

Cisco.300-710.v2026-10-12.q195

Exam Code:	300-710
Exam Name:	Securing Networks with Cisco Firepower
Certification Provider:	Cisco
Free Question Number:	195
Version:	v2026-10-12
# of views:	106
# of Questions views:	1950
https://www.freepdfdumps.com/Cisco.300-710.v2026-10-12.q195.html	

NEW QUESTION: 1

An engineer is troubleshooting an intermittent connectivity issue on a Cisco Secure Firewall Threat Defense appliance and must collect 24 hours worth of data. The engineer started a packet capture, however it stops prematurely during this time period. The engineer notices that the packet capture buffer size is set to the default of 32 MB. Which buffer size is the maximum that the engineer must set to enable the packet capture to run successfully?

- A. 64 MB
- B. 100 GB
- C. 1 GB
- D. 10 GB

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 2

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 ([LEAVE A REPLY](#))

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: 3

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

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

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 4

A network administrator is migrating from a Cisco ASA to a Cisco FTD.

EIGRP is configured on the Cisco ASA but it is not available in the Cisco FMC.

Which action must the administrator take to enable this feature on the Cisco FTD?

- A. Enable advanced configuration options in the FMC.
- B. Create a custom variable set and enable the feature in the variable set.
- C. Add the command feature eigrp via the FTD CLI.
- D. Configure EIGRP parameters using FlexConfig objects.

Answer: D ([LEAVE A REPLY](#))

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

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 6

An engineer must build redundancy into the network and traffic must continuously flow if a redundant switch in front of the firewall goes down. What must be configured to accomplish this task?

- A. redundant interfaces on the firewall cluster mode and switches
- B. redundant interfaces on the firewall noncluster mode and switches
- C. vPC on the switches to the interface mode on the firewall duster
- D. vPC on the switches to the span EtherChannel on the firewall cluster

Answer: ([SHOW ANSWER](#))

Reference: <https://www.ciscolive.com/c/dam/r/ciscolive/us/docs/2018/pdf/BRKSEC-2020.pdf>

NEW QUESTION: 7

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

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

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 8

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

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 9

```
Network_1;Internal network;192.168.1.0/24;  
FQDN_1;Domain Names;FQDN;www.example.com;ipv4_ipv6  
Network_2;Internal network2;192.168.2.0/24;
```

Refer to the exhibit. An engineer must import three network objects into the Cisco Secure Firewall Management Center by using a CSV file. Which header must be configured in the CSV file to accomplish the task?

- A. NAME;DESCRIPTION; TYPE;VALUE;DN;
- B. Name; Description; Type;Value;DN;
- C. NAME;DESCRIPTION;TYPE;VALUE;LOOKUP;
- D. Name; Description; Type;Value;Lookup;

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 10

A network administrator manages a network with multiple firewalls in a datacenter using Cisco Secure Firepower Management Center. The administrator must change a next-generation firewall from routed to transparent mode. Which action must the administrator take next to meet the requirement?

- A. Deregister the firewall in Cisco Secure Firewall Management Center.
- B. Manually delete the interface configuration from the CLI.
- C. Enter the configure transparent firewall command from the CLI.
- D. Create one or more bridge groups from the CLI.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 11

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

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

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 12

A network engineer must provide a high-level statistical summary of a Cisco Secure Firewall Threat Defense device. The organization is approaching its peak season, so network downtime must be minimized. Which type of report must the network engineer use?

- A. Malware
- B. SNMP
- C. Risk
- D. Host

Answer: (SHOW ANSWER)

SNMP provides nonintrusive, read-only monitoring of Secure Firewall Threat Defense devices and is appropriate for collecting high-level device statistics without interrupting production traffic. An external network management system can poll supported Management Information Base objects to obtain CPU utilization, memory usage, interface statistics, Snort information, process status, high-availability state, and cluster health. SNMP traps can also report important events without requiring continuous manual access to the device. Malware reports focus on malicious files and malware events, while risk reports summarize security risks and attacks. Host reports describe discovered hosts, applications, operating systems, and vulnerabilities rather than overall device performance. Because the requirement concerns device-level statistics and minimizing operational disruption during peak season, SNMP monitoring is the most appropriate choice.

