300-725.VCEplus.premium.exam.60q

Number: 300-725
Passing Score: 800
Time Limit: 120 min
File Version: 1.0

300-725

Securing the Web with Cisco Web Security Appliance

Version 1.0

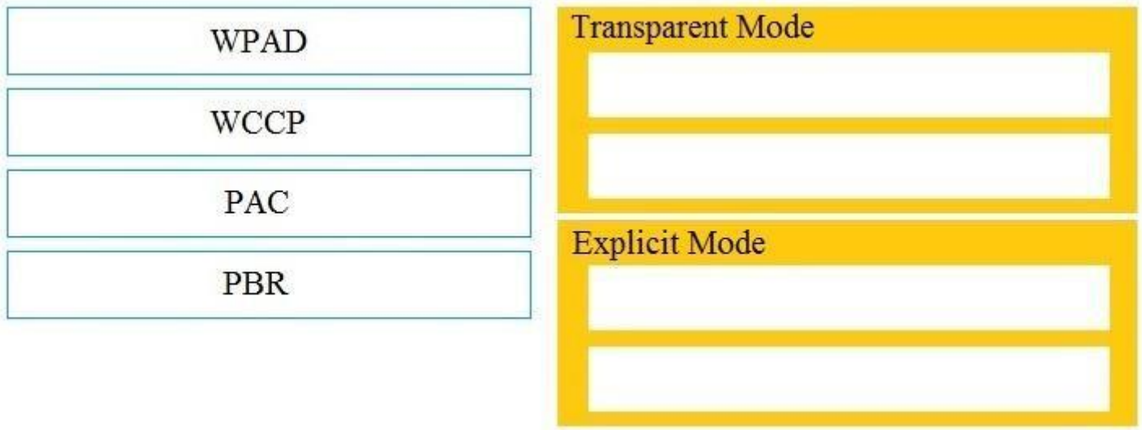
Exam A

QUESTION 1

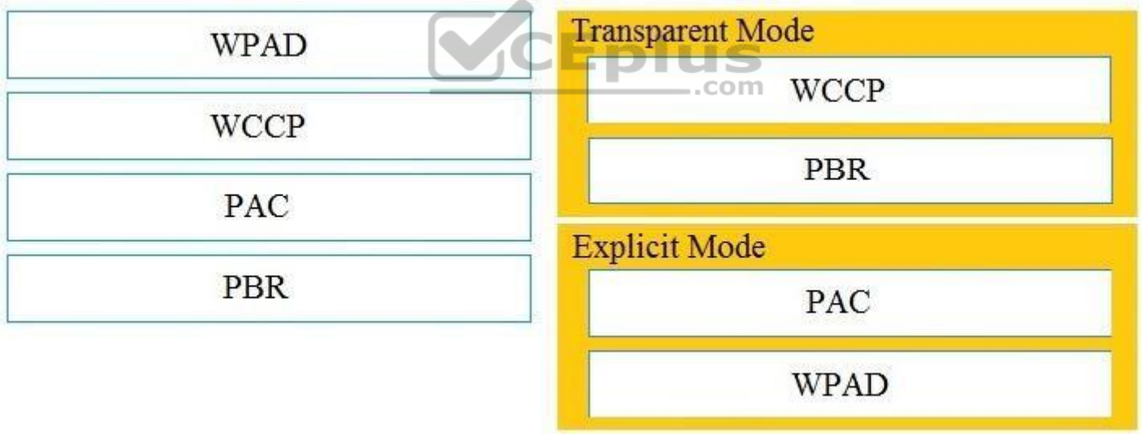
DRAG DROP

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

Select and Place:



Correct Answer:



Section: (none)
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 2 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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
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

