

# Cisco

## Exam Questions 300-710

Securing Networks with Cisco Firepower (SNCF)



#### NEW QUESTION 1

- (Exam Topic 5)

An organization wants to secure traffic from their branch office to the headquarter building using Cisco Firepower devices, They want to ensure that their Cisco Firepower devices are not wasting resources on inspecting the VPN traffic. What must be done to meet these requirements?

- A. Configure the Cisco Firepower devices to ignore the VPN traffic using prefilter policies
- B. Enable a flexconfig policy to re-classify VPN traffic so that it no longer appears as interesting traffic
- C. Configure the Cisco Firepower devices to bypass the access control policies for VPN traffic.
- D. Tune the intrusion policies in order to allow the VPN traffic through without inspection

**Answer: C**

#### Explanation:

When you configure the Cisco Firepower devices to bypass the access control policies for VPN traffic, the devices will not inspect the VPN traffic and thus will not waste resources on it. This is the best option to ensure that the VPN traffic is not wasting resources on the Cisco Firepower devices.

Reference:

<https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/219759-configure-bypass-policies-on-the>

#### NEW QUESTION 2

- (Exam Topic 5)

An administrator is setting up a Cisco PMC and must provide expert mode access for a security engineer. The engineer is permitted to use only a secured out-of-band network workstation with a static IP address to access the Cisco FMC. What must be configured to enable this access?

- A. Enable SSH and define an access list.
- B. Enable HTTP and define an access list.
- C. Enable SCP under the Access List section.
- D. Enable HTTPS and SNMP under the Access List section.

**Answer: A**

#### NEW QUESTION 3

- (Exam Topic 5)

A network administrator is trying to convert from LDAP to LDAPS for VPN user authentication on a Cisco FTD. Which action must be taken on the Cisco FTD objects to accomplish this task?

- A. Add a Key Chain object to acquire the LDAPS certificate.
- B. Create a Certificate Enrollment object to get the LDAPS certificate needed.
- C. Identify the LDAPS cipher suite and use a Cipher Suite List object to define the Cisco FTD connection requirements.
- D. Modify the Policy List object to define the session requirements for LDAPS.

**Answer: B**

#### NEW QUESTION 4

- (Exam Topic 5)

An engineer is configuring a second Cisco FMC as a standby device but is unable to register with the active unit. What is causing this issue?

- A. The primary FMC currently has devices connected to it.
- B. The code versions running on the Cisco FMC devices are different
- C. The licensing purchased does not include high availability
- D. There is only 10 Mbps of bandwidth between the two devices.

**Answer: B**

#### Explanation:

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

#### NEW QUESTION 5

- (Exam Topic 5)

### HIGH BANDWIDTH APPLICATIONS

Some applications use a substantial amount of network bandwidth. This bandwidth usage can be costly to your organization and can negatively impact overall network performance. You may want to restrict the usage of these applications to particular networks; for instance, a wireless network may not be well suited for video streaming. Or, you can shut down these applications entirely or simply get visibility into how your bandwidth is being used.

| Application      | Times Accessed | Application Risk | Productivity Rating | Data Transferred (MB) |
|------------------|----------------|------------------|---------------------|-----------------------|
| YouTube          | 525            | High             | Very Low            | 76.7262               |
| Pandora Audio    | 5              | Medium           | Very Low            | 8.4889                |
| Spotify          | 44             | Medium           | Very Low            | 6.7747                |
| Microsoft Update | 122            | Medium           | Low                 | 2.5577                |
| Flash Video      | 240            | Low              | Low                 | 2.4371                |

### ENCRYPTED APPLICATIONS

Some applications encrypt data they process, causing security administrators to be blind to attacks and usage patterns. With SSL decryption, administrators can look inside these applications and observe their use. An SSL decryption appliance, such as a Cisco SSL Appliance, can decrypt SSL traffic inbound and outbound: inbound by storing the certificates of private web servers, and outbound by acting as an intermediary in browsers' connections to the Internet. It is important to use SSL decryption to obtain visibility into encrypted applications to help mitigate this potential attack vector.

| Application       | Times Accessed | Application Risk | Productivity Rating | Data Transferred (MB) |
|-------------------|----------------|------------------|---------------------|-----------------------|
| Chrome            | 24,658         | Medium           | Medium              | 799.6732              |
| Internet Explorer | 11,030         | Medium           | Medium              | 375.1055              |
| Firefox           | 2,702          | Medium           | Medium              | 88.5616               |
| Safari            | 1,866          | Medium           | Medium              | 43.1158               |
| Kerberos          | 1,756          | Very Low         | High                | 4.9429                |

### EVASIVE APPLICATIONS

Evasive applications try to bypass your security by tunneling over common ports and trying multiple communication methods. Only solutions that reliably identify applications are effective at blocking evasive applications. You should evaluate the risks of these applications and see if they are good candidates for blocking.

