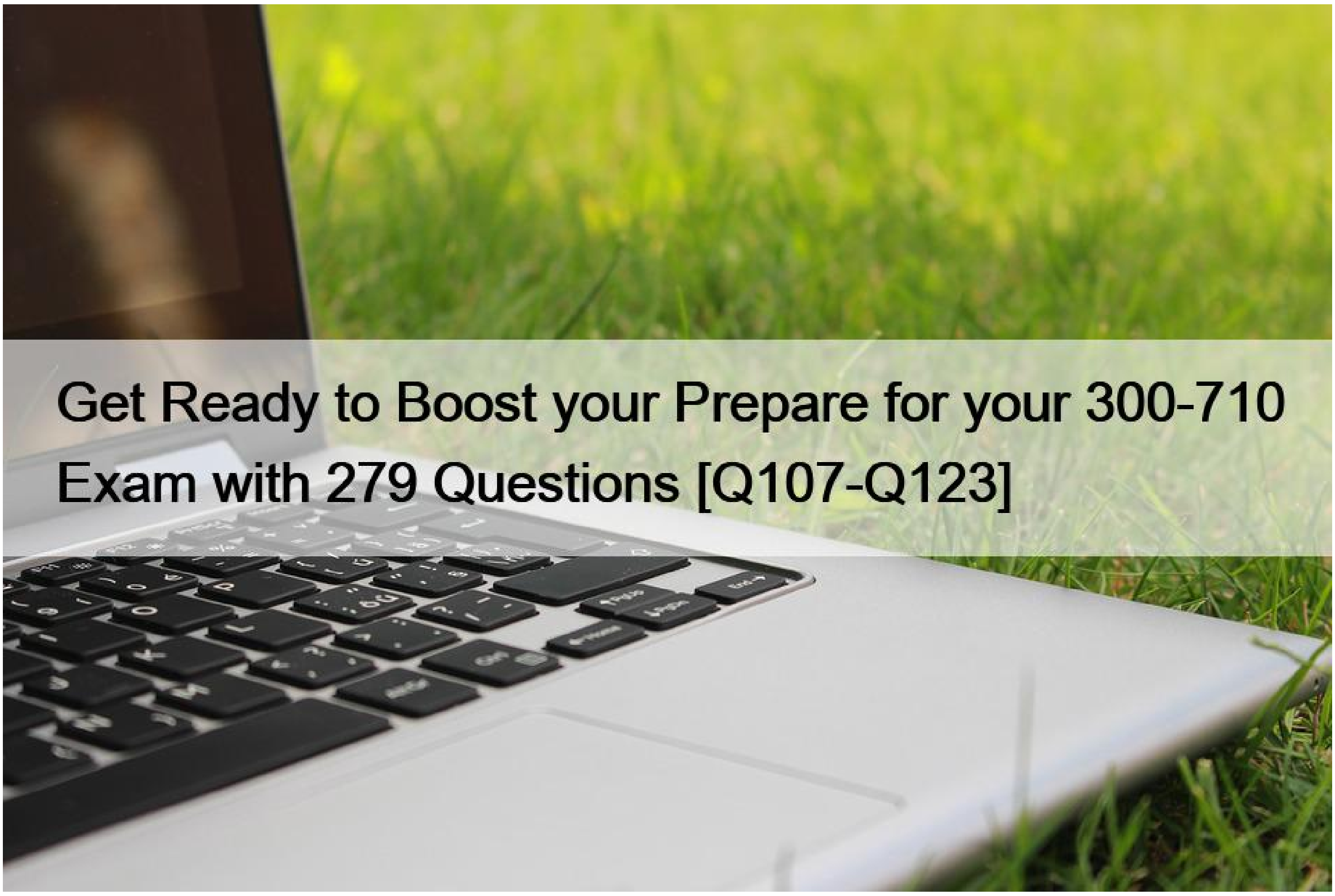
Get Ready to Boost your Prepare for your 300-710 Exam with 279 Questions [Q107-Q123



Get Ready to Boost your Prepare for your 300-710 Exam with 279 Questions Use Free 300-710 Exam Questions that Stimulates Actual EXAM

Cisco 300-710 exam is a challenging exam that requires a lot of study and practice to pass. Candidates should have a good understanding of network security concepts and be familiar with Cisco Firepower devices before taking the exam. Passing the Cisco 300-710 exam demonstrates that the candidate has the skills and knowledge required to secure networks using Cisco Firepower devices, which is a valuable asset in today's job market.

