DRAG DROP -

Drag and drop the Cisco WSA methods from the left onto the correct deployment modes on the right.

Select and Place:

| WPAD | **Transparent Mode** |
|------|----------------------|
| WCCP | |
| PAC | |
| PBR | **Explicit Mode** |
| | |

**Suggested Answer:**

| WPAD | **Transparent Mode** |
|------|----------------------|
| WCCP | WCCP |
| PAC | PBR |
| PBR | **Explicit Mode** |
| | PAC |
| | WPAD |

You could use an explicit setting (browser config/PAC/WPAD) or transparent (WCCP/PBR) to point to the first proxy and then the first proxy will route based on category to one of the two upstream proxies based on your policy configuration.

Reference:

https://community.cisco.com/t5/web-security/route-to-wsa-based-on-destination/td-p/2491179

⊟ 👤 **Certife_dumps5** 4 months ago

correct.

upvoted 1 times

What causes authentication failures on a Cisco WSA when LDAP is used for authentication?

A. when the passphrase contains only 5 characters

B. when the passphrase contains characters that are not 7-bit ASCI

C. when the passphrase contains one of following characters "~@ # $ % ^'

D. when the passphrase contains 50 characters

**Suggested Answer:** *B*

Reference:

https://www.cisco.com/c/en/us/td/docs/security/wsa/wsa11-0/user_guide/b_WSA_UserGuide/b_WSA_UserGuide_appendix_011001.html

*Community vote distribution*

B (100%)

---

👤 **Certife_dumps5** 4 months ago

Selected Answer: B

B is correct.

upvoted 1 times

👤 **c946f3e** 8 months ago

Selected Answer: B

Basic Authentication Fails

AsyncOS for Web only supports 7-bit ASCII characters for passphrases when using the Basic authentication scheme. Basic authentication fails when the passphrase contains characters that are not 7-bit ASCII.

upvoted 1 times

```
1278096903.150 97 172.xx.xx.xx TCP_MISS/200 8187 GET http://my.site.com/ -
DIRECT/my.site.com text/plain DEFAULT_CASE_11-AnalizeSuspectTraffic-Identity-OutboundMalwareScanningPolicy-
DataSecurity Policy-ExternalDLPPolicy-Routing Policy
<IW_comp,6.9,-,"-",-,-,-,-,"-",-,-,-,"-",-,-,"-","","-",-,-,IW_comp,-,"-","-",
"Unknown","Unknown","-","-",198.34,0,-,[Local],"-",37,"W32.CiscoTestVector",33,0,
"WSA-INFECTED-FILE.pdf","fd5ef49d4213e05f448f11ed9c98253d85829614fba368a421d14e64c426da5e"> -
```

Refer to the exhibit. Which statement about the transaction log is true?

    A. The log does not have a date and time

    B. The proxy had the content and did not contact other servers

    C. The transaction used TCP destination port 8187

    D. The AnalizeSuspectTraffic policy group was applied to the transaction

**Suggested Answer:** *D*

*Community vote distribution*

D (100%)

---

☐ 👤 **Certife_dumps5** *4 months ago*

<span style="background:#f2b01e">Selected Answer: D</span>

C is right.

  upvoted 1 times

☐ 👤 **[Removed]** *2 years, 1 month ago*

Not valid this dump, totally outdated

  upvoted 2 times

Which two features can be used with an upstream and downstream Cisco WSA web proxy to have the upstream WSA identify users by their client IP address?
(Choose two.)

A. X-Forwarded-For

B. high availability

C. web cache

D. via

E. IP spoofing

**Suggested Answer:** *AD*
Reference:
https://www.cisco.com/c/en/us/td/docs/security/wsa/wsa11-0/user_guide/b_WSA_UserGuide/b_WSA_UserGuide_chapter_0100.html

*Community vote distribution*

AD (100%)

☐ 👤 **Certife_dumps5** 4 months ago

Selected Answer: AD

A and D is exact answer.

upvoted 1 times

DRAG DROP -

Drag and drop the properties from the left onto the correct advanced web proxy setting descriptions on the right.

