

## 300-710 Dumps

### Securing Networks with Cisco Firepower (SNCF)

<https://www.certleader.com/300-710-dumps.html>



**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)

Which Cisco FMC report gives the analyst information about the ports and protocols that are related to the configured sensitive network for analysis?

- A. Malware Report
- B. Host Report
- C. Firepower Report
- D. Network Report

**Answer: D**

**NEW QUESTION 4**

- (Exam Topic 5)

A user within an organization opened a malicious file on a workstation which in turn caused a ransomware attack on the network. What should be configured within the Cisco FMC to ensure the file is tested for viruses on a sandbox system?

- A. Capacity handling
- B. Local malware analysis
- C. Spere analysis
- D. Dynamic analysis

**Answer: D**

**NEW QUESTION 5**

- (Exam Topic 5)

An engineer integrates Cisco FMC and Cisco ISE using pxGrid. Which role is assigned for Cisco FMC?

- A. controller
- B. publisher
- C. client
- D. server

**Answer: C**

**NEW QUESTION 6**

- (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 7**

- (Exam Topic 5)

A Cisco FTD device is running in transparent firewall mode with a VTEP bridge group member ingress interface. What must be considered by an engineer tasked with specifying a destination MAC address for a packet trace?

- A. The destination MAC address is optional if a VLAN ID value is entered
- B. Only the UDP packet type is supported
- C. The output format option for the packet logs unavailable
- D. The VLAN ID and destination MAC address are optional

**Answer:** A

**NEW QUESTION 8**

- (Exam Topic 5)

A network security engineer must export packet captures from the Cisco FMC web browser while troubleshooting an issue. When navigating to the address <https://<FMC IP>/capture/CAP1/pcap/test.pcap>, an error 403: Forbidden is given instead of the PCAP file. Which action must the engineer take to resolve this issue?

- A. Disable the HTTPS server and use HTTP instead.
- B. Enable the HTTPS server for the device platform policy.
- C. Disable the proxy setting on the browser.
- D. Use the Cisco FTD IP address as the proxy server setting on the browser.

**Answer:** B

**NEW QUESTION 9**

- (Exam Topic 5)

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.....

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

**Answer:** A

**NEW QUESTION 10**

- (Exam Topic 5)

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?

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

**Answer:** A

**NEW QUESTION 10**

- (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 15

- (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 20

- (Exam Topic 5)

An engineer is troubleshooting a device that cannot connect to a web server. The connection is initiated from the Cisco FTD inside interface and attempting to reach 10.0.1.100 over the non-standard port of 9443 The host the engineer is attempting the connection from is at the IP address of 10.20.10.20. In order to determine what is happening to the packets on the network, the engineer decides to use the FTD packet capture tool Which capture configuration should be used to gather the information needed to troubleshoot this issue?

A)

**Add Capture** ? X

Name\*: Server1\_Capture Interface\*: Inside

Match Criteria:

Protocol\*: IP

Source Host\*: 10.0.1.100 Source Network: 10.0.0.0/24

Destination Host\*: 10.20.10.20 Destination Network: 10.20.0.0/24

☐ SGT number: 0 (0-65533)

Buffer:

Packet Size: 1518 14-1522 bytes ☒ Continuous Capture ☒ Trace

Buffer Size: 524288 1534-33554432 bytes ☐ Stop when full Trace Count: 50

Save Cancel

B)

**Add Capture** ? X

Name\*: Server1\_Capture Interface\*: Inside

Match Criteria:

Protocol\*: IP

Source Host\*: 10.20.10.20 Source Network: 10.20.0.0/24

Destination Host\*: 10.0.1.100 Destination Network: 10.0.0.0/24

☐ SGT number: 0 (0-65533)

Buffer:

Packet Size: 1518 14-1522 bytes ☒ Continuous Capture ☒ Trace

Buffer Size: 524288 1534-33554432 bytes ☐ Stop when full Trace Count: 50

C)

**Add Capture** ? X

Name\*: Server1\_Capture Interface\*: diagnostic

Match Criteria:

Protocol\*: IP

Source Host\*: 10.20.10.20 Source Network: 10.20.0.0/24

Destination Host\*: 10.0.1.100 Destination Network: 10.0.0.0/24

☐ SGT number: 0 (0-65533)

Buffer:

Packet Size: 1518 14-1522 bytes ☒ Continuous Capture ☒ Trace

Buffer Size: 524288 1534-33554432 bytes ☐ Stop when full Trace Count: 50

Save Cancel

D)



**Add Capture**

Name\*:  Interface\*:

**Match Criteria:**

Protocol\*:

Source Host\*:  Source Network:

Destination Host\*:  Destination Network:

☐ SGT number:  (0-65533)

**Buffer:**

Packet Size:  14-1522 bytes

Buffer Size:  1534-33554432 bytes

☒ Continuous Capture ☒ Trace

☐ Stop when full Trace Count:

- A. Option A
- B. Option B
- C. Option C
- D. Option D

**Answer:** B

#### NEW QUESTION 25

- (Exam Topic 5)

What is an advantage of adding multiple inline interface pairs to the same inline interface set when deploying an asynchronous routing configuration?

- A. Allows the IPS to identify inbound and outbound traffic as part of the same traffic flow.
- B. The interfaces disable autonegotiation and interface speed is hard coded set to 1000 Mbps.
- C. Allows traffic inspection to continue without interruption during the Snort process restart.
- D. The interfaces are automatically configured as a media-independent interface crossover.

