilled the compliance checks


upvoted 2 times

  **abdulmalik_mail** 2 years, 7 months ago

correct, It's B

Reference :https://www.cisco.com/c/en/us/td/docs/security/ise/1-4/admin_guide/b_ise_admin_guide_14/b_ise_admin_guide_14_chapter_010111.html#ID492

upvoted 2 times

  **Moll** 2 years, 9 months ago

Mandatory Requirements

During policy evaluation, the agent provides remediation options to clients who fail to meet the mandatory requirements defined in the posture policy. End users must remediate to meet the requirements within the time specified in the remediation timer settings.

upvoted 4 times

An organization configures Cisco Umbrella to be used for its DNS services. The organization must be able to block traffic based on the subnet that the endpoint is on, but sees only the requests from its public IP addresses instead of each internal IP address. What must be done to resolve this issue?

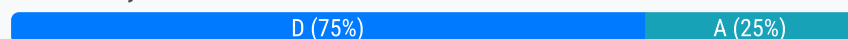
- A. Install the Microsoft Active Directory Connector to give IP address information stitched to the requests in the Cisco Umbrella dashboard.
- B. Use the tenant control features to identify each subnet being used and track the connections within the Cisco Umbrella dashboard.
- C. Configure an internal domain within Cisco Umbrella to help identify each address and create policy from the domains.
- D. Set up a Cisco Umbrella virtual appliance to internally field the requests and see the traffic of each IP address.

Correct Answer: D

Reference:

<https://docs.umbrella.com/deployment-umbrella/docs/internal-networks-setup-guide>

Community vote distribution



angry Highly Voted 1 year, 6 months ago

Cisco is horrible in creating exam questions!
upvoted 12 times

Minion2021 Highly Voted 2 years, 6 months ago

The Answer is D
upvoted 6 times

Smilebloke 2 years, 5 months ago

<https://docs.umbrella.com/deployment-umbrella/docs/internal-networks-setup-guide>
upvoted 1 times

fdl543 Most Recent 1 year, 1 month ago

Selected Answer: D

D. Question says "based on the subnet that the endpoint is on". Nothing about Active Directory. Not all networks use AD...
upvoted 1 times

DWizard 1 year, 2 months ago

Selected Answer: D

The answer seems to be D, according to the link already provided:
<https://docs.umbrella.com/deployment-umbrella/docs/internal-networks-setup-guide>

The following link shows that the MS AD connector is intended to be used for a different purpose:
<https://docs.umbrella.com/umbrella-user-guide/docs/introduction-4>
upvoted 2 times

mmpaing 1 year, 3 months ago

Selected Answer: A

The correct answer is A. Install the Microsoft Active Directory Connector to give IP address information stitched to the requests in the Cisco Umbrella dashboard.

Cisco Umbrella uses the public IP address of the device to identify it. If the organization wants to block traffic based on the subnet that the endpoint is on, it needs to provide Cisco Umbrella with the internal IP address information. This can be done by installing the Microsoft Active Directory Connector (AD Connector) and configuring it to synchronize the organization's Active Directory with Cisco Umbrella.

The AD Connector will synchronize the organization's Active Directory with Cisco Umbrella, which will allow Cisco Umbrella to see the internal IP address of the device. This will allow the organization to block traffic based on the subnet that the endpoint is on.
upvoted 1 times

sull3y 1 year, 7 months ago

D. Set up a Cisco Umbrella virtual appliance to internally field the requests and see the traffic of each IP address.

When using Cisco Umbrella for DNS services, it can be challenging to track traffic based on subnets because the public IP addresses of the endpoint are seen instead of the internal IP addresses. To resolve this issue, an organization can set up a Cisco Umbrella virtual appliance to internally field the requests and see the traffic of each IP address. This will allow the organization to track traffic based on the subnet that the endpoint is on and implement policies to block traffic as needed. The virtual appliance acts as a proxy that fields the requests, enabling visibility into the internal IP addresses and allowing the organization to see the full picture of its network traffic.
upvoted 5 times

[-]  **NikoNiko** 2 years, 2 months ago

"How Umbrella Virtual Appliances Work

VAs act as conditional DNS forwarders in your network, intelligently forwarding public DNS queries to Cisco Umbrella's global network, and local DNS queries to your existing local DNS servers and forwarders. Every public DNS query sent to Umbrella is encrypted, authenticated, and includes the client's internal IP address." <-- CLIENT'S INTERNAL IP ADDRESS.

"VAs record the internal IP address of every DNS request. Security and DNS traffic-related investigations allow you to associate traffic to an individual, internal IP address."

See picture here: <https://docs.umbrella.com/deployment-umbrella/docs/1-introduction>

upvoted 2 times


[-]  **SanchezEldorado** 2 years, 5 months ago

Two links below show that it is NOT C and it IS D. C is for cloud to on prem, where the virtual appliance allows you to bypass NAT which is the crux of the question.

<https://docs.umbrella.com/deployment-umbrella/docs/internal-networks-setup-guide>

<https://docs.umbrella.com/deployment-umbrella/docs/appx-d-internal-domains>

upvoted 3 times

[-]  **Cock** 2 years, 8 months ago

c,c is the answer

upvoted 1 times

Question #262

Topic 1

An engineer adds a custom detection policy to a Cisco AMP deployment and encounters issues with the configuration. The simple detection mechanism is configured, but the dashboard indicates that the hash is not 64 characters and is non-zero. What is the issue?

- A. The hash being uploaded is part of a set in an incorrect format.
- B. The engineer is attempting to upload a file instead of a hash.
- C. The file being uploaded is incompatible with simple detections and must use advanced detections.
- D. The engineer is attempting to upload a hash created using MD5 instead of SHA-256.

Correct Answer: D

[-]  **Minion2021** Highly Voted 2 years, 6 months ago


The answer is D. Correct

upvoted 6 times

[-]  **LTLnetworker** Most Recent 7 months, 3 weeks ago

SHA-256 hash is 32 bytes (64 characters).

upvoted 2 times

[-]  **sull3y** 1 year, 7 months ago

D. The engineer is attempting to upload a hash created using MD5 instead of SHA-256.

When adding a custom detection policy to a Cisco AMP deployment, the hash being uploaded must be in the correct format. If the dashboard indicates that the hash is not 64 characters and is non-zero, it likely means that the engineer is attempting to upload a hash created using MD5 instead of SHA-256. Cisco AMP requires the use of SHA-256 hashes for custom detection policies, as this provides a higher level of security compared to other hash algorithms. If the engineer is attempting to upload a hash created using MD5, the configuration will not be accepted and the dashboard will indicate that the hash is not in the correct format.

upvoted 4 times

[-]  **Jamesy** 1 year, 11 months ago

Hi guys, the correct answer is A in my opinion. Cheers

upvoted 1 times

[-]  **Jamesy** 1 year, 11 months ago

Apology I think D is correct.

upvoted 3 times

What is the benefit of integrating Cisco ISE with a MDM solution?