QUESTION 3

```
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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 4
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

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:
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

QUESTION 5
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

Section: (none)
Explanation

Explanation/Reference:

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 **QUESTION 6**
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
Section: (none)
Explanation

Explanation/Reference:
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

QUESTION 7
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
Section: (none)
Explanation

Explanation/Reference:
Explanation:
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

QUESTION 8 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
Section: (none)
Explanation

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

QUESTION 9 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
Section: (none)
Explanation

Explanation/Reference:
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

QUESTION 10 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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.ironportstore.com/datasheets/data_sheet_c78-729630.pdf

QUESTION 11 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

Correct Answer: D
Section: (none)
Explanation

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

QUESTION 12 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
Section: (none)
Explanation

Explanation/Reference:
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

QUESTION 13 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
Section: (none)
Explanation

Explanation/Reference:
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)

QUESTION 14 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
Section: (none)
Explanation

Explanation/Reference:
Reference: http://www.jguru.com/faq/view.jsp?EID=227532

QUESTION 15 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

Correct Answer: DE
Section: (none)
Explanation

Explanation/Reference:
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

QUESTION 16 What is a valid predefined time range when configuring a Web Tracking query?

A. year
B. minute
C. hour
D. month

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Web tracking query uses minute as a predefined time range to track web related queries.

QUESTION 17
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
Section: (none)
Explanation

Explanation/Reference:
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

QUESTION 18 Which configuration option is suitable for explicit mode deployment?

A. PAC
B. WCCP
C. ITD
D. PBR

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
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.

QUESTION 19 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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 20 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

Section: (none)
Explanation

Explanation/Reference:
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

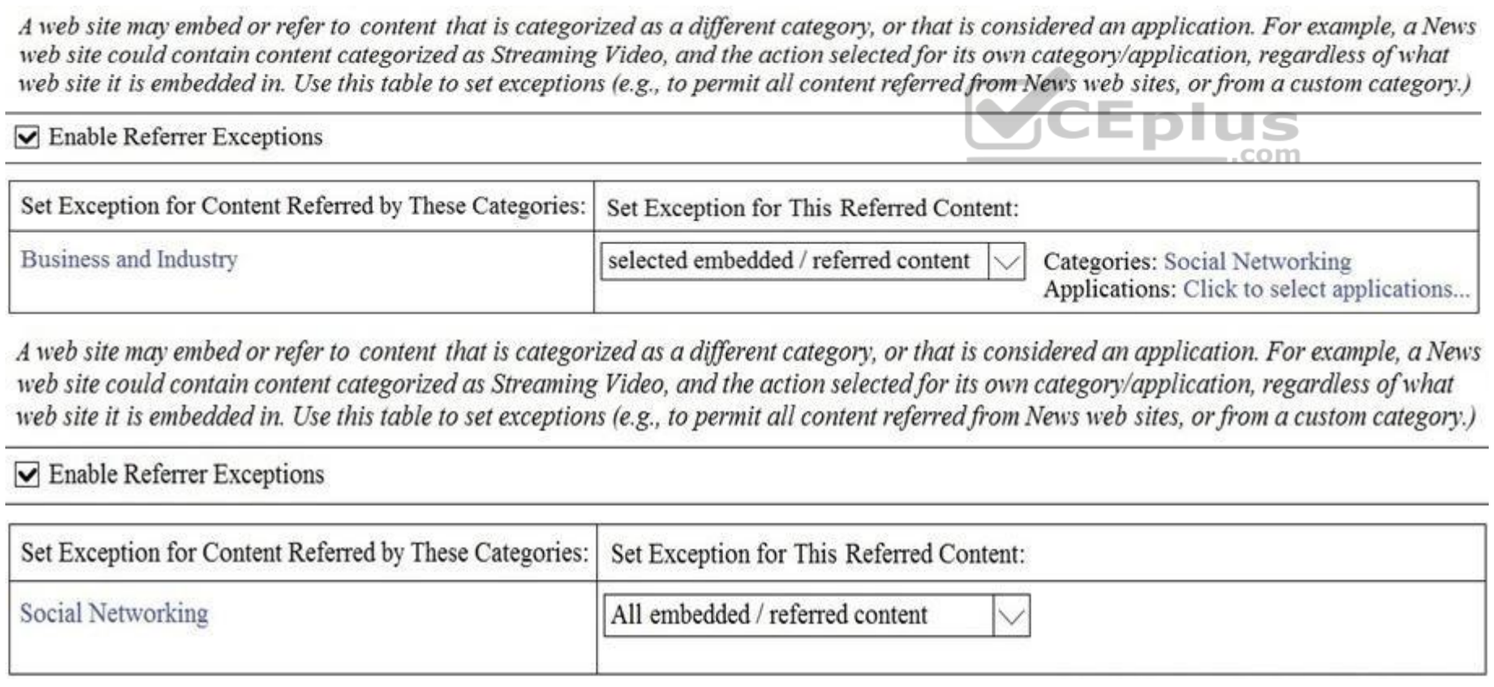
QUESTION 21 Which statement about Cisco Advanced Web Security Reporting integration is true?

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