Evasive applications try to bypass your security by tunneling over common ports and trying multiple communication methods. Only solutions that reliably identify applications are effective at blocking evasive applications. You should evaluate the risks of these applications and see if they are good candidates for blocking.

| Application | Times Accessed | Application Risk | Productivity Rating | Data Transferred (MB) |
|-------------|----------------|------------------|---------------------|-----------------------|
| BitTorrent  | 0              | Very High        | Very Low            | 1.7281                |
| TOR         | 5              | Medium           | Low                 | 0.0006                |
| SSL client  | 10,100         | Medium           | Medium              | 48.4102               |
| Skype       | 644            | Medium           | Medium              | 10.3545               |
| cURL        | 280            | Medium           | Medium              | 0.4840                |

Refer to the exhibit. An engineer is analyzing a Network Risk Report from Cisco FMC. Which application must the engineer take immediate action against to prevent unauthorized network use?

- A. Kerberos
- B. YouTube
- C. Chrome
- D. TOR

Answer: D

**NEW QUESTION 6**

- (Exam Topic 5)

Due to an Increase in malicious events, a security engineer must generate a threat report to include intrusion events, malware events, and security intelligence events. How is this information collected in a single report?

- A. Run the default Firepower report.
- B. Export the Attacks Risk report.
- C. Generate a malware report.
- D. Create a Custom report.

Answer: D

**NEW QUESTION 7**

- (Exam Topic 5)

With Cisco FTD integrated routing and bridging, which interface does the bridge group use to communicate with a routed interface?

- A. switch virtual
- B. bridge group member
- C. bridge virtual
- D. subinterface

Answer: C

**Explanation:**

Reference:

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

#### NEW QUESTION 8

- (Exam Topic 5)

An engineer is attempting to add a new FTD device to their FMC behind a NAT device with a NAT ID of ACME001 and a password of Cisco388267669. Which command set must be used in order to accomplish this?

- A. configure manager add ACME001 <registration key> <FMC IP>
- B. configure manager add <FMC IP> ACME001 <registration key>
- C. configure manager add DONTRESOLVE <FMC IP> AMCE001 <registration key>
- D. configure manager add <FMC IP> registration key> ACME001

**Answer: D**

#### NEW QUESTION 9

- (Exam Topic 5)

The administrator notices that there is malware present with an .exe extension and needs to verify if any of the systems on the network are running the executable file. What must be configured within Cisco AMP for Endpoints to show this data?

- A. prevalence
- B. threat root cause
- C. vulnerable software
- D. file analysis

**Answer: A**

#### NEW QUESTION 10

- (Exam Topic 5)

What is a feature of Cisco AMP private cloud?

- A. It supports anonymized retrieval of threat intelligence
- B. It supports security intelligence filtering.
- C. It disables direct connections to the public cloud.
- D. It performs dynamic analysis

**Answer: C**

#### NEW QUESTION 10

- (Exam Topic 5)

A company is in the process of deploying intrusion protection with Cisco FTDs managed by a Cisco FMC. Which action must be selected to enable fewer rules detect only critical conditions and avoid false positives?

- A. Connectivity Over Security
- B. Balanced Security and Connectivity
- C. Maximum Detection
- D. No Rules Active

**Answer: A**

#### NEW QUESTION 13

- (Exam Topic 5)

A network engineer sets up a secondary Cisco FMC that is integrated with Cisco Security Packet Analyzer. What occurs when the secondary Cisco FMC synchronizes with the primary Cisco FMC?

- A. The existing integration configuration is replicated to the primary Cisco FMC
- B. The existing configuration for integration of the secondary Cisco FMC the Cisco Security Packet Analyzer is overwritten.
- C. The synchronization between the primary and secondary Cisco FMC fails
- D. The secondary Cisco FMC must be reintegrated with the Cisco Security Packet Analyzer after the synchronization

**Answer: B**

#### NEW QUESTION 14

- (Exam Topic 5)

A connectivity issue is occurring between a client and a server which are communicating through a Cisco Firepower device. While troubleshooting, a network administrator sees that traffic is reaching the server, but the client is not getting a response. Which step must be taken to resolve this issue without initiating traffic from the client?

