PassQueen
a.k.a dumpsqueen.com

Securing the Web with Cisco Web Security Appliance (300-725 SWSA)

Cisco 300-725

Version Demo

Total Demo Questions: 9

Total Premium Questions: 90

Buy Premium PDF

https://passqueen.com

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, Web Security Fundamentals	4
Topic 2, Proxy Services	28
Topic 3, Authentication, Authorization, and Accounting	11
Topic 4, Cisco Web Security Appliance Security and Integration	28
Topic 5, Troubleshooting, Monitoring, Reporting	19
Total	90

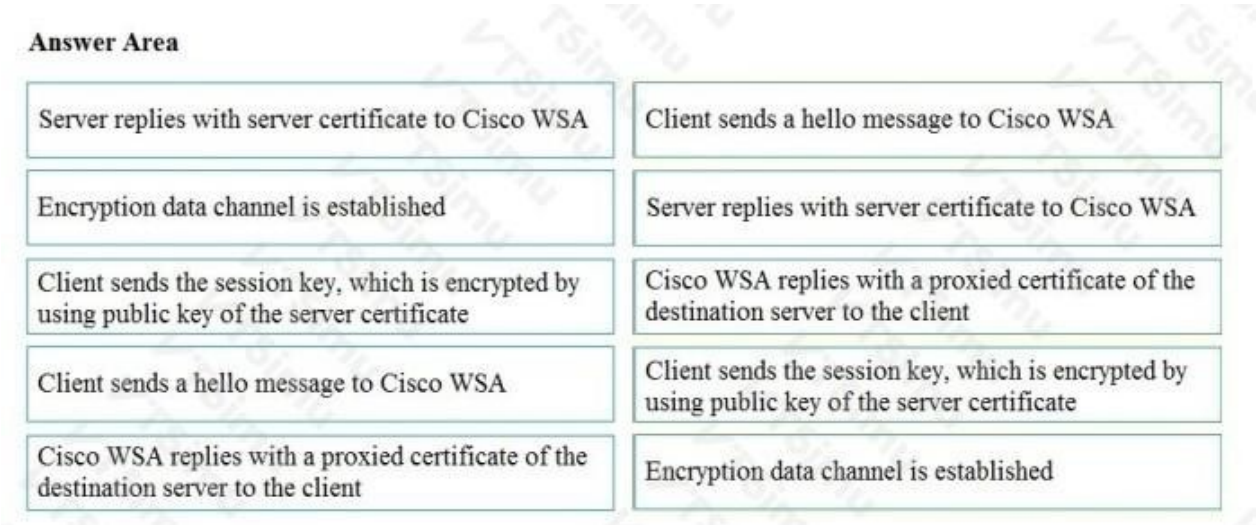
QUESTION NO: 1 - (DRAG DROP)

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:



Explanation:

For an HTTPS session processed by Cisco WSA with HTTPS decryption, the client first initiates the TLS negotiation by sending a ClientHello message to the WSA. The appliance is acting as an explicit TLS proxy, so it must create separate TLS relationships rather than simply pass the original encrypted exchange through unchanged. To prepare the client-facing TLS connection, the WSA contacts the requested destination and receives the destination server certificate. This certificate lets the WSA identify the destination, evaluate the certificate according to its configured trust and decryption policy, and use the destination identity when creating a substitute certificate for the client-facing connection.

After receiving the destination certificate, Cisco WSA presents a proxied certificate for that destination server to the client. The proxied certificate is what enables the client to validate the endpoint it believes it is reaching while establishing TLS with the appliance. Once that certificate has been presented, the client sends the session key material encrypted with the public key contained in the certificate. The WSA can process this key exchange because it generated and possesses the corresponding private key for the proxied certificate. With the TLS handshake key material negotiated, the encrypted data channel is established. Cisco documents that HTTPS decryption creates a proxy TLS connection and dynamically generates certificates signed by a configured root certificate; see Cisco Secure Web Appliance HTTPS Decryption documentation. The normal TLS certificate and key-exchange flow is also described in RFC 5246.

QUESTION NO: 2

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

ANSWER: A C

Explanation:

Cisco WSA access logs are transaction-oriented records generated by the web proxy. They provide the information needed to associate a web request with its originating endpoint and to identify how the proxy processed that request. **Client IP Address** is recorded so administrators can identify the client that initiated the transaction, investigate user activity, and correlate the event with endpoint, firewall, or identity-system records. **HTTP Request Code** is also part of the default transaction information, allowing the log entry to identify the request or processing outcome associated with the HTTP exchange. Together, these fields establish the source of the request and provide a key indication of the request transaction for operational monitoring and incident investigation. Cisco documents access logging as the mechanism for recording web-proxy client transactions and describes the access-log fields and formats available on the appliance. For the applicable AsyncOS release, review the Cisco WSA user-guide documentation at Cisco Web Security Appliance User Guides and the product documentation portal at Cisco Web Security Appliance documentation.

QUESTION NO: 3

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 WSA

C. 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.

ANSWER: D

Explanation:

Users in a specific SGT can be denied access to certain social websites. Integrating Cisco WSA with Cisco ISE and TrustSec enables the WSA to obtain Security Group Tag information associated with authenticated users and use that identity-based context when evaluating web requests. Rather than applying the same web-access rule solely by IP address, subnet, or directory group, administrators can build differentiated web policies for users based on their TrustSec security-group membership.

