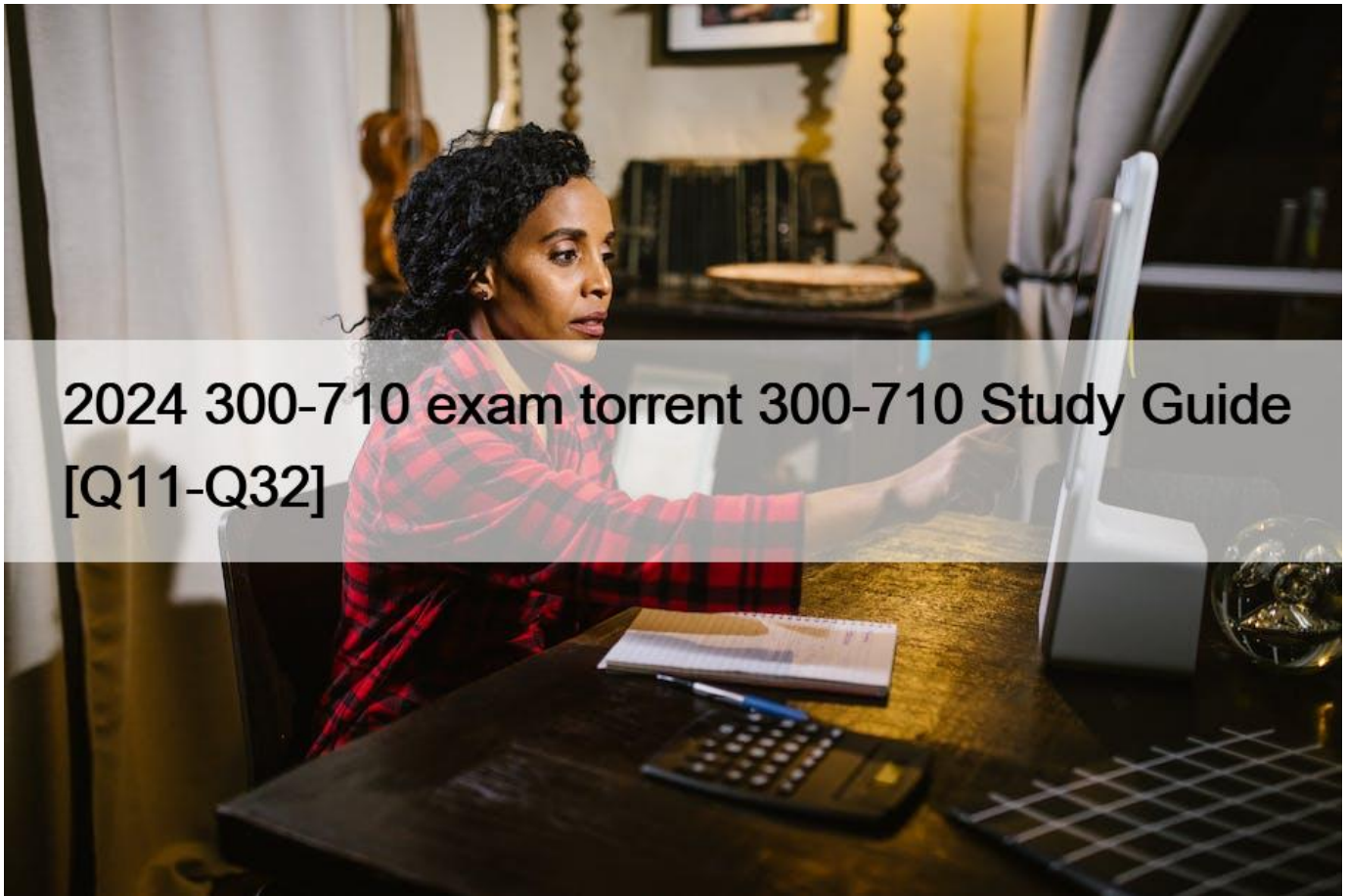


2024 300-710 exam torrent 300-710 Study Guide [Q11-Q32]



2024 300-710 exam torrent 300-710 Study Guide [Q11-Q32]

2024 300-710 exam torrent 300-710 Study Guide
Easily pass 300-710 Exam with our Dumps & PDF Test Engine

NO.11 An engineer wants to change an existing transparent Cisco FTD to routed mode.