- A. Use packet-tracer to ensure that traffic is not being blocked by an access list.
- B. Use packet capture to ensure that traffic is not being blocked by an access list.
- C. Use packet capture to validate that the packet passes through the firewall and is NATed to the corrected IP address.
- D. Use packet-tracer to validate that the packet passes through the firewall and is NATed to the corrected IP address.

**Answer: D**

#### NEW QUESTION 18

- (Exam Topic 5)

Which action must be taken on the Cisco FMC when a packet bypass is configured in case the Snort engine is down or a packet takes too long to process?

- A. Enable Inspect Local Router Traffic
- B. Enable Automatic Application Bypass
- C. Configure Fastpath rules to bypass inspection
- D. Add a Bypass Threshold policy for failures

Answer: B

### NEW QUESTION 20

- (Exam Topic 5)

Refer to the exhibit.

```

6: 15:46:24.605132 192.168.40.11.62B30 > 172.1.1.50.80: SME 1719837470:1719837470(0) win 8192 cwnd 1460,nop,wscale 8,nop,nop,sackOK>
Phase: 1
Type: L2-EGRESS-IFC-LOOKUP
Subtype: Destination MAC L2 Lookup
Result: ALLOW
Config:
Additional Information:
Destination MAC lookup resulted in egress ifc: MGMT40_Outside1

Phase: 2
Type: CAPTURE
Subtype:
Result: ALLOW
Config:
Additional Information:
MAC Access list

Phase: 3
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
MAC Access list

Phase: 4
Type: ACCESS-LIST
Subtype: log
Result: DROP
Config:
access-group CSM_FW_ACL_global
access-list CSM_FW_ACL_advanced deny tcp any any object-group HTTP rule-id 268438528
access-list CSM_FW_ACL_remark rule-id 268438528 ACCESS-POLICY: FT0 Policy - Mandatory
access-list CSM_FW_ACL_remark rule-id 268438528 14 Full HTTP
object-group service HTTP tcp
port-object eq www
Additional Information:
Result:
input-interface: MGMT40_Inside1
input-status: up
input-line-status: up
Action: drop
Drop-reason: (acl-drop) Flow is denied by configured rule, Drop-location: frame 0x00005587afa07120 flow (NA)/NA
    
```

What must be done to fix access to this website while preventing the same communication to all other websites?

- A. Create an intrusion policy rule to have Snort allow port 80 to only 172.1.1.50.
- B. Create an access control policy rule to allow port 80 to only 172.1.1.50.
- C. Create an intrusion policy rule to have Snort allow port 443 to only 172.1.1.50
- D. Create an access control policy rule to allow port 443 to only 172.1.1.50

Answer: B

### NEW QUESTION 25

- (Exam Topic 5)

An engineer is investigating connectivity problems on Cisco Firepower that is using service group tags.

Specific devices are not being tagged correctly, which is preventing clients from using the proper policies when going through the firewall How is this issue resolved?

- A. Use traceroute with advanced options.
- B. Use Wireshark with an IP subnet filter.
- C. Use a packet capture with match criteria.
- D. Use a packet sniffer with correct filtering

Answer: C

### NEW QUESTION 29

- (Exam Topic 5)

A network administrator notices that inspection has been interrupted on all non-managed interfaces of a device. What is the cause of this?

- A. The value of the highest MTU assigned to any non-management interface was changed.
- B. The value of the highest MSS assigned to any non-management interface was changed.
- C. A passive interface was associated with a security zone.
- D. Multiple inline interface pairs were added to the same inline interface.

Answer: A

### NEW QUESTION 33

- (Exam Topic 5)

An engineer currently has a Cisco FTD device registered to the Cisco FMC and is assigned the address of 10.10.50.12. The organization is upgrading the addressing schemes and there is a requirement to convert the addresses to a format that provides an adequate amount of addresses on the network What should the engineer do to ensure that the new addressing takes effect and can be used for the Cisco FTD to Cisco FMC connection?