Section: (none)
Explanation

Explanation/Reference:
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

QUESTION 22
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.



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 except ▽ Categories: Business and Industry Applications: Click to select applications...

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...

C.

D.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
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

QUESTION 23 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

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:
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)

QUESTION 24 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

Correct Answer: C
Section: (none)
Explanation

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

QUESTION 25 Which certificate format does a Cisco WSA need when HTTPS proxy is configured?

A. DER
B. CER
C. PEM
D. CRL

Correct Answer: C
Section: (none)
Explanation

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

QUESTION 26
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

Correct 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

Section: (none)
Explanation

Explanation/Reference:

QUESTION 27 Which command is used to flush a single user from authentication memory?

A. **isedata**
B. **authcache**
C. **diagnostic**
D. **clear**

Correct Answer: B
Section: (none)
Explanation

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

QUESTION 28 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
Section: (none)
Explanation
Explanation/Reference:
Reference: https://www.cisco.com/c/en/us/support/docs/security/web-security-appliance/118259-technote-wsa-00.html

QUESTION 29 How does the Cisco WSA choose which scanning engine verdict to use when there is more than one verdict?

A. based on the least restrictive verdict
B. based on the most restrictive verdict
C. based on the first verdict returned
D. based on the last verdict returned

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.cisco.com/c/en/us/td/docs/security/wsa/wsa11-0/user_guide/b_WSA_UserGuide/b_WSA_UserGuide_chapter_010000.html

QUESTION 30 Which statement about configuring an identification profile for machine authentication is true?

A. Cloud Web Security Connector mode with an active directory enabled supports machine authentication
B. Identification profile machine ID is supported locally, but the Cisco WSA does not support machine ID authentication
C. Cloud Web Security with Kerberos enabled supports machine authentication
D. If an Active Directory realm is used, identification can be performed for an authenticated user or IP address but not for a machine ID

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.cisco.com/c/en/us/td/docs/security/wsa/wsa11-0/user_guide/b_WSA_UserGuide/b_WSA_UserGuide_chapter_01001.html

QUESTION 31 Which two benefits does AMP provide compared to the other scanning engines on the Cisco WSA?
(Choose two.)

A. protection against malware
B. protection against zero-day attacks
C. protection against spam
D. protection against viruses
E. protection against targeted file-based attacks

Correct Answer: BD
Section: (none)
Explanation

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

QUESTION 32