- A. It provides compliance checks for access to the network.
- B. It provides the ability to update other applications on the mobile device.
- C. It provides the ability to add applications to the mobile device through Cisco ISE.
- D. It provides network device administration access.

Correct Answer: A

Community vote distribution

A (100%)

jaciro11 Highly Voted 2 years, 9 months ago

Selected Answer: A

ITS A !!

https://www.cisco.com/c/en/us/td/docs/security/ise/2-4/admin_guide/b_ISE_admin_guide_24/m_ise_interoperability_mdm.html

upvoted 10 times

idto 2 years, 9 months ago

Agreed. This is from the page you shared...

"Cisco ISE queries the MDM servers for the necessary device attributes to create ACLs that provide network access control for those devices."

upvoted 1 times

idto 2 years, 9 months ago

And in the section (Configuring ACLs on the Wireless LAN Controller for Mobile Device Management Interoperability)...

Step 3

Allow access to the MDM server for unregistered and noncompliant devices to download the MDM agent and proceed with compliance checks.

Step 4

Allow all inbound traffic from the client to the server to Cisco ISE for the web portal and supplicant, and certificate provisioning flows.

upvoted 2 times

Cokamaniako Most Recent 1 year, 2 months ago

Selected Answer: A

Aswer A

Cisco ISE queries a connected MDM server for information about various attributes that you can use to create network authorization policies.

upvoted 1 times

sull3y 1 year, 7 months ago

A. It provides compliance checks for access to the network.

The benefit of integrating Cisco ISE with a Mobile Device Management (MDM) solution is that it provides compliance checks for access to the network. This integration allows for the enforcement of security policies for mobile devices accessing the network. The MDM solution provides information about the device, such as its operating system version, security patch level, and any other security-related information. Cisco ISE can then use this information to determine if the device meets the organization's security policies, and either grant or deny access to the network based on the results of this compliance check. This integration helps to ensure that only compliant and secure devices are allowed access to the network, enhancing the overall security posture of the organization.

upvoted 4 times

getafix 2 years, 3 months ago

Selected Answer: A

MDM helps is deploying company policy on BYOD mobile devices/tablets. The ISE when integrated with MDM will ensure that the mobile devices are compliant as per the company policy and ISE will permit/block based on the response received from the MDM

upvoted 2 times

coentror 2 years, 9 months ago

Guys it is D.

A is not correct because MDM should not give access to the network when the devices are non compliant.

This is only possible because of the option D:

<https://cdw-prod.adobecqms.net/content/dam/cdw/on-domain-cdw/brands/cisco/ise-solution-overview.pdf>



"4.Network admin access control. ISE is the only NAC solution that includes TACACS+ for role-based administrative access control to networking equipment"

upvoted 2 times

  **coentror** 2 years, 9 months ago

NVM it is A for sure give access to network for compliant devices.

upvoted 2 times

  **Moll** 2 years, 9 months ago

Will go with A here

upvoted 2 times

  **jccastiyo** 2 years, 9 months ago

Selected Answer: A

Based on <https://community.cisco.com/t5/security-documents/cisco-ise-integration-with-mobile-device-management-mdm/ta-p/3784691>

upvoted 2 times

  **jaciro11** 2 years, 10 months ago

ITS A !!

https://www.cisco.com/c/en/us/td/docs/security/ise/2-4/admin_guide/b_ISE_admin_guide_24/m_ise_interoperability_mdm.html

upvoted 4 times

  **zeroC00L** 3 years ago

this should be a because if you implement MDM integration wiht ISE you can check in the Policy if the Mobile device is compliated from MDM perspective and either allow or deny access based on the answer the MDM is delivering to ISE back

upvoted 3 times

  **birdman6709** 3 years ago

<https://community.cisco.com/t5/security-documents/cisco-ise-integration-with-mobile-device-management-mdm/ta-p/3784691>

The following are the high level use cases in this solution.

Device registration- Non registered endpoints accessing the network on-premises will be redirected to registration page on MDM server for registration based on user role, device type, etc

Remediation- Non compliant endpoints will be given restricted access based on compliance state

Periodic compliance check – Periodically check with MDM server for compliance

Ability for ISE administrators to issue remote actions on the device through the MDM server (e.g.: remote wiping of the managed device)

Ability for end user to leverage the ISE My Devices Portal to manage personal devices, e.g. Full Wipe, Corporate Wipe and PIN Lock.

upvoted 1 times

  **Sarbi** 3 years ago

It should be A

upvoted 3 times

  **Max95** 3 years ago

it should be A?

upvoted 4 times

Which feature is leveraged by advanced antimalware capabilities to be an effective endpoint protection platform?

- A. blocklisting
- B. storm centers
- C. big data
- D. sandboxing

Correct Answer: D

Community vote distribution

D (100%)

  **Felice44** 1 year, 5 months ago

Selected Answer: D

An effective endpoint protection platform needs to leverage advanced anti-malware capabilities such as:

- Machine learning: Machine learning capabilities allow an EPP to leverage large-scale data to determine the true malicious nature of files.
- Threat intelligence: Expansive threat intelligence allows an EPP to leverage both historical and real-time data from billions of threats to automatically block known attacks.
- Sandboxing: Sandboxing allows an EPP to isolate suspect files in a safe environment. Within this environment, the EPP can safely detonate and monitor the nature of the files without risking detriment to the rest of the system.

Even with all these capabilities, no endpoint protection platform can guarantee 100 percent efficacy. That is why a traditional antivirus solution cannot provide sufficient endpoint security. A true next-generation endpoint security solution combines endpoint protection platform capabilities with EDR capabilities.

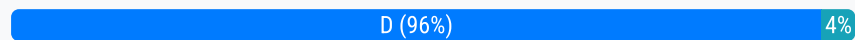
upvoted 4 times

A Cisco AMP for Endpoints administrator configures a custom detection policy to add specific MD5 signatures. The configuration is created in the simple detection policy section, but it does not work. What is the reason for this failure?

- A. The administrator must upload the file instead of the hash for Cisco AMP to use.
- B. The APK must be uploaded for the application that the detection is intended.
- C. The MD5 hash uploaded to the simple detection policy is in the incorrect format.
- D. Detections for MD5 signatures must be configured in the advanced custom detection policies.

