



Actual exam question from Cisco's 350-701

Question #: 1

Topic #: 1

[\[All 350-701 Questions\]](#)

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

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 2

Topic #: 1

[\[All 350-701 Questions\]](#)

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

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 3

Topic #: 1

[\[All 350-701 Questions\]](#)

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

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 4

Topic #: 1

[\[All 350-701 Questions\]](#)

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

Show Suggested Answer



Actual exam question from Cisco's 350-701

Question #: 5

Topic #: 1

[\[All 350-701 Questions\]](#)

```
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

Show Suggested Answer



Actual exam question from Cisco's 350-701

Question #: 6

Topic #: 1

[\[All 350-701 Questions\]](#)

Which form of attack is launched using botnets?

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

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 7

Topic #: 1

[\[All 350-701 Questions\]](#)

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

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 8

Topic #: 1

[\[All 350-701 Questions\]](#)

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

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 9

Topic #: 1

[\[All 350-701 Questions\]](#)

What is the difference between deceptive phishing and spear phishing?

- A. Deceptive phishing is an attacked 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.

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 10

Topic #: 1

[\[All 350-701 Questions\]](#)

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.

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 11

Topic #: 1

[\[All 350-701 Questions\]](#)

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 antispyware software.
- E. Implement email filtering techniques.

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 12

Topic #: 1

[\[All 350-701 Questions\]](#)

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

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

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 13

Topic #: 1

[\[All 350-701 Questions\]](#)

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.

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 14

Topic #: 1

[\[All 350-701 Questions\]](#)

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

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 15

Topic #: 1

[\[All 350-701 Questions\]](#)

What are two rootkit types? (Choose two.)

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

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 16

Topic #: 1

[\[All 350-701 Questions\]](#)

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

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 17

Topic #: 1

[\[All 350-701 Questions\]](#)

Which type of attack is social engineering?

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

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 18

Topic #: 1

[\[All 350-701 Questions\]](#)

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

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

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 19

Topic #: 1

[\[All 350-701 Questions\]](#)

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

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 20

Topic #: 1

[\[All 350-701 Questions\]](#)

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.

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 21

Topic #: 1

[\[All 350-701 Questions\]](#)

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.

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 22

Topic #: 1

[\[All 350-701 Questions\]](#)

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

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 23

Topic #: 1

[\[All 350-701 Questions\]](#)

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

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 24

Topic #: 1

[\[All 350-701 Questions\]](#)

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.

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 25

Topic #: 1

[\[All 350-701 Questions\]](#)

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

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 26

Topic #: 1

[\[All 350-701 Questions\]](#)

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

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

Show Suggested Answer



Actual exam question from Cisco's 350-701

Question #: 27

Topic #: 1

[\[All 350-701 Questions\]](#)

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.

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 28

Topic #: 1

[\[All 350-701 Questions\]](#)

Which algorithm provides encryption and authentication for data plane communication?

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

Show Suggested Answer



Actual exam question from Cisco's 350-701

Question #: 29

Topic #: 1

[\[All 350-701 Questions\]](#)

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

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 30

Topic #: 1

[\[All 350-701 Questions\]](#)

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

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 31

Topic #: 1

[\[All 350-701 Questions\]](#)

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.

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 32

Topic #: 1

[\[All 350-701 Questions\]](#)

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

Show Suggested Answer



Actual exam question from Cisco's 350-701

Question #: 33

Topic #: 1

[\[All 350-701 Questions\]](#)

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	

Show Suggested Answer



Actual exam question from Cisco's 350-701

Question #: 34

Topic #: 1

[\[All 350-701 Questions\]](#)

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

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

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 35

Topic #: 1

[\[All 350-701 Questions\]](#)

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

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 36

Topic #: 1

[\[All 350-701 Questions\]](#)

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

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 37

Topic #: 1

[\[All 350-701 Questions\]](#)

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

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

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 38

Topic #: 1

[\[All 350-701 Questions\]](#)

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

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 39

Topic #: 1

[\[All 350-701 Questions\]](#)

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

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 40

Topic #: 1

[\[All 350-701 Questions\]](#)

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

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 41

Topic #: 1

[\[All 350-701 Questions\]](#)

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

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 42

Topic #: 1

[\[All 350-701 Questions\]](#)

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.

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 43

Topic #: 1

[\[All 350-701 Questions\]](#)

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

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

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 44

Topic #: 1

[\[All 350-701 Questions\]](#)

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

[Show Suggested Answer](#)





Actual exam question from Cisco's 350-701

Question #: 45

Topic #: 1

[\[All 350-701 Questions\]](#)

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

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 46

Topic #: 1

[\[All 350-701 Questions\]](#)

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

[Show Suggested Answer](#)





Actual exam question from Cisco's 350-701

Question #: 47

Topic #: 1

[\[All 350-701 Questions\]](#)

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

Show Suggested Answer



Actual exam question from Cisco's 350-701

Question #: 48

Topic #: 1

[\[All 350-701 Questions\]](#)

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.

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 49

Topic #: 1

[\[All 350-701 Questions\]](#)

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.

Show Suggested Answer



Actual exam question from Cisco's 350-701

Question #: 50

Topic #: 1

[\[All 350-701 Questions\]](#)

DRAG DROP -

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

Select and Place:

phishing

botnet

spam

worm

a software program that copies itself from one computer to another, without human interaction

unwanted messages in an email inbox

group of computers connected to the Internet that have been compromised by a hacker using a virus or Trojan horse

fraudulent attempts by cyber criminals to obtain private information

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 51

Topic #: 1

[\[All 350-701 Questions\]](#)

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

Show Suggested Answer



Actual exam question from Cisco's 350-701

Question #: 52

Topic #: 1

[\[All 350-701 Questions\]](#)

```
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.

Show Suggested Answer

Actual exam question from Cisco's 350-701

Question #: 53

Topic #: 1

[\[All 350-701 Questions\]](#)

```
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.

Show Suggested Answer



Actual exam question from Cisco's 350-701

Question #: 54

Topic #: 1

[\[All 350-701 Questions\]](#)

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

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 55

Topic #: 1

[\[All 350-701 Questions\]](#)

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

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 56

Topic #: 1

[\[All 350-701 Questions\]](#)

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.

Show Suggested Answer



Actual exam question from Cisco's 350-701

Question #: 57

Topic #: 1

[\[All 350-701 Questions\]](#)

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.

Show Suggested Answer



Actual exam question from Cisco's 350-701

Question #: 58

Topic #: 1

[\[All 350-701 Questions\]](#)

```
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.

Show Suggested Answer



Actual exam question from Cisco's 350-701

Question #: 59

Topic #: 1

[\[All 350-701 Questions\]](#)

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.

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 60

Topic #: 1

[\[All 350-701 Questions\]](#)

Which algorithm provides asymmetric encryption?

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

Show Suggested Answer



Actual exam question from Cisco's 350-701

Question #: 61

Topic #: 1

[\[All 350-701 Questions\]](#)

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.

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 62

Topic #: 1

[\[All 350-701 Questions\]](#)

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.

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 63

Topic #: 1

[\[All 350-701 Questions\]](#)

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.

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 64

Topic #: 1

[\[All 350-701 Questions\]](#)

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.

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 65

Topic #: 1

[\[All 350-701 Questions\]](#)

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

Show Suggested Answer



Actual exam question from Cisco's 350-701

Question #: 66

Topic #: 1

[\[All 350-701 Questions\]](#)

```
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.

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 67

Topic #: 1

[\[All 350-701 Questions\]](#)

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

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 68

Topic #: 1

[\[All 350-701 Questions\]](#)

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.

Show Suggested Answer



Actual exam question from Cisco's 350-701

Question #: 69

Topic #: 1

[\[All 350-701 Questions\]](#)

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

Show Suggested Answer



Actual exam question from Cisco's 350-701

Question #: 70

Topic #: 1

[\[All 350-701 Questions\]](#)

```
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

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 71

Topic #: 1

[\[All 350-701 Questions\]](#)

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

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 72

Topic #: 1

[\[All 350-701 Questions\]](#)

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

Show Suggested Answer



Actual exam question from Cisco's 350-701

Question #: 73

Topic #: 1

[\[All 350-701 Questions\]](#)

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.

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 74

Topic #: 1

[\[All 350-701 Questions\]](#)

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.

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 75

Topic #: 1

[\[All 350-701 Questions\]](#)

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

Show Suggested Answer



Actual exam question from Cisco's 350-701

Question #: 76

Topic #: 1

[\[All 350-701 Questions\]](#)

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

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 77

Topic #: 1

[\[All 350-701 Questions\]](#)

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.

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 78

Topic #: 1

[\[All 350-701 Questions\]](#)

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

Show Suggested Answer



Actual exam question from Cisco's 350-701

Question #: 79

Topic #: 1

[\[All 350-701 Questions\]](#)

```
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

Show Suggested Answer

Actual exam question from Cisco's 350-701

Question #: 80

Topic #: 1

[\[All 350-701 Questions\]](#)

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.

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 81

Topic #: 1

[\[All 350-701 Questions\]](#)

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`

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 82

Topic #: 1

[\[All 350-701 Questions\]](#)

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

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 83

Topic #: 1

[\[All 350-701 Questions\]](#)

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

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 84

Topic #: 1

[\[All 350-701 Questions\]](#)

```
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

Show Suggested Answer



Actual exam question from Cisco's 350-701

Question #: 85

Topic #: 1

[\[All 350-701 Questions\]](#)

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

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 86

Topic #: 1

[\[All 350-701 Questions\]](#)

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

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 87

Topic #: 1

[\[All 350-701 Questions\]](#)

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

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 88

Topic #: 1

[\[All 350-701 Questions\]](#)

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

Show Suggested Answer



Actual exam question from Cisco's 350-701

Question #: 89

Topic #: 1

[\[All 350-701 Questions\]](#)

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:

	Cisco Firepower
provides detection, blocking, tracking, analysis and remediation to protect against targeted persistent malware attacks	
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	
provides the ability to perform network discovery	
provides intrusion prevention before malware compromises the host	

	Cisco AMP

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 90

Topic #: 1

[\[All 350-701 Questions\]](#)

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

[Show Suggested Answer](#)





Actual exam question from Cisco's 350-701

Question #: 91

Topic #: 1

[\[All 350-701 Questions\]](#)

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.