Cisco Secure Firewall SNMP monitoring

NEW QUESTION: 13

Which two solutions are used to access and view aggregated log data from the firewalls using Cisco Security Analytics and Logging? (Choose two.)

- A. Cisco Secure Network Analytics
- B. Secure Cloud Analytics
- C. Cisco Defense Orchestrator
- D. Cisco Prime Infrastructure
- E. Cisco Catalyst Center

Answer: A,B (LEAVE A REPLY)

NEW QUESTION: 14

Which Cisco Advanced Malware Protection for Endpoints policy is used only for monitoring endpoint actively?

- A. Windows domain controller
- B. audit
- C. triage
- D. protection

Answer: B (LEAVE A REPLY)

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

NEW QUESTION: 15

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

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

Answer: C (LEAVE A REPLY)

NEW QUESTION: 16

An administrator is attempting to add a Cisco Secure Firewall Threat Defence device to Cisco Secure Firewall Management Center with a password of Cisco0480846211 480846211. The private IP address of the FMC server is 192.168.75.201. Which command must be used in order to accomplish this task?

- A. configure manager add 192.168.75.201/24 <reg_key>
- B. configure manager add 192.16875.201 <reg_key>
- C. configure manager add 192.168.45.45 <reg_key> <nal-ld>
- D. configure manager add 192.168.75.201 255.255.255.0 <reg_key>

Answer: B (LEAVE A REPLY)

To add a Cisco Secure Firewall Threat Defense (FTD) device to Cisco Secure Firewall Management Center (FMC), the correct command to use is configure manager add 192.168.75.201 <reg_key>. This command registers the FTD device with the FMC using the FMC's IP address and the registration key provided during the FMC setup.

Command structure:

* configure manager add <FMC_IP> <reg_key>

For the given scenario:

* FMC IP address: 192.168.75.201

* Registration key: provided during FMC setup

Thus, the correct command is:

* configure manager add 192.168.75.201 <reg_key>

References: Cisco Secure Firewall Management Center Device Configuration Guide, Chapter on Device Registration.

Valid 300-710 Dumps shared by Actual4test.com for Helping Passing 300-710 Exam! Actual4test.com now offer the **newest 300-710 exam dumps**, the Actual4test.com 300-710 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com 300-710 dumps with Test Engine here: https://www.actual4test.com/300-710_examcollection.html (446 Q&As Dumps, **30%OFF Special Discount: Freepdfdumps**)

NEW QUESTION: 17

A security engineer must configure policies for a recently deployed Cisco FTD. The security policy for the company dictates that when five or more connections from external sources are initiated within 2 minutes, there is cause for concern. Which type of policy must be configured in Cisco FMC to generate an alert when this condition is triggered?

- A. application detector
- B. access control
- C. intrusion
- D. correlation

Answer: D (LEAVE A REPLY)

A correlation policy is a feature that allows you to respond in real time to threats or specific conditions on your network, using correlation rules. A correlation rule can trigger when the system generates a specific type of event, or when your network traffic deviates from its normal profile¹. When a correlation rule triggers, the system generates a correlation event and can also launch a response, such as sending an alert, blocking an IP address, or scanning a host¹. In this case, the security engineer can configure a correlation rule that triggers when the system detects five or more connections from external sources within 2 minutes. The engineer can also configure a response that sends an alert to the FMC or an email recipient when this condition is triggered. The engineer can then create a correlation policy that includes this rule and activate it on the FTD device¹.

The other options are incorrect because:

- * An application detector is a feature that allows you to detect web applications, clients, and application protocols based on patterns in network traffic. An application detector does not generate alerts based on the number of connections from external sources².
- * An access control policy is a feature that allows you to control traffic flow through your network and inspect traffic for intrusions, malware, and files. An access control policy does not generate alerts based on the number of connections from external sources³.
- * An intrusion policy is a feature that allows you to detect and prevent malicious network activity using Snort rules. An intrusion policy does not generate alerts based on the number of connections from external sources⁴.