Correct Answer: A

Community vote distribution



nomanlands Highly Voted 2 years, 2 months ago

Selected Answer: D

D, simple can only do SHA256
upvoted 7 times

ross123 1 year, 8 months ago

Incorrect. See <https://docs.amp.cisco.com/en/SecureEndpoint/Secure%20Endpoint%20User%20Guide.pdf>, page 36. MD5 IS supported.
upvoted 1 times

jerac58653 1 year, 5 months ago

On page 36 it says is is supported but on advanced, NOT on simple custom detections.
upvoted 4 times

F0rtyx40 Most Recent 1 year, 1 month ago

Selected Answer: D

Options under Advanced Detection policy

Some of the Signature types available are:

- MD5 Signatures
- MD5, PE section based Signatures
- File Body-based Signatures
- Extended Signature Format (offsets, wildcards, regular expressions)
- Logical Signatures
- Icon Signatures

upvoted 2 times

ums008 1 year, 2 months ago

Selected Answer: D

I believe D is correct:

In Cisco AMP for Endpoints, MD5 signatures for detections must be configured in the advanced custom detection policies rather than the simple detection policy section. The simple detection policy section is designed for basic detection rules and does not support the use of MD5 signatures.

To add specific MD5 signatures for detections, the administrator needs to create or modify an advanced custom detection policy. In the advanced custom detection policy, there are options to define specific detection criteria, including MD5 signatures, to identify and classify threats.

Option A, uploading the file instead of the hash, is not the reason for the failure. MD5 signatures are typically used to identify files based on their unique hash values rather than uploading the entire file.

upvoted 2 times

mmpaing 1 year, 3 months ago

Selected Answer: D

The correct answer is D. Detections for MD5 signatures must be configured in the advanced custom detection policies.

Cisco AMP for Endpoints does not support MD5 signatures in simple detection policies. Only SHA-256 hashes are supported in simple detection policies. If an administrator tries to add an MD5 signature to a simple detection policy, the configuration will not work.

To add an MD5 signature to a custom detection policy, the administrator must create an advanced custom detection policy. In the advanced custom detection policy, the administrator can specify the MD5 signature of the file that they want to block.

upvoted 2 times

Jessie45785 1 year, 5 months ago

Selected Answer: A

you cannot enable md5:

from:

<https://docs.amp.cisco.com/en/SecureEndpoint/Secure%20Endpoint%20User%20Guide.pdf>

You can enter a file's SHA-256 value to find any devices that observed the file.

!!!You can also drag a file to the Search box!!!

and its SHA-256 value will be computed for you. If you only have a file's MD5 or SHA-1 value, Search will attempt to match it to a corresponding SHA-256, then search for that SHA-256.

upvoted 1 times

jerac58653 1 year, 5 months ago

Selected Answer: D

D <https://docs.amp.cisco.com/en/SecureEndpoint/Secure%20Endpoint%20User%20Guide.pdf>

upvoted 1 times

achille5 1 year, 6 months ago

Selected Answer: D

Option B is not relevant to this scenario. Option A is also not correct, as uploading the file itself is not required for MD5-based detections. Option C is incorrect because MD5 hashes are a specific format that should be recognized by the Cisco AMP for Endpoints platform, so this would not be the reason for the failure of the custom detection policy.

upvoted 1 times

eryxcs 1 year, 7 months ago

D is Correct. Absolutely

upvoted 1 times

Emlia1 1 year, 9 months ago

Selected Answer: D

D should be the correct one.

upvoted 1 times

SulSulEi 1 year, 9 months ago

Selected Answer: D

Check the comment by Webster21

upvoted 2 times

Webster21 1 year, 9 months ago

Selected Answer: D

Advanced Custom Detections are like traditional antivirus signatures, but they are written by the user. These signatures can inspect various aspects of a file and have different signature formats. Some of the available signature formats are:

- MD5 signatures
- MD5, PE section-based signatures
- File body-based signatures
- Extended signature format (offsets, wildcards, regular expressions)
- Logical signatures
- Icon signatures

upvoted 3 times

Jamesy 1 year, 11 months ago

C in my opinion. Cheers

upvoted 1 times

SulSulEi 1 year, 9 months ago

I read all of your comments on all questions, and I would advise anyone to ignore any answer given by you. Cheers

PS, correct answer is D

upvoted 8 times

Moe1416 1 year, 9 months ago

Totally agree!

upvoted 2 times

CCNP21 1 year, 7 months ago

Lol boom roasted.

upvoted 2 times

surforlife 2 years, 1 month ago

no Workaround. MD5 is not supported. Pls comment to Cisco on your test. There is no relevant workaround, must use SHA-256.

upvoted 2 times

  **ileri_sec** 2 years, 4 months ago

Selected Answer: D

It is D.

upvoted 3 times

  **Smilebloke** 2 years, 4 months ago

Advanced custom list

<https://docs.amp.cisco.com/en/SecureEndpoint/Secure%20Endpoint%20User%20Guide.pdf>

and for Lolz - <https://quickview.cloudapps.cisco.com/quickview/bug/CSCvg75304>

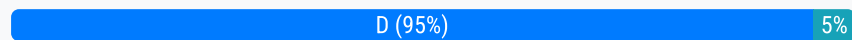
upvoted 3 times

An administrator is adding a new Cisco ISE node to an existing deployment. What must be done to ensure that the addition of the node will be successful when inputting the FQDN?

- A. Change the IP address of the new Cisco ISE node to the same network as the others.
- B. Make the new Cisco ISE node a secondary PAN before registering it with the primary.
- C. Open port 8905 on the firewall between the Cisco ISE nodes.
- D. Add the DNS entry for the new Cisco ISE node into the DNS server.

Correct Answer: A

Community vote distribution



Smilebloke Highly Voted 2 years, 4 months ago

D
FQDN in DNS is a pre-req, NTP is a good call as well.
upvoted 12 times

Fugashi 2 years, 3 months ago

https://www.cisco.com/c/en/us/td/docs/security/ise/2-7/admin_guide/b_ise_27_admin_guide/b_ise_admin_27_deployment.html
Enter the DNS-resolvable fully qualified domain name (FQDN) of the standalone node that you are going to register (in the format hostname.domain-name, for example, abc.xyz.com). The FQDN of the primary PAN and the node being registered must be resolvable from each other.
upvoted 3 times

Korndal Most Recent 2 months, 1 week ago

Selected Answer: D

D is the Answer. A couldnt be more wrong. Many companies have ISE appliances on seperate segments. DNS is a 10000000% requirement, sine the PAN node cannot add the new ISE node if it cannot resolve it based on its hostname!
upvoted 2 times

Ijoakob 11 months, 4 weeks ago

Response B. Is correct
upvoted 1 times

nep1019 1 year, 1 month ago

Selected Answer: D

The nature of an FQDN is that it resolves the name to the IP and DNS is 100% a requirement of this.
https://en.wikipedia.org/wiki/Fully_qualified_domain_name
upvoted 2 times

F0rtyx40 1 year, 1 month ago

Selected Answer: D

These answers are getting annoying...