**Answer:** A

#### Explanation:

<https://www.cisco.com/c/en/us/td/docs/security/firepower/601/configuration/guide/fpmc-config-guide-v601/fpm>

#### NEW QUESTION 29

- (Exam Topic 5)

An engineer installs a Cisco FTD device and wants to inspect traffic within the same subnet passing through a firewall and inspect traffic destined to the internet. Which configuration will meet this requirement?

- A. transparent firewall mode with IRB only
- B. routed firewall mode with BVI and routed interfaces
- C. transparent firewall mode with multiple BVIs
- D. routed firewall mode with routed interfaces only

**Answer:** C

#### NEW QUESTION 33

- (Exam Topic 5)

An organization is configuring a new Cisco Firepower High Availability deployment. Which action must be taken to ensure that failover is as seamless as possible to end users?

- A. Set up a virtual failover MAC address between chassis.
- B. Use a dedicated stateful link between chassis.
- C. Load the same software version on both chassis.
- D. Set the same FQDN for both chassis.

**Answer:** B

#### NEW QUESTION 37

- (Exam Topic 5)

An administrator is configuring their transparent Cisco FTD device to receive ERSPAN traffic from multiple switches on a passive port, but the Cisco FTD is not processing the traffic. What is the problem?

- A. The switches do not have Layer 3 connectivity to the FTD device for GRE traffic transmission.

- B. The switches were not set up with a monitor session ID that matches the flow ID defined on the CiscoFTD.  
C. The Cisco FTD must be in routed mode to process ERSPAN traffic.  
D. The Cisco FTD must be configured with an ERSPAN port not a passive port.

**Answer:** C

#### NEW QUESTION 42

- (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 47

- (Exam Topic 5)

A network engineer wants to add a third-party threat feed into the Cisco FMC for enhanced threat detection. Which action should be taken to accomplish this goal?

- A. Enable Threat Intelligence Director using STIX and TAXII  
B. Enable Rapid Threat Containment using REST APIs  
C. Enable Threat Intelligence Director using REST APIs  
D. Enable Rapid Threat Containment using STIX and TAXII

**Answer:** A

#### NEW QUESTION 51

- (Exam Topic 5)

An engineer must configure a Cisco FMC dashboard in a child domain. Which action must be taken so that the dashboard is visible to the parent domain?

- A. Add a separate tab.  
B. Adjust policy inheritance settings.  
C. Add a separate widget.  
D. Create a copy of the dashboard.

**Answer:** D

#### NEW QUESTION 54

- (Exam Topic 5)

A network administrator configured a NAT policy that translates a public IP address to an internal web server IP address. An access policy has also been created that allows any source to reach the public IP address on port 80. The web server is still not reachable from the Internet on port 80. Which configuration change is needed?

- A. The intrusion policy must be disabled for port 80.  
B. The access policy rule must be configured for the action trust.  
C. The NAT policy must be modified to translate the source IP address as well as destination IP address.  
D. The access policy must allow traffic to the internal web server IP address.

**Answer:** D

#### NEW QUESTION 59

- (Exam Topic 5)

Refer to the exhibit.

II. ASSESSMENT RESULTS	
AUTOMATING THE TUNING EFFORT	
During the assessment period, the following changes to your network were observed.	
NETWORK CHANGE TYPE	NUMBER OF CHANGES
A new operating system was found	310
A new host was added to the network	366
A device started using a new transport protocol	381
A device started using a new network protocol	373

And engineer is analyzing the Attacks Risk Report and finds that there are over 300 instances of new operating systems being seen on the network. How is the Firepower configuration updated to protect these new operating systems?

- A. Cisco Firepower automatically updates the policies.

- B. The administrator requests a Remediation Recommendation Report from Cisco Firepower
- C. Cisco Firepower gives recommendations to update the policies.
- D. The administrator manually updates the policies.

**Answer:** C

**Explanation:**

Ref:

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

**NEW QUESTION 64**

- (Exam Topic 5)

An organization is implementing Cisco FTD using transparent mode in the network. Which rule in the default Access Control Policy ensures that this deployment does not create a loop in the network?

- A. ARP inspection is enabled by default.
- B. Multicast and broadcast packets are denied by default.
- C. STP BPDU packets are allowed by default.
- D. ARP packets are allowed by default.

**Answer:** B

**NEW QUESTION 65**

- (Exam Topic 5)

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?

- A. Configure a second circuit to an ISP for added redundancy
- B. Keep a copy of the current configuration to use as backup
- C. Configure the Cisco FMCs for failover
- D. Configure the Cisco FMC managed devices for clustering.

**Answer:** B

**NEW QUESTION 70**

- (Exam Topic 5)

While integrating Cisco Umbrella with Cisco Threat Response, a network security engineer wants to automatically push blocking of domains from the Cisco Threat Response interface to Cisco Umbrella. Which API meets this requirement?

- A. investigate
- B. reporting
- C. enforcement
- D. REST

**Answer:** D

**NEW QUESTION 72**

- (Exam Topic 5)

What is the advantage of having Cisco Firepower devices send events to Cisco Threat Response via the security services exchange portal directly as opposed to using syslog?

- A. All types of Cisco Firepower devices are supported.
- B. An on-premises proxy server does not need to be set up and maintained.
- C. Cisco Firepower devices do not need to be connected to the Internet.
- D. Supports all devices that are running supported versions of Cisco Firepower.