NEW QUESTION: 18

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

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

Answer: B ([LEAVE A REPLY](#))

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

NEW QUESTION: 19

An engineer attempts to pull the configuration for a Cisco FTD sensor to review with Cisco TAC but does not have direct access to the CU for the device. The CLI for the device is managed by Cisco FMC to which the engineer has access. Which action in Cisco FMC grants access to the CLI for the device?

- A. Export the configuration using the Import/Export tool within Cisco FMC.
- B. Create a backup of the configuration within the Cisco FMC.
- C. Use the show run all command in the Cisco FTD CLI feature within Cisco FMC.
- D. Download the configuration file within the File Download section of Cisco FMC.

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 20

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

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 21

An engineer must configure a new identity policy in Cisco Firepower Management Center. Active authentication must be configured by using a Kerberos connection. Which two realms must be configured?

(Choose two.)

- A. Active directory primary domain
- B. Active directory join password

- C. Directory password
- D. Active directory join username
- E. Directory username

Answer: A,D ([LEAVE A REPLY](#))

NEW QUESTION: 22

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

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 23

An engineer is configuring a Cisco Secure Firewall Threat Defense device to operate in transparent mode between two switch stacks. VLAN 10 is used for in-band management on both switch stacks. Which two actions are required on the device to inspect traffic between the switch stacks without interrupting network traffic? (Choose two.)

- A. Configure a BVI interface for VLAN 10.
- B. Configure at least one bridge group.
- C. Exempt BPDUs from advanced inspection.
- D. Set the MTU to 9198 on all interfaces to support jumbo frames.
- E. Add separate routes for data and management traffic.

Answer: B,C ([LEAVE A REPLY](#))

Transparent firewall mode forwards traffic at Layer 2, so the participating physical interfaces must be assigned to at least one bridge group. This allows the device to inspect traffic while remaining logically transparent to the connected switch stacks. Bridge Protocol Data Units should also be exempted from advanced inspection. BPDUs are essential for spanning-tree operation, and delaying or blocking them during inspection restarts can produce topology instability or an interruption. A BVI provides Layer 3 addressing for device-originated traffic or management but is not inherently required merely to inspect transit traffic. Jumbo-frame configuration is unnecessary unless the network explicitly uses jumbo frames, and separate data and management routes do not establish transparent forwarding. Cisco specifically recommends using an EtherType ACL to trust BPDUs on each bridge-group member interface. Cisco transparent firewall configuration

NEW QUESTION: 24

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: D ([LEAVE A REPLY](#))

Transparent mode is a firewall configuration in which the firewall acts as a "bump in the wire" or a "stealth firewall" and is not seen as a router hop to connected devices. In transparent mode, the firewall can forward traffic at both layer 2 and layer 3 for the same subnet, as it does not perform any address translation or

routing. The firewall inspects the traffic and applies security policies based on the source and destination IP addresses, ports, and protocols. Transparent mode is useful when you want to deploy a firewall without changing the existing network topology or addressing scheme¹.

NEW QUESTION: 25

An engineer is deploying failover capabilities for a pair of Cisco Secure Firewall devices. The core switch keeps the MAC address of the previously active unit in the ARP table. Which action must the engineer take to minimize downtime and ensure that network users keep access to the internet after a Cisco Secure Firewall failover?

- A.** Add the MAC address to the switch ARP table.
- B.** Run a script to send gratuitous ARP after a failover.
- C.** Use a virtual MAC address on both units
- D.** Set the same MAC address on both units.

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 26

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.** Restore the primary Cisco FMC backup configuration to the secondary Cisco FMC device when the primary device fails
- D.** Place the active Cisco FMC device on the same trusted management network as the standby device

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 27

An engineer is analyzing a risk report generated by Cisco Secure Firewall Management Center. The report contains the following fields:

Total Attacks

Events Requiring Attention

Hosts Targeted

Hosts Connected to CnC Servers

Which type of risk report is the engineer analyzing?

- A.** Network Risk Report
- B.** Attacks Risk Report
- C.** Events Risk Report
- D.** Hosts Risk Report

Answer: B ([LEAVE A REPLY](#))

These fields belong to the Attacks Risk Report. Cisco defines Total Attacks as the number of IPS events and Hosts Targeted as the number of unique destination addresses associated with relevant IPS events. Events Requiring Attention represents the proportion of intrusion events with an impact flag indicating relevance.