The device controls traffic between two network segments. Which action is mandatory to allow hosts to reestablish communication between these two segments after the change?

- * remove the existing dynamic routing protocol settings.
- * configure multiple BVIs to route between segments.
- * assign unique VLAN IDs to each firewall interface.
- * implement non-overlapping IP subnets on each segment.

NO.12 Which CLI command is used to control special handling of clientHello messages?

- * system support ssl-client-hello-tuning
- * system support ssl-client-hello-reset
- * system support ssl-client-hello-force-reset
- * system support ssl-client-hello-display

NO.13 When deploying a Cisco ASA Firepower module, an organization wants to evaluate the contents of the traffic without affecting the network. It is currently configured to have more than one instance of the same device on the physical appliance Which deployment mode meets the needs of the organization?

- * inline tap monitor-only mode
- * passive monitor-only mode
- * passive tap monitor-only mode
- * inline mode

Explanation

[https://www.cisco.com/c/en/us/td/docs/security/asa/asa910/configuration/firewall/asa-910-firewall-config/access](https://www.cisco.com/c/en/us/td/docs/security/asa/asa910/configuration/firewall/asa-910-firewall-config/accessInline)Inline tap monitor-only mode (ASA inline)-In an inline tap monitor-only deployment, a copy of the traffic is sent to the ASA FirePOWER module, but it is not returned to the ASA. Inline tap mode lets you see what the ASA FirePOWER module would have done to traffic, and lets you evaluate the content of the traffic, without impacting the network. However, in this mode, the ASA does apply its policies to the traffic, so traffic can be dropped due to access rules, TCP normalization, and so forth.

NO.14 What is a functionality of port objects in Cisco FMC?

- * to mix transport protocols when setting both source and destination port conditions in a rule
- * to represent protocols other than TCP, UDP, and ICMP
- * to represent all protocols in the same way
- * to add any protocol other than TCP or UDP for source port conditions in access control rules.

Reference:

https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-config-guide-v62/reusable_objects.html

NO.15 Which two OSPF routing features are configured in Cisco FMC and propagated to Cisco FTD? (Choose two.)

- * OSPFv2 with IPv6 capabilities
- * virtual links
- * SHA authentication to OSPF packets
- * area boundary router type 1 LSA filtering
- * MD5 authentication to OSPF packets

NO.16 Which two considerations must be made when deleting and re-adding devices while managing them via Cisco FMC (Choose two).

- * Before re-adding the device In Cisco FMC, the manager must be added back.
- * The Cisco FMC web interface prompts users to re-apply access control policies.
- * Once a device has been deleted, It must be reconfigured before it is re-added to the Cisco FMC.
- * An option to re-apply NAT and VPN policies during registration is available, so users do not need to re-apply the policies after registration is completed.
- * There is no option to re-apply NAT and VPN policies during registration is available, so users need to re-apply the policies after registration is completed.

NO.17 A network administrator reviews the file report for the last month and notices that all file types, except exe. show a disposition of unknown. What is the cause of this issue?

- * The malware license has not been applied to the Cisco FTD.
- * The Cisco FMC cannot reach the Internet to analyze files.
- * A file policy has not been applied to the access policy.
- * Only Spero file analysis is enabled.

NO.18 An engineer must build redundancy into the network and traffic must continuously flow if a redundant switch in front of the firewall goes down. What must be configured to accomplish this task?

- * redundant interfaces on the firewall cluster mode and switches

- * redundant interfaces on the firewall noncluster mode and switches
- * vPC on the switches to the interface mode on the firewall duster
- * vPC on the switches to the span EtherChannel on the firewall cluster

NO.19 A network administrator is implementing an active/passive high availability Cisco FTD pair.

When adding the high availability pair, the administrator cannot select the secondary peer.

What is the cause?

