

Cisco

Exam Questions 300-710

Securing Networks with Cisco Firepower (SNCF)



NEW QUESTION 1

- (Exam Topic 5)

An engineer is creating an URL object on Cisco FMC How must it be configured so that the object will match for HTTPS traffic in an access control policy?

- A. Specify the protocol to match (HTTP or HTTPS).
- B. Use the FQDN including the subdomain for the website
- C. Define the path to the individual webpage that uses HTTPS.
- D. Use the subject common name from the website certificate

Answer: B

NEW QUESTION 2

- (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 3

- (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 native 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 4

- (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?

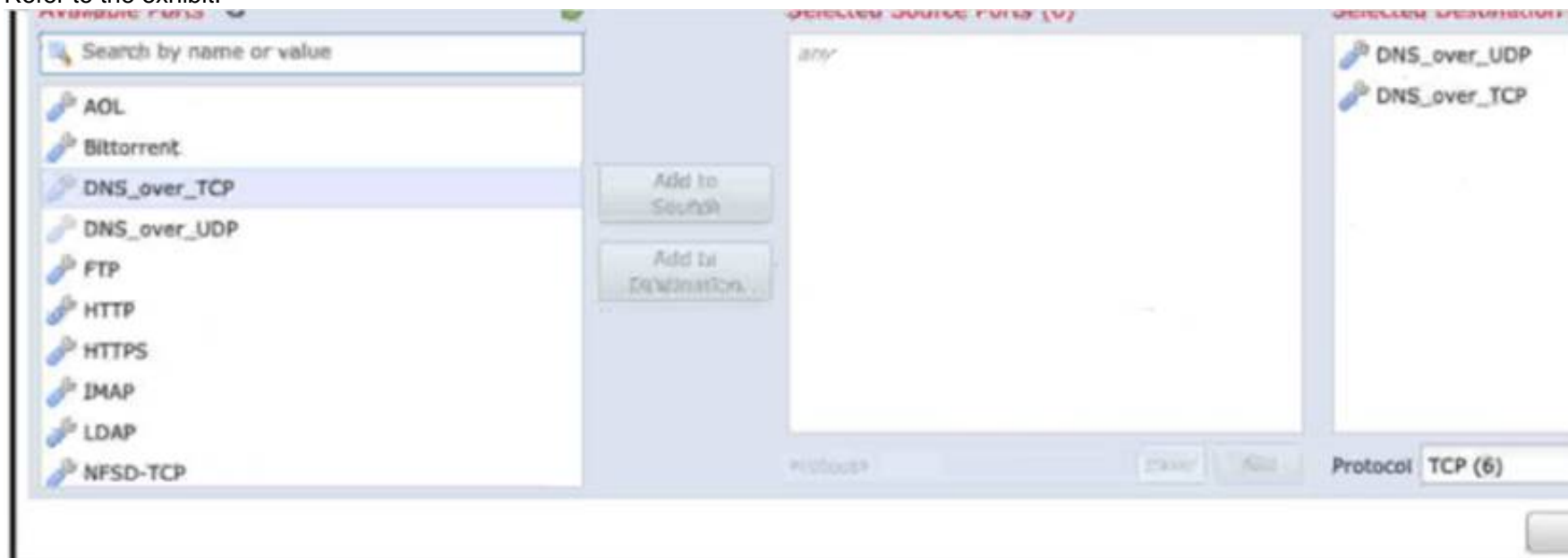
- A. Disable the HTTPS server and use HTTP instead.
- B. Enable the HTTPS server for the device platform policy.
- C. Disable the proxy setting on the browser.
- D. Use the Cisco FTD IP address as the proxy server setting on the browser.

Answer: B

NEW QUESTION 5

- (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 6

- (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 7

- (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.