Hosts Connected to CnC Servers identifies unique hosts associated with the "CnC Connected" indication-of-compromise category. Together, these measurements summarize attack activity, affected assets, and potentially compromised systems. A Network Risk Report focuses on broader network-level risk and does not use this exact field collection. "Events Risk Report" and "Hosts Risk Report" are not the applicable standard risk-report templates. List B

incorrectly marks Network Risk Report; Cisco's report documentation explicitly assigns all four fields to the Attacks Risk Report, so the verified answer is B.
Cisco risk-report templates

NEW QUESTION: 28

A VPN administrator converted an instance of Cisco Secure Firewall Threat Defense, which is managed by Cisco Secure Firewall Management Center, from using LDAP to LDAPS for remote access VPN authentication. Which certificate must be added to allow for remote users to authenticate over the VPN?

- A.** LDAPS server certificate must be added to Secure Firewall Management Center realms.
- B.** Secure Firewall Management Center certificate must be added to the LDAPS server.
- C.** LDAPS server certificate must be added to Secure Firewall Threat Defense.
- D.** Secure Firewall Threat Defense certificate must be added to the LDAPS server.

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 29

A network administrator must send a daily email report to management detailing changes made during the previous 24 hours in Cisco Secure Firewall Management Center. Which system setting must be enabled to meet this requirement?

- A.** Change Reconciliation
- B.** Send Audit Log to HTTP Server
- C.** Send Audit Log to Syslog
- D.** STIG Compliance

Answer: A ([LEAVE A REPLY](#))

Change Reconciliation records snapshots whenever users save system-configuration changes and combines those snapshots into a detailed report covering the previous 24 hours. Under System > Configuration > Change Reconciliation, the administrator enables the feature, selects the daily execution time, and specifies management's recipient email addresses. The administrator can also include policy-configuration changes and enable the full change history instead of receiving only a consolidated view. An email relay host must be configured so that Management Center can deliver the report. Sending audit logs to an HTTP or syslog server streams audit events to an external collector; it does not generate the required daily email summary. STIG Compliance applies security-hardening settings and is unrelated to scheduled change reporting. Cisco Change Reconciliation documentation

NEW QUESTION: 30

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

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 31

Which feature sets up multiple interfaces on a Cisco Secure Firewall Threat Defense to be on the same subnet?

- A.** EtherChannel
- B.** security levels
- C.** SVI

D. BVI

Answer: D ([LEAVE A REPLY](#))

Valid 300-710 Dumps shared by Actual4test.com for Helping Passing 300-710 Exam! Actual4test.com now offer the **newest 300-710 exam dumps**, the Actual4test.com 300-710 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com 300-710 dumps with Test Engine here: https://www.actual4test.com/300-710_examcollection.html (446 Q&As Dumps, **30%OFF** Special Discount: **Freepdfdumps**)

NEW QUESTION: 32

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

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

Answer: A ([LEAVE A REPLY](#))

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

NEW QUESTION: 33

A security analyst is investigating a potential network compromise. The analyst must produce a report of the suspicious activity from Cisco Secure Firewall Management Center. Which two details must be included in the report to assist the investigation? (Choose two.)

- A. Client applications by user
- B. Intrusion events
- C. Host connections
- D. Number of attacked machines
- E. User connections

Answer: B,C ([LEAVE A REPLY](#))

Intrusion events provide the detection evidence needed to understand which signatures fired, the affected source and destination addresses, event severity, protocol information, and other indicators associated with the suspected compromise. Host connections provide the corresponding network context, allowing the analyst to determine which systems communicated, when the sessions occurred, and which ports, applications, or protocols were involved. Together, these details connect security detections with the traffic flows that produced them and support reconstruction of the incident. Client applications by user and user connections are useful when the investigation is primarily identity-focused, but they do not provide the same direct combination of exploit evidence and host-level network activity. The number of attacked machines is an aggregate measurement and lacks the granular information necessary to investigate the suspicious communications and determine their cause.