**Answer:** B

**NEW QUESTION 77**

- (Exam Topic 5)

A security engineer needs to configure a network discovery policy on a Cisco FMC appliance and prevent excessive network discovery events from overloading the FMC database? Which action must be taken to accomplish this task?

- A. Change the network discovery method to TCP/SYN.
- B. Configure NetFlow exporters for monitored networks.
- C. Monitor only the default IPv4 and IPv6 network ranges.
- D. Exclude load balancers and NAT devices in the policy.

**Answer:** D

**NEW QUESTION 80**

- (Exam Topic 5)

An organization has seen a lot of traffic congestion on their links going out to the internet There is a Cisco Firepower device that processes all of the traffic going to the internet prior to leaving the enterprise. How is the congestion alleviated so that legitimate business traffic reaches the destination?

- A. Create a flexconfig policy to use WCCP for application aware bandwidth limiting
- B. Create a VPN policy so that direct tunnels are established to the business applications



- C. Create a NAT policy so that the Cisco Firepower device does not have to translate as many addresses
- D. Create a QoS policy rate-limiting high bandwidth applications

**Answer:** D

#### NEW QUESTION 82

- (Exam Topic 5)

Which two considerations must be made when deleting and re-adding devices while managing them via Cisco FMC (Choose two).

- A. Before re-adding the device In Cisco FMC, the manager must be added back.
- B. The Cisco FMC web interface prompts users to re-apply access control policies.
- C. Once a device has been deleted, It must be reconfigured before it is re-added to the Cisco FMC.
- D. 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.
- E. 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.

**Answer:** BE

#### NEW QUESTION 87

- (Exam Topic 5)

An engineer is troubleshooting application failures through a FTD deployment. While using the FMC CLI. it has been determined that the traffic in question is not matching the desired policy. What should be done to correct this?

- A. Use the system support firewall-engine-debug command to determine which rules the traffic matching and modify the rule accordingly
- B. Use the system support application-identification-debug command to determine which rules the traffic matching and modify the rule accordingly
- C. Use the system support firewall-engine-dump-user-f density-data command to change the policy and allow the application through the firewall.
- D. Use the system support network-options command to fine tune the policy.

**Answer:** A

#### NEW QUESTION 91

- (Exam Topic 5)

An engineer is configuring two new Cisco FTD devices to replace the existing high availability firewall pair in a highly secure environment. The information exchanged between the FTD devices over the failover link must be encrypted. Which protocol supports this on the Cisco FTD?

- A. IPsec
- B. SSH
- C. SSL
- D. MACsec

**Answer:** A

#### NEW QUESTION 94

- (Exam Topic 5)

The network administrator wants to enhance the network security posture by enabling machine learning for malware detection due to a concern with suspicious Microsoft executable file types that were seen while creating monthly security reports for the CIO. Which feature must be enabled to accomplish this goal?

- A. Spero
- B. dynamic analysis
- C. static analysis
- D. Ethos

**Answer:** A

#### NEW QUESTION 95

- (Exam Topic 5)

A company is deploying intrusion protection on multiple Cisco FTD appliances managed by Cisco FMC. Which system-provided policy must be selected if speed and detection are priorities?

- A. Connectivity Over Security
- B. Security Over Connectivity
- C. Maximum Detection
- D. Balanced Security and Connectivity

**Answer:** D

#### NEW QUESTION 99

- (Exam Topic 5)

While configuring FTD, a network engineer wants to ensure that traffic passing through the appliance does not require routing or Vlan rewriting. Which interface mode should the engineer implement to accomplish this task?

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

**Answer:** B

**NEW QUESTION 104**

- (Exam Topic 5)

An engineer is configuring multiple Cisco FTD appliances (or use in the network. Which rule must the engineer follow while defining interface objects in Cisco FMC for use with interfaces across multiple devices?

- A. An interface cannot belong to a security zone and an interface group
- B. Interface groups can contain multiple interface types
- C. Interface groups can contain interfaces from many devices.
- D. Two security zones can contain the same interface

**Answer:** C

**NEW QUESTION 107**

- (Exam Topic 5)

A network administrator has converted a Cisco FTD from using LDAP to LDAPS for VPN authentication. The Cisco FMC can connect to the LDAPS server, but the Cisco FTD is not connecting. Which configuration must be enabled on the Cisco FTD?

- A. SSL must be set to a use TLSv1.2 or lower.
- B. The LDAPS must be allowed through the access control policy.
- C. DNS servers must be defined for name resolution.
- D. The RADIUS server must be defined.

**Answer:** B

**NEW QUESTION 112**

- (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 116**

- (Exam Topic 5)

An administrator is adding a new URL-based category feed to the Cisco FMC for use within the policies. The intelligence source does not use STIX. but instead uses a .txt file format. Which action ensures that regular updates are provided?

- A. Add a URL source and select the flat file type within Cisco FMC.
- B. Upload the .txt file and configure automatic updates using the embedded URL.
- C. Add a TAXII feed source and input the URL for the feed.
- D. Convert the .txt file to STIX and upload it to the Cisco FMC.

**Answer:** A

**NEW QUESTION 119**

- (Exam Topic 5)

An engineer needs to configure remote storage on Cisco FMC. Configuration backups must be available from a secure location on the network for disaster recovery. Reports need to back up to a shared location that auditors can access with their Active Directory logins. Which strategy must the engineer use to meet these objectives?