Cisco Firepower NGFW is a powerful and advanced security solution that provides comprehensive threat protection for network infrastructures. The Cisco 300-710 certification exam covers the latest Cisco Firepower NGFW features, including access control policies, network analysis policies, and intrusion policies. Candidates will also learn how to configure advanced security features, such as VPNs, SSL decryption, and advanced malware protection.

QUESTION 107

Which Cisco Advanced Malware Protection for Endpoints policy is used only for monitoring endpoint actively?
* Windows domain controller
* audit
* triage
* protection
Reference:

https://www.cisco.com/c/en/us/support/docs/security/amp-endpoints/214933-amp-for-endpoints- deployment-methodology.html

QUESTION 108

A network engineer is extending a user segment through an FTD device for traffic inspection without creating another IP subnet How is this accomplished on an FTD device in routed mode?
* by leveraging the ARP to direct traffic through the firewall
* by assigning an inline set interface
* by using a BVI and create a BVI IP address in the same subnet as the user segment
* by bypassing protocol inspection by leveraging pre-filter rules
https://www.cisco.com/c/en/us/td/docs/security/firepower/640/configuration/guide/fpmc-config-guide-v64/transparent_or_routed_firewall_mode_for_firepower_threat_defense.html

QUESTION 109

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.
Explanation

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.

QUESTION 110

How many report templates does the Cisco Firepower Management Center support?
* 20
* 10
* 5
* unlimited
Section: Management and Troubleshooting

Explanation/Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Working_with_Reports.html

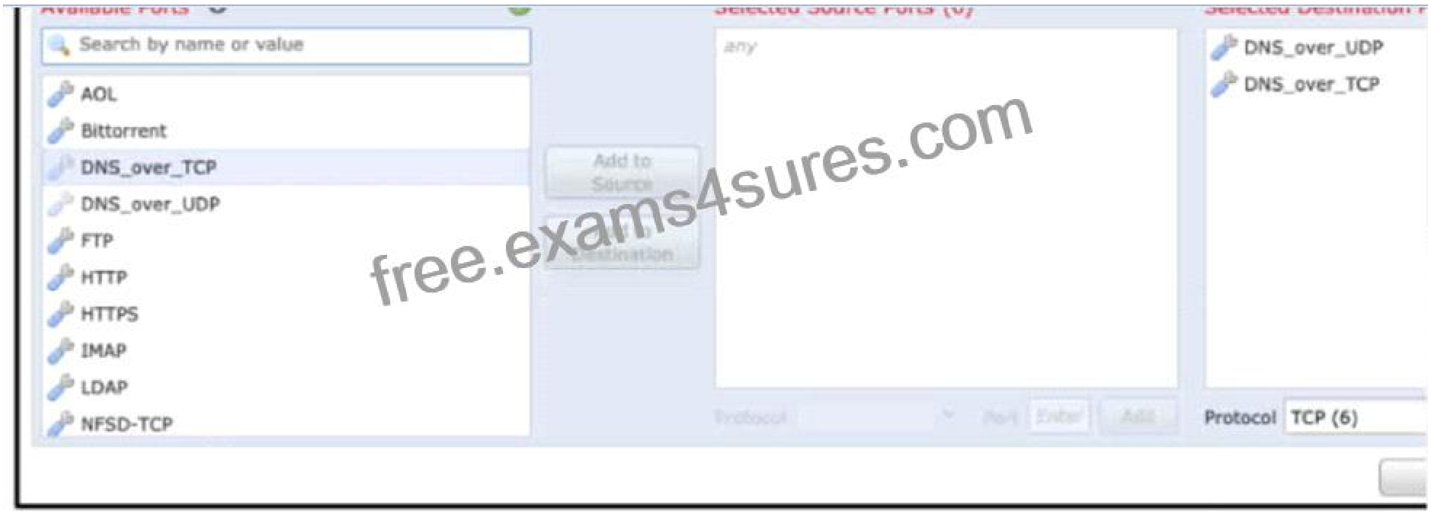
QUESTION 111

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

QUESTION 112

Refer to the exhibit.