NEW QUESTION: 34

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

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

Answer: ([SHOW ANSWER](#))

Reference: <https://www.cisco.com/c/en/us/td/docs/security/firesight/541/user-guide/FireSIGHT-System- UserGuide-v5401/Reports.html#87267>

NEW QUESTION: 35

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

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

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 36

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. Perform the trace within the Cisco FMC GUI instead of the Cisco FTD CLI.
- 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. Use the verbose option as a part of the capture-traffic command

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 37

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 ([LEAVE A REPLY](#))

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-cisco-firepow.html>

NEW QUESTION: 38

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

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

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 39

An engineer must implement Cisco Secure Firewall transparent mode due to a new server recently being added that must communicate with an existing server that is currently separated by the firewall. Which implementation action must be taken next by the engineer to accomplish the goal?

- A. Ensure that both servers are in the same bridge domain.
- B. Enable both servers to share the same VXLAN segment.
- C. Assign the same subnet to both servers.
- D. Configure the same default gateway for both servers.

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 40

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

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

Answer: C ([LEAVE A REPLY](#))

Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/660/configuration/guide/fpmc-config-guide-v66/command_line_reference.pdf

NEW QUESTION: 41

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

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 42

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 application-identification-debug command to determine which rules the traffic matching and modify the rule accordingly
- B. Use the system support network-options command to fine tune the policy.
- 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 firewall-engine-debug command to determine which rules the traffic matching and modify the rule accordingly

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 43

An engineer is integrating Cisco Secure Endpoint with Cisco Secure Firewall Management Center in high availability mode. Malware events detected by Secure Endpoint must also be received by Secure Firewall Management Center and public cloud services are used. Which two configurations must be selected on both high availability peers independently? (Choose two.)

- A. Smart Software Manager Satellite

- B. Cisco Success Network
- C. internet connection
- D. Secure Endpoint Cloud Connection
- E. security group tag

Answer: C,D ([LEAVE A REPLY](#))

NEW QUESTION: 44

Refer to the exhibit.

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

- A. Create an access control policy rule to allow port 443 to only 172.1.1 50
- B. Create an intrusion policy rule to have Snort allow port 443 to only 172.1.1.50
- C. Create an intrusion policy rule to have Snort allow port 80 to only 172.1.1 50.
- D. Create an access control policy rule to allow port 80 to only 172.1.1 50.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 45

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

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

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 46

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

Answer: C ([LEAVE A REPLY](#))

Valid 300-710 Dumps shared by Actual4test.com for Helping Passing 300-710 Exam! Actual4test.com now offer the **newest 300-710 exam dumps**, the Actual4test.com 300-710 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com 300-710 dumps with Test Engine here: https://www.actual4test.com/300-710_examcollection.html (446 Q&As Dumps, **30%OFF** Special Discount: **Freepdfdumps**)

NEW QUESTION: 47

A network engineer detects a connectivity issue between Cisco Secure Firewall Management Centre and Cisco Secure Firewall Threat Defense Initial troubleshooting indicates that heartbeats and events not being received. The engineer re-establishes the secure channels between both peers Which two commands must the engineer run to resolve the issue? (Choose two.)

- A. manage_procs.pl
- B. sudo stats_unified.pl
- C. sudo perfstats -Cq < /var/sf/rna/correlator-stats/now
- D. show history
- E. show disk-manager

Answer: A,B (LEAVE A REPLY)

When connectivity issues are detected between Cisco Secure Firewall Management Center (FMC) and Cisco Secure Firewall Threat Defense (FTD) devices, and initial troubleshooting indicates that heartbeats and events are not being received, the engineer can run the following commands to resolve the issue by re-establishing secure channels and checking process statuses:

* manage_procs.pl: This script is used to manage and restart processes on the FTD device. Running this script can help restart any malfunctioning processes and re-establish connectivity between the FMC and FTD.

* sudo stats_unified.pl: This command provides detailed statistics and status of the unified system processes. It helps in diagnosing and resolving issues related to the secure channel and event reporting.

Steps:

- * Access the FTD CLI.
- * Run the command `manage_procs.pl` to restart processes.
- * Run the command `sudo stats_unified.pl` to gather detailed process statistics and verify the status.