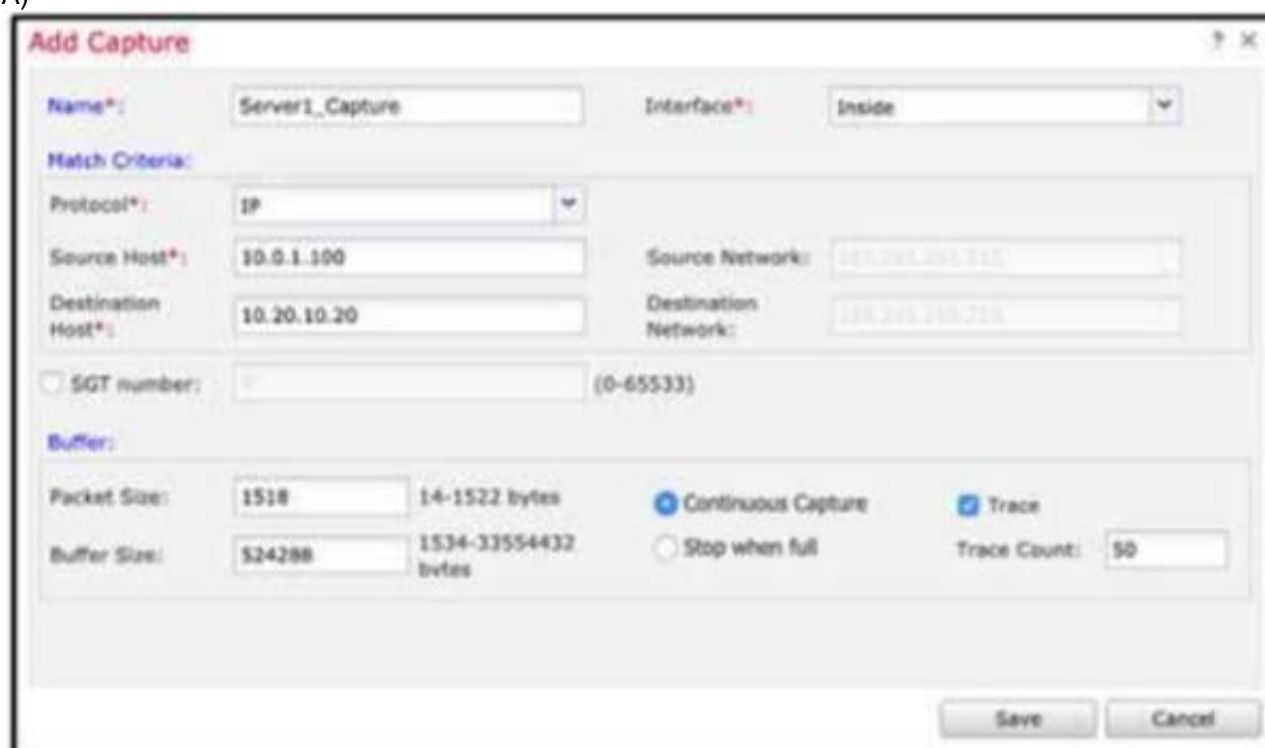
Answer: D

NEW QUESTION 8

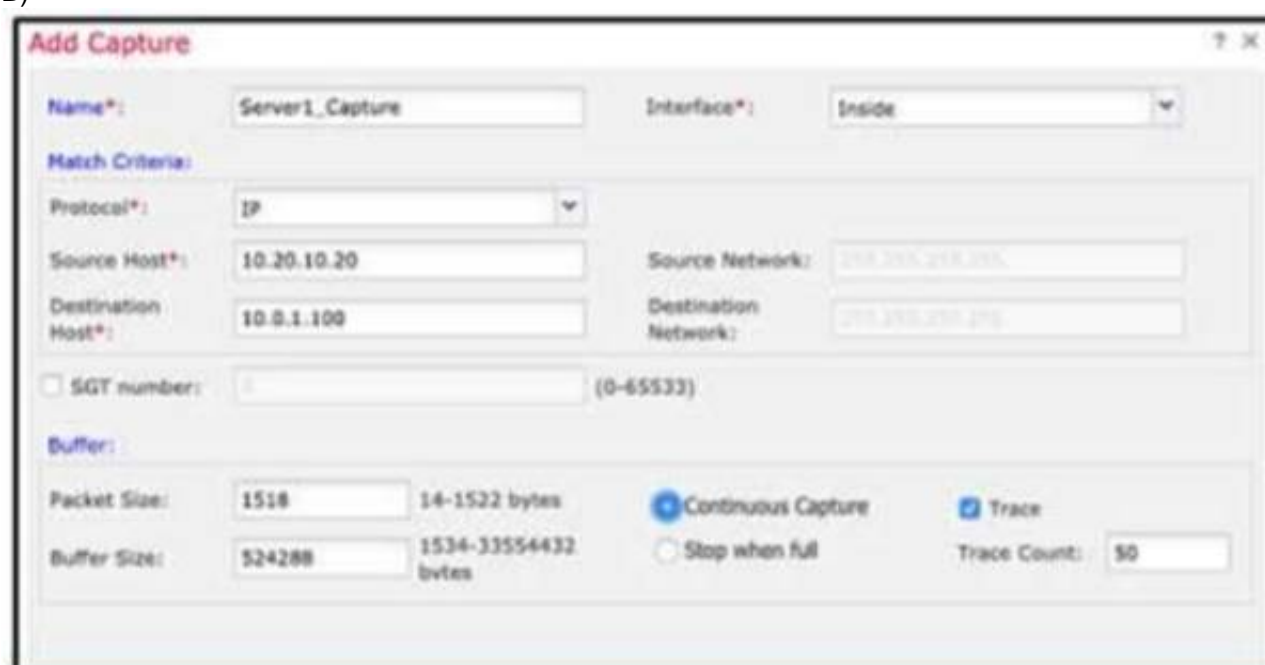
- (Exam Topic 5)

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)



B)



C)

Add Capture ? X

Name*: Interface*:

Match Criteria:

Protocol*:

Source Host*: Source Network:

Destination Host*: Destination Network:

☐ SGT number: (0-65533)

Buffer:

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

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

D)

Add Capture ? X

Name*: Interface*:

Match Criteria:

Protocol*:

Source Host*: Source Network:

Destination Host*: Destination Network:

☐ SGT number: (0-65533)

Buffer:

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

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

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

Answer: B

NEW QUESTION 9

- (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 10

- (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 10

- (Exam Topic 5)

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

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

Answer: C

Explanation:

Reference:

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

NEW QUESTION 14

- (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 17

- (Exam Topic 5)

An engineer configures an access control rule that deploys file policy configurations to security zones or tunnel zones, and it causes the device to restart. What is the reason for the restart?

- A. Source or destination security zones in the access control rule matches the security zones that are associated with interfaces on the target devices.
- B. The source tunnel zone in the rule does not match a tunnel zone that is assigned to a tunnel rule in the destination policy.