Show Suggested Answer



Actual exam question from Cisco's 350-701

Question #: 92

Topic #: 1

[\[All 350-701 Questions\]](#)

```
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

Show Suggested Answer

Actual exam question from Cisco's 350-701

Question #: 93

Topic #: 1

[\[All 350-701 Questions\]](#)

```
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

Show Suggested Answer

Actual exam question from Cisco's 350-701

Question #: 94

Topic #: 1

[\[All 350-701 Questions\]](#)

```
> 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.

Show Suggested Answer

Actual exam question from Cisco's 350-701

Question #: 95

Topic #: 1

[\[All 350-701 Questions\]](#)

```
*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

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 96

Topic #: 1

[\[All 350-701 Questions\]](#)

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

[Show Suggested Answer](#)





Actual exam question from Cisco's 350-701

Question #: 97

Topic #: 1

[\[All 350-701 Questions\]](#)

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

[Show Suggested Answer](#)





Actual exam question from Cisco's 350-701

Question #: 98

Topic #: 1

[\[All 350-701 Questions\]](#)

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

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 99

Topic #: 1

[\[All 350-701 Questions\]](#)

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

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 100

Topic #: 1

[\[All 350-701 Questions\]](#)

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

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 101

Topic #: 1

[\[All 350-701 Questions\]](#)

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

[Show Suggested Answer](#)





Actual exam question from Cisco's 350-701

Question #: 102

Topic #: 1

[\[All 350-701 Questions\]](#)

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

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 103

Topic #: 1

[\[All 350-701 Questions\]](#)

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

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 104

Topic #: 1

[\[All 350-701 Questions\]](#)

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

[Show Suggested Answer](#)





Actual exam question from Cisco's 350-701

Question #: 105

Topic #: 1

[\[All 350-701 Questions\]](#)

What is managed by Cisco Security Manager?

- A. Cisco WLC
- B. Cisco ESA
- C. Cisco WSA
- D. Cisco ASA

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 106

Topic #: 1

[\[All 350-701 Questions\]](#)

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

[Show Suggested Answer](#)





Actual exam question from Cisco's 350-701

Question #: 107

Topic #: 1

[\[All 350-701 Questions\]](#)

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

[Show Suggested Answer](#)





Actual exam question from Cisco's 350-701

Question #: 108

Topic #: 1

[\[All 350-701 Questions\]](#)

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.

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 109

Topic #: 1

[\[All 350-701 Questions\]](#)

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.

Show Suggested Answer



Actual exam question from Cisco's 350-701

Question #: 110

Topic #: 1

[\[All 350-701 Questions\]](#)

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.

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 111

Topic #: 1

[\[All 350-701 Questions\]](#)

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.

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 112

Topic #: 1

[\[All 350-701 Questions\]](#)

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

Show Suggested Answer



Actual exam question from Cisco's 350-701

Question #: 113

Topic #: 1

[\[All 350-701 Questions\]](#)

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

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 114

Topic #: 1

[\[All 350-701 Questions\]](#)

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.

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 115

Topic #: 1

[\[All 350-701 Questions\]](#)

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

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 116

Topic #: 1

[\[All 350-701 Questions\]](#)

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.

Show Suggested Answer



Actual exam question from Cisco's 350-701

Question #: 117

Topic #: 1

[\[All 350-701 Questions\]](#)

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

[Show Suggested Answer](#)





Actual exam question from Cisco's 350-701

Question #: 118

Topic #: 1

[\[All 350-701 Questions\]](#)

Which term describes when the Cisco Firepower downloads threat intelligence updates from Cisco Talos?

- A. authoring
- B. consumption
- C. sharing
- D. analysis

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 119

Topic #: 1

[\[All 350-701 Questions\]](#)

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.

[Show Suggested Answer](#)





Actual exam question from Cisco's 350-701

Question #: 120

Topic #: 1

[\[All 350-701 Questions\]](#)

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.

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 121

Topic #: 1

[\[All 350-701 Questions\]](#)

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.

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 122

Topic #: 1

[\[All 350-701 Questions\]](#)

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

[Show Suggested Answer](#)



Actual exam question from Cisco's 350-701

Question #: 123

Topic #: 1

[\[All 350-701 Questions\]](#)

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

Show Suggested Answer



Actual exam question from Cisco's 350-701

Question #: 124

Topic #: 1

[\[All 350-701 Questions\]](#)

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: DfltGrpPolicy **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

Show Suggested Answer



Actual exam question from Cisco's 350-701

Question #: 125

Topic #: 1

[\[All 350-701 Questions\]](#)

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

Show Suggested Answer



Actual exam question from Cisco's 350-701

Question #: 126

Topic #: 1

[\[All 350-701 Questions\]](#)

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`

Show Suggested Answer



Actual exam question from Cisco's 350-701

Question #: 127

Topic #: 1

[\[All 350-701 Questions\]](#)

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.

Show Suggested Answer



Actual exam question from Cisco's 350-701

Question #: 128

Topic #: 1

[\[All 350-701 Questions\]](#)

Add Device

Host:†

Display Name:

Registration Key:*

Group: ▼

Access Control Policy:* ▼

Smart Licensing

Malware:

Threat:

URL Filtering:

Advanced

Unique NAT ID:†

Transfer Packets:

i 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>

Show Suggested Answer

Actual exam question from Cisco's 350-701

Question #: 129

Topic #: 1

[\[All 350-701 Questions\]](#)

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

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 130

Topic #: 1

[\[All 350-701 Questions\]](#)

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

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 131

Topic #: 1

[\[All 350-701 Questions\]](#)

Which attribute has the ability to change during the RADIUS CoA?

- A. authorization
- B. NTP
- C. accessibility
- D. membership

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 132

Topic #: 1

[\[All 350-701 Questions\]](#)

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.

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 133

Topic #: 1

[\[All 350-701 Questions\]](#)

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

[Show Suggested Answer](#)



Actual exam question from Cisco's 350-701

Question #: 134

Topic #: 1

[\[All 350-701 Questions\]](#)

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.

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 135

Topic #: 1

[\[All 350-701 Questions\]](#)

```
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.

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 136

Topic #: 1

[\[All 350-701 Questions\]](#)

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.

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 137

Topic #: 1

[\[All 350-701 Questions\]](#)

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.

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 138

Topic #: 1

[\[All 350-701 Questions\]](#)

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`

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 139

Topic #: 1

[\[All 350-701 Questions\]](#)

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.

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 140

Topic #: 1

[\[All 350-701 Questions\]](#)

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.

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 141

Topic #: 1

[\[All 350-701 Questions\]](#)

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

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 142

Topic #: 1

[\[All 350-701 Questions\]](#)

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.

Show Suggested Answer



Actual exam question from Cisco's 350-701

Question #: 143

Topic #: 1

[\[All 350-701 Questions\]](#)

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.

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 144

Topic #: 1

[\[All 350-701 Questions\]](#)

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.

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 145

Topic #: 1

[\[All 350-701 Questions\]](#)

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.

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 146

Topic #: 1

[\[All 350-701 Questions\]](#)

Which feature requires a network discovery policy on the Cisco Firepower NGIPS?

- A. security intelligence
- B. impact flags
- C. health monitoring
- D. URL filtering

Show Suggested Answer



Actual exam question from Cisco's 350-701

Question #: 148

Topic #: 1

[\[All 350-701 Questions\]](#)

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.

Show Suggested Answer



Actual exam question from Cisco's 350-701

Question #: 149

Topic #: 1

[\[All 350-701 Questions\]](#)

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

Show Suggested Answer



Actual exam question from Cisco's 350-701

Question #: 150

Topic #: 1

[\[All 350-701 Questions\]](#)

```
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.

Show Suggested Answer



Actual exam question from Cisco's 350-701

Question #: 151

Topic #: 1

[\[All 350-701 Questions\]](#)

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

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 152

Topic #: 1

[\[All 350-701 Questions\]](#)

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.

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 153

Topic #: 1

[\[All 350-701 Questions\]](#)

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

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 154

Topic #: 1

[\[All 350-701 Questions\]](#)

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

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 155

Topic #: 1

[\[All 350-701 Questions\]](#)

In which cloud services model is the tenant responsible for virtual machine OS patching?

- A. IaaS
- B. UCaaS
- C. PaaS
- D. SaaS

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 156

Topic #: 1

[\[All 350-701 Questions\]](#)

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

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 157

Topic #: 1

[\[All 350-701 Questions\]](#)

Which feature is supported when deploying Cisco ASA in AWS public cloud?

- A. multiple context mode
- B. user deployment of Layer 3 networks
- C. IPv6
- D. clustering

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 158

Topic #: 1

[\[All 350-701 Questions\]](#)

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

[Show Suggested Answer](#)





Actual exam question from Cisco's 350-701

Question #: 159

Topic #: 1

[\[All 350-701 Questions\]](#)

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

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 160

Topic #: 1

[\[All 350-701 Questions\]](#)

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

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 161

Topic #: 1

[\[All 350-701 Questions\]](#)

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

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 162

Topic #: 1

[\[All 350-701 Questions\]](#)

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

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 163

Topic #: 1

[\[All 350-701 Questions\]](#)

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

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 164

Topic #: 1

[\[All 350-701 Questions\]](#)

On which part of the IT environment does DevSecOps focus?

- A. application development
- B. wireless network
- C. data center
- D. perimeter network

Show Suggested Answer



Actual exam question from Cisco's 350-701

Question #: 166

Topic #: 1

[\[All 350-701 Questions\]](#)

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

Show Suggested Answer



Actual exam question from Cisco's 350-701

Question #: 167

Topic #: 1

[\[All 350-701 Questions\]](#)

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

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 168

Topic #: 1

[\[All 350-701 Questions\]](#)

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.