```
Currently configured logs:
1. "accesslogs" Type: "Access Logs" Retrieval: FTP Poll
2. "amp logs" Type: "AMP Engine Logs" Retrieval: FTP Poll
3. "authlogs" Type: "Authentication Framework Logs" Retrieval: FTP Poll
4. "avc_logs" Type: "AVC Engine Logs" Retrieval: FTP Poll
5. "bypasslogs" Type: "Proxy Bypass Logs" Retrieval: FTP Poll
...
42. "webcat_logs" Type: "Web Categorization Logs" Retrieval: FTP Poll
43. "webrootlogs" Type: "Webroot Logs" Retrieval: FTP Poll
44. "welcomeack_logs" Type: "Welcome Page Acknowledgement Logs" Retrieval: FTP Poll
Enter the number of the log you wish to grep.
[]> 1
Enter the regular expression to grep.
[]> domain.com
Do you want this search to be case insensitive? [Y]>
Do you want to search for non-matching lines? [N]>
Do you want to tail the logs? (N]>
Do you want to paginate the output? [N]>
```

Refer to the exhibit. Which command displays this output?

A. **grep**
B. **logconfig**
C. **rollovernow**
D. **tail**

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.cisco.com/c/en/us/support/docs/security/web-security-appliance/117938-configure-wsa-00.html

QUESTION 33 Which information within Cisco Advanced Web Security Reporting is used to generate a report that lists visited domains?

A. URL categories
B. web reputation
C. websites
D. application visibility

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.cisco.com/c/dam/en/us/td/docs/security/wsa/Advanced_Reporting/WSA_Advanced_Reporting_6/Advanced_Web_Security_Reporting_6_6.pdf (39) **QUESTION 34** What is required on the Cisco WSA when an AMP file reputation server private cloud is configured?

A. private key from the server to encrypt messages
B. private key to decrypt messages
C. public and private keys from the server
D. public key from the server

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.cisco.com/c/en/us/td/docs/security/wsa/wsa11-0/user_guide/b_WSA_UserGuide/b_WSA_UserGuide_chapter_010001.html

QUESTION 35 Which IP address and port are used by default to run the system setup wizard?

A. http://192.168.42.42:80
B. https://192.168.42.42:8080
C. https://192.168.42.10:8443
D. http://192.168.43.42:8080

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.cisco.com/c/dam/en/us/td/docs/security/content_security/hardware/x95_series/Sx95_GSG.pdf (14)

QUESTION 36 What is the function of a PAC file on a Cisco WSA?

A. The file allows redirection of web traffic to a specific proxy server
B. The file is mandatory for a transparent proxy to redirect user traffic
C. The file provides instructions about which URL categories are permitted
D. The file is mandatory for an explicit proxy to forward user traffic

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wlan-security/116052-config-webauth-proxy-00.html

QUESTION 37 Which two modes of operation does the Cisco WSA provide?
(Choose two.)

A. connector
B. proxy
C. transparent
D. standard
E. explicit

Correct Answer: CE
Section: (none)
Explanation
Explanation/Reference:
Reference: https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/Aug2013/CVD-WebSecurityUsingCiscoWSADesignGuide-AUG13.pdf

QUESTION 38 Which response code in the access logs indicates that a transaction was blocked due to policy?

A. TCP_DENIED/407
B. TCP_DENIED/401C. TCP_DENIED/403
D. TCP_DENIED/307

Correct Answer: A
Section: (none)
Explanation
Explanation/Reference:
Reference: https://docuri.com/download/instructions_59a8d562f581719e12ad43fe_pdf

QUESTION 39 Which two features on the Cisco WSA help prevent outbound data loss for HTTP or FTP traffic?
(Choose two.)

A. web reputation filters
B. Advanced Malware Protection
C. third-party DLP integration
D. data security filters
E. SOCKS proxy

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:
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_010000.pdf

QUESTION 40 Which configuration mode does the Cisco WSA use to create an Active Directory realm for Kerberos authentication?

A. Forward
B. Connector
C. Transparent
D. Standard

Correct Answer: D

Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.cisco.com/c/en/us/td/docs/security/wsa/wsa11-0/user_guide/b_WSA_UserGuide/b_WSA_UserGuide_chapter_01001.html#con_1406137

QUESTION 41 Which statement about identification profile default settings on the Cisco WSA is true?