- A. Use SMB for backups and NFS for reports.
- B. Use NFS for both backups and reports.
- C. Use SMB for both backups and reports.
- D. Use SSH for backups and NFS for reports.

**Answer:** C

**Explanation:**

<https://www.cisco.com/c/en/us/td/docs/security/firepower/640/configuration/guide/fpmc-config-guide-v64/syste> "You cannot send backups to one remote system and reports to another, but you can choose to send either to a remote system and store the other on the Firepower Management Center."

**NEW QUESTION 120**

- (Exam Topic 5)

What is the advantage of having Cisco Firepower devices send events to Cisco Threat response via the security services exchange portal directly as opposed to using syslog?

- A. Firepower devices do not need to be connected to the internet.
- B. All types of Firepower devices are supported.
- C. Supports all devices that are running supported versions of Firepower
- D. An on-premises proxy server does not need to set up and maintained

**Answer:** D

**Explanation:**

Reference: [https://www.cisco.com/c/en/us/td/docs/security/firepower/integrations/CTR/Firepower\\_and\\_Cisco\\_Threat\\_Response\\_Integration\\_Guide.pdf](https://www.cisco.com/c/en/us/td/docs/security/firepower/integrations/CTR/Firepower_and_Cisco_Threat_Response_Integration_Guide.pdf)

**NEW QUESTION 123**

- (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 127**

- (Exam Topic 5)

What must be implemented on Cisco Firepower to allow multiple logical devices on a single physical device to have access to external hosts?

- A. Add at least two container instances from the same module.
- B. Set up a cluster control link between all logical devices
- C. Add one shared management interface on all logical devices.
- D. Define VLAN subinterfaces for each logical device.

**Answer: C**

**NEW QUESTION 128**

- (Exam Topic 5)

When using Cisco Threat Response, which phase of the Intelligence Cycle publishes the results of the investigation?

- A. direction
- B. dissemination
- C. processing
- D. analysis

**Answer: B**

**Explanation:**

Disseminate: The dissemination phase

publishes the results of the investigation or threat hunt. This

information is disseminated with a focus on the receivers of the information. At the tactical level, this information feeds back into the beginning of the F3EAD model, Find. Figure 3 illustrates the F3EAD model.

**NEW QUESTION 131**

- (Exam Topic 5)

A network administrator registered a new FTD to an existing FMC. The administrator cannot place the FTD in transparent mode. Which action enables transparent mode?

- A. Add a Bridge Group Interface to the FTD before transparent mode is configured.
- B. Deregister the FTD device from FMC and configure transparent mode via the CLI.
- C. Obtain an FTD model that supports transparent mode.
- D. Assign an IP address to two physical interfaces.

**Answer: B**

**NEW QUESTION 136**

- (Exam Topic 5)

An organization recently implemented a transparent Cisco FTD in their network. They must ensure that the device does not respond to insecure SSL/TLS protocols. Which action accomplishes the task?

- A. Modify the device's settings using the device management feature within Cisco FMC to force only secure protocols.
- B. Use the Cisco FTD platform policy to change the minimum SSL version on the device to TLS 1.2.
- C. Enable the UCAPL/CC compliance on the device to support only the most secure protocols available.
- D. Configure a FlexConfig object to disable any insecure TLS protocols on the Cisco FTD device.

**Answer: B**

**NEW QUESTION 139**

- (Exam Topic 5)

An organization has a Cisco IPS running in inline mode and is inspecting traffic for malicious activity. When traffic is received by the Cisco IPS, if it is not dropped, how does the traffic get to its destination?

- A. It is retransmitted from the Cisco IPS inline set.
- B. The packets are duplicated and a copy is sent to the destination.
- C. It is transmitted out of the Cisco IPS outside interface.
- D. It is routed back to the Cisco ASA interfaces for transmission.

**Answer:** A

**NEW QUESTION 140**

- (Exam Topic 5)

A network administrator needs to create a policy on Cisco Firepower to fast-path traffic to avoid Layer 7 inspection. The rate at which traffic is inspected must be optimized. What must be done to achieve this goal?

- A. Enable the FXOS for multi-instance.
- B. Configure a prefilter policy.
- C. Configure modular policy framework.
- D. Disable TCP inspection.

**Answer:** B

**NEW QUESTION 145**

- (Exam Topic 5)

A network administrator is configuring an FTD in transparent mode. A bridge group is set up and an access policy has been set up to allow all IP traffic. Traffic is not passing through the FTD. What additional configuration is needed?

- A. The security levels of the interfaces must be set.
- B. A default route must be added to the FTD.
- C. An IP address must be assigned to the BVI.
- D. A mac-access control list must be added to allow all MAC addresses.

**Answer:** C

**NEW QUESTION 149**

- (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 153**

- (Exam Topic 5)

A security engineer is configuring an Access Control Policy for multiple branch locations. These locations share a common rule set and utilize a network object called INSIDE\_NET which contains the locally significant internal network subnets at each location. Which technique will retain the policy consistency at each location but allow only the locally significant network subnet within the applicable rules?