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 169

Topic #: 1

[\[All 350-701 Questions\]](#)

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

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 170

Topic #: 1

[\[All 350-701 Questions\]](#)

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

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 171

Topic #: 1

[\[All 350-701 Questions\]](#)

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

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 172

Topic #: 1

[\[All 350-701 Questions\]](#)

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

[Show Suggested Answer](#)





Actual exam question from Cisco's 350-701

Question #: 174

Topic #: 1

[\[All 350-701 Questions\]](#)

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

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 175

Topic #: 1

[\[All 350-701 Questions\]](#)

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

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 176

Topic #: 1

[\[All 350-701 Questions\]](#)

An organization wants to secure users, data, and applications in the cloud. The solution must be API-based on 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 Nest-Generation Firewall

[Show Suggested Answer](#)



Actual exam question from Cisco's 350-701

Question #: 177

Topic #: 1

[\[All 350-701 Questions\]](#)

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

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 178

Topic #: 1

[\[All 350-701 Questions\]](#)

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

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 179

Topic #: 1

[\[All 350-701 Questions\]](#)

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

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 180

Topic #: 1

[\[All 350-701 Questions\]](#)

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.

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 181

Topic #: 1

[\[All 350-701 Questions\]](#)

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

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 182

Topic #: 1

[\[All 350-701 Questions\]](#)

Which system facilitates deploying microsegmentation and multi-tenancy services with a policy-based container?

- A. SDLC
- B. Lambda
- C. Contiv
- D. Docker

Show Suggested Answer



Actual exam question from Cisco's 350-701

Question #: 184

Topic #: 1

[\[All 350-701 Questions\]](#)

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.

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 185

Topic #: 1

[\[All 350-701 Questions\]](#)

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.

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 186

Topic #: 1

[\[All 350-701 Questions\]](#)

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

[Show Suggested Answer](#)





Actual exam question from Cisco's 350-701

Question #: 187

Topic #: 1

[\[All 350-701 Questions\]](#)

Where are individual sites specified to be blacklisted in Cisco Umbrella?

- A. application settings
- B. content categories
- C. security settings
- D. destination lists

Show Suggested Answer



Actual exam question from Cisco's 350-701

Question #: 188

Topic #: 1

[\[All 350-701 Questions\]](#)

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.

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 189

Topic #: 1

[\[All 350-701 Questions\]](#)

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

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 190

Topic #: 1

[\[All 350-701 Questions\]](#)

Which API is used for Content Security?

- A. NX-OS API
- B. IOS XR API
- C. OpenVuln API
- D. AsyncOS API

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 191

Topic #: 1

[\[All 350-701 Questions\]](#)

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

[Show Suggested Answer](#)





Actual exam question from Cisco's 350-701

Question #: 192

Topic #: 1

[\[All 350-701 Questions\]](#)

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

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 193

Topic #: 1

[\[All 350-701 Questions\]](#)

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

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 194

Topic #: 1

[\[All 350-701 Questions\]](#)

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.

Show Suggested Answer



Actual exam question from Cisco's 350-701

Question #: 195

Topic #: 1

[\[All 350-701 Questions\]](#)

```
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.

Show Suggested Answer



Actual exam question from Cisco's 350-701

Question #: 196

Topic #: 1

[\[All 350-701 Questions\]](#)

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.

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 197

Topic #: 1

[\[All 350-701 Questions\]](#)

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.

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 198

Topic #: 1

[\[All 350-701 Questions\]](#)

Which technology is used to improve web traffic performance by proxy caching?

- A. WSA
- B. firepower
- C. FireSIGHT
- D. ASA

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 199

Topic #: 1

[\[All 350-701 Questions\]](#)

Which proxy mode must be used on Cisco WSA to redirect TCP traffic with WCCP?

- A. transparent
- B. redirection
- C. forward
- D. proxy gateway

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 200

Topic #: 1

[\[All 350-701 Questions\]](#)

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.

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 201

Topic #: 1

[\[All 350-701 Questions\]](#)

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

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 202

Topic #: 1

[\[All 350-701 Questions\]](#)

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

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 203

Topic #: 1

[\[All 350-701 Questions\]](#)

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.

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 204

Topic #: 1

[\[All 350-701 Questions\]](#)

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

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 205

Topic #: 1

[\[All 350-701 Questions\]](#)

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.

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 206

Topic #: 1

[\[All 350-701 Questions\]](#)

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.

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 207

Topic #: 1

[\[All 350-701 Questions\]](#)

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

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 208

Topic #: 1

[\[All 350-701 Questions\]](#)

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

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 209

Topic #: 1

[\[All 350-701 Questions\]](#)

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

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 210

Topic #: 1

[\[All 350-701 Questions\]](#)

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.

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 211

Topic #: 1

[\[All 350-701 Questions\]](#)

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

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 212

Topic #: 1

[\[All 350-701 Questions\]](#)

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.

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 213

Topic #: 1

[\[All 350-701 Questions\]](#)

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.

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 214

Topic #: 1

[\[All 350-701 Questions\]](#)

Which attack is preventable by Cisco ESA but not by the Cisco WSA?

- A. SQL injection
- B. phishing
- C. buffer overflow
- D. DoS

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 215

Topic #: 1

[\[All 350-701 Questions\]](#)

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.

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 216

Topic #: 1

[\[All 350-701 Questions\]](#)

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

Show Suggested Answer



Actual exam question from Cisco's 350-701

Question #: 217

Topic #: 1

[\[All 350-701 Questions\]](#)

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.

Show Suggested Answer



Actual exam question from Cisco's 350-701

Question #: 218

Topic #: 1

[\[All 350-701 Questions\]](#)

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.

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 219

Topic #: 1

[\[All 350-701 Questions\]](#)

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.

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 220

Topic #: 1

[\[All 350-701 Questions\]](#)

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

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 221

Topic #: 1

[\[All 350-701 Questions\]](#)

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

[Show Suggested Answer](#)





Actual exam question from Cisco's 350-701

Question #: 222

Topic #: 1

[\[All 350-701 Questions\]](#)

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.

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 223

Topic #: 1

[\[All 350-701 Questions\]](#)

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.

Show Suggested Answer



Actual exam question from Cisco's 350-701

Question #: 224

Topic #: 1

[\[All 350-701 Questions\]](#)

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

[Show Suggested Answer](#)



Actual exam question from Cisco's 350-701

Question #: 225

Topic #: 1

[\[All 350-701 Questions\]](#)

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.

Show Suggested Answer



Actual exam question from Cisco's 350-701

Question #: 226


Topic #: 1


[\[All 350-701 Questions\]](#)


ACME Policy


Applied To 2 Identities Contains 4 Policy Settings Last Modified May 6, 2020


Policy Name


 **2 Identities Affected**
2 Networks
[Edit Identity](#)


 **Security Setting Applied: ACME-Security-Settings-Trial**
Command and Control Callbacks, Malware, and Phishing Attacks will be blocked.
No integration is enabled
[Edit](#) [Disable](#)

 **Content Setting Applied: ACME-Content-Settings-Trial**
Pornography and German Youth Protection will be blocked
[Edit](#) [Disable](#)

 **No Application Settings Applied**
[Enable](#)

 **3 Destination Lists Enforced**
1 Block List
1 Allow Lists
[Edit](#)

 **File Analysis Enabled**
File Inspection Enabled
[Edit](#)

 **Umbrella Default Block Page Applied**
[Edit](#)

[▶ 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.

[Show Suggested Answer](#)



Actual exam question from Cisco's 350-701

Question #: 227

Topic #: 1

[\[All 350-701 Questions\]](#)

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.

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 228

Topic #: 1

[\[All 350-701 Questions\]](#)

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.

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 229

Topic #: 1

[\[All 350-701 Questions\]](#)

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

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 230

Topic #: 1

[\[All 350-701 Questions\]](#)

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

[Show Suggested Answer](#)





Actual exam question from Cisco's 350-701

Question #: 231

Topic #: 1

[\[All 350-701 Questions\]](#)

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

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 232

Topic #: 1

[\[All 350-701 Questions\]](#)

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

Show Suggested Answer



Actual exam question from Cisco's 350-701

Question #: 233

Topic #: 1

[\[All 350-701 Questions\]](#)

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

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 234

Topic #: 1

[\[All 350-701 Questions\]](#)

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

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 235

Topic #: 1

[\[All 350-701 Questions\]](#)

Which Cisco product provides proactive endpoint protection and allows administrators to centrally manage the deployment?

- A. NGFW
- B. AMP
- C. WSA
- D. ESA

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 236

Topic #: 1

[\[All 350-701 Questions\]](#)

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.

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 237

Topic #: 1

[\[All 350-701 Questions\]](#)

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.

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 238

Topic #: 1

[\[All 350-701 Questions\]](#)

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.

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 239

Topic #: 1

[\[All 350-701 Questions\]](#)

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

[Show Suggested Answer](#)



Actual exam question from Cisco's 350-701

Question #: 240

Topic #: 1

[\[All 350-701 Questions\]](#)

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

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 241

Topic #: 1

[\[All 350-701 Questions\]](#)

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

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 242

Topic #: 1

[\[All 350-701 Questions\]](#)

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

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 243

Topic #: 1

[\[All 350-701 Questions\]](#)

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

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 244

Topic #: 1

[\[All 350-701 Questions\]](#)

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.

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 246

Topic #: 1

[\[All 350-701 Questions\]](#)

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

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 247

Topic #: 1

[\[All 350-701 Questions\]](#)

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

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 248

Topic #: 1

[\[All 350-701 Questions\]](#)

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

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 249

Topic #: 1

[\[All 350-701 Questions\]](#)

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

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 250

Topic #: 1

[\[All 350-701 Questions\]](#)

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

Show Suggested Answer



Actual exam question from Cisco's 350-701

Question #: 251

Topic #: 1

[\[All 350-701 Questions\]](#)

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

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 252

Topic #: 1

[\[All 350-701 Questions\]](#)

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

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 253

Topic #: 1

[\[All 350-701 Questions\]](#)

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

[Show Suggested Answer](#)





Actual exam question from Cisco's 350-701

Question #: 254

Topic #: 1

[\[All 350-701 Questions\]](#)

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.

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 255

Topic #: 1

[\[All 350-701 Questions\]](#)

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

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 256

Topic #: 1

[\[All 350-701 Questions\]](#)

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.

Show Suggested Answer



Actual exam question from Cisco's 350-701

Question #: 257

Topic #: 1

[\[All 350-701 Questions\]](#)

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

[Show Suggested Answer](#)





Actual exam question from Cisco's 350-701

Question #: 258

Topic #: 1

[\[All 350-701 Questions\]](#)

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.

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 259

Topic #: 1

[\[All 350-701 Questions\]](#)

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.

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 260

Topic #: 1

[\[All 350-701 Questions\]](#)

Which posture assessment requirement provides options to the client for remediation within a certain timeframe?

- A. audit
- B. mandatory
- C. visibility
- D. optional

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 261

Topic #: 1

[\[All 350-701 Questions\]](#)

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.

Show Suggested Answer



Actual exam question from Cisco's 350-701

Question #: 262

Topic #: 1

[\[All 350-701 Questions\]](#)

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.

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 263

Topic #: 1

[\[All 350-701 Questions\]](#)

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.

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 264

Topic #: 1

[\[All 350-701 Questions\]](#)

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

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 265

Topic #: 1

[\[All 350-701 Questions\]](#)

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.

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 266

Topic #: 1

[\[All 350-701 Questions\]](#)

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.

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 267

Topic #: 1

[\[All 350-701 Questions\]](#)

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

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 268

Topic #: 1

[\[All 350-701 Questions\]](#)

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.

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 269

Topic #: 1

[\[All 350-701 Questions\]](#)

Which solution protects hybrid cloud deployment workloads with application visibility and segmentation?

- A. Nexus
- B. Stealthwatch
- C. firepower
- D. Tetration

Show Suggested Answer



Actual exam question from Cisco's 350-701

Question #: 270

Topic #: 1

[\[All 350-701 Questions\]](#)

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

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 271

Topic #: 1

[\[All 350-701 Questions\]](#)

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.

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 272

Topic #: 1

[\[All 350-701 Questions\]](#)

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

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 273

Topic #: 1

[\[All 350-701 Questions\]](#)

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

Show Suggested Answer



Actual exam question from Cisco's 350-701

Question #: 274

Topic #: 1

[\[All 350-701 Questions\]](#)

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

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 275

Topic #: 1

[\[All 350-701 Questions\]](#)

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

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 276

Topic #: 1

[\[All 350-701 Questions\]](#)

What provides visibility and awareness into what is currently occurring on the network?

- A. CMX
- B. WMI
- C. Cisco Prime Infrastructure
- D. Telemetry

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 277

Topic #: 1

[\[All 350-701 Questions\]](#)

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

Show Suggested Answer



Actual exam question from Cisco's 350-701

Question #: 278

Topic #: 1

[\[All 350-701 Questions\]](#)