Select and Place:

**Answer Area**

| | |
|---|---|
| In-Use Connection Timeout | maximum time (in seconds) that the web proxy keeps open a connection to a client or server after a transaction has been completed and no further activity is detected |
| Simultaneous Persistent Connections | maximum time (in seconds) that the web proxy waits for more data from an idle client or server when the current transaction has not yet been completed |
| Use Received Headers | maximum number of TCP sockets that the web proxy keeps open with servers |
| Persistent Connection Timeout | allows an upstream web proxy to identify clients by IP address |

**Correct Answer:**

**Answer Area**

| | |
|---|---|
| In-Use Connection Timeout | Persistent Connection Timeout |
| Simultaneous Persistent Connections | In-Use Connection Timeout |
| Use Received Headers | Simultaneous Persistent Connections |
| Persistent Connection Timeout | Use Received Headers |

Reference:

https://www.cisco.com/c/en/us/td/docs/security/wsa/wsa11-0/user_guide/b_WSA_UserGuide/b_WSA_UserGuide_chapter_0100.html

Currently there are no comments in this discussion, be the first to comment!

Which two configuration options are available on a Cisco WSA within a decryption policy? (Choose two.)

A. Pass Through

B. Warn

C. Decrypt

D. Allow

E. Block

**Correct Answer:** *AC*
Reference:
https://www.cisco.com/c/en/us/td/docs/security/wsa/wsa11-
7/user_guide/b_WSA_UserGuide_11_7/b_WSA_UserGuide_11_7_chapter_01011.html

Currently there are no comments in this discussion, be the first to comment!

Which information in the HTTP request is used to determine if it is subject to the referrer exceptions feature in the Cisco WSA?

    A. protocol

    B. version

    C. header

    D. payload

**Correct Answer:** *C*

Requests for embedded content usually include the address of the site from which the request originated (this is known as the "referer" field in the request's HTTP header). This header information is used to determine categorization of the referred content.

Reference -
https://www.cisco.com/c/en/us/td/docs/security/wsa/wsa11-0/user_guide/b_WSA_UserGuide/b_WSA_UserGuide_chapter_01100.html

Currently there are no comments in this discussion, be the first to comment!

What is used to configure WSA as an explicit proxy?

A. IP Spoofing from router

B. Network settings from user browser

C. WCCP redirection from firewall

D. Auto redirection using PBR from switch

**Correct Answer:** *B*
Reference:
https://www.cisco.com/c/en/us/support/docs/security/web-security-appliance/117940-qa-wsa-00.html

Currently there are no comments in this discussion, be the first to comment!

Which key is needed to pair a Cisco WSA and Cisco ScanCenter for CTA?

A. public SSH key that the Cisco WSA generates

B. public SSH key that Cisco ScanCenter generates

C. private SSH key that Cisco ScanCenter generates

D. private SSH key that the Cisco WSA generates

**Correct Answer:** *A*
Reference:
https://www.cisco.com/c/en/us/td/docs/security/wsa/wsa11-0/user_guide/b_WSA_UserGuide/b_WSA_UserGuide_chapter_010111.html

Currently there are no comments in this discussion, be the first to comment!

What is a benefit of integrating Cisco Cognitive Threat Analytics with a Cisco WSA?

    A. It adds additional information to the Cisco WSA reports

    B. It adds additional malware protection to the Cisco WSA

    C. It provides the ability to use artificial intelligence to block viruses

    D. It reduces time to identify threats in the network

**Suggested Answer:** *B*
Reference:
https://www.ironportstore.com/datasheets/data_sheet_c78-729630.pdf

👤 **wfexco** 3 weeks, 5 days ago
Agreed D is the answer
  upvoted 4 times

👤 **samismayilov** 3 months, 1 week ago
It reduces time to identify threats in the network
--
Cisco Cognitive Threat Analytics is a cloud-based solution that reduces time to discovery of threats operating inside the network. It addresses gaps in perimeter-based defenses by identifying the symptoms of a malware infection or data breach using behavioral analysis and anomaly detection. Take advantage of Cisco Cognitive Threat Analytics with a simple add-on license to your Web Security solution. Reduce complexity while gaining superior protection that evolves with your changing threat landscape
  upvoted 4 times

Which method is used by AMP against zero-day and targeted file-based attacks?

