

## 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)

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 3**

- (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 4**

- (Exam Topic 5)

An engineer is monitoring network traffic from their sales and product development departments, which are on two separate networks What must be configured in order to maintain data privacy for both departments?

- A. Use a dedicated IPS inline set for each department to maintain traffic separation
- B. Use 802 1Q mime set Trunk interfaces with VLANs to maintain logical traffic separation
- C. Use passive IDS ports for both departments
- D. Use one pair of inline set in TAP mode for both departments

**Answer: B**

**NEW QUESTION 5**

- (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/CAP/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 6**

- (Exam Topic 5)

Which feature is supported by IRB on Cisco FTD devices?

- A. redundant interface
- B. dynamic routing protocol
- C. EtherChannel interface
- D. high-availability cluster

**Answer: B**

#### NEW QUESTION 7

- (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 8

- (Exam Topic 5)

A security engineer found a suspicious file from an employee email address and is trying to upload it for analysis, however the upload is failing. The last registration status is still active. What is the cause for this issue?

- A. Cisco AMP for Networks is unable to contact Cisco Threat Grid on premise.
- B. Cisco AMP for Networks is unable to contact Cisco Threat Grid Cloud.
- C. There is a host limit set.
- D. The user agent status is set to monitor.

**Answer: B**

#### NEW QUESTION 9

- (Exam Topic 5)

An engineer is restoring a Cisco FTD configuration from a remote backup using the command restore remote-manager-backup location 1.1.1.1 admin /volume/home/admin BACKUP\_Cisc394602314.zip on a Cisco FMG. After connecting to the repository, an error occurred that prevents the FTD device from accepting the backup file. What is the problem?

- A. The backup file is not in .cfg format.
- B. The backup file is too large for the Cisco FTD device
- C. The backup file extension was changed from tar to zip
- D. The backup file was not enabled prior to being applied

**Answer: C**

#### NEW QUESTION 10

- (Exam Topic 5)

What is a characteristic of bridge groups on a Cisco FTD?

- A. In routed firewall mode, routing between bridge groups must pass through a routed interface.
- B. In routed firewall mode, routing between bridge groups is supported.
- C. In transparent firewall mode, routing between bridge groups is supported
- D. Routing between bridge groups is achieved only with a router-on-a-stick configuration on a connected router

**Answer: B**

#### NEW QUESTION 10

- (Exam Topic 5)

An organization must be able to ingest NetFlow traffic from their Cisco FTD device to Cisco Stealthwatch for behavioral analysis. What must be configured on the Cisco FTD to meet this requirement?

- A. flexconfig object for NetFlow
- B. interface object to export NetFlow
- C. security intelligence object for NetFlow
- D. variable set object for NetFlow

**Answer: A**

#### NEW QUESTION 15

- (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 correctedIP address.

**Answer: D**

#### NEW QUESTION 16

- (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 19

- (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 21

- (Exam Topic 5)