- * The second Cisco FTD is not the same model as the primary Cisco FTD.
- * An high availability license must be added to the Cisco FMC before adding the high availability pair.
- * The failover link must be defined on each Cisco FTD before adding the high availability pair.
- * Both Cisco FTD devices are not at the same software Version

NO.20 When an engineer captures traffic on a Cisco FTD to troubleshoot a connectivity problem, they receive a large amount of output data in the GUI tool. The engineer found that viewing the Captures this way is time-consuming and difficult to sort and filter. Which file type must the engineer export the data in so that it can be reviewed using a tool built for this type of analysis?

- * NetFlow v9
- * PCAP
- * NetFlow v5
- * IPFIX

When capturing traffic on a Cisco FTD device to troubleshoot a connectivity problem, a file type that can be exported for reviewing using a tool built for this type of analysis is PCAP. PCAP stands for Packet Capture and it is a file format used to store network packet data captured from a network interface⁸. PCAP files contain the raw data of network packets, including the headers and payloads of each packet⁸.

PCAP files are widely used in network analysis and troubleshooting tasks. They enable network administrators, analysts, and researchers to inspect and analyze network traffic for various purposes, such as diagnosing network issues, detecting malicious activity, measuring network performance, and understanding network protocols⁸. PCAP files can be read by applications that understand that format, such as Wireshark, tcpdump, CA NetMaster, or Microsoft Network Monitor⁸.

The other options are incorrect because:

* NetFlow v9 is not a file type, but a protocol for collecting and exporting information about network flows. A network flow is a sequence of packets that share common attributes such as source and destination IP addresses, ports, and protocols⁹. NetFlow v9 records contain summary information about network flows, such as start and end times, byte counts, packet counts, and so on⁹. NetFlow v9 records do not contain the raw data of network packets.

* NetFlow v5 is not a file type, but an earlier version of the NetFlow protocol for collecting and exporting information about network flows. NetFlow v5 records contain similar information as NetFlow v9 records, but with fewer fields and less flexibility¹⁰. NetFlow v5 records do not contain the raw data of network packets.

* IPFIX is not a file type, but a protocol for collecting and exporting information about network flows. IPFIX stands for IP Flow Information Export and it is based on NetFlow v9, but with some extensions and improvements¹¹. IPFIX records contain similar information as NetFlow v9 records, but with more fields and more flexibility¹¹. IPFIX records do not contain the raw data of network packets.

NO.21 Which two actions can be used in an access control policy rule? (Choose two.)

- * Block with Reset
- * Monitor

- * Analyze
- * Discover
- * Block ALL

Section: Configuration

Explanation/Reference: <https://www.cisco.com/c/en/us/td/docs/security/firesight/541/firepower-module-user-guide/asa-firepower-module-user-guide-v541/AC-Rules-Tuning-Overview.html#71854>

NO.22 An engineer is setting up a new Firepower deployment and is looking at the default FMC policies to start the implementation. During the initial trial phase, the organization wants to test some common Snort rules while still allowing the majority of network traffic to pass. Which default policy should be used?

- * Maximum Detection
- * Security Over Connectivity
- * Balanced Security and Connectivity
- * Connectivity Over Security

<https://www.cisco.com/c/en/us/td/docs/security/firepower/623/fdm/fptd-fdm-config-guide-623/fptd-fdm-intrusion.html>

NO.23 What is a result of enabling Cisco FTD clustering?

- * For the dynamic routing feature, if the master unit fails, the newly elected master unit maintains all existing connections.
- * Integrated Routing and Bridging is supported on the master unit.
- * Site-to-site VPN functionality is limited to the master unit, and all VPN connections are dropped if the master unit fails.
- * All Firepower appliances can support Cisco FTD clustering.

Reference:

https://www.cisco.com/c/en/us/td/docs/security/firepower/640/configuration/guide/fpmc-config-guide-v64/clustering_for_the_firepower_threat_defense.html

NO.24 An engineer must deploy a Cisco FTD device. Management wants to examine traffic without requiring network changes that will disrupt end users. Corporate security policy requires the separation of management traffic from data traffic and the use of SSH over Telnet for remote administration. How must the device be deployed to meet these requirements?