- A. Delete and reregister the device to Cisco FMC
- B. Update the IP addresses from IPv4 to IPv6 without deleting the device from Cisco FMC
- C. Format and reregister the device to Cisco FMC.
- D. Cisco FMC does not support devices that use IPv4 IP addresses.

**Answer:** A

#### **NEW QUESTION 38**

- (Exam Topic 5)

An administrator receives reports that users cannot access a cloud-hosted web server. The access control policy was recently updated with several new policy additions and URL filtering. What must be done to troubleshoot the issue and restore access without sacrificing the organization's security posture?

- A. Create a new access control policy rule to allow ports 80 and 443 to the FQDN of the web server.
- B. Identify the blocked traffic in the Cisco FMC connection events to validate the block, and modify the policy to allow the traffic to the web server.
- C. Verify the blocks using the packet capture tool and create a rule with the action monitor for the traffic.
- D. Download a PCAP of the traffic attempts to verify the blocks and use the flexconfig objects to create a rule that allows only the required traffic to the destination server.

**Answer:** B

#### **NEW QUESTION 40**

- (Exam Topic 5)

An engineer wants to connect a single IP subnet through a Cisco FTD firewall and enforce policy. There is a requirement to present the internal IP subnet to the outside as a different IP address. What must be configured to meet these requirements?

- A. Configure the downstream router to perform NAT.
- B. Configure the upstream router to perform NAT.
- C. Configure the Cisco FTD firewall in routed mode with NAT enabled.
- D. Configure the Cisco FTD firewall in transparent mode with NAT enabled.

**Answer:** C

#### **NEW QUESTION 44**

- (Exam Topic 5)

A Cisco FMC administrator wants to configure fastpathing of trusted network traffic to increase performance. In which type of policy would the administrator configure this feature?

- A. Identity policy
- B. Prefilter policy
- C. Network Analysis policy
- D. Intrusion policy

**Answer:** B

#### **NEW QUESTION 47**

- (Exam Topic 5)

A network engineer is receiving reports of users randomly getting disconnected from their corporate applications which traverses the data center FTD appliance. Network monitoring tools show that the FTD appliance utilization is peaking above 90% of total capacity. What must be done in order to further analyze this issue?

- A. Use the Packet Export feature to save data onto external drives
- B. Use the Packet Capture feature to collect real-time network traffic
- C. Use the Packet Tracer feature for traffic policy analysis
- D. Use the Packet Analysis feature for capturing network data

**Answer:** B

#### **NEW QUESTION 52**

- (Exam Topic 5)

With a recent summer time change, system logs are showing activity that occurred to be an hour behind real time. Which action should be taken to resolve this issue?

- A. Manually adjust the time to the correct hour on all managed devices
- B. Configure the system clock settings to use NTP with Daylight Savings checked
- C. Manually adjust the time to the correct hour on the Cisco FMC.
- D. Configure the system clock settings to use NTP

**Answer:** B

#### **NEW QUESTION 57**

- (Exam Topic 5)

An engineer is reviewing a ticket that requests to allow traffic for some devices that must connect to a server over 8699/udp. The request mentions only one IP address, 172.16.18.15, but the requestor asked for the engineer to open the port for all machines that have been trying to connect to it over the last week. Which action must the engineer take to troubleshoot this issue?

- A. Use the context explorer to see the application blocks by protocol.
- B. Use the context explorer to see the destination port blocks
- C. Filter the connection events by the source port 8699/udp.

D. Filter the connection events by the destination port 8699/udp.

**Answer:** D

**NEW QUESTION 62**

- (Exam Topic 5)

A network engineer is logged into the Cisco AMP for Endpoints console and sees a malicious verdict for an identified SHA-256 hash. Which configuration is needed to mitigate this threat?

- A. Use regular expressions to block the malicious file.
- B. Add the hash from the infected endpoint to the network block list.
- C. Add the hash to the simple custom detection list.
- D. Enable a personal firewall in the infected endpoint.

**Answer:** C

**NEW QUESTION 64**

- (Exam Topic 5)

An engineer is troubleshooting connectivity to the DNS servers from hosts behind a new Cisco FTD device. The hosts cannot send DNS queries to servers in the DMZ. Which action should the engineer take to troubleshoot this issue using the real DNS packets?