- A. utilizing a dynamic Access Control Policy that updates from Cisco Talos
- B. utilizing policy inheritance
- C. creating a unique Access Control Policy per device
- D. creating an Access Control Policy with an INSIDE\_NET network object and object overrides

**Answer:** D

**NEW QUESTION 154**

- (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 159**

- (Exam Topic 5)

An engineer has been tasked with using Cisco FMC to determine if files being sent through the network are malware. Which two configuration tasks must be performed to achieve this file lookup? (Choose two).

- A. The Cisco FMC needs to include a SSL decryption policy.
- B. The Cisco FMC needs to connect to the Cisco AMP for Endpoints service.
- C. The Cisco FMC needs to connect to the Cisco ThreatGrid service directly for sandboxing.
- D. The Cisco FMC needs to connect with the FireAMP Cloud.
- E. The Cisco FMC needs to include a file inspection policy for malware lookup.

**Answer:** BE

**NEW QUESTION 160**

- (Exam Topic 5)

Which firewall design will allow It to forward traffic at layers 2 and 3 for the same subnet?

- A. Cisco Firepower Threat Defense mode
- B. routed mode
- C. Integrated routing and bridging
- D. transparent mode

**Answer:** C

**Explanation:**

Integrated routing and bridging (IRB) is a feature of Cisco Firepower Threat Defense (FTD) that allows the firewall to forward traffic at both layers 2 and 3 for the same subnet. In this mode, the firewall can act as a switch or a bridge to forward traffic at layer 2 and as a router to forward traffic at layer 3. This allows the firewall to maintain full control over the traffic, while still allowing it to forward traffic at both layers.

<https://www.cisco.com/c/en/us/td/docs/security/firepower/ftd-config-guide/FTD-Config-Guide-v6/Integrated-Ro>

**NEW QUESTION 162**

- (Exam Topic 5)

An engineer is attempting to create a new dashboard within the Cisco FMC to have a single view with widgets from many of the other dashboards. The goal is to have a mixture of threat and security related widgets along with Cisco Firepower device health information. Which two widgets must be configured to provide this information? (Choose two).

- A. Intrusion Events
- B. Correlation Information
- C. Appliance Status
- D. Current Sessions
- E. Network Compliance

**Answer:** AE

**NEW QUESTION 163**

- (Exam Topic 5)

An organization has a Cisco FTD that uses bridge groups to pass traffic from the inside interfaces to the outside interfaces. They are unable to gather information about neighbouring Cisco devices or use multicast in their environment. What must be done to resolve this issue?

- A. Create a firewall rule to allow CDP traffic.
- B. Create a bridge group with the firewall interfaces.
- C. Change the firewall mode to routed.
- D. Change the firewall mode to transparent.

**Answer:** C

**NEW QUESTION 166**

- (Exam Topic 5)

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?

- A. Maximum Detection
- B. Security Over Connectivity
- C. Balanced Security and Connectivity
- D. Connectivity Over Security

**Answer:** C

**Explanation:**

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

**NEW QUESTION 168**

- (Exam Topic 5)

After using Firepower for some time and learning about how it interacts with the network, an administrator is trying to correlate malicious activity with a user Which widget should be configured to provide this visibility on the Cisco Firepower dashboards?

- A. Custom Analysis
- B. Current Status
- C. Current Sessions
- D. Correlation Events

**Answer:** A

**NEW QUESTION 172**

- (Exam Topic 5)

A Cisco FTD device is running in transparent firewall mode with a VTEP bridge group member ingress interface. What must be considered by an engineer tasked with specifying a destination MAC address for a packet trace?

- A. Only the UDP packet type is supported.
- B. The output format option for the packet logs is unavailable.
- C. The destination MAC address is optional if a VLAN ID value is entered.



D. The VLAN ID and destination MAC address are optional.

**Answer:** C

**NEW QUESTION 174**

- (Exam Topic 5)

What is the role of the casebook feature in Cisco Threat Response?

- A. sharing threat analysts
- B. pulling data via the browser extension
- C. triage automaton with alerting
- D. alert prioritization

**Answer:** A

**Explanation:**

The casebook and pivot menu are widgets available in Cisco Threat Response. Casebook - It is used to record, organize, and share sets of observables of interest primarily during an investigation and threat analysis. You can use a casebook to get the current verdicts or dispositions on the observables.

[https://www.cisco.com/c/en/us/td/docs/se curity/ces/user\\_guide/esa\\_user\\_guide\\_13-5-1/b\\_ESA\\_Admin\\_Guide\\_ces\\_13-5-1/b\\_ESA\\_Admin\\_Guide\\_13-0\\_chapter\\_0110001.pdf](https://www.cisco.com/c/en/us/td/docs/security/ces/user_guide/esa_user_guide_13-5-1/b_ESA_Admin_Guide_ces_13-5-1/b_ESA_Admin_Guide_13-0_chapter_0110001.pdf)

**NEW QUESTION 175**

- (Exam Topic 5)

Drag and drop the configuration steps from the left into the sequence on the right to enable external authentication on Cisco FMC to a RADIUS server.

Select Authentication Method and RADIUS.	step 1
Configure the primary and secondary servers and user roles.	step 2
Select Users and External Authentication.	step 3
Add External Authentication Object.	step 4

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

4, 1, 2, 3

**NEW QUESTION 176**

- (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 177**

- (Exam Topic 5)

Which protocol is needed to exchange threat details in rapid threat containment on Cisco FMC?

- A. SGT
- B. SNMP v3
- C. BFD
- D. pxGrid

**Answer:** D

**NEW QUESTION 178**

- (Exam Topic 5)

Refer to the exhibit.