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

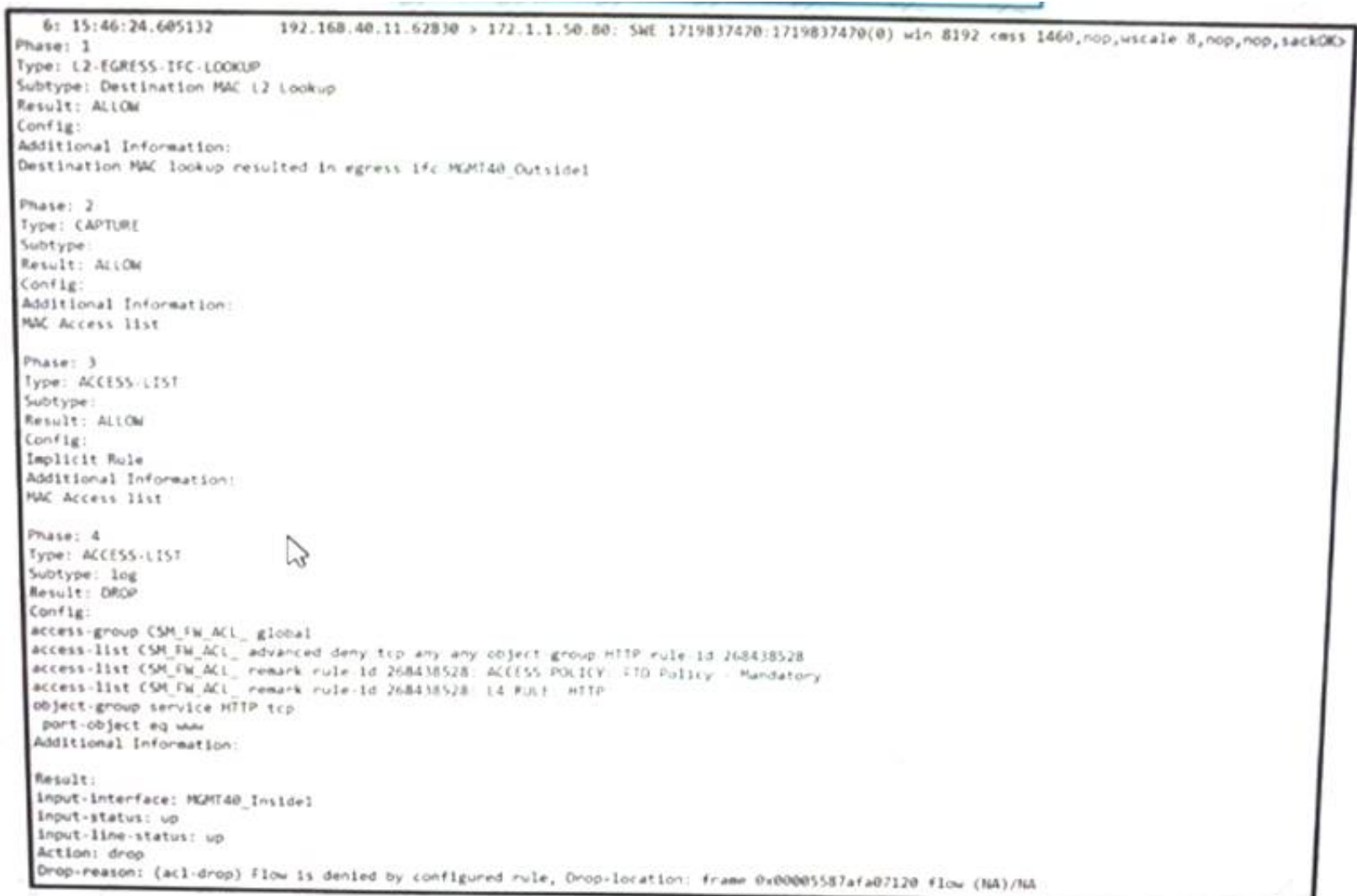
- A. Diagnostic
- B. EtherChannel
- C. BVI
- D. Physical
- E. Subinterface

**Answer: AC**

#### NEW QUESTION 23

- (Exam Topic 5)

Refer to the exhibit.



```
6: 15:46:24.605132 192.168.40.11.62830 > 172.1.1.50.80: SWE 1719837470:1719837470(0) win 8192 <css 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: FTD Policy - Mandatory
access-list CSM_FW_ACL_remark rule-id 268438528 14 Permit 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 28

- (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 30

- (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 32

- (Exam Topic 5)

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-reset

**Answer:** D

#### NEW QUESTION 34

- (Exam Topic 5)

An administrator needs to configure Cisco FMC to send a notification email when a data transfer larger than 10 MB is initiated from an internal host outside of standard business hours. Which Cisco FMC feature must be configured to accomplish this task?

- A. file and malware policy
- B. application detector
- C. intrusion policy
- D. correlation policy

**Answer:** A

#### NEW QUESTION 36

- (Exam Topic 5)

An engineer wants to perform a packet capture on the Cisco FTD to confirm that the host using IP address 192.168.100.100 has the MAC address of 0042 7734.103 to help troubleshoot a connectivity issue What is the correct tcpdump command syntax to ensure that the MAC address appears in the packet capture output?

- A. -nm src 192.168.100.100
- B. -ne src 192.168.100.100
- C. -w capture.pcap -s 1518 host 192.168.100.100 mac
- D. -w capture.pcap -s 1518 host 192.168.100.100 ether

**Answer:** B

#### Explanation:

Reference:

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

#### NEW QUESTION 38

- (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 39

- (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 41

- (Exam Topic 5)

An organization has implemented Cisco Firepower without IPS capabilities and now wants to enable inspection for their traffic. They need to be able to detect protocol anomalies and utilize the Snort rule sets to detect malicious behaviour. How is this accomplished?

- A. Modify the access control policy to redirect interesting traffic to the engine
- B. Modify the network discovery policy to detect new hosts to inspect
- C. Modify the network analysis policy to process the packets for inspection
- D. Modify the intrusion policy to determine the minimum severity of an event to inspect.

**Answer:** D

#### NEW QUESTION 46

- (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 51

- (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 54

- (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 59

- (Exam Topic 5)

Refer to the exhibit.