These commands help resolve connectivity issues by ensuring that all necessary processes are running correctly and secure channels are re-established.

References: Cisco Secure Firewall Threat Defense Configuration Guide, Chapter on Troubleshooting and CLI Commands.

NEW QUESTION: 48

A network engineer detects a connectivity issue between Cisco Secure Firewall Management Center and Cisco Secure Firewall Threat Defense. Initial troubleshooting indicates that heartbeats and events are not being received. The engineer re-establishes the secure channels between both peers. Which two commands must the engineer run to resolve the issue? (Choose two.)

- A. show disk-manager
- B. sudo perfstats -Cq < /var/sf/rna/correlator-stats/now
- C. show history
- D. sudo stats_unified.pl
- E. manage_procs.pl

Answer: D,E (LEAVE A REPLY)

NEW QUESTION: 49

An engineer is configuring Cisco FMC and wants to allow multiple physical interfaces to be part of the same VLAN. The managed devices must be able to perform Layer 2 switching between interfaces, including sub-interfaces. What must be configured to meet these requirements?

- A. integrated routing and bridging
- B. Cisco ISE Security Group Tag
- C. interface-based VLAN switching
- D. inter-chassis clustering VLAN

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 50

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

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 51

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

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

Answer: (SHOW ANSWER)

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

NEW QUESTION: 52

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: (SHOW ANSWER)

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

NEW QUESTION: 53

Which communication is blocked from the bridge groups when multiple are configured in transparent mode on a Cisco Secure Firewall Threat Defense appliance?

- A. With other routers
- B. With each other
- C. With client devices
- D. With the internet

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 54

An engineer plans to reconfigure an existing Cisco FTD from transparent mode to routed mode. Which additional action must be taken to maintain communication between the two network segments?

- A. Configure a NAT rule so that traffic between the segments is exempt from NAT.
- B. Update the IP addressing so that each segment is a unique IP subnet.
- C. Deploy inbound ACLs on each interface to allow traffic between the segments.
- D. Assign a unique VLAN ID for the interface in each segment.

Answer: B (LEAVE A REPLY)

When reconfiguring an existing Cisco FTD from transparent mode to routed mode, an additional action that must be taken to maintain communication between the two network segments is to update the IP addressing so that each segment is a unique IP subnet. This is because in routed mode, the FTD device acts as a router hop in the network and requires each interface to be on a different subnet. In transparent mode, the FTD device acts as a layer 2 firewall and does not require different subnets for each interface¹.

The other options are incorrect because:

- * Configuring a NAT rule so that traffic between the segments is exempt from NAT is not necessary to maintain communication between the two network segments. NAT is used to translate IP addresses between different networks, but it does not affect the routing of packets. Moreover, NAT is optional in routed mode and can be disabled if not needed².
- * Deploying inbound ACLs on each interface to allow traffic between the segments is not required to maintain communication between the two network segments. ACLs are used to control access to network resources based on source and destination addresses, protocols, and ports. They do not affect the routing of packets. Furthermore, ACLs are optional in routed mode and can be configured as needed³.
- * Assigning a unique VLAN ID for the interface in each segment is not relevant to maintain communication between the two network segments. VLANs are used to create logical groups of hosts that share the same broadcast domain, regardless of their physical location or connection. They do not affect the routing of packets. Besides, VLANs are not supported in routed mode and can only be used in transparent mode⁴.

NEW QUESTION: 55

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: (SHOW ANSWER)

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

NEW QUESTION: 56

An engineer must replace a Cisco Secure Firewall high-availability device due to a failure. When the replacement device arrives, the engineer must separate the high-availability pair from Cisco Secure Firewall Management Center. Which action must the engineer take first to restore high availability?

- A. Register the secondary device
- B. Force a break between the devices.
- C. Unregister the secondary device.
- D. Configure NTP time synchronization.

Answer: C (LEAVE A REPLY)

When replacing a Cisco Secure Firewall high-availability (HA) device due to a failure, the first step the engineer must take is to unregister the secondary (failed) device from the Cisco Secure Firewall Management Center (FMC). This action separates the HA pair and ensures that the new replacement device can be registered and configured correctly.