What is the effect of the existing Cisco FMC configuration?

- A. The remote management port for communication between the Cisco FMC and the managed device changes to port 8443.
- B. The managed device is deleted from the Cisco FMC.
- C. The SSL-encrypted communication channel between the Cisco FMC and the managed device becomes plain-text communication channel.
- D. The management connection between the Cisco FMC and the Cisco FTD is disabled.

**Answer:** D

#### NEW QUESTION 180

- (Exam Topic 5)

A company wants a solution to aggregate the capacity of two Cisco FTD devices to make the best use of resources such as bandwidth and connections per second. Which order of steps must be taken across the Cisco FTDs with Cisco FMC to meet this requirement?

- A. Configure the Cisco FTD interfaces, add members to FMC, configure cluster members in FMC, and create cluster in Cisco FMC.
- B. Add members to Cisco FMC, configure Cisco FTD interfaces in Cisco FM
- C. configure cluster members in Cisco FMC, create cluster in Cisco FM
- D. and configure cluster members in Cisco FMC.
- E. Configure the Cisco FTD interfaces and cluster members, add members to Cisco FM
- F. and create the cluster in Cisco FMC.
- G. Add members to the Cisco FMC, configure Cisco FTD interfaces, create the cluster in Cisco FMC, and configure cluster members in Cisco FMC.

**Answer:** D

#### NEW QUESTION 184

- (Exam Topic 5)

An engineer has been tasked with providing disaster recovery for an organization's primary Cisco FMC. What must be done on the primary and secondary Cisco FMCs to ensure that a copy of the original corporate policy is available if the primary Cisco FMC fails?

- A. Configure high-availability in both the primary and secondary Cisco FMCs
- B. Connect the primary and secondary Cisco FMC devices with Category 6 cables of not more than 10 meters in length.
- C. Place the active Cisco FMC device on the same trusted management network as the standby device
- D. Restore the primary Cisco FMC backup configuration to the secondary Cisco FMC device when the primary device fails

**Answer:** D

#### NEW QUESTION 185

- (Exam Topic 5)

A security engineer must configure a Cisco FTD appliance to inspect traffic coming from the internet. The Internet traffic will be mirrored from the Cisco Catalyst 9300 Switch. Which configuration accomplishes the task?

- A. Set interface configuration mode to none.
- B. Set the firewall mode to transparent.
- C. Set the firewall mode to routed.
- D. Set interface configuration mode to passive.

**Answer:** D

#### NEW QUESTION 188

- (Exam Topic 5)

An analyst is investigating a potentially compromised endpoint within the network and pulls a host report for the endpoint in question to collect metrics and documentation. What information should be taken from this report for the investigation?

- A. client applications by user, web applications, and user connections
- B. number of attacked machines, sources of the attack, and traffic patterns
- C. intrusion events, host connections, and user sessions
- D. threat detections over time and application protocols transferring malware

**Answer:** C

#### NEW QUESTION 193

- (Exam Topic 5)

An analyst using the security analyst account permissions is trying to view the Correlations Events Widget but is not able to access it. However, other dashboards are accessible. Why is this occurring?

- A. An API restriction within the Cisco FMC is preventing the widget from displaying.
- B. The widget is configured to display only when active events are present.
- C. The widget is not configured within the Cisco FMC.
- D. The security analyst role does not have permission to view this widget.

**Answer:** C

#### NEW QUESTION 197

- (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 199

- (Exam Topic 5)

There is an increased amount of traffic on the network, and for compliance reasons, management needs visibility into the encrypted traffic. What is a result of enabling TLS/SSL decryption to allow this visibility?

- A. It prompts the need for a corporate managed certificate.
- B. It has minimal performance impact.
- C. It is not subject to any Privacy regulations.
- D. It will fail if certificate pinning is not enforced.

**Answer:** A

#### NEW QUESTION 200

- (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 204

- (Exam Topic 5)

An engineer has been asked to show application usages automatically on a monthly basis and send the information to management. What mechanism should be used to accomplish this task?

- A. event viewer
- B. reports
- C. dashboards
- D. context explorer

**Answer:** B

#### NEW QUESTION 205

- (Exam Topic 4)

What is a valid Cisco AMP file disposition?

- A. non-malicious
- B. malware
- C. known-good
- D. pristine

**Answer:** B

#### Explanation:

Reference:

[https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Reference\\_a\\_wrapper\\_Chapter\\_topic\\_here.html](https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Reference_a_wrapper_Chapter_topic_here.html)

#### NEW QUESTION 210

- (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-remediati.html>

**NEW QUESTION 212**

- (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 213**

- (Exam Topic 4)

What is the maximum SHA level of filtering that Threat Intelligence Director supports?

- A. SHA-1024
- B. SHA-4096
- C. SHA-512
- D. SHA-256

**Answer:** D

**Explanation:**

Reference:

<https://www.cisco.com/c/en/us/td/docs/security/firepower/623/configuration/guide/fpmc-config-guide-v623/cisc>

**NEW QUESTION 216**

- (Exam Topic 4)

Which connector is used to integrate Cisco ISE with Cisco FMC for Rapid Threat Containment?

- A. pxGrid
- B. FTD RTC
- C. FMC RTC
- D. ISEGrid

**Answer:** A

**NEW QUESTION 221**

- (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 223**

- (Exam Topic 3)

After deploying a network-monitoring tool to manage and monitor networking devices in your organization, you realize that you need to manually upload an MIB for the Cisco FMC. In which folder should you upload the MIB file?