```
Phase: 16
Type: SNORT
Subtype:
Result: DROP
Config:
Additional Information:
Snort Trace:
Packet: ICMP
Session: new snort session
Firewall: starting rule matching, zone 4 => 1, geo 0 => 0, vlan 0, sgt 0, src sgt type 0, dest_sgt_tag 0, dest sgt type 0, username "No Authentication Required", , icmpType 0, icmpCode 0
Firewall: block rule, "Ping", drop
Snort: processed decoder alerts or actions queue, drop
Snort id 0, NAP id 2, IPS id 0, Verdict BLACKLIST, Blocked by Firewall
Snort Verdict: (black-list) black list this flow

Result:
Input-Interface: ACCESS41_Inside1
Input-status: up
Input-line-status: up
Action: drop
Drop-reason: (firewall) Blocked or blacklisted by the firewall preprocessor, Drop-location: frame 0x00055e2b0f8b7e0 flow (NA)/NA
```

A systems administrator conducts a connectivity test to their SCCM server from a host machine and gets no response from the server. Which action ensures that the ping packets reach the destination and that the host receives replies?

- A. Create an access control policy rule that allows ICMP traffic.
- B. Configure a custom Snort signature to allow ICMP traffic after Inspection.

- C. Modify the Snort rules to allow ICMP traffic.
- D. Create an ICMP allow list and add the ICMP destination to remove it from the implicit deny list.

**Answer:** A

#### NEW QUESTION 62

- (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 65

- (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 66

- (Exam Topic 5)

IT management is asking the network engineer to provide high-level summary statistics of the Cisco FTD appliance in the network. The business is approaching a peak season so the need to maintain business uptime is high. Which report type should be used to gather this information?

- A. Malware Report
- B. Standard Report
- C. SNMP Report
- D. Risk Report

**Answer:** B

#### NEW QUESTION 70

- (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

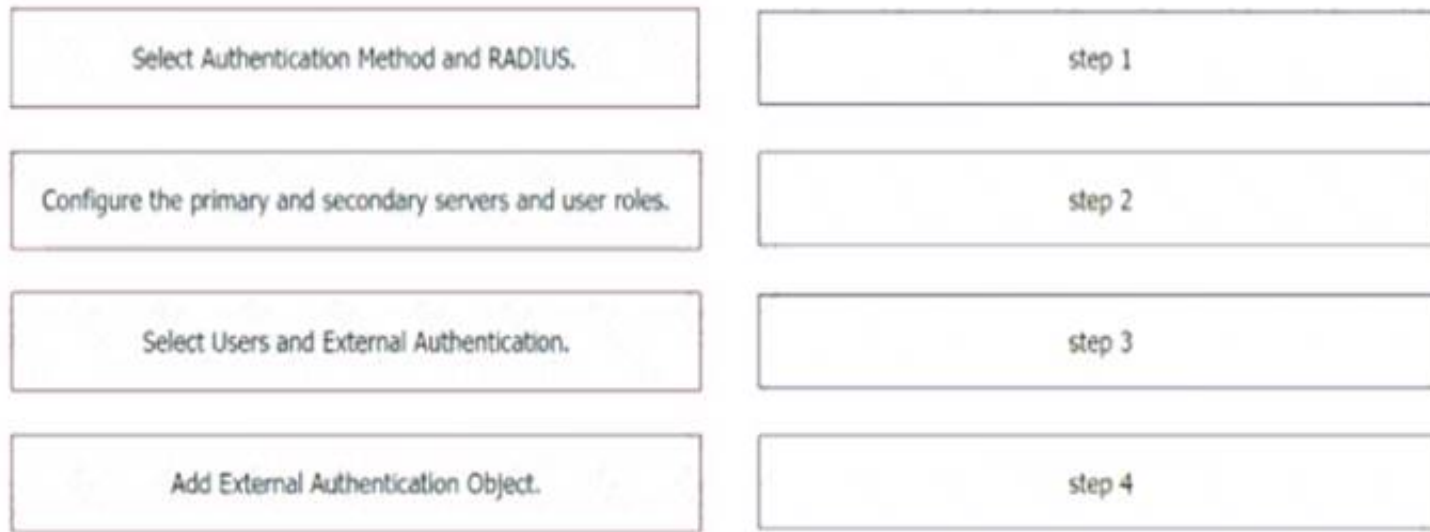
#### Explanation:

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

#### NEW QUESTION 72

- (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.



- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

4, 1, 2, 3

#### NEW QUESTION 74

- (Exam Topic 5)

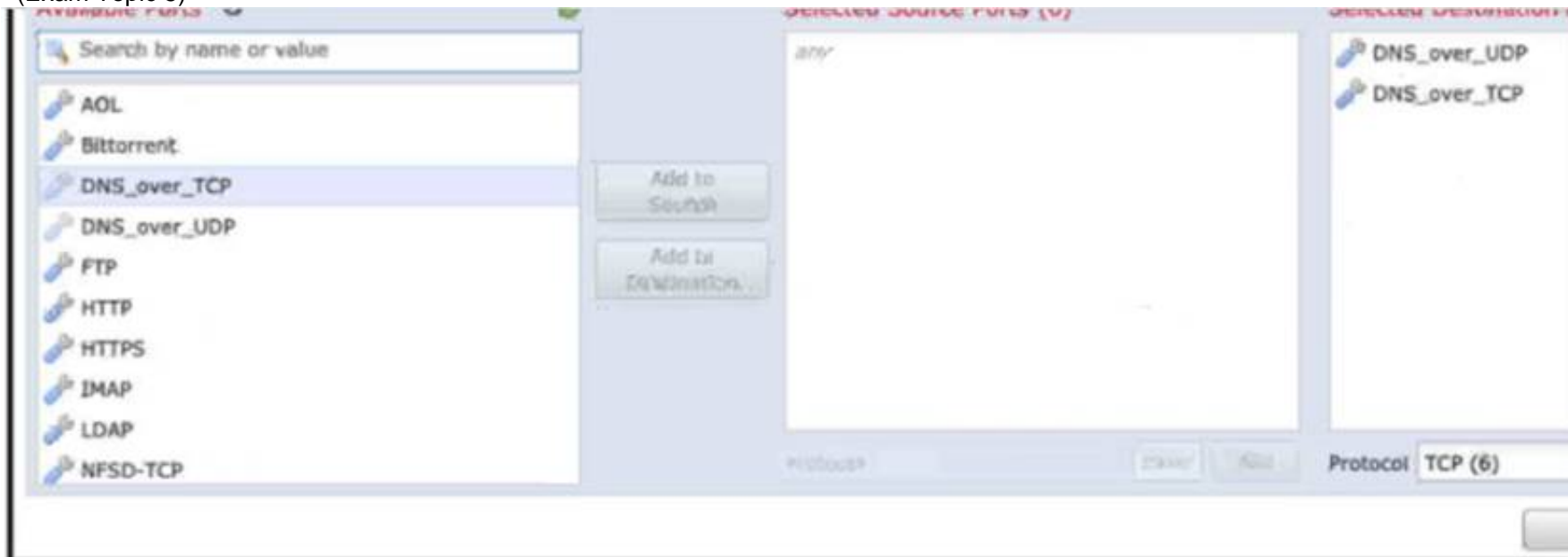
An engainer must add DNS-specific rules to me Cisco FTD intrusion policy. The engineer wants to use the rules currently in the Cisco FTD Snort database that are not already enabled but does not want to enable more than are needed. Which action meets these requirements?

- A. Change the dynamic state of the rule within the policy.
- B. Change the base policy to Security over Connectivity.
- C. Change the rule state within the policy being used.
- D. Change the rules using the Generate and Use Recommendations feature.

**Answer:** C

#### NEW QUESTION 79

- (Exam Topic 5)



Refer to the exhibit An engineer is modifying an access control pokey to add a rule to inspect all DNS traffic that passes through the firewall After making the change and deploying the pokey they see that DNS traffic is not bang inspected by the Snort engine What is the problem?

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

**Answer:** C

#### NEW QUESTION 81

- (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 blockedtraffic.