```
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

Show Suggested Answer



Actual exam question from Cisco's 350-701

Question #: 279

Topic #: 1

[\[All 350-701 Questions\]](#)

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

[Show Suggested Answer](#)





Actual exam question from Cisco's 350-701

Question #: 280

Topic #: 1

[\[All 350-701 Questions\]](#)

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

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 282

Topic #: 1

[\[All 350-701 Questions\]](#)

Which compliance status is shown when a configured posture policy requirement is not met?

- A. authorized
- B. compliant
- C. unknown
- D. noncompliant

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 283

Topic #: 1

[\[All 350-701 Questions\]](#)

An organization is trying to implement micro-segmentation on the network and wants to be able to gain visibility on the applications within the network. The solution must be able to maintain and force compliance. Which product should be used to meet these requirements?

- A. Cisco Stealthwatch
- B. Cisco Tetration
- C. Cisco AMP
- D. Cisco Umbrella

[Show Suggested Answer](#)





Actual exam question from Cisco's 350-701

Question #: 284

Topic #: 1

[\[All 350-701 Questions\]](#)

An organization has a Cisco Stealthwatch Cloud deployment in their environment. Cloud logging is working as expected, but logs are not being received from the on-premise network. What action will resolve this issue?

- A. Deploy a Cisco FTD sensor to send events to Cisco Stealthwatch Cloud.
- B. Deploy a Cisco Stealthwatch Cloud sensor on the network to send data to Cisco Stealthwatch Cloud.
- C. Configure security appliances to send syslogs to Cisco Stealthwatch Cloud.
- D. Configure security appliances to send NetFlow to Cisco Stealthwatch Cloud.

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 285

Topic #: 1

[\[All 350-701 Questions\]](#)

A network engineer has been tasked with adding a new medical device to the network. Cisco ISE is being used as the NAC server, and the new device does not have a supplicant available. What must be done in order to securely connect this device to the network?

- A. Use 802.1X with posture assessment.
- B. Use MAB with profiling.
- C. Use 802.1X with profiling.
- D. Use MAB with posture assessment.

[Show Suggested Answer](#)



Actual exam question from Cisco's 350-701

Question #: 286

Topic #: 1

[\[All 350-701 Questions\]](#)

Drag and drop the solutions from the left onto the solution's benefits on the right.

Select and Place:

Cisco Stealthwatch

obtains contextual identity and profiles for all the users and devices connected on a network.

Cisco ISE

software-defines segmentation that uses SGTs and allows administrators to quickly scale and enforce policies across the network

Cisco TrustSec

rapidly collects and analyzes NetFlow and telemetry data to deliver in-depth visibility and understanding of network traffic

Cisco Umbrella

secure Internet gateway in the cloud that provides a security solution that protects endpoints on and off the network against threats on the Internet by using DNS

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 287

Topic #: 1

[\[All 350-701 Questions\]](#)

A network engineer must monitor user and device behavior within the on-premises network. This data must be sent to the Cisco Stealthwatch Cloud analytics platform for analysis. What must be done to meet this requirement, using the Ubuntu-based VM appliance deployed in a VMware-based hypervisor?

- A. Deploy a Cisco FTD sensor to send network events to Cisco Stealthwatch Cloud.
- B. Configure a Cisco FMC to send syslogs to Cisco Stealthwatch Cloud.
- C. Deploy the Cisco Stealthwatch Cloud PNM sensor that sends data to Cisco Stealthwatch Cloud.
- D. Configure a Cisco FMC to send NetFlow to Cisco Stealthwatch Cloud.

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 288

Topic #: 1

[\[All 350-701 Questions\]](#)

An organization wants to provide visibility and to identify active threats in its network using a VM. The organization wants to extract metadata from network packet flow while ensuring that payloads are not retained or transferred outside the network. Which solution meets these requirements?

- A. Cisco Umbrella Cloud
- B. Cisco Stealthwatch Cloud PNM
- C. Cisco Stealthwatch Cloud PCM
- D. Cisco Umbrella On-Premises

[Show Suggested Answer](#)





Actual exam question from Cisco's 350-701

Question #: 289

Topic #: 1

[\[All 350-701 Questions\]](#)

What is a benefit of performing device compliance?

- A. providing multi-factor authentication
- B. verification of the latest OS patches
- C. providing attribute-driven policies
- D. device classification and authorization

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 290

Topic #: 1

[\[All 350-701 Questions\]](#)

Which type of DNS abuse exchanges data between two computers even when there is no direct connection?

- A. malware installation
- B. network footprinting
- C. command-and-control communication
- D. data exfiltration

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 291

Topic #: 1

[\[All 350-701 Questions\]](#)

How is data sent out to the attacker during a DNS tunneling attack?

- A. as part of the domain name
- B. as part of the UDP/53 packet payload
- C. as part of the TCP/53 packet header
- D. as part of the DNS response packet

Show Suggested Answer



Actual exam question from Cisco's 350-701

Question #: 292

Topic #: 1

[\[All 350-701 Questions\]](#)

```
interface GigabitEthernet1/0/18
switchport access vlan 41
switchport mode access
switchport voice vlan 44
device-tracking attach-policy IPDT_MAX_10
auauthentication periodic
authentication timer reauthenticate server
access-session host-mode multi-domain
access-session port-control auto
dot1x pae authenticator
dot1x timeout tx-period 7dot1x max-reauth-req 3
spanning-tree portfast
```

Refer to the exhibit. A Cisco ISE administrator adds a new switch to an 802.1X deployment and has difficulty with some endpoints gaining access. Most PCs and IP phones can connect and authenticate using their machine certificate credentials; however, printers and video cameras cannot. Based on the interface configuration provided, what must be done to get these devices onto the network using Cisco ISE for authentication and authorization while maintaining security controls?

- A. Configure authentication event fail retry 2 action authorize vlan 41 on the interface.
- B. Add mab to the interface configuration.
- C. Enable insecure protocols within Cisco ISE in the allowed protocols configuration.
- D. Change the default policy in Cisco ISE to allow all devices not using machine authentication.

Show Suggested Answer



Actual exam question from Cisco's 350-701

Question #: 293

Topic #: 1

[\[All 350-701 Questions\]](#)

Cisco SensorBase gathers threat information from a variety of Cisco products and services and performs analytics to find pattern on threats. Which term describes this process?

- A. authoring
- B. consumption
- C. deployment
- D. sharing

[Show Suggested Answer](#)



Actual exam question from Cisco's 350-701

Question #: 294

Topic #: 1

[\[All 350-701 Questions\]](#)

```
interface GigabitEthernet1/0/18
description ISE dot1x Port
switchport access vlan 41
switchport mode access
switchport voice vlan 44
device tracking attach-policy IPDT_MAX_10
authentication periodic
authentication timer reauthenticate server
access-session host-mode multi-domain
access-session port-control auto
snmp trap mac-notification change added
snap trap mac-notification change removed
dot1x pae authenticator
dot1x timeout tx-period 7
dot1x max-reauth-req 3
spanning-tree portfast
service policy type control subscriber POLICY_Gi1/0/18
```

Refer to the exhibit. What will occur when this device tries to connect to the port?