- * in routed mode with a diagnostic interface
- * in transparent mode with a management Interface
- * in transparent mode with a data interface
- * in routed mode with a bridge virtual interface

To deploy a Cisco FTD device that meets the requirements of the question, the engineer must use transparent mode with a management interface. Transparent mode is a firewall configuration in which the FTD device acts as a "bump in the wire"; or a "stealth firewall"; and is not seen as a router hop to connected devices. In transparent mode, the FTD device can examine traffic without requiring network changes that will disrupt end users, such as changing IP addresses or routing configurations¹. A management interface is a dedicated interface that is used for managing the FTD device and separating management traffic from data traffic. A management interface can be configured to allow SSH access for remote administration, which is more secure than Telnet².

The other options are incorrect because:

- * Routed mode is a firewall configuration in which the FTD device acts as a router and performs address translation and routing for connected networks. Routed mode requires network changes that may disrupt end users, such as changing IP addresses or routing configurations¹. A diagnostic interface is a special interface that is used for troubleshooting and capturing traffic on the FTD device. A diagnostic interface does not separate management traffic from data traffic or allow SSH access for remote administration.
- * Transparent mode with a data interface does not meet the requirement of separating management traffic from data traffic. A data

interface is a regular interface that is used for passing and inspecting traffic on the FTD device. A data interface does not allow SSH access for remote administration².

* Routed mode with a bridge virtual interface (BVI) does not meet the requirement of examining traffic without requiring network changes that will disrupt end users. A BVI is a logical interface that acts as a container for one or more physical or logical interfaces that belong to the same layer 2 broadcast domain. A BVI allows the FTD device to route between different bridge groups on the same security module/engine. However, routed mode still requires network changes that may disrupt end users, such as changing IP addresses or routing configurations.

NO.25 Which CLI command is used to control special handling of ClientHello messages?

- * system support ssl-client-hello-tuning
- * system support ssl-client-hello-display
- * system support ssl-client-hello-force-reset
- * system support ssl-client-hello-enabled

Reference:

https://www.cisco.com/c/en/us/td/docs/security/firepower/610/configuration/guide/fpmc-config-guide-v61/firepower_command_line_reference.html

NO.26 An engineer plans to reconfigure an existing Cisco FTD from transparent mode to routed mode. Which additional action must be taken to maintain communication Between me two network segments?

- * Configure a NAT rule so mat traffic between the segments is exempt from NAT.
- * Update the IP addressing so that each segment is a unique IP subnet.
- * Deploy inbound ACLs on each interface to allow traffic between the segments.
- * Assign a unique VLAN ID for the interface in each segment.

When reconfiguring an existing Cisco FTD from transparent mode to routed mode, an additional action that must be taken to maintain communication between the two network segments is to update the IP addressing so that each segment is a unique IP subnet. This is because in routed mode, the FTD device acts as a router hop in the network and requires each interface to be on a different subnet. In transparent mode, the FTD device acts as a layer 2 firewall and does not require different subnets for each interface¹.

The other options are incorrect because:

* Configuring a NAT rule so that traffic between the segments is exempt from NAT is not necessary to maintain communication between the two network segments. NAT is used to translate IP addresses between different networks, but it does not affect the routing of packets. Moreover, NAT is optional in routed mode and can be disabled if not needed².

* Deploying inbound ACLs on each interface to allow traffic between the segments is not required to maintain communication between the two network segments. ACLs are used to control access to network resources based on source and destination addresses, protocols, and ports. They do not affect the routing of packets. Furthermore, ACLs are optional in routed mode and can be configured as needed³.

* Assigning a unique VLAN ID for the interface in each segment is not relevant to maintain communication between the two network segments. VLANs are used to create logical groups of hosts that share the same broadcast domain, regardless of their physical location or connection. They do not affect the routing of packets. Besides, VLANs are not supported in routed mode and can only be used in transparent mode⁴.

NO.27 An organization is using a Cisco FTD and Cisco ISE to perform identity-based access controls. A network administrator is analyzing the Cisco FTD events and notices that unknown user traffic is being allowed through the firewall. How should this be addressed to block the traffic while allowing legitimate user traffic?

- * Modify the Cisco ISE authorization policy to deny this access to the user.
- * Modify Cisco ISE to send only legitimate usernames to the Cisco FTD.
- * Add the unknown user in the Access Control Policy in Cisco FTD.
- * Add the unknown user in the Malware & File Policy in Cisco FTD.