**Answer:** A



**NEW QUESTION 84**

- (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 88**

- (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 93**

- (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 98**

- (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 100**

- (Exam Topic 5)

An organization has noticed that malware was downloaded from a website that does not currently have a known bad reputation. How will this issue be addressed globally in the quickest way possible and with the least amount of impact?

- A. by denying outbound web access
- B. Cisco Talos will automatically update the policies.
- C. by Isolating the endpoint
- D. by creating a URL object in the policy to block the website

**Answer:** D

**NEW QUESTION 105**

- (Exam Topic 5)

An engineer must investigate a connectivity issue and decides to use the packet capture feature on Cisco FTD. The goal is to see the real packet going through the Cisco FTD device and see the Snort detection actions as a part of the output. After the `capture-traffic` command is issued, only the packets are displayed. Which action resolves this issue?

- A. Use the verbose option as a part of the `capture-traffic` command
- B. Use the `capture` command and specify the `trace` option to get the required information.
- C. Specify the `trace` using the `-T` option after the `capture-traffic` command.
- D. Perform the trace within the Cisco FMC GUI instead of the Cisco FTD CLI.

**Answer:** B

**NEW QUESTION 109**

- (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 110**

- (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 112**

- (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 115**

- (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:** DE

**NEW QUESTION 117**

- (Exam Topic 3)

Which command must be run to generate troubleshooting files on an FTD?

- A. system support view-files
- B. sudo sf\_troubleshoot.pl
- C. system generate-troubleshoot all
- D. show tech-support

**Answer:** C

**Explanation:**

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

**NEW QUESTION 122**

- (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 127**

- (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 132**

- (Exam Topic 3)

Which action should be taken after editing an object that is used inside an access control policy?

- A. Delete the existing object in use.
- B. Refresh the Cisco FMC GUI for the access control policy.
- C. Redeploy the updated configuration.
- D. Create another rule using a different object name.

**Answer:** C

**Explanation:**

Reference: [https://www.cisco.com/c/en/us/td/docs/security/firepower/630/configuration/guide/fpmc-config-guide-v63/reusable\\_objects.html](https://www.cisco.com/c/en/us/td/docs/security/firepower/630/configuration/guide/fpmc-config-guide-v63/reusable_objects.html)

**NEW QUESTION 136**

- (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 137**

- (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 142**

- (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 145**

- (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 148**

- (Exam Topic 1)

Which firewall design allows a firewall to forward traffic at layer 2 and layer 3 for the same subnet?

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

**Answer:** B

**NEW QUESTION 150**

- (Exam Topic 1)