- C. Source or destination security zones in the source tunnel zone do not match the security zones that are associated with interfaces on the target devices.
- D. The source tunnel zone in the rule does not match a tunnel zone that is assigned to a tunnel rule in the source policy.

Answer: A

NEW QUESTION 21

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

Answer: C

NEW QUESTION 23

- (Exam Topic 5)

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

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

Answer: D

NEW QUESTION 25

- (Exam Topic 5)

An engineer is configuring Cisco FMC and wants to limit the time allowed for processing packets through the interface. However, if the time is exceeded, the configuration must allow packets to bypass detection. What must be configured on the Cisco FMC to accomplish this task?

- A. Fast-Path Rules Bypass
- B. Cisco ISE Security Group Tag

- C. Inspect Local Traffic Bypass
- D. Automatic Application Bypass

Answer: D

NEW QUESTION 29

- (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 32

- (Exam Topic 5)

A security engineer is adding three Cisco FTD devices to a Cisco FMC. Two of the devices have successfully registered to the Cisco FMC. The device that is unable to register is located behind a router that translates all outbound traffic to the router's WAN IP address. Which two steps are required for this device to register to the Cisco FMC? (Choose two.)

- A. Reconfigure the Cisco FMC to use the device's private IP address instead of the WAN address.
- B. Configure a NAT ID on both the Cisco FMC and the device.
- C. Add the port number being used for PAT on the router to the device's IP address in the Cisco FMC.
- D. Reconfigure the Cisco FMC to use the device's hostname instead of IP address.
- E. Remove the IP address defined for the device in the Cisco FMC.