A. Identification profiles do not require authentication
B. Guest identification profile should be processed first
C. Identification profiles can include only one user group
D. AsyncOS processes identification profiles alphabetically

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.cisco.com/c/en/us/td/docs/security/wsa/wsa11-0/user_guide/b_WSA_UserGuide/b_WSA_UserGuide_chapter_011001.html#con_1415970

QUESTION 42
Which action is a valid default for the Global Access Policy in the Application Visibility Control engine on the Cisco WSA?

A. bandwidth limit
B. permit
C. restrict
D. monitor

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://hrouhani.org/cisco-web-security-appliance-ironport/

QUESTION 43
A network administrator noticed that all traffic that is redirected to the Cisco WSA from the Cisco ASA firewall cannot get to the Internet in a Transparent proxy environment using WCCP.

Which troubleshooting action must be taken on the CLI to make sure that WCCP communication is not failing?

A. Disable WCCP to see if the WCCP service is causing the issue
B. Explicitly point the browser to the proxy
C. Ping the WCCP device
D. Check WCCP logs in debug mode

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 44
DRAG DROP

Drag and drop the Cisco WSA access policy elements from the left into the order in which they are processed on the right.

Select and Place:

Answer Area

custom URL category	action 1
malware scanning	action 2
MIME type filter	action 3
application filter	action 4
URL category	action 5

Correct Answer:

Answer Area

custom URL category	application filter
malware scanning	MIME type filter
MIME type filter	malware scanning
application filter	URL category
URL category	custom URL category

Section: (none)
Explanation

Explanation/Reference:

QUESTION 45 What must be configured to require users to click through an acceptance page before they are allowed to go to the Internet through the Cisco WSA?

A. Enable End-User Acknowledgement Page and set to *Required* in Identification Profiles
B. Enable End -User URL Filtering Warning Page and set to *Required* in Identification Profiles
C. Enable End-User Acknowledgement Page and set to *Required* in Access Policies
D. Enable End-User URL Filtering Warning Page and set to *Required* in Access Policies

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

Reference: https://www.cisco.com/c/en/us/td/docs/security/wsa/wsa11-0/user_guide/b_WSA_UserGuide/b_WSA_UserGuide_chapter_010100.html **QUESTION 46** What is the default action when a new custom category is created and added to an access policy?

A. monitor
B. allow
C. block
D. decrypt

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
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

QUESTION 47 Which type of FTP proxy does the Cisco WSA support?

A. non-native FTP
B. FTP over UDP tunneling
C. FTP over HTTP
D. hybrid FTP

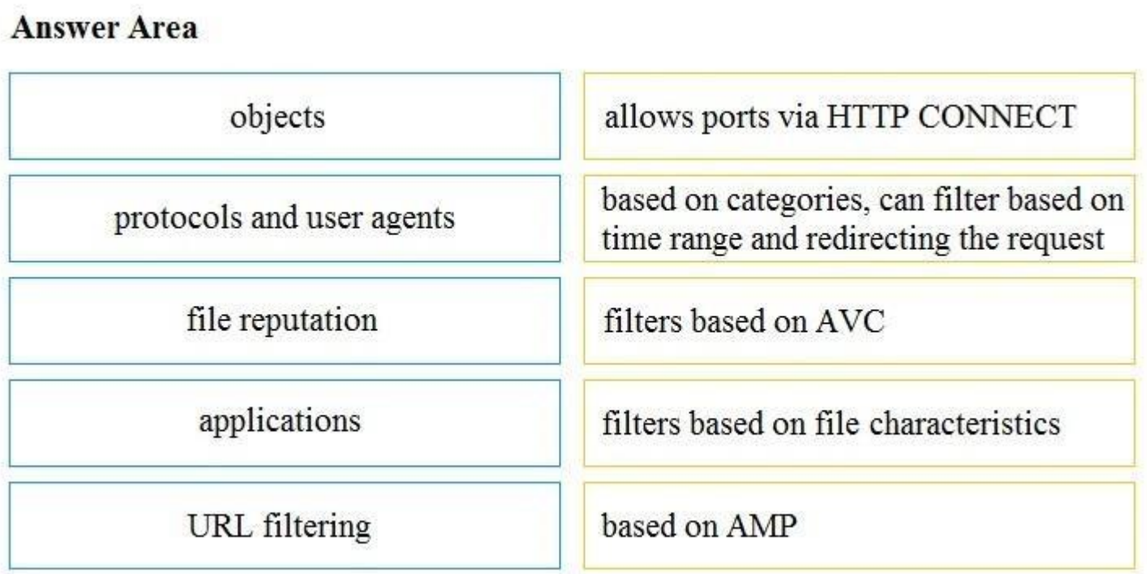
Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.cisco.com/c/en/us/support/docs/security/web-security-appliance/117984-qanda-wsa-00.html

QUESTION 48
DRAG DROP

Drag and drop the access policy options from the left onto the correct descriptions on the right.

Select and Place:



Correct Answer:

Answer Area

objects	protocols and user agents
protocols and user agents	URL filtering
file reputation	applications
applications	objects
URL filtering	file reputation

Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.cisco.com/c/en/us/td/docs/security/wsa/wsa11-0/user_guide/b_WSA_UserGuide/b_WSA_UserGuide_chapter_01101.pdf (10)

QUESTION 49 An administrator wants to restrict file uploads to Facebook using the AVC feature.

Under which two actions must the administrator apply this restriction to an access policy? (Choose two.)

A. Monitor Facebook General
B. Monitor Social Networking
C. Monitor Facebook Photos and Videos
D. Monitor Facebook Messages and Chat
E. Monitor Facebook Application

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.cisco.com/c/en/us/products/collateral/security/web-security-appliance/datasheet-c78-741272.html

QUESTION 50 Which two caching modes are available in the Cisco WSA?
(Choose two.)

A. active cache