- A. /etc/sf/DCMIB.ALERT
- B. /sf/etc/DCEALERT.MIB
- C. /etc/sf/DCEALERT.MIB
- D. system/etc/DCEALERT.MIB

**Answer:** C

**Explanation:**

Reference: <https://www.cisco.com/c/en/us/td/docs/security/firesight/541/firepower-module-user-guide/asa-firepower-module-user-guide-v541/Intrusion-External-Responses.pdf>

**NEW QUESTION 224**

- (Exam Topic 3)

What is the benefit of selecting the trace option for packet capture?

- A. The option indicates whether the packet was dropped or successful.
- B. The option indicated whether the destination host responds through a different path.
- C. The option limits the number of packets that are captured.
- D. The option captures details of each packet.

**Answer:** A

**NEW QUESTION 226**

- (Exam Topic 3)

What is a functionality of port objects in Cisco FMC?

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

**Answer:** B

**Explanation:**

Reference: [https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-config-guide-v62/reusable\\_objects.html](https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-config-guide-v62/reusable_objects.html)

**NEW QUESTION 231**

- (Exam Topic 3)

Within Cisco Firepower Management Center, where does a user add or modify widgets?

- A. dashboard
- B. reporting
- C. context explorer
- D. summary tool

**Answer:** A

**Explanation:**

Reference:

[https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Using\\_Dashboards.html](https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Using_Dashboards.html)

**NEW QUESTION 232**

- (Exam Topic 3)

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.	Step 1
Unregister the device from the standby Cisco FMC.	Step 2
Register the affected device on the active Cisco FMC.	Step 3
Enter the "configure manager delete" command at the CLI of the affected device.	Step 4
Register the affected device on the standby Cisco FMC.	
Unregister the device from the active Cisco FMC.	

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Reference: [https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-config-guide-v62/firepower\\_management\\_center\\_high\\_availability.html#id\\_32288](https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-config-guide-v62/firepower_management_center_high_availability.html#id_32288)



**NEW QUESTION 236**

- (Exam Topic 4)

In a Cisco AMP for Networks deployment, which disposition is returned if the cloud cannot be reached?

- A. unavailable
- B. unknown
- C. clean
- D. disconnected

**Answer:** A

**NEW QUESTION 239**

- (Exam Topic 3)

Which command is run at the CLI when logged in to an FTD unit, to determine whether the unit is managed locally or by a remote FMC server?

- A. system generate-troubleshoot
- B. show configuration session
- C. show managers
- D. show running-config | include manager

**Answer:** C

**Explanation:**

Reference: [https://www.cisco.com/c/en/us/td/docs/security/firepower/command\\_ref/b\\_Command\\_Reference\\_for\\_Firepower\\_Threat\\_Defense/c\\_3.html](https://www.cisco.com/c/en/us/td/docs/security/firepower/command_ref/b_Command_Reference_for_Firepower_Threat_Defense/c_3.html)

**NEW QUESTION 241**

- (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 245**

- (Exam Topic 3)

Which limitation applies to Cisco Firepower Management Center dashboards in a multidomain environment?

- A. Child domains can view but not edit dashboards that originate from an ancestor domain.
- B. Child domains have access to only a limited set of widgets from ancestor domains.
- C. Only the administrator of the top ancestor domain can view dashboards.
- D. Child domains cannot view dashboards that originate from an ancestor domain.

**Answer:** D

**Explanation:**

Reference:

[https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Using\\_Dashboards.html](https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Using_Dashboards.html)

**NEW QUESTION 248**

- (Exam Topic 3)

Which group within Cisco does the Threat Response team use for threat analysis and research?

- A. Cisco Deep Analytics
- B. OpenDNS Group
- C. Cisco Network Response
- D. Cisco Talos

**Answer:** D

**Explanation:**

Reference: <https://www.cisco.com/c/en/us/products/security/threat-response.html#~benefits>

**NEW QUESTION 251**

- (Exam Topic 3)

Which CLI command is used to control special handling of ClientHello messages?

- A. system support ssl-client-hello-tuning
- B. system support ssl-client-hello-display
- C. system support ssl-client-hello-force-reset

D. system support ssl-client-hello-enabled

**Answer:** A

#### NEW QUESTION 252

- (Exam Topic 2)

Which two actions can be used in an access control policy rule? (Choose two.)

- A. Block with Reset
- B. Monitor
- C. Analyze
- D. Discover
- E. Block ALL

**Answer:** AB

#### 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>

#### NEW QUESTION 257

- (Exam Topic 3)

Which command is entered in the Cisco FMC CLI to generate a troubleshooting file?

- A. show running-config
- B. show tech-support chassis
- C. system support diagnostic-cli
- D. sudo sf\_troubleshoot.pl

**Answer:** D

#### Explanation:

Reference: <https://www.cisco.com/c/en/us/support/docs/security/sourcefire-defense-center/117663-technote-SourceFire-00.html>

#### NEW QUESTION 260

- (Exam Topic 3)

Which command-line mode is supported from the Cisco Firepower Management Center CLI?