A. analyzing behavior of all files that are not yet known to the reputation service

B. periodically evaluating emerging threats as new information becomes available

C. implementing security group tags

D. obtaining the reputation of known files

**Suggested Answer:** *D*

Reference:
https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/advanced-malware-protection/solution-overview-c22-734228.html

 **wfexco** 3 weeks, 5 days ago
D is the Answer -
The reason A is not the answer is that it says " of ALL files"

Advanced Malware Protection protects against zero-day and targeted file-based threatsby:

Obtaining the reputation of known files.

Analyzing behavior of certain files that are not yet known to the reputation service.

Continuously evaluating emerging threats as new information becomes available, and notifying you about files that are determined to be threats after they have entered your network.
upvoted 2 times

 **Spardaefit** 1 month ago
D is correct, Advanced Malware Protection protects against zero-day and targeted file-based threats in email attachments by:

Obtaining the reputation of known files.
Analyzing behavior of certain files that are not yet known to the reputation service.
Continuously evaluating emerging threats as new information becomes available, and notifying you about files that are determined to be threats after they have entered your network.
https://www.cisco.com/c/en/us/td/docs/security/esa/esa13-5/user_guide/b_ESA_Admin_Guide_13-
5/b_ESA_Admin_Guide_12_1_chapter_010001.html
upvoted 3 times

 **vyskopepek** 1 month, 3 weeks ago
it is IMHO A - as obtaining reputation of the known files will not help you with zero day attacks
upvoted 2 times

Which behavior is seen while the policy trace tool is used to troubleshoot a Cisco WSA?

A. External DLP polices are evaluated by the tool

B. A real client request is processed and an EUN page is displayed

C. SOCKS policies are evaluated by the tool

D. The web proxy does not record the policy trace test requests in the access log when the tool is in use

**Correct Answer:** *D*
Reference:
https://www.cisco.com/c/en/us/td/docs/security/wsa/wsa11-0/user_guide/b_WSA_UserGuide/
b_WSA_UserGuide_appendix_011001.html#con_1415277

Currently there are no comments in this discussion, be the first to comment!

What are all of the available options for configuring an exception to blocking for referred content?

A. all embedded/referred and all embedded/referred except

B. selected embedded/referred except, all embedded/referred, and selected embedded/referred

C. selected embedded/referred and all embedded/referred except

D. all embedded/referred, selected embedded/referred, and all embedded/referred except

**Correct Answer:** *D*
Reference:
https://www.cisco.com/c/en/us/td/docs/security/wsa/wsa11-7/user_guide/b_WSA_UserGuide_11_7/b_WSA_UserGuide_11_7_chapter_01001.html
(procedure)

Currently there are no comments in this discussion, be the first to comment!

Which statement about the SOCKS proxy is true?

A. SOCKS is a general purpose proxy

B. SOCKS operates on TCP port 80, 443, and 8334

C. SOCKS is used only for traffic that is redirected through a firewall

D. SOCKS is used for UDP traffic only

**Correct Answer:** *A*
Reference:
http://www.jguru.com/faq/view.jsp?EID=227532

Currently there are no comments in this discussion, be the first to comment!

Which two parameters are mandatory to control access to websites with proxy authentication on a Cisco WSA? (Choose two.)

 A. External Authentication

 B. Identity Enabled Authentication

 C. Transparent User Identification

 D. Credential Encryption

 E. Authentication Realm

**Suggested Answer:** *DE*
Reference:

https://www.cisco.com/c/en/us/td/docs/security/wsa/wsa11-7/user_guide/b_WSA_UserGuide_11_7/b_WSA_UserGuide_11_7_appendix_010111.html

👤 **ahmadakim** `Highly Voted 👍` 6 months, 2 weeks ago
BE.
it is not credential encryption
upvoted 6 times

　👤 **Spardaefit** 3 weeks, 3 days ago
　Credential encryption is optional
　upvoted 2 times

What is a valid predefined time range when configuring a Web Tracking query?