- A. Use the Connection Events dashboard to check the block reason and adjust the inspection policy as needed.
- B. Use the packet capture tool to check where the traffic is being blocked and adjust the access control or intrusion policy as needed.
- C. Use the packet tracer tool to determine at which hop the packet is being dropped.
- D. Use the show blocks command in the Threat Defense CLI tool and create a policy to allow the blocked traffic.

**Answer:** A

**NEW QUESTION 67**

- (Exam Topic 5)

A security engineer must deploy a Cisco FTD appliance as a bump in the wire to detect intrusion events without disrupting the flow of network traffic. Which two features must be configured to accomplish the task? (Choose two.)

- A. inline set pair
- B. transparent mode
- C. tapemode
- D. passive interfaces
- E. bridged mode

**Answer:** BC

**NEW QUESTION 68**

- (Exam Topic 5)

A network administrator is troubleshooting access to a website hosted behind a Cisco FTD device. External clients cannot access the web server via HTTPS. The IP address configured on the web server is 192.168.7.46. The administrator is running the command capture CAP interface outside match ip any 192.168.7.46 255.255.255.255 but cannot see any traffic in the capture. Why is this occurring?

- A. The capture must use the public IP address of the web server.
- B. The FTD has no route to the web server.
- C. The access policy is blocking the traffic.
- D. The packet capture shows only blocked traffic.

**Answer:** A

**NEW QUESTION 73**

- (Exam Topic 5)

An engineer runs the command `restore remote-manager-backup location 2.2.2.2 admin /Volume/home/admin FTD408566513.zip` on a Cisco FMC. After connecting to the repository, the Cisco FTD device is unable to accept the backup file. What is the reason for this failure?

- A. The backup file is not in .cfg format.
- B. The wrong IP address is used.
- C. The backup file extension was changed from .tar to .zip.
- D. The directory location is incorrect.

**Answer:** C

**Explanation:**

Reference: <https://www.ciscolive.com/c/dam/r/ciscolive/emea/docs/2019/pdf/BRKSEC-3455.pdf>

**NEW QUESTION 77**

- (Exam Topic 5)

An engineer must configure the firewall to monitor traffic within a single subnet without increasing the hop count of that traffic. How would the engineer achieve this?

- A. Configure Cisco Firepower as a transparent firewall.
- B. Set up Cisco Firepower as managed by Cisco FDM.
- C. Configure Cisco Firepower in FXOS monitor only mode.

D. Set up Cisco Firepower in intrusion prevention mode

**Answer:** A

**NEW QUESTION 79**

- (Exam Topic 5)

A mid-sized company is experiencing higher network bandwidth utilization due to a recent acquisition. The network operations team is asked to scale up their one Cisco FTD appliance deployment to higher capacities due to the increased network bandwidth. Which design option should be used to accomplish this goal?

- A. Deploy multiple Cisco FTD appliances in firewall clustering mode to increase performance.
- B. Deploy multiple Cisco FTD appliances using VPN load-balancing to scale performance.
- C. Deploy multiple Cisco FTD HA pairs to increase performance.
- D. Deploy multiple Cisco FTD HA pairs in clustering mode to increase performance.

**Answer:** A

**NEW QUESTION 81**

- (Exam Topic 5)

An administrator must use Cisco FMC to install a backup route within the Cisco FTD to route traffic in case of a routing failure with the primary route. Which action accomplishes this task?

- A. Install the static backup route and modify the metric to be less than the primary route.
- B. Configure EIGRP routing on the FMC to ensure that dynamic routes are always updated.
- C. Use a default route on the FMC instead of having multiple routes contending for priority.
- D. Create the backup route and use route tracking on both routes to a destination IP address in the network.

**Answer:** A

**NEW QUESTION 85**

- (Exam Topic 5)

What is the RTC workflow when the infected endpoint is identified?

- A. Cisco ISE instructs Cisco AMP to contain the infected endpoint.
- B. Cisco ISE instructs Cisco FMC to contain the infected endpoint.
- C. Cisco AMP instructs Cisco FMC to contain the infected endpoint.
- D. Cisco FMC instructs Cisco ISE to contain the infected endpoint.

**Answer:** D

**NEW QUESTION 86**

- (Exam Topic 4)

Which two remediation options are available when Cisco FMC is integrated with Cisco ISE? (Choose two.)