- A. privileged
- B. user
- C. configuration
- D. admin

**Answer:** C

#### Explanation:

Reference: [https://www.cisco.com/c/en/us/td/docs/security/firepower/660/configuration/guide/fpmc-config-guide-v66/command\\_line\\_reference.pdf](https://www.cisco.com/c/en/us/td/docs/security/firepower/660/configuration/guide/fpmc-config-guide-v66/command_line_reference.pdf)

#### NEW QUESTION 264

- (Exam Topic 2)

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?

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

**Answer:** C

#### Explanation:

A file policy defines the actions that the Cisco Firepower Threat Defense (FTD) device should take when it encounters different types of files. The file policy is applied as part of an access control policy. If an access control policy does not include a file policy, the FTD device will not take any action on the files it encounters, resulting in a disposition of "unknown" for all file types except exe.

Reference:

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

#### NEW QUESTION 267

- (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 269**

- (Exam Topic 2)

What is the result of specifying of QoS rule that has a rate limit that is greater than the maximum throughput of an interface?

- A. The rate-limiting rule is disabled.
- B. Matching traffic is not rate limited.
- C. The system rate-limits all traffic.
- D. The system repeatedly generates warnings.

**Answer:** B

**Explanation:**

Reference: [https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-config-guide-v62/quality\\_of\\_service\\_qos.pdf](https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-config-guide-v62/quality_of_service_qos.pdf)

**NEW QUESTION 270**

- (Exam Topic 2)

Which two OSPF routing features are configured in Cisco FMC and propagated to Cisco FTD? (Choose two.)

- A. OSPFv2 with IPv6 capabilities
- B. virtual links
- C. SHA authentication to OSPF packets
- D. area boundary router type 1 LSA filtering
- E. MD5 authentication to OSPF packets

**Answer:** BE

**Explanation:**

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

**NEW QUESTION 275**

- (Exam Topic 2)

Which two types of objects are reusable and supported by Cisco FMC? (Choose two.)

- A. dynamic key mapping objects that help link HTTP and HTTPS GET requests to Layer 7 application protocols.
- B. reputation-based objects that represent Security Intelligence feeds and lists, application filters based on category and reputation, and file lists
- C. network-based objects that represent IP address and networks, port/protocols pairs, VLAN tags, security zones, and origin/destination country
- D. network-based objects that represent FQDN mappings and networks, port/protocol pairs, VXLAN tags, security zones and origin/destination country
- E. reputation-based objects, such as URL categories

**Answer:** BC

**Explanation:**

Reference: [https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-config-guide-v62/reusable\\_objects.html#ID-2243-00000414](https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-config-guide-v62/reusable_objects.html#ID-2243-00000414)

**NEW QUESTION 279**

- (Exam Topic 1)

What is a result of enabling Cisco FTD clustering?

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

**Answer:** C

**Explanation:**

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](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)

**NEW QUESTION 284**

- (Exam Topic 2)

Which Firepower feature allows users to configure bridges in routed mode and enables devices to perform Layer 2 switching between interfaces?

- A. FlexConfig
- B. BDI
- C. SGT
- D. IRB

**Answer:** D

**Explanation:**

Reference: [https://www.cisco.com/c/en/us/td/docs/security/firepower/620/relnotes/Firepower\\_System\\_Release\\_Notes\\_Version\\_620/new\\_features\\_and\\_functionality.html](https://www.cisco.com/c/en/us/td/docs/security/firepower/620/relnotes/Firepower_System_Release_Notes_Version_620/new_features_and_functionality.html)

**NEW QUESTION 289**

- (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 292**

- (Exam Topic 1)

A Cisco FTD has two physical interfaces assigned to a BVI. Each interface is connected to a different VLAN on the same switch. Which firewall mode is the Cisco FTD set up to support?

- A. active/active failover
- B. transparent
- C. routed
- D. high availability clustering

**Answer:** B

**NEW QUESTION 293**

- (Exam Topic 1)

Within an organization's high availability environment where both firewalls are passing traffic, traffic must be segmented based on which department it is destined for. Each department is situated on a different LAN. What must be configured to meet these requirements?

- A. span EtherChannel clustering
- B. redundant interfaces
- C. high availability active/standby firewalls
- D. multi-instance firewalls

**Answer:** D

**NEW QUESTION 294**

- (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 295**

- (Exam Topic 1)

What are two application layer preprocessors? (Choose two.)

- A. CIFS
- B. IMAP
- C. SSL
- D. DNP3
- E. ICMP

**Answer:** BC

**Explanation:**

Reference:

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

**NEW QUESTION 296**

- (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 300**

- (Exam Topic 1)

Which two conditions are necessary for high availability to function between two Cisco FTD devices? (Choose two.)

- A. The units must be the same version
- B. Both devices can be part of a different group that must be in the same domain when configured within the FMC.
- C. The units must be different models if they are part of the same series.
- D. The units must be configured only for firewall routed mode.
- E. The units must be the same model.

**Answer:** AE

**Explanation:**

Reference: <https://www.cisco.com/c/en/us/support/docs/security/firepower-management-center/212699-configure-ftd-high-availability-on-firep.html>

**NEW QUESTION 302**

.....



## Thank You for Trying Our Product

\* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

\* One year free update

You can enjoy free update one year. 24x7 online support.

\* Trusted by Millions

We currently serve more than 30,000,000 customers.

\* Shop Securely

All transactions are protected by VeriSign!

**100% Pass Your 300-710 Exam with Our Prep Materials Via below:**

<https://www.certleader.com/300-710-dumps.html>