Steps:

- * Access the FMC and navigate to the device management section.
- * Unregister the failed secondary device to remove it from the HA pair.
- * Register the replacement device to the FMC.
- * Reconfigure the HA settings to restore the high-availability configuration.

By unregistering the failed device first, the engineer ensures a clean setup for the replacement device, avoiding potential conflicts or issues in the HA configuration.

References: Cisco Secure Firewall Management Center Administrator Guide, Chapter on High Availability Configuration.

NEW QUESTION: 57

A security engineer must create a malware and file policy on a Cisco Secure Firewall Threat Defense device.

The solution must ensure that PDF, DOCX, and XLSX files are not sent to Cisco Secure Malware analytics.

What must be configured to meet the requirements?

- A. capacity handling
- B. Spero analysis
- C. dynamic analysis
- D. local malware analysis

Answer: D (LEAVE A REPLY)

To create a malware and file policy on a Cisco Secure Firewall Threat Defense (FTD) device that ensures PDF, DOCX, and XLSX files are not sent to Cisco Secure Malware Analytics, the security engineer must configure local malware analysis. Local malware analysis allows the FTD to inspect and analyze files locally without sending them to the cloud-based Cisco Secure Malware Analytics.

Steps to configure local malware analysis:

- * In FMC, navigate to Policies > Access Control > Malware & File Policies.
- * Create a new malware and file policy or edit an existing one.
- * Define rules to inspect specific file types, ensuring that PDF, DOCX, and XLSX files are handled locally.
- * Set the action for these file types to "Local Analysis."
- * Apply the policy to the relevant access control policy.

This configuration ensures that the specified file types are analyzed locally, meeting the requirement to avoid sending them to Cisco Secure Malware Analytics.

References: Cisco Secure Firewall Management Center Configuration Guide, Chapter on Malware and File Policies

NEW QUESTION: 58

A security engineer wants to add the Interface Traffic widget to the Summary Dashboard in Cisco Secure Firewall Management Center. The engineer clicks Add Widgets and enters edit mode. Which set of actions must the security engineer take to complete the configuration?

- A. Click All Categories, open the Analysis & Reporting tab, and then click the Add widget button.
- B. Click All Categories, open the New tab, and then click the Add widget button.
- C. Click All Categories, open the Operations tab, and then click the Add widget button.
- D. Click All Categories, open the Miscellaneous tab, and then click the Add widget button.

Answer: C (LEAVE A REPLY)

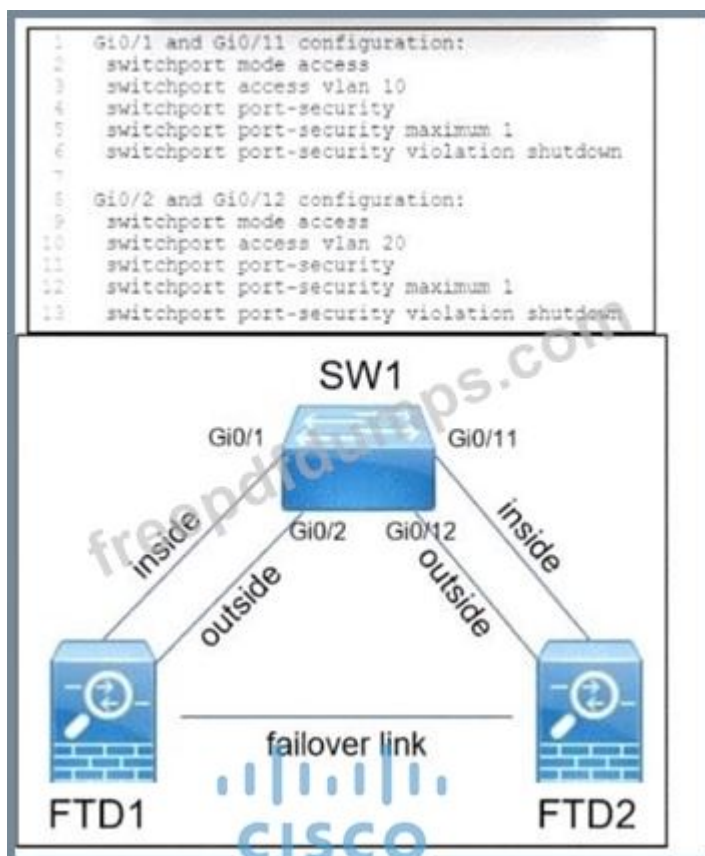
The Interface Traffic widget belongs to the Operations category because it displays operational information about appliance interfaces, specifically received and transmitted traffic rates. After selecting Add Widgets, the engineer can select All Categories and open Operations to locate Interface Traffic, then click Add next to the widget. Analysis & Reporting contains widgets based on collected security events and analytical data.