- A. dynamic null route configured
- B. DHCP pool disablement
- C. quarantine
- D. port shutdown
- E. host shutdown

**Answer:** CD

**Explanation:**

Reference: <https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/210524-configure-firepower-6-1-pxgrid-remediate.html>

**NEW QUESTION 87**

- (Exam Topic 4)

Which action should you take when Cisco Threat Response notifies you that AMP has identified a file as malware?

- A. Add the malicious file to the block list.
- B. Send a snapshot to Cisco for technical support.
- C. Forward the result of the investigation to an external threat-analysis engine.
- D. Wait for Cisco Threat Response to automatically block the malware.

**Answer:** A

**NEW QUESTION 89**

- (Exam Topic 5)

An analyst is reviewing the Cisco FMC reports for the week. They notice that some peer-to-peer applications are being used on the network and they must identify which poses the greatest risk to the environment. Which report gives the analyst this information?

- A. Attacks Risk Report
- B. User Risk Report
- C. Network Risk Report
- D. Advanced Malware Risk Report

**Answer:** C

#### NEW QUESTION 94

- (Exam Topic 5)

The event dashboard within the Cisco FMC has been inundated with low priority intrusion drop events, which are overshadowing high priority events. An engineer has been tasked with reviewing the policies and reducing the low priority events. Which action should be configured to accomplish this task?

- A. generate events
- B. drop packet
- C. drop connection
- D. drop and generate

**Answer: B**

#### Explanation:

Reference"

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

#### NEW QUESTION 97

- (Exam Topic 5)

An engineer must define a URL object on Cisco FMC. What is the correct method to specify the URL without performing SSL inspection?

- A. Use Subject Common Name value.
- B. Specify all subdomains in the object group.
- C. Specify the protocol in the object.
- D. Include all URLs from CRL Distribution Points.

**Answer: B**

#### NEW QUESTION 101

- (Exam Topic 3)

Which command should be used on the Cisco FTD CLI to capture all the packets that hit an interface?

- A. configure coredump packet-engine enable
- B. capture-traffic
- C. capture
- D. capture WORD

**Answer: C**

#### Explanation:

Reason: the command "capture-traffic" is used for SNORT Engine Captures. To capture a LINA Engine Capture, you use the "capture" command. Since the Lina Engine represents the actual physical interface of the device, "capture" is the only reasonable choice Reference:

<https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/212474-working-with-firepower-threat-de>

The command is `firepower# capture DMZ interface dmz trace detail match ip host 192.168.76.14 host 192.168.76.100 firepower# capture INSIDE interface inside trace detail match ip host 192.168.76.14 host 192.168.75.14`

#### NEW QUESTION 106

- (Exam Topic 4)

Which two features of Cisco AMP for Endpoints allow for an uploaded file to be blocked? (Choose two.)

- A. application blocking
- B. simple custom detection
- C. file repository
- D. exclusions
- E. application whitelisting

**Answer: AB**

#### NEW QUESTION 111

- (Exam Topic 3)

Which command is typed at the CLI on the primary Cisco FTD unit to temporarily stop running high- availability?

- A. configure high-availability resume
- B. configure high-availability disable
- C. system support network-options
- D. configure high-availability suspend

**Answer: B**

#### Explanation:

Reference: [https://www.cisco.com/c/en/us/td/docs/security/firepower/610/configuration/guide/fpmc-config-guide-v61/firepower\\_threat\\_defense\\_high\\_availability.html](https://www.cisco.com/c/en/us/td/docs/security/firepower/610/configuration/guide/fpmc-config-guide-v61/firepower_threat_defense_high_availability.html)

#### NEW QUESTION 116

- (Exam Topic 3)

Which CLI command is used to generate firewall debug messages on a Cisco Firepower?

- A. system support firewall-engine-debug
- B. system support ssl-debug
- C. system support platform
- D. system support dump-table

**Answer:** A

**Explanation:**

Reference: <https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/212330-firepower-management-center-display-acc.html>

**NEW QUESTION 117**

- (Exam Topic 3)

Which two packet captures does the FTD LINA engine support? (Choose two.)

- A. Layer 7 network ID
- B. source IP
- C. application ID
- D. dynamic firewall importing
- E. protocol

**Answer:** BE

**Explanation:**

Reference: <https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/212474-working-with-firepower-threat-defense-f.html>

**NEW QUESTION 122**

- (Exam Topic 2)

An engineer configures a network discovery policy on Cisco FMC. Upon configuration, it is noticed that excessive and misleading events filling the database and overloading the Cisco FMC. A monitored NAT device is executing multiple updates of its operating system in a short period of time. What configuration change must be made to alleviate this issue?