- A. 802.1X will not work, but MAB will start and allow the device on the network.
- B. 802.1X will work and the device will be allowed on the network.
- C. 802.1X will not work and the device will not be allowed network access.
- D. 802.1X and MAB will both be used and ISE can use policy to determine the access level.

Show Suggested Answer



Actual exam question from Cisco's 350-701

Question #: 295

Topic #: 1

[\[All 350-701 Questions\]](#)

Which telemetry data captures variations seen within the flow, such as the packets TTL, IP/TCP flags, and payload length?

- A. flow insight variation
- B. software package variation
- C. interpacket variation
- D. process details variation

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 296

Topic #: 1

[\[All 350-701 Questions\]](#)

Which network monitoring solution uses streams and pushes operational data to provide a near real-time view of activity?

- A. SNMP
- B. SMTP
- C. syslog
- D. model-driven telemetry

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 297

Topic #: 1

[\[All 350-701 Questions\]](#)

What two mechanisms are used to redirect users to a web portal to authenticate to ISE for guest services? (Choose two.)

- A. TACACS+
- B. central web auth
- C. single sign-on
- D. multiple factor auth
- E. local web auth

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 298

Topic #: 1

[\[All 350-701 Questions\]](#)

Which ID store requires that a shadow user be created on Cisco ISE for the admin login to work?

- A. RSA SecureID
- B. Internal Database
- C. Active Directory
- D. LDAP

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 299

Topic #: 1

[\[All 350-701 Questions\]](#)

An administrator wants to ensure that all endpoints are compliant before users are allowed access on the corporate network. The endpoints must have the corporate antivirus application installed and be running the latest build of Windows 10.

What must the administrator implement to ensure that all devices are compliant before they are allowed on the network?

- A. Cisco Identity Services Engine and AnyConnect Posture module
- B. Cisco Stealthwatch and Cisco Identity Services Engine integration
- C. Cisco ASA firewall with Dynamic Access Policies configured
- D. Cisco Identity Services Engine with PxGrid services enabled

Show Suggested Answer



Actual exam question from Cisco's 350-701

Question #: 301

Topic #: 1

[\[All 350-701 Questions\]](#)

What are two things to consider when using PAC files with the Cisco WSA? (Choose two.)

- A. If the WSA host port is changed, the default port redirects web traffic to the correct port automatically.
- B. PAC files use if-else statements to determine whether to use a proxy or a direct connection for traffic between the PC and the host.
- C. The WSA hosts PAC files on port 9001 by default.
- D. The WSA hosts PAC files on port 6001 by default.
- E. By default, they direct traffic through a proxy when the PC and the host are on the same subnet.

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 302

Topic #: 1

[\[All 350-701 Questions\]](#)

Which IETF attribute is supported for the RADIUS CoA feature?

- A. 24 State
- B. 30 Calling-Station-ID
- C. 42 Acct-Session-ID
- D. 81 Message-Authenticator

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 303

Topic #: 1

[\[All 350-701 Questions\]](#)

When a transparent authentication fails on the Web Security Appliance, which type of access does the end user get?

- A. guest
- B. limited Internet
- C. blocked
- D. full Internet

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 304

Topic #: 1

[\[All 350-701 Questions\]](#)

What are two ways that Cisco Container Platform provides value to customers who utilize cloud service providers? (Choose two.)

- A. Allows developers to create code once and deploy to multiple clouds
- B. helps maintain source code for cloud deployments
- C. manages Docker containers
- D. manages Kubernetes clusters
- E. Creates complex tasks for managing code

Show Suggested Answer



Actual exam question from Cisco's 350-701

Question #: 305

Topic #: 1

[\[All 350-701 Questions\]](#)

DRAG DROP -

Drag and drop the posture assessment flow actions from the left into a sequence on the right.

Select and Place:

Validate user credentials

Check device compliance with
security policy

Grant appropriate access with
compliant device

Apply updates or take other
necessary action

Permit just enough for the posture
assessment

step 1

step 2

step 3

step 4

step 5

Show Suggested Answer



Actual exam question from Cisco's 350-701

Question #: 306

Topic #: 1

[\[All 350-701 Questions\]](#)

```
import requests

client_id = 'a1b2c3d4e5f6g7h8i9j0'

api_key = 'a1b2c3d4-e5f6-g7h8-i9j0-k1l2m3n4o5p6'
```

Refer to the exhibit.

What does the API key do while working with <https://api.amp.cisco.com/v1/computers>?

- A. displays client ID
- B. HTTP authorization
- C. Imports requests
- D. HTTP authentication

Show Suggested Answer

Actual exam question from Cisco's 350-701

Question #: 307

Topic #: 1

[\[All 350-701 Questions\]](#)

Which statement describes a serverless application?

- A. The application delivery controller in front of the server farm designates on which server the application runs each time.
- B. The application runs from an ephemeral, event-triggered, and stateless container that is fully managed by a cloud provider.
- C. The application is installed on network equipment and not on physical servers.
- D. The application runs from a containerized environment that is managed by Kubernetes or Docker Swarm.

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 308

Topic #: 1

[\[All 350-701 Questions\]](#)

What is a description of microsegmentation?

- A. Environments deploy a container orchestration platform, such as Kubernetes, to manage the application delivery.
- B. Environments apply a zero-trust model and specify how applications on different servers or containers can communicate.
- C. Environments deploy centrally managed host-based firewall rules on each server or container.
- D. Environments implement private VLAN segmentation to group servers with similar applications.

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 309

Topic #: 1

[\[All 350-701 Questions\]](#)

Which Cisco WSA feature supports access control using URL categories?

- A. transparent user identification
- B. SOCKS proxy services
- C. web usage controls
- D. user session restrictions

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 311

Topic #: 1

[\[All 350-701 Questions\]](#)

An engineer enabled SSL decryption for Cisco Umbrella intelligent proxy and needs to ensure that traffic is inspected without alerting end-users. Which action accomplishes this goal?

- A. Restrict access to only websites with trusted third-party signed certificates.
- B. Modify the user's browser settings to suppress errors from Cisco Umbrella.
- C. Upload the organization root CA to Cisco Umbrella.
- D. Install the Cisco Umbrella root CA onto the user's device.

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 312

Topic #: 1

[\[All 350-701 Questions\]](#)

What is the purpose of joining Cisco WSAs to an appliance group?

- A. All WSAs in the group can view file analysis results.
- B. The group supports improved redundancy
- C. It supports cluster operations to expedite the malware analysis process.
- D. It simplifies the task of patching multiple appliances.

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 314

Topic #: 1

[\[All 350-701 Questions\]](#)

Which technology should be used to help prevent an attacker from stealing usernames and passwords of users within an organization?

- A. RADIUS-based REAP
- B. fingerprinting
- C. Dynamic ARP Inspection
- D. multifactor authentication

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 316

Topic #: 1

[\[All 350-701 Questions\]](#)

Which solution for remote workers enables protection, detection, and response on the endpoint against known and unknown threats?

- A. Cisco AMP for Endpoints
- B. Cisco AnyConnect
- C. Cisco Umbrella
- D. Cisco Duo

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 317

Topic #: 1

[\[All 350-701 Questions\]](#)

Which two actions does the Cisco Identity Services Engine posture module provide that ensures endpoint security? (Choose two.)

- A. Assignments to endpoint groups are made dynamically, based on endpoint attributes.
- B. Endpoint supplicant configuration is deployed.
- C. A centralized management solution is deployed.
- D. Patch management remediation is performed.
- E. The latest antivirus updates are applied before access is allowed.

Show Suggested Answer



Actual exam question from Cisco's 350-701

Question #: 318

Topic #: 1

[\[All 350-701 Questions\]](#)

What is an advantage of the Cisco Umbrella roaming client?

- A. the ability to see all traffic without requiring TLS decryption
- B. visibility into IP-based threats by tunneling suspicious IP connections
- C. the ability to dynamically categorize traffic to previously uncategorized sites
- D. visibility into traffic that is destined to sites within the office environment

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 319

Topic #: 1

[\[All 350-701 Questions\]](#)

Which Cisco platform provides an agentless solution to provide visibility across the network including encrypted traffic analytics to detect malware in encrypted traffic without the need for decryption?

- A. Cisco Advanced Malware Protection
- B. Cisco Stealthwatch
- C. Cisco Identity Services Engine
- D. Cisco AnyConnect

[Show Suggested Answer](#)





Actual exam question from Cisco's 350-701

Question #: 320

Topic #: 1

[\[All 350-701 Questions\]](#)

Which two Cisco ISE components must be configured for BYOD? (Choose two.)

- A. local WebAuth
- B. central WebAuth
- C. null WebAuth
- D. guest
- E. dual

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 321

Topic #: 1

[\[All 350-701 Questions\]](#)

Which system performs compliance checks and remote wiping?

- A. MDM
- B. ISE
- C. AMP
- D. OTP

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 322

Topic #: 1

[\[All 350-701 Questions\]](#)

An engineer is configuring Cisco WSA and needs to enable a separated email transfer flow from the Internet and from the LAN. Which deployment mode must be used to accomplish this goal?

- A. single interface
- B. multi-context
- C. transparent
- D. two-interface

[Show Suggested Answer](#)





Actual exam question from Cisco's 350-701

Question #: 323

Topic #: 1

[\[All 350-701 Questions\]](#)

A network engineer is tasked with configuring a Cisco ISE server to implement external authentication against Active Directory. What must be considered about the authentication requirements? (Choose two.)

- A. RADIUS communication must be permitted between the ISE server and the domain controller.
- B. The ISE account must be a domain administrator in Active Directory to perform JOIN operations.
- C. Active Directory only supports user authentication by using MSCHAPv2.
- D. LDAP communication must be permitted between the ISE server and the domain controller.
- E. Active Directory supports user and machine authentication by using MSCHAPv2.

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 324

Topic #: 1

[\[All 350-701 Questions\]](#)

Which configuration method provides the options to prevent physical and virtual endpoint devices that are in the same base EPG or uSeg from being able to communicate with each other with Vmware VDS or Microsoft vSwitch?