It's D, they can be on different networks.
upvoted 2 times

ums008 1 year, 2 months ago

Selected Answer: D

I believe Answer is D:

When adding a new Cisco ISE node to an existing deployment and inputting the Fully Qualified Domain Name (FQDN) of the new node, it is essential to ensure that the DNS entry for the new node is added into the DNS server. This allows the other nodes in the deployment to resolve and communicate with the new node using its FQDN.

Option A, changing the IP address of the new Cisco ISE node to the same network as the others, is not necessary for ensuring the successful addition of the node. It is generally recommended to have the new node on the same network as the existing nodes, but it is not directly related to the inputting of the FQDN.

upvoted 2 times

mmpaing 1 year, 3 months ago


Selected Answer: D

The correct answer is D. Add the DNS entry for the new Cisco ISE node into the DNS server.

When adding a new Cisco ISE node to an existing deployment, the administrator must ensure that the new node can be resolved by the DNS

server. This can be done by adding a DNS entry for the new node into the DNS server. The DNS entry should include the FQDN of the new node and its IP address.

upvoted 1 times

  **Jessie45785** 1 year, 5 months ago

Selected Answer: D

Ensure that the primary PAN and the node being registered are DNS resolvable to each other. If the node that is being registered uses an untrusted self-signed certificate, you are prompted with a certificate warning along with details of the certificate. If you accept the certificate, it is added to the trusted certificate store of the primary PAN to enable TLS communication with the node.

upvoted 2 times

  **Jessie45785** 1 year, 5 months ago

Selected Answer: A

you cannot enable md5:

from:


<https://docs.amp.cisco.com/en/SecureEndpoint/Secure%20Endpoint%20User%20Guide.pdf>

You can enter a file's SHA-256 value to find any devices that observed the file.

!!!You can also drag a file to the Search box!!!



and its SHA-256 value will be computed for you. If you only have a file's MD5 or SHA-1 value, Search will attempt to match it to a corresponding SHA-256, then search for that SHA-256.

upvoted 1 times

  **Jessie45785** 1 year, 5 months ago

I have commented wrong question - PLEASE DO NOT APPROVE

upvoted 1 times

  **sull3y** 1 year, 7 months ago

D. Add the DNS entry for the new Cisco ISE node into the DNS server. The Fully Qualified Domain Name (FQDN) is used to resolve the hostname of a device to its IP address. When adding a new Cisco ISE node, it is important to ensure that the FQDN of the node can be resolved to its IP address through the DNS server. This can be accomplished by adding a DNS entry for the new node into the DNS server, so that the FQDN can be resolved to the IP address of the new node. This is a crucial step in ensuring that the addition of the new node to the existing deployment will be successful.

upvoted 3 times

  **bmayer** 1 year, 7 months ago

Selected Answer: D

100% D . I work with ISE and Join many to the cluster. If DNS is not correct the node fails to join.

upvoted 4 times

  **Webster21** 1 year, 9 months ago

Selected Answer: D

It's D

upvoted 1 times

  **sis_net_sec** 1 year, 10 months ago

Selected Answer: D

Enter the DNS-resolvable fully qualified domain name (FQDN) of the standalone node that you are going to register (in the format hostname.domain-name, for example, abc.xyz.com). The FQDN of the primary PAN and the node being registered must be resolvable from each other.

https://www.cisco.com/c/en/us/td/docs/security/ise/2-7/admin_guide/b_ise_27_admin_guide/b_ise_admin_27_deployment.html

upvoted 1 times

  **getafix** 2 years, 3 months ago

Selected Answer: D

To add a new ISE node to an existing deployment it asks for the FQDN of the new node not the IP address. As long as the firewall rules (if any firewall is installed in the environment) permit comms between the existing deployment and the new node, the FQDN is sufficient. NTP servers ensure that the nodes are in sync

The answer is D

upvoted 4 times

Which portion of the network do EPP solutions solely focus on and EDR solutions do not?

- A. East-West gateways
- B. server farm
- C. core
- D. perimeter

Correct Answer: D

Reference:

<https://www.cisco.com/c/en/us/products/security/endpoint-security/what-is-endpoint-detection-response-edr.html>

  **Smilebloke** Highly Voted  2 years, 4 months ago

EDR focuses primarily on detecting advanced threats, those designed to evade front-line defenses and have successfully entered the environment. An EPP focuses solely on prevention at the perimeter. It is difficult, if not impossible, for an EPP to block 100 percent of threats. A holistic endpoint security solution deploys both EPP and EDR capabilities.

upvoted 5 times


Which benefit does endpoint security provide the overall security posture of an organization?

- A. It streamlines the incident response process to automatically perform digital forensics on the endpoint.
- B. It allows the organization to mitigate web-based attacks as long as the user is active in the domain.
- C. It allows the organization to detect and respond to threats at the edge of the network.
- D. It allows the organization to detect and mitigate threats that the perimeter security devices do not detect.

Correct Answer: D

Community vote distribution

C (100%)



  **Hormore** Highly Voted  2 years, 11 months ago

D is very correct
upvoted 5 times

  **Korndal** Most Recent  2 months, 1 week ago

Selected Answer: C

Cannot be D, since its protects the parameter of the network
upvoted 1 times

  **NoUserName1234** 1 year, 9 months ago

IMHO is Endpoint protection on the perimeter of your network.
While interpreting the question:
What does EPP help you with in the overall sec of your network.
Answer C
upvoted 1 times

Which solution protects hybrid cloud deployment workloads with application visibility and segmentation?

- A. Nexus
- B. Stealthwatch
- C. Firepower
- D. Tetration

Correct Answer: D

Reference:

<https://www.cisco.com/c/en/us/solutions/security/secure-data-center-solution/index.html#~products>

Community vote distribution



7f37374 10 months, 3 weeks ago

Cisco Secure Workload (Tetration)
upvoted 1 times

Felice44 1 year, 5 months ago

Selected Answer: D

Cisco Secure Workload (formerly Tetration)
upvoted 2 times

An engineer needs a solution for TACACS+ authentication and authorization for device administration. The engineer also wants to enhance wired and wireless network security by requiring users and endpoints to use 802.1X, MAB, or WebAuth.

Which product meets all of these requirements?

- A. Cisco Prime Infrastructure
- B. Cisco Identity Services Engine
- C. Cisco Stealthwatch
- D. Cisco AMP for Endpoints

Correct Answer: B

Community vote distribution



cyberwhizzy0 1 year, 1 month ago

Selected Answer: B

<https://www.trustradius.com/reviews/cisco-identity-services-engine-ise-2023-06-07-13-01-16>
upvoted 1 times

How does Cisco Stealthwatch Cloud provide security for cloud environments?

- A. It delivers visibility and threat detection.
- B. It prevents exfiltration of sensitive data.
- C. It assigns Internet-based DNS protection for clients and servers.
- D. It facilitates secure connectivity between public and private networks.