- A. Leave default networks.
- B. Change the method to TCP/SYN.
- C. Increase the number of entries on the NAT device.
- D. Exclude load balancers and NAT devices.

**Answer:** D

**Explanation:**

Reference:

<https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Netwo>

**NEW QUESTION 123**

- (Exam Topic 2)

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?

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

**Answer:** D

**Explanation:**

<https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-config-guide-v62/reusa> "All interfaces in an interface object must be of the same type: all inline, passive, switched, routed, or ASA FirePOWER. After you create an interface object, you cannot change the type of interfaces it contains."

**NEW QUESTION 126**

- (Exam Topic 2)

What is the disadvantage of setting up a site-to-site VPN in a clustered-units environment?

- A. VPN connections can be re-established only if the failed master unit recovers.
- B. Smart License is required to maintain VPN connections simultaneously across all cluster units.
- C. VPN connections must be re-established when a new master unit is elected.
- D. Only established VPN connections are maintained when a new master unit is elected.

**Answer:** C

**Explanation:**

Reference: [https://www.cisco.com/c/en/us/td/docs/security/firepower/fxos/clustering/ftd-cluster-solution.html#concept\\_g32\\_yml\\_y2b](https://www.cisco.com/c/en/us/td/docs/security/firepower/fxos/clustering/ftd-cluster-solution.html#concept_g32_yml_y2b)

**NEW QUESTION 127**

- (Exam Topic 2)

A company has many Cisco FTD devices managed by a Cisco FMC. The security model requires that access control rule logs be collected for analysis. The security engineer is concerned that the Cisco FMC will not be able to process the volume of logging that will be generated. Which configuration addresses this concern?

- A. Send Cisco FTD connection events and security events directly to SIEM system for storage and analysis.
- B. Send Cisco FTD connection events and security events to a cluster of Cisco FMC devices for storage and analysis.
- C. Send Cisco FTD connection events and security events to Cisco FMC and configure it to forward logs to SIEM for storage and analysis.
- D. Send Cisco FTD connection events directly to a SIEM system and forward security events from Cisco FMC to the SIEM system for storage and analysis.

**Answer: C**

#### **NEW QUESTION 130**

- (Exam Topic 2)

Which two statements about bridge-group interfaces in Cisco FTD are true? (Choose two.)

- A. The BVI IP address must be in a separate subnet from the connected network.
- B. Bridge groups are supported in both transparent and routed firewall modes.
- C. Bridge groups are supported only in transparent firewall mode.
- D. Bidirectional Forwarding Detection echo packets are allowed through the FTD when using bridge-group members.
- E. Each directly connected network must be on the same subnet.

**Answer: BE**

#### **Explanation:**

Reference: [https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-config\\_guide-v62/transparent\\_or\\_routed\\_firewall\\_mode\\_for\\_firepower\\_threat\\_defense.html](https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-config_guide-v62/transparent_or_routed_firewall_mode_for_firepower_threat_defense.html)

#### **NEW QUESTION 132**

- (Exam Topic 1)

Which interface type allows packets to be dropped?

- A. passive
- B. inline
- C. ERSPAN
- D. TAP

**Answer: B**

#### **Explanation:**

Reference:

<https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/200908-configuring-firepower-threat-defense-int.html>

#### **NEW QUESTION 135**

- (Exam Topic 1)

An organization is migrating their Cisco ASA devices running in multicontext mode to Cisco FTD devices. Which action must be taken to ensure that each context on the Cisco ASA is logically separated in the Cisco FTD devices?

- A. Add a native instance to distribute traffic to each Cisco FTD context.
- B. Add the Cisco FTD device to the Cisco ASA port channels.
- C. Configure a container instance in the Cisco FTD for each context in the Cisco ASA.
- D. Configure the Cisco FTD to use port channels spanning multiple networks.

**Answer: C**

#### **NEW QUESTION 136**

- (Exam Topic 1)

Which two deployment types support high availability? (Choose two.)