- A. inter-EPG isolation
- B. inter-VLAN security
- C. intra-EPG isolation
- D. placement in separate EPGs

Show Suggested Answer



Actual exam question from Cisco's 350-701

Question #: 325

Topic #: 1

[\[All 350-701 Questions\]](#)

What are two ways a network administrator transparently identifies users using Active Directory on the Cisco WSA? (Choose two.)

- A. Create an LDAP authentication realm and disable transparent user identification.
- B. Create NTLM or Kerberos authentication realm and enable transparent user identification.
- C. Deploy a separate Active Directory agent such as Cisco Context Directory Agent.
- D. The eDirectory client must be installed on each client workstation.
- E. Deploy a separate eDirectory server; the client IP address is recorded in this server.

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 326

Topic #: 1

[\[All 350-701 Questions\]](#)

Which baseline form of telemetry is recommended for network infrastructure devices?

- A. SDNS
- B. NetFlow
- C. passive taps
- D. SNMP

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 327

Topic #: 1

[\[All 350-701 Questions\]](#)

In which scenario is endpoint-based security the solution?

- A. inspecting encrypted traffic
- B. device profiling and authorization
- C. performing signature-based application control
- D. inspecting a password-protected archive

Show Suggested Answer



Actual exam question from Cisco's 350-701

Question #: 328

Topic #: 1

[\[All 350-701 Questions\]](#)

```
def dnac_login(host, username, password):  
    url = "https://{}/api/system/v1/auth/token".format(host)  
    response = requests.request("POST", url,  
    auth=HTTPBasicAuth(username, password),  
                                headers=headers, verify=False)  
    return response.json() ["Token"]
```

Refer to the exhibit. What is the result of the Python script?

- A. It uses the POST HTTP method to obtain a username and password to be used for authentication.
- B. It uses the POST HTTP method to obtain a token to be used for authentication.
- C. It uses the GET HTTP method to obtain a token to be used for authentication.
- D. It uses the GET HTTP method to obtain a username and password to be used for authentication

Show Suggested Answer



Actual exam question from Cisco's 350-701

Question #: 330

Topic #: 1

[\[All 350-701 Questions\]](#)

Which two parameters are used for device compliance checks? (Choose two.)

- A. endpoint protection software version
- B. Windows registry values
- C. DHCP snooping checks
- D. DNS integrity checks
- E. device operating system version

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 331

Topic #: 1

[\[All 350-701 Questions\]](#)

Which Cisco cloud security software centrally manages policies on multiple platforms such as Cisco ASA, Cisco Firepower, Cisco Meraki, and AWS?

- A. Cisco Defense Orchestrator
- B. Cisco Configuration Professional
- C. Cisco Secureworks
- D. Cisco DNAC

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 332

Topic #: 1

[\[All 350-701 Questions\]](#)

Which Cisco security solution determines if an endpoint has the latest OS updates and patches installed on the system?

- A. Cisco Endpoint Security Analytics
- B. Cisco AMP for Endpoints
- C. Endpoint Compliance Scanner
- D. Security Posture Assessment Service

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 333

Topic #: 1

[\[All 350-701 Questions\]](#)

Which open standard creates a framework for sharing threat intelligence in a machine-digestible format?

- A. OpenIOC
- B. OpenC2
- C. CybOX
- D. STIX

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 334

Topic #: 1

[\[All 350-701 Questions\]](#)

What is a difference between Cisco AMP for Endpoints and Cisco Umbrella?

- A. Cisco AMP for Endpoints is a cloud-based service, and Cisco Umbrella is not
- B. Cisco AMP for Endpoints automatically researches indicators of compromise and confirms threats and Cisco Umbrella does not
- C. Cisco AMP for Endpoints prevents, detects, and responds to attacks before damage can be done, and Cisco Umbrella provides the first line of defense against Internet threats
- D. Cisco AMP for Endpoints prevents connections to malicious destinations, and Cisco Umbrella works at the file level to prevent the initial execution of malware

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 335

Topic #: 1

[\[All 350-701 Questions\]](#)

What are two functionalities of northbound and southbound APIs within Cisco SDN architecture? (Choose two.)

- A. Northbound APIs utilize RESTful API methods such as GET, POST, and DELETE
- B. Southbound APIs utilize CLI, SNMP, and RESTCONF
- C. Southbound APIs are used to define how SDN controllers integrate with applications
- D. Northbound interfaces utilize OpenFlow and OpFlex to integrate with network devices
- E. Southbound interfaces utilize device configurations such as VLANs and IP addresses

Show Suggested Answer



Actual exam question from Cisco's 350-701

Question #: 336

Topic #: 1

[\[All 350-701 Questions\]](#)

```
... #{code snipped}
...
api_path = "/api/access/global/rules"
url = server + api_path
f = None

post_data = {
    "sourceService": {
        "kind": serviceKind,
        "value": sourceServiceValue
    },
    "destinationAddress": {
        "kind": destinationAddressKind,
        "value": destinationAddress
    },
    "remarks": [],
    "destinationService": {
        "kind": serviceKind,
        "value": destinationServiceValue
    },
    "permit": trueORfalse,
    "active": "true",
    "position": "1",
    "sourceAddress": {
        "kind": sourceAddressKind,
        "value": sourceAddress
    }
}

req = urllib2.Request(url, json.dumps(post_data), headers)
base64string = base64.encodestring("%s:%s" % (username, password)).replace("\n", "")
req.add_header("Authorization", "Basic %s" % base64string)
try:
    f = urllib2.urlopen(req)
    status_code = f.getcode()

    print "Status code is "+str(status_code)
    if status_code == 201:
        print "Operation successful"
    except urllib2.HTTPError, err:
        print "Error received from server. HTTP Status code :"+str(err.code)
    try:
```

Refer to the exhibit. What is the function of the Python script code snippet for the Cisco ASA REST API?

- A. changes the hostname of the Cisco ASA
- B. adds a global rule into policies
- C. deletes a global rule from policies
- D. obtains the saved configuration of the Cisco ASA firewall

Show Suggested Answer

Actual exam question from Cisco's 350-701

Question #: 337

Topic #: 1

[\[All 350-701 Questions\]](#)

DRAG DROP -

Drag and drop the features of Cisco ASA with Firepower from the left onto the benefits on the right.

Select and Place:

Full Context Awareness

detection, blocking and remediation to protect the enterprise against targeted malware attacks

NGIPS

policy enforcement based on complete visibility of users and communication between virtual machines

AMP

real-time threat intelligence and security protection

Collective Security Intelligence

threat prevention and mitigation for known and unknown threats

Show Suggested Answer



Actual exam question from Cisco's 350-701

Question #: 338

Topic #: 1

[\[All 350-701 Questions\]](#)

What are two functions of secret key cryptography? (Choose two.)

- A. utilization of less memory
- B. utilization of large prime number iterations
- C. utilization of different keys for encryption and decryption
- D. key selection without integer factorization
- E. provides the capability to only know the key on one side

Show Suggested Answer

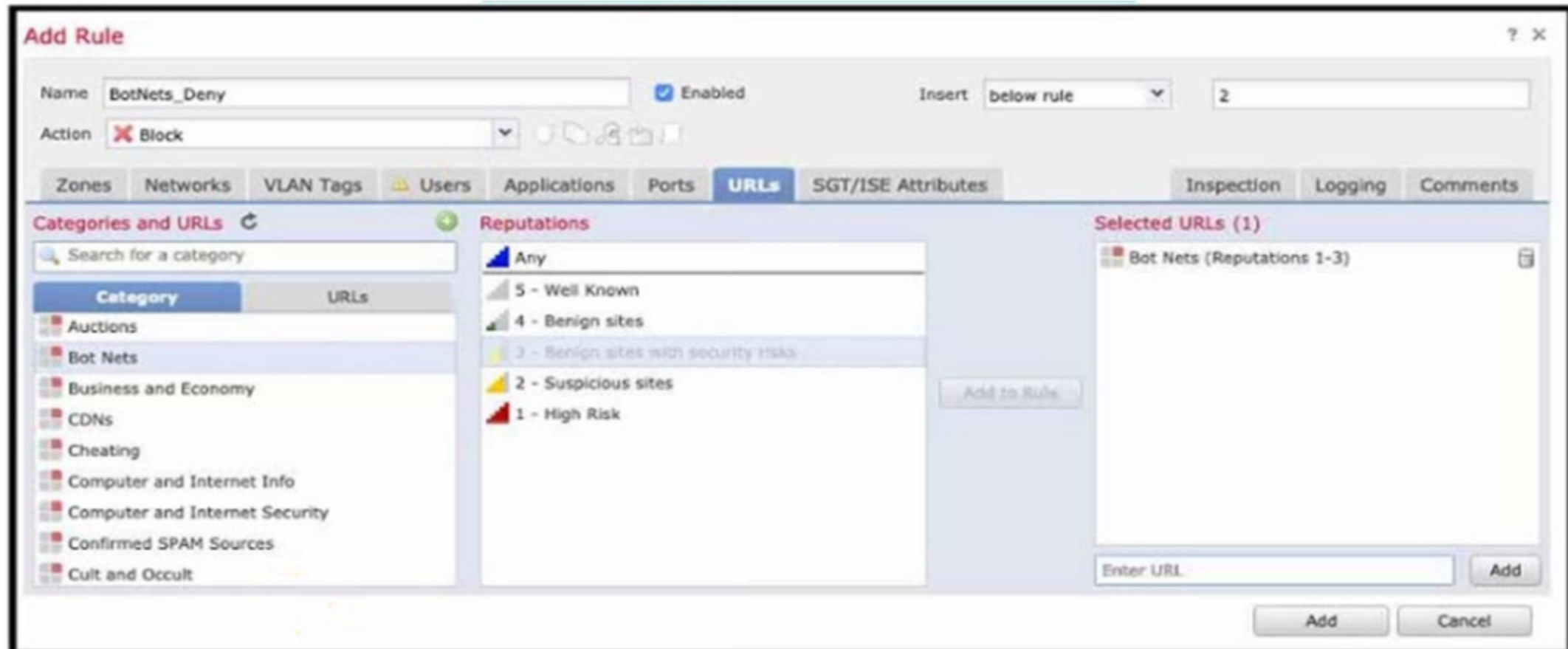


Actual exam question from Cisco's 350-701

Question #: 339

Topic #: 1

[\[All 350-701 Questions\]](#)



Refer to the exhibit. When creating an access rule for URL filtering a network engineer adds certain categories and individual URLs to block. What is the result of the configuration?