A. year

B. minute

C. hour

D. month

**Suggested Answer:** *B*
Web tracking query uses minute as a predefined time range to track web related queries.

□ 👤 **Spardaefit** 1 month, 1 week ago
B is correct, -->Web tracking query uses minute as a predefined time range to track web related queries
.
upvoted 1 times

□ 👤 **samismayilov** 3 months, 1 week ago
answer is C. hour
upvoted 3 times

□ 👤 **ahmadakim** 6 months, 2 weeks ago
from gui wsa.... houe,day,week,30days
upvoted 3 times

□ 👤 **ahmadakim** 6 months, 2 weeks ago
from gui wsa. web tracking is . hour,day,week,30
upvoted 1 times

When a Cisco WSA is installed with default settings, which port is assigned to the web proxy if the M1 port is used exclusively for management?

A. T1

B. P2

C. T2

D. P1

**Correct Answer:** *D*
Reference:
https://www.cisco.com/c/en/us/td/docs/security/wsa/wsa11-
5/user_guide/b_WSA_UserGuide_11_5_1/b_WSA_UserGuide_11_5_1_chapter_01.html

Currently there are no comments in this discussion, be the first to comment!

Which configuration option is suitable for explicit mode deployment?

A. PAC

B. WCCP

C. ITD

D. PBR

**Correct Answer:** *A*
In explicit-mode deployment, users will point the proxy setting to WSA. This can be done by pointing directly to WSA or via a PAC (Proxy Auto-Config) file.

Currently there are no comments in this discussion, be the first to comment!

By default, which two pieces of information does the Cisco WSA access log contain? (Choose two.)

A. HTTP Request Code

B. Content Type

C. Client IP Address

D. User Agent

E. Transaction ID

**Correct Answer:** *AC*

Currently there are no comments in this discussion, be the first to comment!

Which two sources provide data to Cisco Advanced Web Security Reporting to create dashboards? (Choose two.)

A. Cisco WSA devices

B. Cisco ISE

C. Cisco ASAv

D. Cisco Security MARS

E. Cisco Cloud Web Security gateways

**Correct Answer:** *AE*
Reference:
https://www.cisco.com/c/dam/en/us/td/docs/security/wsa/Advanced_Reporting/WSA_Advanced_Reporting_6/
Advanced_Web_Security_Reporting_6_1.pdf

Currently there are no comments in this discussion, be the first to comment!

Which statement about Cisco Advanced Web Security Reporting integration is true?

A. AWSR uses IP addresses to differentiate Cisco WSA deployments

B. AWSR does not require a license to index data

C. AWSR can remove log files after they are indexed

D. AWSR installation is CLI-based on Windows and Red Hat Linux systems

**Correct Answer:** *D*

Reference:

https://www.cisco.com/c/dam/en/us/td/docs/security/wsa/Advanced_Reporting/WSA_Advanced_Reporting_7/
Advanced_Web_Security_Reporting_7_0.pdf

Currently there are no comments in this discussion, be the first to comment!

A user browses to a company website that is categorized as "Business and Industry" and contains a Facebook post. The user cannot see the Facebook post because the category "Social Networking" is blocked.

Which configuration allows the user to see the Facebook post?

A.

*A web site may embed or refer to content that is categorized as a different category, or that is considered an application. For example, a News web site could contain content categorized as Streaming Video, and the action selected for its own category/application, regardless of what web site it is embedded in. Use this table to set exceptions (e.g., to permit all content referred from News web sites, or from a custom category.)*

☑ Enable Referrer Exceptions

| Set Exception for Content Referred by These Categories: | Set Exception for This Referred Content: |
|---|---|
| Business and Industry | selected embedded / referred content ∨   Categories: Social Networking    Applications: Click to select applications... |

B.