Correct Answer: A

Reference:

<https://www.content.shi.com/SHIcom/ContentAttachmentImages/SharedResources/FBLP/Cisco/Cisco-091919-Simple-IT-Whitepaper.pdf>

Community vote distribution

A (100%)

  **ums008** 1 year, 2 months ago

Selected Answer: A

I believe A is correct:

Cisco Stealthwatch Cloud provides security for cloud environments by delivering visibility and threat detection capabilities. It enables organizations to gain insights into their cloud infrastructure, detect potential threats, and respond to security incidents.

Option B, preventing exfiltration of sensitive data, is not a specific capability of Cisco Stealthwatch Cloud. While it can help detect indicators of data exfiltration by monitoring network traffic, the prevention of data exfiltration typically involves a combination of security measures and data loss prevention (DLP) solutions.

upvoted 1 times

  **Jessie45785** 1 year, 3 months ago

Selected Answer: A

A & B are correct ... Typical Cisco question which puts your nerve on the edge:

<https://cisco.bravais.com/s/169ZRg2tWIOXb0uBjfWX>



Customer situation

A company or organization's most valuable assets include its intellectual property, confidential information, and information stored in its networks. Data breaches cost millions of dollars, and proper mitigation can prevent this and the loss of trust that can follow.

Solution:

The Cisco Stealthwatch® Exfiltration alarms track Inside Hosts and Outside Hosts to which an abnormal amount of data has been transferred. If a host triggers a number of these events and exceeds a configured threshold, it results in a Data Exfiltration alarm

upvoted 1 times

  **Jessie45785** 1 year, 3 months ago

<https://cisco.bravais.com/s/15jOM9fFMK78ei07JnYK>

Customer situation

As the attack landscape changes, network security becomes increasingly difficult. Cloud networks are growing in popularity, making it even more challenging for security teams to plan and execute security strategies. One of the key threats to network security is data exfiltration, which can be carried out manually by a user on the network, or by an automated process using a malicious program.

Solution:

Cisco Stealthwatch® has ways to detect data exfiltration attacks facing on-premise networks. For protection against data exfiltration in a cloud environment, Stealthwatch Cloud uses dynamic learning and entity modeling to provide similar detection. Stealthwatch Cloud monitors the cloud network and alerts on possible data exfiltration.

upvoted 1 times

Which Cisco security solution protects remote users against phishing attacks when they are not connected to the VPN?

- A. Cisco Umbrella
- B. Cisco Firepower NGIPS
- C. Cisco Stealthwatch
- D. Cisco Firepower

Correct Answer: A

Community vote distribution

A (100%)

- [-] **bazinga31** Highly Voted 3 years, 2 months ago
A - Cisco Umbrella <https://www.cisco.com/c/dam/en/us/products/collateral/security/firewalls/umbrella-roaming-package.pdf>
upvoted 26 times
- [-] **deathfrom** Highly Voted 3 years, 2 months ago
"A. Cisco Umbrella " ?
upvoted 8 times
- [-] **FortiSherlock** Most Recent 2 years, 1 month ago
Selected Answer: A
Obviously it is Umbrella.
upvoted 1 times
- [-] **surforlife** 2 years, 1 month ago
The solution
Cisco NGFW + Cisco Umbrella
Roaming
• Security when the VPN is off
• No action required from end users
• Protect against threats over any port
• For Windows and Mac OS X roaming laptops! Choose "Cisco Umbrella"
upvoted 1 times
- [-] **djsonicdh** 2 years, 4 months ago
Selected Answer: A
Umbrella
upvoted 4 times
- [-] **Kyle1776** 2 years, 6 months ago
Selected Answer: A
Cloud-delivered security service for Cisco's next-generation firewall
Umbrella Roaming protects employees when they are off the VPN by blocking malicious domain requests and IP responses as DNS queries are resolved. By enforcing security at the DNS-layer, connections are never established and files are never downloaded. Malware will not infect laptops and command & control (C2) callbacks or phishing will not exfiltrate data over any port. Plus, you gain real-time visibility of infected laptops with C2 activity.
<https://www.cisco.com/c/dam/en/us/products/collateral/security/firewalls/umbrella-roaming-package.pdf>
upvoted 4 times
- [-] **Pupu** 2 years, 6 months ago
Selected Answer: A
<https://www.cisco.com/c/dam/en/us/products/collateral/security/firewalls/umbrella-roaming-package.pdf>
upvoted 2 times
- [-] **Moll** 2 years, 9 months ago
Will go with A here
upvoted 2 times
- [-] **jccastiyo** 2 years, 9 months ago
Selected Answer: A
<https://www.cisco.com/c/dam/en/us/products/collateral/security/firewalls/umbrella-roaming-package.pdf>

upvoted 4 times

 **Sarbi** 3 years ago

Cisco Umbrella A

upvoted 4 times

Question #273

Topic 1

What must be used to share data between multiple security products?

- A. Cisco Platform Exchange Grid
- B. Cisco Rapid Threat Containment
- C. Cisco Stealthwatch Cloud
- D. Cisco Advanced Malware Protection

Correct Answer: A

 **Random000** 1 year, 11 months ago

PxGrid

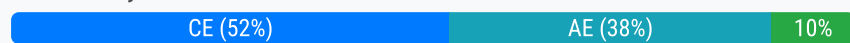
upvoted 1 times

Which two characteristics of messenger protocols make data exfiltration difficult to detect and prevent? (Choose two.)

- A. Messenger applications cannot be segmented with standard network controls
- B. Malware infects the messenger application on the user endpoint to send company data
- C. Traffic is encrypted, which prevents visibility on firewalls and IPS systems
- D. An exposed API for the messaging platform is used to send large amounts of data
- E. Outgoing traffic is allowed so users can communicate with outside organizations

Correct Answer: AE

Community vote distribution



itisfakemailol Highly Voted 3 years, 2 months ago

Vote for C and E
upvoted 15 times

Dinges Highly Voted 3 years, 2 months ago

I think AE is correct.
https://www.cisco.com/c/en_uk/products/security/network-visibility-segmentation/index.html
upvoted 14 times

Premium_Pils Most Recent 3 weeks, 6 days ago

Selected Answer: CE

C and E are preventing visibility. Encryption and allowed outgoing traffic for DNS protocols
upvoted 1 times

ums008 1 year, 2 months ago

Selected Answer: CE

I believe C & E are correct:

C. Traffic is encrypted: Messenger protocols often use encryption to secure the communication between users. While encryption provides privacy and security for legitimate users, it can also make it challenging for firewalls and intrusion prevention systems (IPS) to inspect and detect any potential data exfiltration. Encrypted traffic can bypass traditional security measures and make it difficult to identify if sensitive data is being transmitted.