Protocol TCP (6)

An engineer is modifying an access control policy to add a rule to Inspect all DNS traffic that passes it making the change and deploying the policy, they see that DNS traffic Is not being Inspected by the Snort engine. What is&#8230;&#8230;

* The rule must specify the security zone that originates the traffic.
* The rule Is configured with the wrong setting for the source port.
* The rule must define the source network for inspection as well as the port.

QUESTION 113

A hospital network needs to upgrade their Cisco FMC managed devices and needs to ensure that a disaster recovery process is in place. What must be done in order to minimize downtime on the network?
* Configure a second circuit to an ISP for added redundancy
* Keep a copy of the current configuration to use as backup
* Configure the Cisco FMCs for failover
* Configure the Cisco FMC managed devices for clustering.

QUESTION 114

An engineer configures an access control rule that deploys file policy configurations to security zones or tunnel zones, and it causes the device to restart. What is the reason for the restart?
* Source or destination security zones in the access control rule matches the security zones that are associated with interfaces on the target devices.
* The source tunnel zone in the rule does not match a tunnel zone that is assigned to a tunnel rule in the destination policy.
* Source or destination security zones in the source tunnel zone do not match the security zones that are associated with interfaces on the target devices.
* The source tunnel zone in the rule does not match a tunnel zone that is assigned to a tunnel rule in the source policy.

QUESTION 115

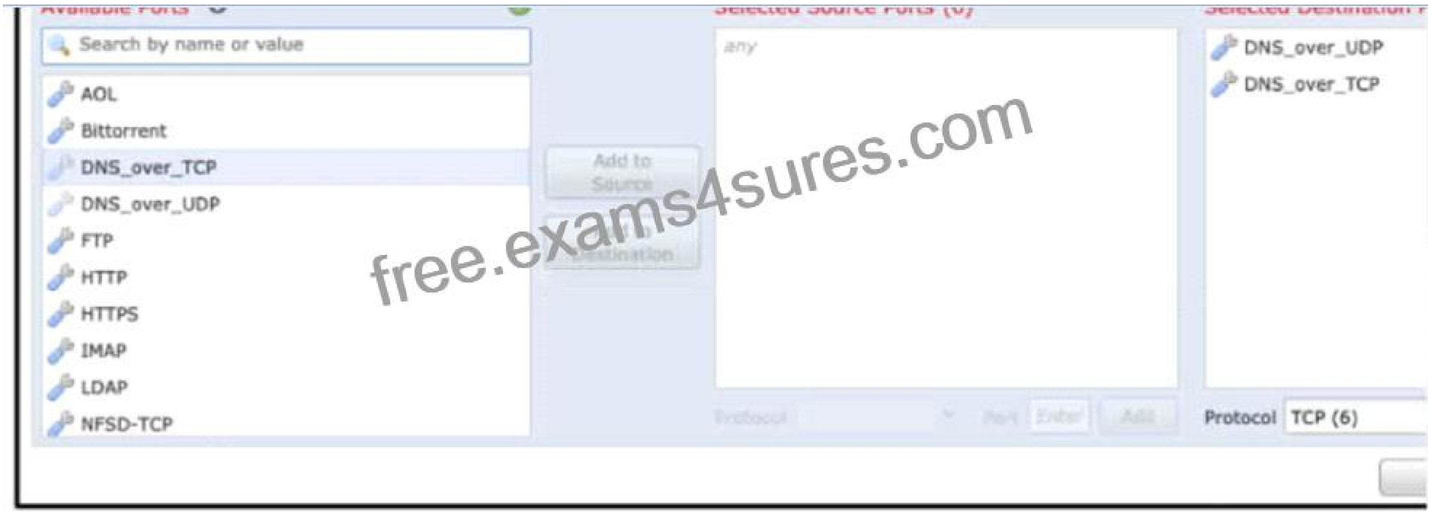
Which action should you take when Cisco Threat Response notifies you that AMP has identified a file as malware?
* Add the malicious file to the block list.
* Send a snapshot to Cisco for technical support.
* Forward the result of the investigation to an external threat-analysis engine.
* Wait for Cisco Threat Response to automatically block the malware.