*A web site may embed or refer to content that is categorized as a different category, or that is considered an application. For example, a News web site could contain content categorized as Streaming Video, and the action selected for its own category/application, regardless of what web site it is embedded in. Use this table to set exceptions (e.g., to permit all content referred from News web sites, or from a custom category.)*

☑ Enable Referrer Exceptions

| Set Exception for Content Referred by These Categories: | Set Exception for This Referred Content: |
|---|---|
| Social Networking | All embedded / referred content ∨ |

C.

*A web site may embed or refer to content that is categorized as a different category, or that is considered an application. For example, a News web site could contain content categorized as Streaming Video, and the action selected for its own category/application, regardless of what web site it is embedded in. Use this table to set exceptions (e.g., to permit all content referred from News web sites, or from a custom category.)*

☑ Enable Referrer Exceptions

| Set Exception for Content Referred by These Categories: | Set Exception for This Referred Content: |
|---|---|
| Social Networking | All embedded / referred content except ∨   Categories: Business and Industry    Applications: Click to select applications... |

D.

*A web site may embed or refer to content that is categorized as a different category, or that is considered an application. For example, a News web site could contain content categorized as Streaming Video, and the action selected for its own category/application, regardless of what web site it is embedded in. Use this table to set exceptions (e.g., to permit all content referred from News web sites, or from a custom category.)*

☑ Enable Referrer Exceptions

| Set Exception for Content Referred by These Categories: | Set Exception for This Referred Content: |
|---|---|
| Business and Industry | All embedded / referred content except ∨   Categories: Social Networking    Applications: Click to select applications... |

**Correct Answer:** *A*

Reference:

https://www.cisco.com/c/en/us/td/docs/security/wsa/wsa11-7/user_guide/b_WSA_UserGuide_11_7/b_WSA_UserGuide_11_7_chapter_01001.html

Currently there are no comments in this discussion, be the first to comment!

Which two types of reports are scheduled on the Cisco WSA to analyze traffic? (Choose two.)

    A. Layer 3 traffic monitor

    B. URL categories

    C. host statistics

    D. application visibility

    E. system capacity

**Suggested Answer:** *AD*
Reference:
https://www.cisco.com/c/en/us/td/docs/security/wsa/wsa11-0/user_guide/b_WSA_UserGuide/b_WSA_UserGuide_chapter_010101.pdf
(8)

👤 **jeromvdhoek** 2 months ago

L3 Traffic monitor should be L4 Traffic monitor, if that is adjusted then the answer is correct.

upvoted 2 times

👤 **ahmjrd** 7 months, 2 weeks ago

B and D are the correct answers

upvoted 2 times

👤 **Mcamacho27** 1 year, 2 months ago

B and D are the correct answer. Layer 3 Traffic Monitor does not exist,

upvoted 1 times

👤 **ahmadakim** 2 years, 6 months ago

B and D

You can schedule reports to run on a daily, weekly, or monthly basis. Scheduled reports can be configured to include data for the previous day, previous seven days, or previous month.

You can schedule reports for the following types of reports:

Overview
Users
Web Sites
URL Categories
Application Visibility
Anti-Malware
Advanced Malware Protection
Advanced Malware Protection Verdict Updates
Client Malware Risk
Web Reputation Filters
L4 Traffic Monitor
SOCKS Proxy
Reports by User Location
System Capacity
My Dashboard

upvoted 4 times

    👤 **samismayilov** 2 years, 3 months ago

    yes . B and D

    upvoted 3 times

        👤 **funnnny** 1 year, 10 months ago

        A & D is also correct , refer to the list above

        upvoted 1 times

**funnnny** 1 year, 10 months ago

B and D

**funnnny** 1 year, 10 months ago

B and D

What must be configured first when creating an access policy that matches the Active Directory group?

- A. authentication, authorization, and accounting of groups

- B. FQDN specification

- C. authentication realm

- D. authorized groups specification

**Suggested Answer:** *C*

Reference:

https://www.cisco.com/c/en/us/support/docs/security/web-security-appliance/118005-configure-ntlm-00.html

👤 **Zoli6** 1 month, 2 weeks ago

How do I create Access Policy Groups that match Active Directory (AD) Groups?