A. Messenger applications cannot be segmented with standard network controls: This statement is not accurate. Messenger applications can be subject to network segmentation, firewall rules, and network access controls like any other application. However, the ability to segment them may vary based on the specific implementation and network architecture.
upvoted 1 times

jku2cya 1 year, 2 months ago

Selected Answer: AE

Not C as SSL Decryption can be done on NGFW/IPS
upvoted 1 times

Jessie45785 1 year, 5 months ago

Selected Answer: CE

A is incorrect - most of the modern communicators enforce SSL pinning - hence man in the middle approach is not an option cause traffic is encrypted

it leaves us only with C and E
https://docs.diladele.com/faq/squid/sslbump_exlusions/whatsapp.html
upvoted 4 times

Jessie45785 1 year, 5 months ago

Selected Answer: AE

C is incorrect - most of the modern communicators enforce SSL pinning - hence man in the middle approach is not an option

it leaves us only with A and E
https://docs.diladele.com/faq/squid/sslbump_exlusions/whatsapp.html
upvoted 3 times

Jessie45785 1 year, 5 months ago

I meant A is Incorrect - traffic is encrypted !!! - remove that vote

upvoted 2 times

  **Totosos1** 1 year, 5 months ago

Selected Answer: AE

It's weird how many people are suggesting 'C' for encrypted traffic when any security engineer knows a modern NGFWs have Decryption policies for such traffic, C is definitely not the right answer!

I'm going A & E.


upvoted 3 times

  **Tuxzinator** 1 year, 6 months ago

Selected Answer: AC

Messenger applications are often designed to bypass traditional network segmentation controls such as firewalls and proxies, making it difficult to detect and prevent data exfiltration

upvoted 1 times

  **Rododendron2** 2 months, 3 weeks ago

How you will magically bypass designed and setup traffic flow ? David Copperfield ? :-)



upvoted 1 times

  **achille5** 1 year, 6 months ago

Selected Answer: CE

Messenger protocols often use encryption to protect communication between endpoints, which makes it difficult for firewalls and IPS systems to detect and prevent data exfiltration. Additionally, since messenger applications are designed to allow outgoing traffic so users can communicate with outside organizations, it can be difficult to distinguish legitimate communications from unauthorized data exfiltration attempts.

upvoted 5 times

  **sull3y** 1 year, 7 months ago

The two characteristics of messenger protocols that make data exfiltration difficult to detect and prevent are:

C. Traffic encryption: Encrypting traffic makes it difficult for firewalls and IPS (Intrusion Prevention Systems) to inspect the content of the data. Encryption obscures the data being sent, making it more challenging to detect malicious activity.

E. Outgoing traffic allowed: Allowing outgoing traffic for legitimate communication purposes makes it difficult to detect and prevent malicious data exfiltration. This is because the data being exfiltrated can be disguised as normal communication traffic, making it harder for security systems to distinguish between benign and malicious activity.

upvoted 4 times

  **amtf8888** 1 year, 8 months ago

Selected Answer: AE

AE , answer is correct

upvoted 1 times

  **Emlia1** 1 year, 9 months ago

I think AE



upvoted 1 times

  **sis_net_sec** 1 year, 11 months ago

Selected Answer: AC



..encrypting traffic prevents intrusion detection systems and firewalls from inspecting the contents of the traffic (Fawcett, 2012).....there is a significant risk of data exfiltration via Skype traffic or more importantly, traffic that simply mimics the characteristics of Skype communication.....

upvoted 1 times

  **Pwned** 2 years, 3 months ago

vote for C and E... opcion B is not correct because a malware infection is not a "messenger protocol characteristic" as the question asked

upvoted 4 times

  **TWu2** 2 years, 7 months ago

Protocol is what the question is asking.

upvoted 1 times

  **flejd** 2 years, 8 months ago

B and E. Just look guys what can be decrypted in firepowers ssl policy... whatsapp, messenger etc

upvoted 1 times

Which solution combines Cisco IOS and IOS XE components to enable administrators to recognize applications, collect and send network metrics to Cisco Prime and other third-party management tools, and prioritize application traffic?

- A. Cisco Security Intelligence
- B. Cisco Application Visibility and Control
- C. Cisco Model Driven Telemetry
- D. Cisco DNA Center

Correct Answer: B

Community vote distribution

B (100%)

🗳️ **sull3y** 1 year, 7 months ago

B.

"Cisco Application Visibility and Control" on the Cisco website: <https://www.cisco.com/c/en/us/products/security/application-visibility-control/index.html>

upvoted 4 times

🗳️ **Anonymous983475** 1 year, 7 months ago

Selected Answer: B

AVC Is correct

<https://www.cisco.com/c/en/us/products/routers/avc-control.html>

Set up an application-aware network

Now you can detect every application in your network and optimize bandwidth with application-aware policies. Cisco AVC monitors application performance and troubleshoots issues that arise. It helps you deliver business-intent policies across the entire network. And it does all this without additional appliances in a simple and powerful way.

upvoted 3 times

🗳️ **NikoNiko** 2 years, 1 month ago

B - AVC is correct.

"he Cisco Prime Infrastructure management and reporting system is an integral part of the Cisco AVC solution and provides extensive management and reporting features, including provisioning the system, storing exported data, and generating reports.

...

Management and reporting systems, such as Cisco Prime Infrastructure or third-party tools, receive the network metrics data in Netflow v9 or IPFIX format, and provide a wide variety of system management and reporting functions. These functions include configuring metrics reporting, creating application and network performance reports, system provisioning, configuring alerts, and assisting in troubleshooting."

https://www.cisco.com/c/en/us/td/docs/ios/solutions_docs/avc/guide/avc-user-guide/avc_tech_overview.html

upvoted 2 times

🗳️ **NikoNiko** 2 years, 1 month ago

Model-Driven Telemetry looks ok too at first sight but it's NOT related to Prime (I haven't found a note about it) and it is probably also not supported by IOS but only IOS XE, XR, NX-OS (I haven't found anything about pure IOS).

"Model-driven telemetry is a new approach for network monitoring in which data is streamed from network devices continuously using a push model and provides near real-time access to operational statistics. Applications can subscribe to specific data items they need, by using standard-based YANG data models over NETCONF-YANG. Cisco IOS XE streaming telemetry allows to push data off of the device to an external collector at a much higher frequency, more efficiently, as well as data on-change streaming."

<https://blogs.cisco.com/developer/model-driven-telemetry-sandbox>

upvoted 1 times

What provides visibility and awareness into what is currently occurring on the network?