- A. Only URLs for botnets with a reputation score of 3 will be allowed while the rest will be blocked.
- B. Only URLs for botnets with reputation scores of 1-3 will be blocked.
- C. Only URLs for botnets with reputation scores of 3-5 will be blocked.
- D. Only URLs for botnets with a reputation score of 3 will be blocked.

Show Suggested Answer



Actual exam question from Cisco's 350-701

Question #: 340

Topic #: 1

[\[All 350-701 Questions\]](#)

Which security product enables administrators to deploy Kubernetes clusters in air-gapped sites without needing Internet access?

- A. Cisco Container Controller
- B. Cisco Cloud Platform
- C. Cisco Container Platform
- D. Cisco Content Platform

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 341

Topic #: 1

[\[All 350-701 Questions\]](#)

A network engineer must migrate a Cisco WSA virtual appliance from one physical host to another physical host by using VMware vMotion. What is a requirement for both physical hosts?

- A. The hosts must run Cisco AsyncOS 10.0 or greater.
- B. The hosts must run different versions of Cisco AsyncOS.
- C. The hosts must have access to the same defined network.
- D. The hosts must use a different datastore than the virtual appliance.

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 342

Topic #: 1

[\[All 350-701 Questions\]](#)

An engineer must modify a policy to block specific addresses using Cisco Umbrella. The policy is created already and is actively used by devices, using many of the default policy elements. What else must be done to accomplish this task?

- A. Create a destination list for addresses to be allowed or blocked
- B. Use content categories to block or allow specific addresses
- C. Add the specified addresses to the identities list and create a block action
- D. Modify the application settings to allow only applications to connect to required addresses

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 343

Topic #: 1

[\[All 350-701 Questions\]](#)

What must be enabled to secure SaaS-based applications?

- A. two-factor authentication
- B. end-to-end encryption
- C. application security gateway
- D. modular policy framework

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 344

Topic #: 1

[\[All 350-701 Questions\]](#)

An engineer configures new features within the Cisco Umbrella dashboard and wants to identify and proxy traffic that is categorized as risky domains and may contain safe and malicious content. Which action accomplishes these objectives?

- A. Upload the threat intelligence database to Cisco Umbrella for the most current information on reputations and to have the destination lists block them
- B. Configure URL filtering within Cisco Umbrella to track the URLs and proxy the requests for those categories and below
- C. Create a new site within Cisco Umbrella to block requests from those categories so they can be sent to the proxy device
- D. Configure intelligent proxy within Cisco Umbrella to intercept and proxy the requests for only those categories

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 345

Topic #: 1

[\[All 350-701 Questions\]](#)

An engineer is configuring Cisco Umbrella and has an identity that references two different policies. Which action ensures that the policy that the identity must use takes precedence over the second one?

- A. Place the policy with the most-specific configuration last in the policy order
- B. Configure the default policy to redirect the requests to the correct policy
- C. Make the correct policy first in the policy order
- D. Configure only the policy with the most recently changed timestamp

Show Suggested Answer



Actual exam question from Cisco's 350-701

Question #: 346

Topic #: 1

[\[All 350-701 Questions\]](#)

A Cisco ISE engineer configures Central Web Authentication (CWA) for wireless guest access and must have the guest endpoints redirect to the guest portal for authentication and authorization. While testing the policy, the engineer notices that the device is not redirected and instead gets full guest access. What must be done for the redirect to work?

- A. Tag the guest portal in the CWA part of the Common Tasks section of the authorization profile for the authorization policy line that the unauthenticated devices hit.
- B. Create an advanced attribute setting of Cisco:cisco-gateway-id=guest within the authorization profile for the authorization policy line that the unauthenticated devices hit.
- C. Add the DACL name for the Airespace ACL configured on the WLC in the Common Tasks section of the authorization profile for the authorization policy line that the unauthenticated devices hit.
- D. Use the track movement option within the authorization profile for the authorization policy line that the unauthenticated devices hit.

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 347

Topic #: 1

[\[All 350-701 Questions\]](#)

What is the intent of a basic SYN flood attack?

- A. to solicit DNS responses
- B. to flush the register stack to re-initiate the buffers
- C. to exceed the threshold limit of the connection queue
- D. to cause the buffer to overflow

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 348

Topic #: 1

[\[All 350-701 Questions\]](#)

What is an advantage of network telemetry over SNMP pulls?

- A. security
- B. scalability
- C. accuracy
- D. encapsulation

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 350

Topic #: 1

[\[All 350-701 Questions\]](#)

What are two functions of TAXII in threat intelligence sharing? (Choose two.)

- A. allows users to describe threat motivations and abilities
- B. determines how threat intelligence information is relayed
- C. determines the "what" of threat intelligence
- D. exchanges trusted anomaly intelligence information
- E. supports STIX information

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 351

Topic #: 1

[\[All 350-701 Questions\]](#)

What are two functionalities of SDN Northbound APIs? (Choose two.)

- A. OpenFlow is a standardized northbound API protocol
- B. Northbound APIs form the interface between the SDN controller and business applications
- C. Northbound APIs provide a programmable interface for applications to dynamically configure the network
- D. Northbound APIs form the interface between the SDN controller and the network switches or routers
- E. Northbound APIs use the NETCONF protocol to communicate with applications.

Show Suggested Answer



Actual exam question from Cisco's 350-701

Question #: 352

Topic #: 1

[\[All 350-701 Questions\]](#)

What is the result of the ACME-Router(config)#login block-for 100 attempts 4 within 60 command on a Cisco IOS router?

- A. If four failures occur in 60 seconds, the router goes to quiet mode for 100 seconds
- B. After four unsuccessful log in attempts the line is blocked for 100 seconds and only permit IP addresses are permitted in ACL 60
- C. After four unsuccessful log in attempts the line is blocked for 60 seconds and only permit IP addresses are permitted in ACL 100
- D. If four log in attempts fail in 100 seconds, wait for 60 seconds to next log in prompt

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 353

Topic #: 1

[\[All 350-701 Questions\]](#)

What is a benefit of using a multifactor authentication strategy?

- A. It provides an easy, single sign-on experience against multiple applications
- B. It provides secure remote access for applications
- C. It protects data by enabling the use of a second validation of identity
- D. It provides visibility into devices to establish device trust

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 354

Topic #: 1

[\[All 350-701 Questions\]](#)

Which endpoint solution protects a user from a phishing attack?

- A. Cisco AnyConnect with Network Access Manager module
- B. Cisco AnyConnect with Umbrella Roaming Security module
- C. Cisco Identity Services Engine
- D. Cisco AnyConnect with ISE Posture module

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 355

Topic #: 1

[\[All 350-701 Questions\]](#)

Which role is a default guest type in Cisco ISE?

- A. Contractor
- B. Full-Time
- C. Monthly
- D. Yearly

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 356

Topic #: 1

[\[All 350-701 Questions\]](#)

An engineer is trying to decide between using L2TP or GRE over IPsec for their site-to-site VPN implementation. What must be understood before choosing a solution?

- A. L2TP is an IP packet encapsulation protocol, and GRE over IPsec is a tunneling protocol
- B. GRE over IPsec cannot be used as a standalone protocol, and L2TP can
- C. L2TP uses TCP port 47 and GRE over IPsec uses UDP port 1701
- D. GRE over IPsec adds its own header, and L2TP does not

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 357

Topic #: 1

[\[All 350-701 Questions\]](#)

An administrator enables Cisco Threat Intelligence Director on a Cisco FMC. Which process uses STIX and allows uploads and downloads of block lists?

- A. editing
- B. sharing
- C. authoring
- D. consumption

Show Suggested Answer



Actual exam question from Cisco's 350-701

Question #: 359

Topic #: 1

[\[All 350-701 Questions\]](#)

Which two methods must be used to add switches into the fabric so that administrators can control how switches are added into DCNM for private cloud management?
(Choose two.)

- A. Cisco Prime Infrastructure
- B. CDP AutoDiscovery
- C. Seed IP
- D. PowerOn Auto Provisioning
- E. Cisco Cloud Director