B. all cache
C. aggressive cache
D. safe cache
E. no cache

Correct Answer: CD

Section: (none)
Explanation

Explanation/Reference:
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_0100.html#task_1214899

QUESTION 51 How does dynamic content analysis improve URL categorization?

A. It analyzes content based on cached destination content
B. It adds intelligence to detect categories by analyzing responses
C. It can be used as the only URL analysis method
D. It analyzes content of categorized URL to tune decisions and correct categorization errors

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.cisco.com/c/en/us/support/docs/security/web-security-appliance/118063-qanda-wsa-00.html

QUESTION 52
What is needed to enable an HTTPS proxy?

A. self-signed server certificate
B. trusted third-party CA signed root certificate
C. self-signed CSR
D. self-signed root certificate

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: https://community.cisco.com/t5/web-security/cisco-wsa-https-proxy-certificate-issue/td-p/3019392

QUESTION 53
Which two configuration options can be configured when invalid certificates are processed with the HTTPS proxy on WSA enabled? (Choose two.)

A. allow
B. monitor
C. drop
D. block
E. redirect

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:
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

QUESTION 54 What is the purpose of using AMP file analysis on a Cisco WSA to continuously evaluate emerging threats?

A. to take appropriate action on new files that enter the network
B. to remove files from quarantine by stopping their retention period

C. to notify you of files that are determined to be threats after they have entered your network
D. to send all files downloaded through the Cisco WSA to the AMP cloud

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
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_01110.html

QUESTION 55 Which type of certificate must be installed on a Cisco WSA for HTTPS inspection?

A. server
B. client
C. root
D. wildcard

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.cisco.com/c/en/us/support/docs/security/web-security-appliance/117792-technote-wsa-00.html

QUESTION 56
Which two log types does the Cisco WSA provide to troubleshoot Cisco data security and external data loss prevention policies? (Choose two.)

A. upload data
B. data security
C. default proxyD. data access
E. external data

Correct Answer: CE
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.cisco.com/c/en/us/td/docs/security/wsa/wsa11-0/user_guide/b_WSA_UserGuide/b_WSA_UserGuide_chapter_010011.html

QUESTION 57 Which port is configured in a browser to use the Cisco WSA web proxy with default settings?

A. 8080
B. 8443
C. 8021
D. 3128

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/Aug2013/CVD-WebSecurityUsingCiscoWSADesignGuide-AUG13.pdf (16)

QUESTION 58
What is a benefit of integrating Cisco WSA with TrustSec in ISE?
A. The policy trace tool can be used to match access policies using specific SGT

B. Traffic of authenticated users who use 802.1x can be tagged with SGT to identification profiles in a Cisco WSAC. ISE can block authentication for users who generate multiple sessions using suspect TCP ports

D. Users in a specific SGT can be denied access to certain social websites.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.cisco.com/c/en/us/td/docs/security/ise/1-3/ISE-WSAIntegrationDoc/b_ISE-WSAIntegration.html

QUESTION 59 When an access policy is created, what is the default option for the Application Settings?

A. Use Global Policy Applications Settings
B. Define the Applications Custom Setting
C. Set all applications to Block
D. Set all applications to Monitor

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
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_01111.html

QUESTION 60 What is the primary benefit of using Cisco Advanced Web Security Reporting?

A. ability to see the malicious activity of a user
B. L4TM report with client-malware risk
C. centralized and granular reporting
D. access to a day report with historical data

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.cisco.com/c/en/us/products/collateral/security/web-security-appliance/datasheet_c78-729104.html