- A. CMX
- B. WMI
- C. Cisco Prime Infrastructure
- D. Telemetry

Correct Answer: D

Community vote distribution

D (100%)

Farman Highly Voted 4 years, 2 months ago

This is a tricky questions as there are multiple answers to it. CMX provides visibility and intelligence into wireless network. PI provides wired-wireless client visibility but PI is more for network device management and provides least amount of visibility as compared to CMX and Telemetry. If I had to pick one I would go with Telemetry. Network devices for example can push the telemetry data to a receiver and provides visibility. An example of this is Cisco Stealthwatch where the network devices sends telemetry data to Steathwatch receiver and stealthwacth can tell us from this data what IP are talking to each other, what ports are being used. How much data is being transferred etc.

upvoted 17 times

Vic25H Highly Voted 4 years, 3 months ago

I guess should be D

upvoted 17 times

jaciro11 Most Recent 2 years, 6 months ago

Selected Answer: D

Telemetry tells you what is going on in the network

upvoted 2 times

Minion2021 2 years, 6 months ago

Answer is Telemetry for sure

upvoted 1 times

Moll 2 years, 9 months ago

Will go with D here

upvoted 1 times

hisho72 3 years, 2 months ago

Correct Answer: Telemetry

Telemetry- Information and/or data that provides awareness and visibility into what is occurring on the network at any given time from networking devices, appliances, applications or servers in which the core function of the device is not to generate security alerts designed to detect unwanted or malicious activity from computer networks.

https://www.cisco.com/c/dam/en_us/about/doing_business/legal/service_descriptions/docs/activethreat-analytics-premier.pdf

upvoted 8 times

trickbot 3 years, 4 months ago

I am going with D because I've never heard of CMX, WMI can not be the answer because this isnt a test on Microsoft technologies, and Prime Infrastructure I only know of from test questions, and it's always the wrong answer.

upvoted 4 times

5tuple 3 years, 7 months ago

The correct answer is D: Telemetry

Per the documentation: "In order to operate and ensure availability of a network, it is critical to have visibility and awareness into what is occurring on the network at any one time. Network telemetry offers extensive and useful detection capabilities..."

https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Security/Baseline_Security/securebasebook/sec_chap5.html

upvoted 8 times

myccnptest 3 years, 9 months ago

<https://www.youtube.com/watch?v=QrdbHBcUBwU>

upvoted 2 times

gamertwo 4 years, 2 months ago

Yes It's D

Telemetry

upvoted 4 times



Question #277

Topic 1

How is ICMP used as an exfiltration technique?

- A. by flooding the destination host with unreachable packets
- B. by sending large numbers of ICMP packets with a targeted hosts source IP address using an IP broadcast address
- C. by encrypting the payload in an ICMP packet to carry out command and control tasks on a compromised host
- D. by overwhelming a targeted host with ICMP echo-request packets



Correct Answer: C

  **sull3y** 1 year, 4 months ago

Using ICMP packets to carry out command and control tasks on a compromised host is a common technique used in malware attacks. Malware can embed commands within the payload of ICMP packets, which are then sent to a command and control server controlled by the attacker. The server can then send responses back to the compromised host using ICMP packets, allowing the attacker to execute commands remotely without being detected.

C:To make it more difficult for security personnel to detect the malicious traffic, attackers can encrypt the payload of the ICMP packets using various encryption algorithms. This makes it harder for network security devices to detect and identify the malicious traffic as it passes through the network.

upvoted 2 times

  **sull3y** 1 year, 4 months ago

ANSWER IS C:Here are some reference links related to the use of ICMP in malware attacks:

"Using ICMP for Command and Control" - SANS Institute: <https://www.sans.org/reading-room/whitepapers/detection/icmp-command-control-34325>

"Malware Using ICMP Tunneling" - Palo Alto Networks: <https://unit42.paloaltonetworks.com/malware-using-icmp-tunneling/>

"Using ICMP to Build Covert Channels in Malware" - Trend Micro: https://www.trendmicro.com/en_us/research/11/d/using-icmp-to-build-covert-channels-in-malware.html

upvoted 3 times

  **luisseijuro** 1 year, 7 months ago

C is correct

<https://socfortress.medium.com/data-exfiltration-using-icmp-and-how-to-detect-it-69a799cca234>



upvoted 1 times

```
SwitchA (config)# interface gigabitethernet1/0/1
SwitchA (config-if)# dot1x host-mode multi-host
SwitchA (config-if)# dot1x timeout quiet-period 3
SwitchA (config-if)# dot1x timeout tx-period 15
SwitchA (config-if)# authentication port-control auto
SwitchA (config-if)# switchport mode access
SwitchA (config-if)# switchport access vlan 12
```

Refer to the exhibit. An engineer configured wired 802.1x on the network and is unable to get a laptop to authenticate. Which port configuration is missing?

- A. dot1x reauthentication
- B. cisp enable
- C. dot1x pae authenticator
- D. authentication open

Correct Answer: C

  **sull3y** 1 year, 7 months ago

The missing port configuration is C. dot1x pae authenticator.

In order to successfully configure wired 802.1x on a network, the port must be configured as a PAE (Port Access Entity) authenticator. This is accomplished using the "dot1x pae authenticator" command in the switch configuration. The PAE authenticator is responsible for managing the 802.1x authentication process, including sending and receiving EAP (Extensible Authentication Protocol) messages, and determining whether a device should be granted access to the network based on its authentication credentials. Without the "dot1x pae authenticator" configuration, the laptop will not be able to authenticate and gain access to the network.

upvoted 4 times

  **Kyle1776** 2 years, 6 months ago

How to Configure IEEE 802.1X Port-Based Authentication
Enabling IEEE 802.1X Authentication and Authorization
SUMMARY STEPS

1. enable
2. configure terminal
3. aaa new-model
4. aaa authentication dot1x {default | listname} method1 [method2...]
5. dot1x system-auth-control
6. identity profile default
7. interface type slot/port
8. access-session port-control {auto | force-authorized | force-unauthorized}
9. dot1x pae [supplicant | authenticator | both] ***Answer***
10. end
11. show dot1x

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_8021x/configuration/xo-3se/3850/sec-user-8021x-xo-3se-3850-book/config-ieee-802x-pba.html

upvoted 3 times

An engineer is configuring 802.1X authentication on Cisco switches in the network and is using CoA as a mechanism. Which port on the firewall must be opened to allow the CoA traffic to traverse the network?

- A. UDP 1700
- B. TCP 6514
- C. UDP 1812
- D. TCP 49

Correct Answer: A

Community vote distribution

A (100%)

surforlife Highly Voted 2 years, 1 month ago

Session for:

- RADIUS Authentication: UDP/1645, 1812
- RADIUS Accounting: UDP/1646, 1813
- RADIUS DTLS Authentication/Accounting: UDP/2083.
- RADIUS Change of Authorization (CoA) Send: UDP/1700
- RADIUS Change of Authorization (CoA) Listen/Relay: UDP/1700, 3799

For CoA is UDP 1700 "A" is correct.

upvoted 7 times

Alizade Most Recent 11 months, 2 weeks ago

Selected Answer: A

The answer is A. UDP 1700.

upvoted 1 times

What are two Detection and Analytics Engines of Cognitive Threat Analytics? (Choose two.)