Show Suggested Answer

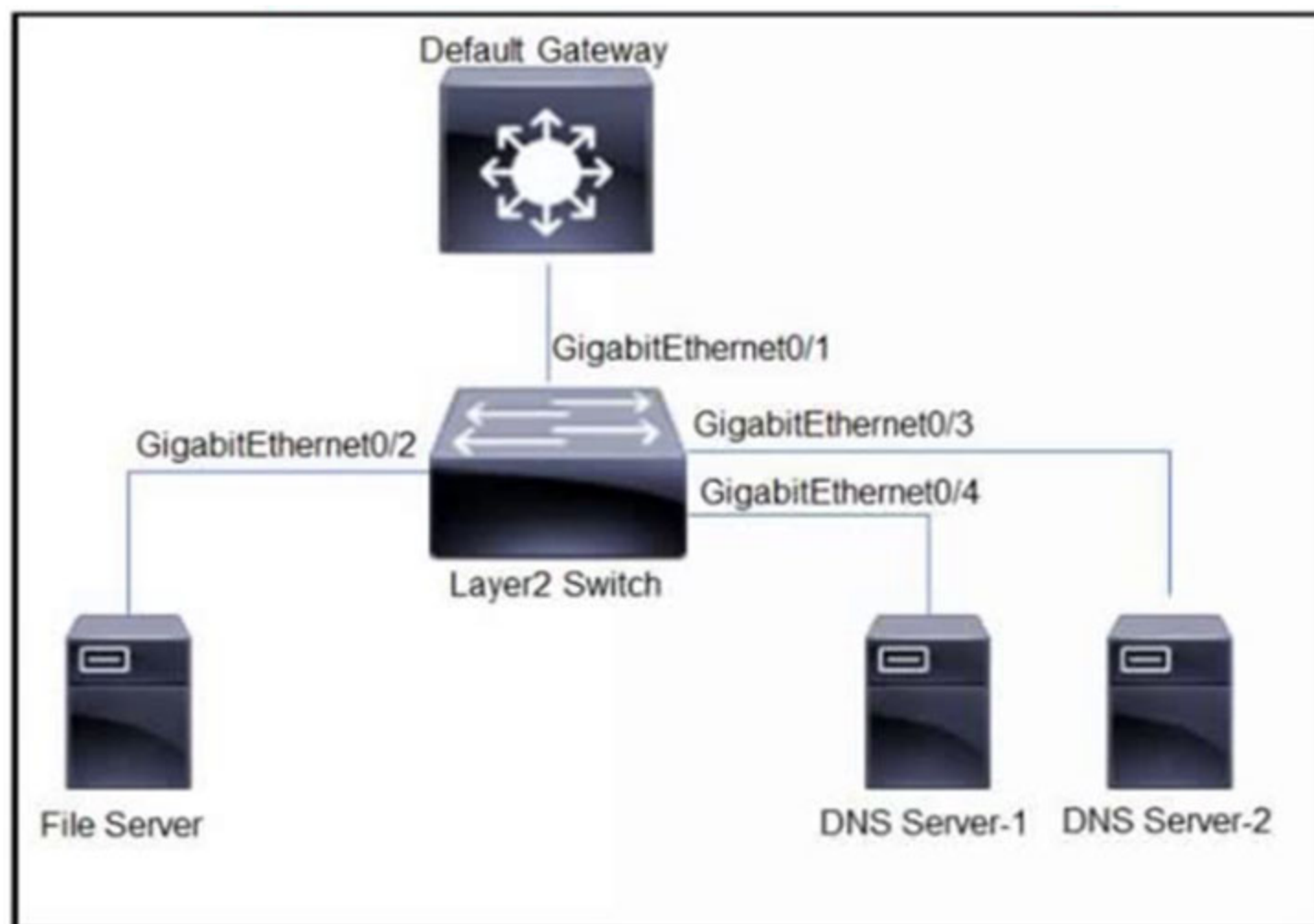


Actual exam question from Cisco's 350-701

Question #: 360

Topic #: 1

[\[All 350-701 Questions\]](#)



Refer to the exhibit. All servers are in the same VLAN/Subnet DNS Server-1 and DNS Server-2 must communicate with each other and all servers must communicate with default gateway multilayer switch. Which type of private VLAN ports should be configured to prevent communication between DNS servers and the file server?

- A. Configure GigabitEthernet0/1 as community port, GigabitEthernet0/2 as promiscuous port, GigabitEthernet0/3 and GigabitEthernet0/4 as isolated ports
- B. Configure GigabitEthernet0/1 as community port, GigabitEthernet0/2 as isolated port, and GigabitEthernet0/3 and GigabitEthernet0/4 as promiscuous ports
- C. Configure GigabitEthernet0/1 as promiscuous port, GigabitEthernet0/2 as community port, and GigabitEthernet0/3 and GigabitEthernet0/4 as isolated ports
- D. Configure GigabitEthernet0/1 as promiscuous port, GigabitEthernet0/2 as isolated port, and GigabitEthernet0/3 and GigabitEthernet0/4 as community ports

Show Suggested Answer

Actual exam question from Cisco's 350-701

Question #: 361

Topic #: 1

[\[All 350-701 Questions\]](#)

```
Interface: GigabitEthernet1/0/18
 IIF-ID: 0x14E3317D
 MAC Address: 0001.2e34.f101
 IPv6 Address: fe80::f86d:7f42:8d7b:58f3
 IPv4 Address: 192.168.41.7
 User-Name: 00-01-2E-34-F1-01
 Device-type: Microsoft-Workstation
 Status: Authorized
 Domain: DATA
 Oper host mode: multi-domain
 Oper control dir: both
 Session timeout: N/A
 Common Session ID: C0A82902000004CABED04789
 Acct Session ID: 0x00000039
 Handle: 0xd300004c
 Current Policy: POLICY_Gi1/0/18

Local Policies:
 Service Template: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150)
 Security Policy: Should Secure

Server Policies:

Method status list:
 Method      State
 dot1x       Stopped
 mab         Authc Success
```

Refer to the exhibit. Which configuration item makes it possible to have the AAA session on the network?

- A. aaa authentication enable default enable
- B. aaa authorization network default group ise
- C. aaa authentication login console ise
- D. aaa authorization exec default ise

Show Suggested Answer



Actual exam question from Cisco's 350-701

Question #: 362

Topic #: 1

[\[All 350-701 Questions\]](#)

Which method of attack is used by a hacker to send malicious code through a web application to an unsuspecting user to request that the victim's web browser executes the code?

- A. cross-site scripting
- B. browser WGET
- C. buffer overflow
- D. SQL injection

[Show Suggested Answer](#)





Actual exam question from Cisco's 350-701

Question #: 363

Topic #: 1

[\[All 350-701 Questions\]](#)

Which two solutions help combat social engineering and phishing at the endpoint level? (Choose two.)

- A. Cisco ISE
- B. Cisco Duo Security
- C. Cisco DNA Center
- D. Cisco Umbrella
- E. Cisco TrustSec

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 364

Topic #: 1

[\[All 350-701 Questions\]](#)

An engineer is implementing Cisco CES in an existing Microsoft Office 365 environment and must route inbound email to Cisco CES addresses. Which DNS record must be modified to accomplish this task?

- A. CNAME
- B. DKIM
- C. MX
- D. SPF

[Show Suggested Answer](#)





Actual exam question from Cisco's 350-701

Question #: 365

Topic #: 1

[\[All 350-701 Questions\]](#)

A large organization wants to deploy a security appliance in the public cloud to form a site-to-site VPN and link the public cloud environment to the private cloud in the headquarters data center. Which Cisco security appliance meets these requirements?

- A. Cisco Stealthwatch Cloud
- B. Cisco WSAv
- C. Cisco Cloud Orchestrator
- D. Cisco ASAv

[Show Suggested Answer](#)



Actual exam question from Cisco's 350-701

Question #: 366

Topic #: 1

[\[All 350-701 Questions\]](#)

```
ASA# show service-policy sfr

Global policy:
  Service-policy: global_policy
    Class=map: SFR
      SFR: card status Up, mode fail-open monitor-only
        packet input 0, packet output 44715478687, drop 0, reset-drop 0
```

Refer to the exhibit. What are two indications of the Cisco Firepower Services Module configuration? (Choose two.)

- A. The module is operating in IDS mode.
- B. Traffic is blocked if the module fails.
- C. The module fails to receive redirected traffic.
- D. The module is operating in IPS mode.
- E. Traffic continues to flow if the module fails.

Show Suggested Answer



Actual exam question from Cisco's 350-701

Question #: 367

Topic #: 1

[\[All 350-701 Questions\]](#)

Which two parameters are used to prevent a data breach in the cloud? (Choose two.)

- A. DLP solutions
- B. complex cloud-based web proxies
- C. strong user authentication
- D. antispoofing programs
- E. encryption

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 368

Topic #: 1

[\[All 350-701 Questions\]](#)

What is the concept of continuous integration/continuous delivery pipelining?

- A. The project code is centrally maintained, and each code change should trigger an automated build and test sequence.
- B. The project is split into time-limited cycles, and focuses on pair programming for continuous code review.
- C. The project is split into several phases where one phase cannot start before the previous phase finishes successfully.
- D. Each project phase is independent from other phases to maintain adaptiveness and continual improvement.

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 369

Topic #: 1

[\[All 350-701 Questions\]](#)

Which security solution uses NetFlow to provide visibility across the network, data center, branch offices, and cloud?

- A. Cisco Stealthwatch
- B. Cisco Encrypted Traffic Analytics
- C. Cisco Umbrella
- D. Cisco CTA

Show Suggested Answer



Actual exam question from Cisco's 350-701

Question #: 370

Topic #: 1

[\[All 350-701 Questions\]](#)

Which two functions does the Cisco Advanced Phishing Protection solution perform in trying to protect from phishing attacks? (Choose two.)

- A. uses a static algorithm to determine malicious
- B. determines if the email messages are malicious
- C. provides a defense for on-premises email deployments
- D. blocks malicious websites and adds them to a block list
- E. does a real-time user web browsing behavior analysis

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 371

Topic #: 1

[\[All 350-701 Questions\]](#)

Which technology provides the benefit of Layer 3 through Layer 7 innovative deep packet inspection, enabling the platform to identify and output various applications within the network traffic flows?

- A. Cisco ASA
- B. Account on Resolution
- C. Cisco NBAR2
- D. Cisco Prime Infrastructure

[Show Suggested Answer](#)



Actual exam question from Cisco's 350-701

Question #: 372

Topic #: 1

[\[All 350-701 Questions\]](#)

Which Cisco DNA Center Intent API action is used to retrieve the number of devices known to a DNA Center?

- A. GET `https://fqdnOrIPofDnaCenterPlatform/dna/intent/api/v1/network-device/count`
- B. GET `https://fqdnOrIPofDnaCenterPlatform/dna/intent/api/v1/network-device?parameter1=value¶meter2=value&...`
- C. GET `https://fqdnOrIPofDnaCenterPlatform/dna/intent/api/v1/network-device/startIndex/recordsToReturn`
- D. GET `https://fqdnOrIPofDnaCenterPlatform/dna/intent/api/v1/network-device`

Show Suggested Answer





Actual exam question from Cisco's 350-701

Question #: 373

Topic #: 1

[\[All 350-701 Questions\]](#)

Which function is performed by certificate authorities but is a limitation of registration authorities?

- A. CRL publishing
- B. certificate re-enrollment
- C. verifying user identity
- D. accepts enrollment requests

Show Suggested Answer