- A. transparent
- B. routed
- C. clustered
- D. intra-chassis multi-instance
- E. virtual appliance in public cloud

**Answer: AB**

#### **Explanation:**

Reference: [https://www.cisco.com/c/en/us/td/docs/security/firepower/610/configuration/guide/fpmc-config\\_guide-v61/firepower\\_threat\\_defense\\_high\\_availability.html](https://www.cisco.com/c/en/us/td/docs/security/firepower/610/configuration/guide/fpmc-config_guide-v61/firepower_threat_defense_high_availability.html)

#### **NEW QUESTION 138**

- (Exam Topic 1)

What are the minimum requirements to deploy a managed device inline?

- A. inline interfaces, security zones, MTU, and mode
- B. passive interface, MTU, and mode
- C. inline interfaces, MTU, and mode
- D. passive interface, security zone, MTU, and mode

**Answer: C**

**Explanation:**

Reference: [https://www.cisco.com/c/en/us/td/docs/security/firepower/650/configuration/guide/fpmc-config-guide-v65/ips\\_device\\_deployments\\_and\\_configuration.html](https://www.cisco.com/c/en/us/td/docs/security/firepower/650/configuration/guide/fpmc-config-guide-v65/ips_device_deployments_and_configuration.html)

**NEW QUESTION 142**

- (Exam Topic 1)

With Cisco Firepower Threat Defense software, which interface mode must be configured to passively receive traffic that passes through the appliance?

- A. inline set
- B. passive
- C. routed
- D. inline tap

**Answer: B**

**Explanation:**

Reference: [https://www.cisco.com/c/en/us/td/docs/security/firepower/640/configuration/guide/fpmc-config-guide-v64/interface\\_overview\\_for\\_firepower\\_threat\\_defense.html](https://www.cisco.com/c/en/us/td/docs/security/firepower/640/configuration/guide/fpmc-config-guide-v64/interface_overview_for_firepower_threat_defense.html)

**NEW QUESTION 145**

- (Exam Topic 1)

Which two conditions must be met to enable high availability between two Cisco FTD devices? (Choose two.)

- A. same flash memory size
- B. same NTP configuration
- C. same DHCP/PPoE configuration
- D. same host name
- E. same number of interfaces

**Answer: BE**

**Explanation:**

<https://www.cisco.com/c/en/us/support/docs/security/firepower-management-center/212699-configure-ftd-high-Conditions>

In order to create an HA between 2 FTD devices, these conditions must be met: Same model

Same version (this applies to FXOS and to FTD - (major (first number), minor (second number), and maintenance (third number) must be equal))

Same number of interfaces

Same type of interfaces

Both devices as part of same group/domain in FMC

Have identical Network Time Protocol (NTP) configuration Be fully deployed on the FMC without uncommitted changes Be in the same firewall mode: routed or transparent.

Note that this must be checked on both FTD devices and FMC GUI since there have been cases where the FTDs had the same mode, but FMC does not reflect this.

Does not have DHCP/Point-to-Point Protocol over Ethernet (PPPoE) configured in any of the interface Different hostname (Fully Qualified Domain Name (FQDN)) for both chassis. In order to check the chassis

hostname navigate to FTD CLI and run this command

**NEW QUESTION 147**

- (Exam Topic 1)

An engineer is configuring a Cisco IPS to protect the network and wants to test a policy before deploying it. A copy of each incoming packet needs to be monitored while traffic flow remains constant. Which IPS mode should be implemented to meet these requirements?

- A. Inline tap
- B. passive
- C. transparent
- D. routed

**Answer: A**

**NEW QUESTION 150**

- (Exam Topic 1)

Which two dynamic routing protocols are supported in Firepower Threat Defense without using FlexConfig? (Choose two.)

- A. EIGRP
- B. OSPF
- C. static routing
- D. IS-IS
- E. BGP

**Answer: BE**

**Explanation:**

Reference:

<https://www.cisco.com/c/en/us/td/docs/security/firepower/660/fdm/fptd-fdm-config-guide-660/fptd-fdm-routing.html>

**NEW QUESTION 152**

.....

## **Thank You for Trying Our Product**

### **We offer two products:**

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

### **300-710 Practice Exam Features:**

- \* 300-710 Questions and Answers Updated Frequently
- \* 300-710 Practice Questions Verified by Expert Senior Certified Staff
- \* 300-710 Most Realistic Questions that Guarantee you a Pass on Your First Try
- \* 300-710 Practice Test Questions in Multiple Choice Formats and Updates for 1 Year

**100% Actual & Verified — Instant Download, Please Click**  
**[Order The 300-710 Practice Test Here](#)**