- A. data exfiltration
- B. command and control communication
- C. intelligent proxy
- D. snort
- E. URL categorization

Correct Answer: AB

Reference:

<https://www.cisco.com/c/dam/en/us/products/collateral/security/cognitive-threat-analytics/at-a-glance-c45-736555.pdf>

  **Oz3006** Highly Voted 3 years, 11 months ago

A and B



<https://www.cisco.com/c/dam/en/us/products/collateral/security/cognitive-threat-analytics/at-a-glance-c45-736555.pdf>

upvoted 11 times

  **Premium_Pils** Most Recent 3 weeks, 6 days ago

I am a bit confused, The question is asking what are the two engines, and not which threats is this capable to detect. I did not find any relevant information about engines though.

upvoted 1 times

  **sull3y** 1 year, 4 months ago

AB:Cognitive Threat Analytics (CTA) is a security solution provided by Cisco that uses machine learning to detect and analyze advanced security threats. CTA uses several detection and analytics engines to identify security threats, including data exfiltration and command and control communication. REFERENCE:<https://www.cisco.com/c/en/us/products/security/cognitive-threat-analytics/index.html>

upvoted 2 times

  **davezz** 1 year, 6 months ago

This must be a very old question.

<https://community.cisco.com/t5/security-knowledge-base/cognitive-intelligence-formerly-cognitive-threat-analytics-or/ta-p/3651030#:~:text=Formerly%20known%20as%20Cognitive%20Threat,for%20Endpoints%2C%20and%20Threat%20Grid.>

And this was published on Oct 26th 2017: "Formerly known as Cognitive Threat Analytics (CTA), Cognitive Intelligence has evolved from a point product to an embedded feature of several Cisco Security products, including Stealthwatch, AMP for Endpoints, and Threat Grid."

And this was published on Feb 1st 2021: "Cognitive Intelligence changing its name to global threat alerts"

<https://community.cisco.com/t5/security-blogs/cognitive-release-note-january-2021-cognitive-intelligence/ba-p/4283808>

upvoted 1 times

  **sis_net_sec** 2 years, 1 month ago

Data exfiltration:- Cognitive Threat Analytics uses statistical modeling of an organization's network to identify anomalous web traffic and pinpoint the exfiltration of sensitive data. It recognizes data exfiltration even in HTTPS-encoded traffic, without any need for you to decrypt transferred content.

Command-and-control

(C2) communication:-

Cognitive Threat Analytics combines a wide range of data, ranging from statistics collected on an Internet-wide level to host-specific local anomaly scores. Combining these indicators inside the statistical detection algorithms allows us to distinguish C2 communication from benign traffic and from other malicious activities. Cognitive Threat Analytics recognizes C2 even in HTTPS-encoded or anonymous traffic, including Tor, without any need to decrypt

So the correct answer is AB

upvoted 3 times

Which Cisco product is open, scalable, and built on IETF standards to allow multiple security products from Cisco and other vendors to share data and interoperate with each other?

- A. Platform Exchange Grid
- B. Multifactor Platform Integration
- C. Firepower Threat Defense
- D. Advanced Malware Protection

Correct Answer: A

Reference:

<https://www.cisco.com/c/en/us/products/security/pxgrid.html>

Which compliance status is shown when a configured posture policy requirement is not met?

- A. authorized
- B. compliant
- C. unknown
- D. noncompliant

Correct Answer: D

  **fabio3wz** Highly Voted 3 years ago

Why are some people talking about unknown? It is clearly noncompliant! It is saying that the device fails to meet the requirements, so it has already been scanned and deemed non compliant.

upvoted 13 times

  **Amedeou** Highly Voted 3 years ago

Unknown Profile

If no matching posture policy is defined for an endpoint, then the posture compliance status of the endpoint may be set to unknown. A posture compliance status of unknown can also apply to an endpoint where a matching posture policy is enabled but posture assessment has not yet occurred for that endpoint and, therefore no compliance report has been provided by the client agent.

Noncompliant Profile

The posture compliance status of an endpoint is set to noncompliant when a matching posture policy is defined for that endpoint but it fails to meet all the mandatory requirements during posture assessment. An endpoint that is postured noncompliant matches a posture requirement with a remediation action, and it should be granted limited network access to remediation resources in order to remediate itself.

upvoted 10 times

  **XBfoundX** Most Recent 9 months, 1 week ago

When a client fails to be a compliant status the status is updated to noncompliant so answer is D:



Client System Stuck in Noncompliant State

If a client machine is unable to remediate a mandatory requirement, the posture status changes to "noncompliant" and the agent session is quarantined. To get the client machine past this "noncompliant" state, you need to restart the posture session so that the agent starts posture assessment on the client machine again.

OR

With an initial posture check, any endpoint that fails to satisfy all mandatory requirements is deemed non-compliant.

upvoted 1 times

  **XBfoundX** 9 months, 1 week ago

https://www.cisco.com/c/en/us/td/docs/security/ise/2-2/admin_guide/b_ise_admin_guide_22/b_ise_admin_guide_22_chapter_010111.html#ID898

https://www.cisco.com/c/en/us/td/docs/security/vpn_client/anyconnect/Cisco-Secure-Client-5/admin/guide/b-cisco-secure-client-admin-guide-5-0/configure-posture.html#:~:text=With%20an%20initial%20posture%20check,requirements%20is%20deemed%20non%2Dcompliant.

upvoted 1 times

  **cyberwhizzy0** 1 year, 2 months ago

D

If a client machine is unable to remediate a mandatory requirement, the session posture status changes to "non-compliant" and the agent session is quarantined. The only way to get the client machine past this "non-compliant" state is by initiating a new RADIUS or posture session where the agent starts posture assessment on the client machine again.

https://www.cisco.com/en/US/docs/security/ise/1.0/user_guide/ise10_pos_pol.html

upvoted 1 times

  **Thusi26** 2 years, 2 months ago

D

Cause

Unknown Profile



If no matching posture policy is defined for an endpoint, then the posture compliance status of the endpoint may be set to unknown. A posture compliance status of unknown can also apply to an endpoint where a matching posture policy is enabled but posture assessment has not yet occurred for that endpoint and, therefore no compliance report has been provided by the client agent.

upvoted 2 times

  **Moll** 2 years, 9 months ago



Agree with D

upvoted 3 times

  **kvirk** 2 years, 12 months ago

D is correct

upvoted 7 times

  **Sarbi** 3 years ago

It is unknown only

upvoted 1 times

  **SegaMasterSystemAdmin** 1 year, 4 months ago

no its not

upvoted 1 times

  **AbdiAden** 3 years, 1 month ago

Should be unknown.

upvoted 1 times

  **SegaMasterSystemAdmin** 1 year, 4 months ago

no its not

upvoted 1 times