Answer: BE

NEW QUESTION 34

- (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 36

- (Exam Topic 5)

A security analyst must create a new report within Cisco FMC to show an overview of the daily attacks, vulnerabilities, and connections. The analyst wants to reuse specific dashboards from other reports to create this consolidated one. Which action accomplishes this task?

- A. Create a new dashboard object via Object Management to represent the desired views.
- B. Modify the Custom Workflows within the Cisco FMC to feed the desired data into the new report.
- C. Copy the Malware Report and modify the sections to pull components from other reports.
- D. Use the import feature in the newly created report to select which dashboards to add.

Answer: D

NEW QUESTION 39

- (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 43

- (Exam Topic 5)

An engineer must configure a Cisco FMC dashboard in a multidomain deployment. Which action must the engineer take to edit a report template from an ancestor domain?

- A. Add it as a separate widget.
- B. Copy it to the current domain
- C. Assign themselves ownership of it
- D. Change the document attributes.

Answer: B

NEW QUESTION 46

- (Exam Topic 5)

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

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

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

Answer: C

NEW QUESTION 51

- (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 53

- (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 58

- (Exam Topic 5)

An engineer is working on a LAN switch and has noticed that its network connection to the Cisco IPS has gone down. Upon troubleshooting, it is determined that the switch is working as expected. What must have been implemented for this failure to occur?

- A. The upstream router has a misconfigured routing protocol.
- B. Link-state propagation is enabled.
- C. The Cisco IPS has been configured to be in fail-open mode.
- D. The Cisco IPS is configured in detection mode.

Answer: D

NEW QUESTION 59

- (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 60

- (Exam Topic 5)

A network administrator is configuring a Cisco AMP public cloud instance and wants to capture infections and polymorphic variants of a threat to help detect families of malware. Which detection engine meets this requirement?

- A. RBAC
- B. Tetra
- C. Ethos
- D. Spero

Answer: C

NEW QUESTION 61

- (Exam Topic 5)

An engineer is setting up a remote access VPN on a Cisco FTD device and wants to define which traffic gets sent over the VPN tunnel. Which named object type in Cisco FMC must be used to accomplish this task?

- A. split tunnel
- B. crypto map
- C. access list
- D. route map

Answer: A

NEW QUESTION 62

- (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 IRS, 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 67

- (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 72

- (Exam Topic 5)