This makes it possible to apply a web-access control policy that matches a particular SGT and blocks a chosen URL category, including social networking sites, while allowing different access for users assigned to another SGT. The approach supports consistent role-based policy enforcement: ISE determines and distributes the user's security-group context, and the WSA consumes that context to make web filtering decisions. This is especially useful when users change location or network address, because the policy follows the authenticated identity and assigned tag rather than depending only on the endpoint's IP address. Cisco documents that the ISE–WSA integration supports applying WSA access policies based on TrustSec Security Group Tags. See Cisco ISE–WSA Integration Guide and Cisco Secure Web Appliance documentation.

QUESTION NO: 4 - (SIMULATION)

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

B. 8443

C. 8021

D. 3128

ANSWER: See the explanation for the answer

Explanation:

Answer: D. `3128`

With the default Cisco Web Security Appliance (WSA) proxy configuration, browsers are configured to use the web proxy on TCP port `3128`. This is the default explicit forward-proxy listener port.

Port `8443` is commonly associated with secure management/web interfaces, while `8021` is not the default browser proxy port.

QUESTION NO: 5

Which two connection settings are required when configuring a Cisco WSA to forward requests to an upstream proxy? (Choose two.)

A. Upstream proxy hostname or IP address

B. Upstream proxy port

C. Client browser user-agent string

D. Web cache mode

E. DNS search suffix

ANSWER: A B

Explanation:

Upstream proxy hostname or IP address and **upstream proxy port** are required connection settings. The Cisco WSA uses the hostname or IP address to identify the upstream proxy that receives forwarded requests. The port specifies the listener on that upstream proxy to which the WSA establishes the connection.

Additional settings, such as authentication credentials or exceptions for destinations that should bypass the upstream proxy, can be configured when required by the deployment. However, the remote proxy address and listening port establish the basic connectivity needed for request forwarding. Cisco documents upstream proxy configuration in the Cisco WSA User Guide.

QUESTION NO: 6

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

ANSWER: C

Explanation:

Cisco Advanced Web Security Reporting primarily provides **centralized and granular reporting**. It consolidates web-security activity into a reporting capability that gives administrators detailed visibility into web usage, policy enforcement, threats, identities, destinations, and traffic patterns. This central view is valuable operationally because security teams can investigate activity and produce reports without having to manually correlate isolated log entries or rely on a narrow, single-purpose report. Granularity lets administrators focus reports on the users, groups, time ranges, URL categories, security events, and other dimensions relevant to an investigation, audit, or policy decision.

Cisco describes the Web Security Appliance reporting capability as providing detailed visibility and reporting for web-security events and web use. Advanced reporting therefore supports both day-to-day monitoring and deeper analysis by making the collected data centrally accessible and filterable. This broad reporting and analysis capability is the principal benefit, rather than access to one specific report type or a particular historical-report interval. See Cisco's Web Security Appliance data sheet and the Cisco Secure Web Appliance documentation for reporting feature information.

QUESTION NO: 7

Which access policy does the Cisco WSA apply when a web request matches more than one access policy?

A. The first matching access policy in the policy order

B. The access policy with the most conditions

C. The last matching access policy in the policy order

D. The Global Access Policy only

ANSWER: A

Explanation:

The Cisco WSA applies the first matching access policy in the configured policy order. Access policies are evaluated from top to bottom, and processing stops when the appliance finds a policy whose identification-profile, identity, group, client-IP, or other membership criteria match the request. Administrators should therefore place more-specific policies above broader policies, such as a default policy that applies to all users.

After modifying policy order, administrators should verify the resulting match with Policy Trace before deploying the change. Cisco documents access-policy processing and policy order in the Cisco Secure Web Appliance User Guide.

QUESTION NO: 8

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

A. TCP_DENIED/407

B. TCP_DENIED/401

C. TCP_DENIED/403

D. TCP_DENIED/307

ANSWER: C

Explanation:

TCP_DENIED/403 indicates that the Web Security Appliance denied the client transaction because access to the requested resource was not permitted. In an access log entry, `TCP_DENIED` identifies a request that the proxy did not allow to proceed,

and the accompanying HTTP status code `403` represents “Forbidden.” This is the expected result when an applicable web-access policy, URL filtering decision, destination restriction, or similar configured enforcement rule blocks the request.

This distinction is useful during troubleshooting because the access log result describes the proxy’s handling of the transaction, while the status code communicates the HTTP outcome returned to the client. A `TCP_DENIED/403` entry therefore directs an administrator toward reviewing the policies and access controls that matched the request, including the identity, URL category or reputation, destination, and configured action. Cisco documents Web Security Appliance logging and access-log interpretation in its product documentation, and the underlying proxy result-code conventions are also documented by Squid. See the Cisco Web Security Appliance documentation and the Squid access_log documentation.

QUESTION NO: 9

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

ANSWER: A C

Explanation:

Pass Through and **Decrypt** are decryption-policy actions on a Cisco Web Security Appliance. A decryption policy is evaluated for HTTPS traffic after the appliance receives the TLS connection request and determines whether the traffic matches the policy’s conditions, such as destination category, URL, identity, or protocol characteristics.

When **Decrypt** is selected, the WSA performs HTTPS decryption so that the encrypted request and response can be inspected by the web proxy security controls. This enables policy enforcement and scanning capabilities that require visibility into the HTTP content carried inside the TLS session. The appliance uses its configured root certificate to establish the trusted decrypted session with the client and a separate TLS session to the destination server.

When **Pass Through** is selected, the WSA permits the HTTPS connection to continue without decrypting its content. This action is appropriate for destinations that should not, or cannot, be decrypted, including sites subject to privacy requirements or applications that use certificate pinning. Cisco documents these as available actions when configuring HTTPS decryption policies. See the Cisco WSA User Guide: Decryption Policies and Cisco’s Web Security Appliance user-guide library.