QUESTION 116

An administrator is attempting to add a new FTD device to their FMC behind a NAT device with a NAT ID of NAT001 and a password of Cisco0420l06525. The private IP address of the FMC server is 192.168.45.45. which is being translated to the public IP address of 209.165.200.225/27. Which command set must be used in order to accomplish this task?
* configure manager add 209.165.200.225 <reg_key> <nat_id>
* configure manager add 192.168.45,45 <reg_key> <nat_id>
* configure manager add 209.165.200.225 255.255.255.224 <reg_key> <nat_id>
* configure manager add 209.165.200.225/27 <reg_key> <nat_id>

QUESTION 117

Refer to the exhibit.



An engineer is modifying an access control policy to add a rule to Inspect all DNS traffic that passes it making the change and deploying the policy, they see that DNS traffic Is not being Inspected by the Snort engine. What is&#8230;&#8230;

* The action of the rule is set to trust instead of allow.
* The rule must specify the security zone that originates the traffic.
* The rule Is configured with the wrong setting for the source port.
* The rule must define the source network for inspection as well as the port.

QUESTION 118

A network engineer is tasked with minimising traffic interruption during peak traffic limes. When the SNORT inspection engine is overwhelmed, what must be configured to alleviate this issue?

* Enable IPS inline link state propagation
* Enable Pre-filter policies before the SNORT engine failure.
* Set a Trust ALL access control policy.
* Enable Automatic Application Bypass.

QUESTION 119

When creating a report template, how can the results be limited to show only the activity of a specific subnet?

* Create a custom search in Firepower Management Center and select it in each section of the report.
* Add an Input Parameter in the Advanced Settings of the report, and set the type to Network/IP.
* Add a Table View section to the report with the Search field defined as the network in CIDR format.
* Select IP Address as the X-Axis in each section of the report.

QUESTION 120

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

Reference:

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

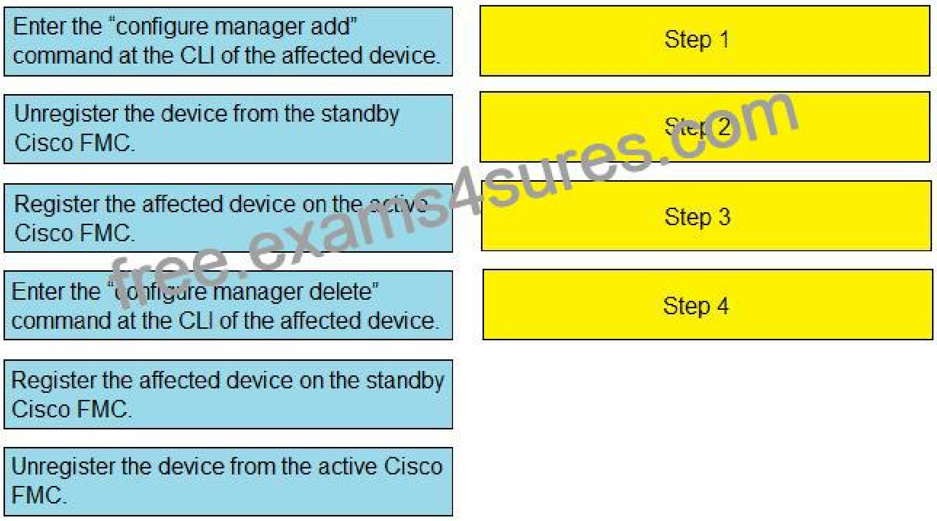
QUESTION 121

When a Cisco FTD device is configured in transparent firewall mode, on which two interface types can an IP address be configured? (Choose two.)

* Diagnostic
* EtherChannel
* BVI
* Physical
* Subinterface

QUESTION 122

Drag and drop the steps to restore an automatic device registration failure on the standby Cisco FMC from the left into the correct order on the right. Not all options are used.



Enter the "configure manager add" command at the CLI of the affected device.