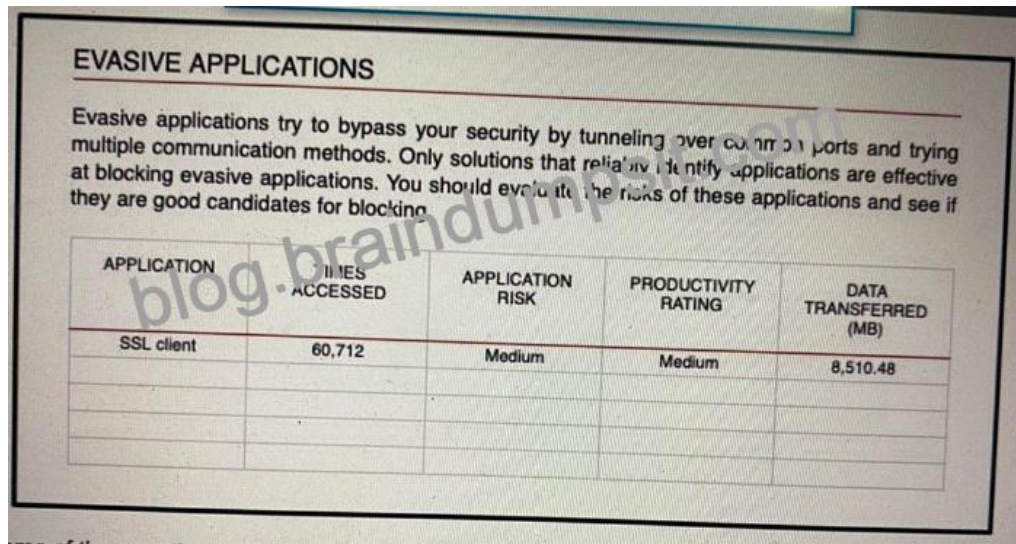
NO.28 Which two OSPF routing features are configured in Cisco FMC and propagated to Cisco FTD? (Choose two.)

- * OSPFv2 with IPv6 capabilities
- * virtual links
- * SHA authentication to OSPF packets
- * area boundary router type 1 LSA filtering
- * MD5 authentication to OSPF packets

Reference:

https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-config-guide-v62/ospf_for_firepower_threat_defense.html

NO.29 Refer to the exhibit.



The slide is titled "EVASIVE APPLICATIONS". It contains a paragraph explaining that evasive applications bypass security by tunneling over common ports and trying multiple communication methods. It states that only solutions that reliably identify applications are effective at blocking them, and that one should evaluate the risks of these applications to see if they are good candidates for blocking.

APPLICATION	FILES ACCESSED	APPLICATION RISK	PRODUCTIVITY RATING	DATA TRANSFERRED (MB)
SSL client	60,712	Medium	Medium	8,510.48

An administrator is looking at some of the reporting capabilities for Cisco Firepower and noticed this section of the Network Risk report showing a lot of SSL activity that could be used for evasion. Which action will mitigate this risk?

- * Use SSL decryption to analyze the packets.
- * Use encrypted traffic analytics to detect attacks
- * Use Cisco AMP for Endpoints to block all SSL connection
- * Use Cisco Tetration to track SSL connections to servers.

NO.30 Which CLI command is used to control special handling of ClientHello messages?

- * system support ssl-client-hello-tuning
- * system support ssl-client-hello-display
- * system support ssl-client-hello-force-reset
- * system support ssl-client-hello-enabled

NO.31 Which interface type allows packets to be dropped?

- * passive
- * inline
- * ERSPAN
- * TAP

NO.32 An administrator is creating interface objects to better segment their network but is having trouble adding interfaces to the objects. What is the reason for this failure?

- * The interfaces are being used for NAT for multiple networks.
- * The administrator is adding interfaces of multiple types.
- * The administrator is adding an interface that is in multiple zones.
- * The interfaces belong to multiple interface groups.

300-710 PDF Pass Leader, 300-710 Latest Real Test: https://www.braindumpsit.com/300-710_real-exam.html]