An engineer must configure high availability for the Cisco Firepower devices. The current network topology does not allow for two devices to pass traffic concurrently. How must the devices be implemented in this environment?

- A. in active/active mode
- B. in a cluster span EtherChannel
- C. in active/passive mode
- D. in cluster interface mode

**Answer:** C

**NEW QUESTION 153**

- (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 154**

- (Exam Topic 1)

Which Cisco Firepower Threat Defense, which two interface settings are required when configuring a routed interface? (Choose two.)

- A. Redundant Interface
- B. EtherChannel
- C. Speed
- D. Media Type
- E. Duplex

**Answer:** CE

**Explanation:**

<https://www.cisco.com/c/en/us/td/docs/security/firepower/610/fdm/fptd-fdm-config-guide-610/fptd-fdm-interfaces.html>

**NEW QUESTION 159**

- (Exam Topic 1)

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 transparent.
- D. Change the firewall mode to routed.

**Answer:** C

**Explanation:**

"In routed firewall mode, broadcast and multicast traffic is blocked even if you allow it in an access rule..." "The bridge group does not pass CDP packets packets..." <https://www.cisco.com/c/en/us/td/docs/security/asa/asa913/configuration/general/asa-913-general-config/intro-f>

Passing Traffic Not Allowed in Routed Mode

In routed mode, some types of traffic cannot pass through the ASA even if you allow it in an access rule. The bridge group, however, can allow almost any traffic through using either an access rule (for IP traffic) or an EtherType rule (for non-IP traffic):

IP traffic—In routed firewall mode, broadcast and "multicast traffic is blocked even if you allow it in an access rule," including unsupported dynamic routing protocols and DHCP (unless you configure DHCP relay). Within a bridge group, you can allow this traffic with an access rule (using an extended ACL).

Non-IP traffic—AppleTalk, IPX, BPDUs, and MPLS, for example, can be configured to go through using an EtherType rule.

Note

"The bridge group does not pass CDP packets packets, or any packets that do not have a valid EtherType greater than or equal to 0x600. An exception is made for BPDUs and IS-IS, which are supported. "

**NEW QUESTION 164**

- (Exam Topic 1)

An engineer is tasked with deploying an internal perimeter firewall that will support multiple DMZs Each DMZ has a unique private IP subnet range. How is this requirement satisfied?

- A. Deploy the firewall in transparent mode with access control policies.
- B. Deploy the firewall in routed mode with access control policies.
- C. Deploy the firewall in routed mode with NAT configured.
- D. Deploy the firewall in transparent mode with NAT configured.

**Answer:** C

**Explanation:**

Reference:

<https://www.cisco.com/c/en/us/td/docs/security/asa/asa96/configuration/general/asa-96-general-config/intro-fw>.

**NEW QUESTION 167**

- (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 168**

- (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 169**

- (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.html>

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 174**

- (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 178**

.....

## 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>