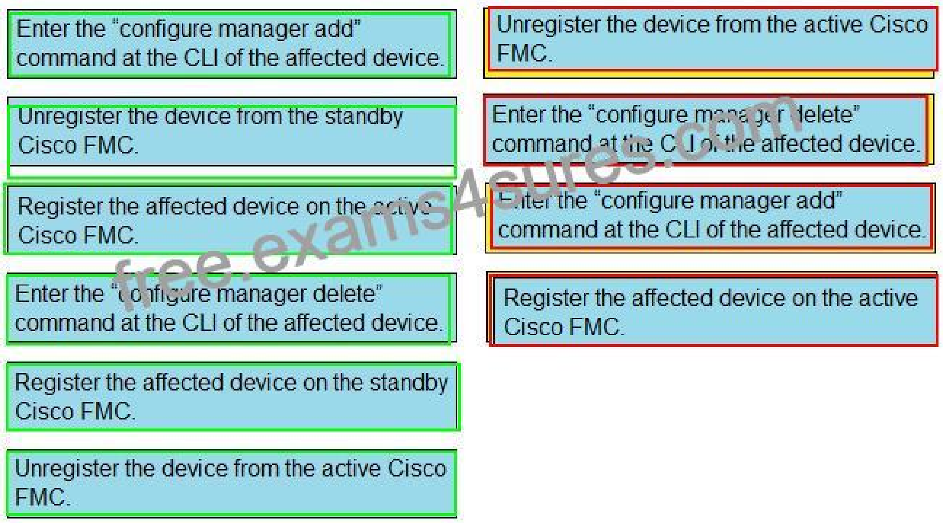
Unregister the device from the standby Cisco FMC.

Register the affected device on the active Cisco FMC.

Enter the "configure manager delete" command at the CLI of the affected device.

Register the affected device on the standby Cisco FMC.

Unregister the device from the active Cisco FMC.



Enter the "configure manager add" command at the CLI of the affected device.

Unregister the device from the standby Cisco FMC.

Register the affected device on the active Cisco FMC.

Enter the "configure manager delete" command at the CLI of the affected device.

Register the affected device on the standby Cisco FMC.

Unregister the device from the active Cisco FMC.

Unregister the device from the active Cisco FMC.

Enter the "configure manager delete" command at the CLI of the affected device.

Enter the "configure manager add" command at the CLI of the affected device.

Register the affected device on the active Cisco FMC.

QUESTION 123

What are two application layer preprocessors? (Choose two.)
* CIFS
* IMAP
* SSL
* DNP3
* ICMP

Exam Content

The content of the Cisco 300-710 test revolves around four domains, each containing specific knowledge and skills that the candidates must develop competency in. These areas have different percentage weights in the exam syllabus, which shows how many questions related to this or that topic will appear in the test. While preparing for your certification exam, you need to pay special attention to the sections with higher weight. However, you need to remember that only mastering all the topics will guarantee success in your test. The detailed outline of the domains covered in Cisco 300-710 is provided below.

Deployment ? 30%

Within this first topic, the examinees need to demonstrate that they have the relevant skills in implementing NGFW modes (including routed mode as well as transparent mode); implementing NGIPS modes (including passive & inline); implementing high availability options (including link redundancy, standby/active failover, multi-instance); describing IRB configurations.

Configuration ? 30%

This domain requires that the students have the expertise in a wide range of knowledge areas. For starters, they should have proficiency in configuring system settings within Cisco Firepower Management Center as well as configuring the policies, such as access control, malware & file, intrusion, identity, SSL, DNS, prefilter within Cisco Firepower Management Center. In addition, they need to able to customize the following features with the help of Cisco Firepower Management Center: network discovery, correlation, application detectors (Open AppID), and actions. This part also encompasses such skills as customizing objects with the help of Firepower Management Center (including object management as well as intrusion rules) and customizing devices with the help of Firepower Management Center (including device Management, VPN, NAT, QoS, Certificates, Platform Settings).

Management & Troubleshooting ? 25%

To tackle the questions associated with this subject area, the test takers should develop their competency in performing troubleshooting with the help of FMC CLI as well as GUI; customizing dashboards as well as reporting in FMC; troubleshooting with the help of packet capture actions; analyzing standard reports and risk.

Integration ? 15%

The last section in the Cisco 300-710 exam encompasses the individuals' skills, such as customizing Cisco AMP for Networks within Firepower Management Center; configuring Cisco AMP for Endpoints within Firepower Management Center; implementing Threat Intelligence Director for third-party security intelligence feeds. Moreover, the learners should possess the expertise in describing the utilization of Cisco Threat Response for the needs of security investigations; describing Cisco FMC PxGrid Integration using Cisco Identify Services Engine (ISE); describing the functionality of Rapid Threat Containment (RTC) within Firepower Management Center.