Refer to the exhibit.

```
Phase: 16
Type: SNORT
Subtype:
Result: DROP
Config:
Additional Information:
Snort Trace:
Packets: 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, NMAP 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 0x00055d2b0f8b7e0 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 76

- (Exam Topic 5)

An administrator is adding a QoS policy to a Cisco FTD deployment. When a new rule is added to the policy and QoS is applied on 'Interfaces in Destination Interface Objects', no interface objects are available What is the problem?

- A. The FTD is out of available resources for us
- B. so QoS cannot be added
- C. The network segments that the interfaces are on do not have contiguous IP space
- D. QoS is available only on routed interfaces, and this device is in transparent mode.
- E. A conflict exists between the destination interface types that is preventing QoS from being added

Answer: C

NEW QUESTION 81

- (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 85

- (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/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 87

- (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 88

- (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 93

- (Exam Topic 5)

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

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

Answer: C

NEW QUESTION 94

- (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 96

- (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 100

- (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 102

- (Exam Topic 5)

Upon detecting a flagrant threat on an endpoint, which two technologies instruct Cisco Identity Services Engine to contain the infected endpoint either manually or automatically? (Choose two.)

- A. Cisco ASA 5500 Series
- B. Cisco FMC
- C. Cisco AMP
- D. Cisco Stealthwatch
- E. Cisco ASR 7200 Series

Answer: CD

NEW QUESTION 106

- (Exam Topic 5)

An engineer wants to change an existing transparent Cisco FTD to routed mode.

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

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

Answer: D

NEW QUESTION 110

- (Exam Topic 5)

A security engineer is configuring a remote Cisco FTD that has limited resources and internet bandwidth. Which malware action and protection option should be configured to reduce the requirement for cloud lookups?

- A. Malware Cloud Lookup and dynamic analysis
- B. Block Malware action and dynamic analysis
- C. Block Malware action and local malware analysis
- D. Block File action and local malware analysis

Answer: C

NEW QUESTION 113

- (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-remediation.html>

NEW QUESTION 116

- (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 120

- (Exam Topic 3)

When do you need the file-size command option during troubleshooting with packet capture?

- A. when capture packets are less than 16 MB
- B. when capture packets are restricted from the secondary memory
- C. when capture packets exceed 10 GB
- D. when capture packets exceed 32 MB

Answer: D

Explanation:

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

NEW QUESTION 123

- (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/piresight/541/firepower-module-user-guide/asa-firepower-module-user-guide-v541/Intrusion-External-Responses.pdf>

NEW QUESTION 124

- (Exam Topic 3)

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

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

Answer: C

Explanation:

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

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

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

NEW QUESTION 128

- (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

NEW QUESTION 132

- (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 133

- (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

NEW QUESTION 137

- (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

NEW QUESTION 140

- (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 143

- (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 144

- (Exam Topic 2)

Which object type supports object overrides?

- A. time range
- B. security group tag
- C. network object
- D. DNS server group

Answer: C

Explanation:

Reference:

https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Reusable_Objects.html#concept_8BFE8B9A83D742D9B647A74F7AD50053

NEW QUESTION 147

- (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

NEW QUESTION 151

- (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

NEW QUESTION 152

- (Exam Topic 2)

Which command is run on an FTD unit to associate the unit to an FMC manager that is at IP address 10.0.0.10, and that has the registration key Cisco123?

- A. configure manager local 10.0.0.10 Cisco123
- B. configure manager add Cisco123 10.0.0.10
- C. configure manager local Cisco123 10.0.0.10
- D. configure manager add 10.0.0.10 Cisco123

Answer: D

Explanation:

Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/misc/fmc-ftd-mgmt-nw/fmc-ftd-mgmt-nw.html#id_106101

NEW QUESTION 153

- (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

NEW QUESTION 158

- (Exam Topic 1)

A network security engineer must replace a faulty Cisco FTD device in a high availability pair. Which action must be taken while replacing the faulty unit?

- A. Shut down the Cisco FMC before powering up the replacement unit.
- B. Ensure that the faulty Cisco FTD device remains registered to the Cisco FMC.
- C. Unregister the faulty Cisco FTD device from the Cisco FMC
- D. Shut down the active Cisco FTD device before powering up the replacement unit.

Answer: C

NEW QUESTION 160

- (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 163

- (Exam Topic 1)

A network engineer implements a new Cisco Firepower device on the network to take advantage of its intrusion detection functionality. There is a requirement to analyze the traffic going across the device, alert on any malicious traffic, and appear as a bump in the wire How should this be implemented?

- A. Specify the BVI IP address as the default gateway for connected devices.
- B. Enable routing on the Cisco Firepower
- C. Add an IP address to the physical Cisco Firepower interfaces.
- D. Configure a bridge group in transparent mode.

Answer: D

Explanation:

Traditionally, a firewall is a routed hop and acts as a default gateway for hosts that connect to one of its screened subnets. A transparent firewall, on the other hand, is a Layer 2 firewall that acts like a “bump in the wire,” or a “stealth firewall,” and is not seen as a router hop to connected devices. However, like any other firewall, access control between interfaces is controlled, and all of the usual firewall checks are in place. Layer 2 connectivity is achieved by using a "bridge group" where you group together the inside and outside interfaces for a network, and the ASA uses bridging techniques to pass traffic between the interfaces. Each bridge group includes a Bridge Virtual Interface (BVI) to which you assign an IP address on the network. You can have multiple bridge groups for multiple networks. In transparent mode, these bridge groups cannot communicate with each other.

<https://www.cisco.com/c/en/us/td/docs/security/asa/asa97/configuration/general/asa-97-general-config/intro-fw>.

NEW QUESTION 168

- (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

NEW QUESTION 171

- (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 173

.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questions and Answers in PDF Format

300-710 Practice Exam Features:

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

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