The first step is to configure an authentication realm (NT LAN Manager (NTLM) realm) and an Identity which uses the authentication realm.
upvoted 3 times

👤 **ahmadakim** 6 months, 2 weeks ago

D.

question ask about when creating access policy and not when creating identification profile
upvoted 1 times

Which certificate format does a Cisco WSA need when HTTPS proxy is configured?

A. DER

B. CER

C. PEM

D. CRL

**Suggested Answer:** *C*

Reference:

https://community.cisco.com/t5/security-documents/wsa-training-series-how-to-configure-the-https-proxy-on-the/ta-p/3148673

👤 **ahmjrd** 1 month, 2 weeks ago

The Web Proxy uses the first certificate or key in the file. The certificate file must be in PEM format.

DER format is not supported

upvoted 1 times

DRAG DROP -

Drag and drop the actions from the left into the correct order on the right in which they occur as an HTTPS session passes through the Cisco WSA.

Select and Place:

**Answer Area**

| | |
|---|---|
| Server replies with server certificate to Cisco WSA | step 1 |
| Encryption data channel is established | step 2 |
| Client sends the session key, which is encrypted by using public key of the server certificate | step 3 |
| Client sends a hello message to Cisco WSA | step 4 |
| Cisco WSA replies with a proxied certificate of the destination server to the client | step 5 |

**Suggested Answer:**

**Answer Area**

| | |
|---|---|
| Server replies with server certificate to Cisco WSA | Client sends a hello message to Cisco WSA |
| Encryption data channel is established | Client sends the session key, which is encrypted by using public key of the server certificate |
| Client sends the session key, which is encrypted by using public key of the server certificate | Encryption data channel is established |
| Client sends a hello message to Cisco WSA | Cisco WSA replies with a proxied certificate of the destination server to the client |
| Cisco WSA replies with a proxied certificate of the destination server to the client | Server replies with server certificate to Cisco WSA |

😐 👤 **ahmjrd** 1 month, 2 weeks ago

[1] Client sent hello message to cisco wsa

( WSA is trying to find if the server certificate is valid )

[2] server replies with server certificate to Cisco WSA

[3] Cisco WSA replies with a proxied certificate of the destination server to the client.

[4] Client sends the session key, wich is encrypted by using public key of the server certificate.

[5] Encrypted data channel is stablished.

upvoted 2 times

😐 👤 **vyskopepek** 1 year, 8 months ago

How can it reply with server certificate key in step 2 when the key is received in step 5? this is incorrect!

upvoted 1 times

   😐 👤 **Spardaefit** 1 year, 7 months ago

   In fact it´s correct, the step says - client sends the session key, wich is encrypted using ---------public key------ of the ------server certificate----------.

   Every one can use the public key of a public server, because as the name say ¡its public!. Be careful when you read a question, in Cisco always have a tricky word.

   upvoted 1 times

      😐 👤 **Spardaefit** 1 year, 7 months ago

The order most be:

-Client sent hello message to cisco wsa

--server replies with server certificate to Cisco WSA

-Cisco WSA replies with a proxied certificate of the destination server to the client.

-Client sends the session key, wich is encrypted by using public key of the server certificate.

-Encrypted data channel is stablished.

upvoted 6 times

☐ 👤 **funnnny** 1 year, 4 months ago

then what is the correct answser ? is ot the one on the capture or the one on your last response ?

upvoted 1 times

Which command is used to flush a single user from authentication memory?

A. isedata

B. authcache

C. diagnostic

D. clear

**Correct Answer:** *B*
Reference:
https://www.cisco.com/c/en/us/support/docs/security/web-security-appliance/118259-technote-wsa-00.html

Currently there are no comments in this discussion, be the first to comment!

Which two caches must be cleared on a Cisco WSA to resolve an issue in processing requests? (Choose two.)

A. authentication cache

B. application cache

C. logging cache

D. DNS cache

E. HTTP cache

**Correct Answer:** *AD*
Reference:
https://www.cisco.com/c/en/us/support/docs/security/web-security-appliance/118259-technote-wsa-00.html

Currently there are no comments in this discussion, be the first to comment!