Miscellaneous contains widgets that display neither event nor operational data, such as the RSS Feed widget.

"New" is not a valid predefined widget category. Cisco classifies Operations widgets as those that display system status and overall health information. The Interface Traffic widget is not included on predefined dashboards by default, so it must be added manually using this procedure. Cisco Secure Firewall dashboard documentation

NEW QUESTION: 59

Refer to the exhibit.



A company is deploying a pair of Cisco Secure Firewall Threat defence devices named FTD1 and FTD2.

FTD1 and FTD2 have been configured as an active/standby pair with a failover link but without a stateful link. What must be implemented next to ensure that users on the internal network still communicate with outside devices if FTD1 fails?

- A. Disable port security on the switch interfaces connected to FTD1 and FTD2.
- B. Set maximum secured addresses to two on the switch interfaces on FTD1 and FTD2.
- C. Connect and configure a stateful link and then deploy the changes.
- D. Configure the spanning-tree PortFast feature on SW1 and FTD2

Answer: C (LEAVE A REPLY)

In a failover configuration with Cisco Secure Firewall Threat Defense (FTD) devices, ensuring that users on the internal network can continue to communicate with outside devices if the primary device (FTD1) fails requires the implementation of a stateful failover link. The stateful failover link allows the secondary device (FTD2) to maintain session information and state data, ensuring seamless failover and minimizing disruptions.

Steps to implement a stateful failover link:

* Physically connect a stateful failover link between FTD1 and FTD2.

- * Configure the stateful failover link in the FMC.
- * Ensure that both devices are properly synchronized and that stateful failover is enabled.
- * Deploy the changes to both FTD devices.

By configuring a stateful link, the secondary FTD can take over active sessions without requiring users to re-establish their connections, thus ensuring continuous communication.

References: Cisco Secure Firewall Threat Defense Configuration Guide, Chapter on Failover Configuration.

NEW QUESTION: 60

Cisco Security Analytics and Logging SaaS licenses come with how many days of data retention by default?

- A. 60
- B. 365
- C. 90
- D. 120

Answer: C ([LEAVE A REPLY](#))

Cisco Security Analytics and Logging (SaaS) licenses come with a default data retention period of 90 days.

This retention period allows organizations to store and analyze their security event data for up to 90 days, providing sufficient time for security monitoring and forensic investigations.

References: Cisco Security Analytics and Logging Documentation, Chapter on License Information and Data Retention.

NEW QUESTION: 61

A network administrator is trying to configure a previously created file policy on a new access policy. Which action must the administrator take before applying the file policy?

- A. Assign the file policy to the default action.
- B. Set up an inspection policy.
- C. Create a new access control rule.
- D. Apply an application to an access control rule.

Answer: ([SHOW ANSWER](#))

Valid 300-710 Dumps shared by Actual4test.com for Helping Passing 300-710 Exam! Actual4test.com now offer the **newest 300-710 exam dumps**, the Actual4test.com 300-710 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com 300-710 dumps with Test Engine here: https://www.actual4test.com/300-710_examcollection.html (446 Q&As Dumps, **30%OFF** Special Discount: **Freepdfdumps**)

NEW QUESTION: 62

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

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

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 63

An engineer must configure an ERSPAN passive interface on a Cisco Secure IPS by using the Cisco Secure Firewall Management Center. These configurations have been performed already:

* Configure the passive interface.

* Configure the ERSPAN IP address.

Which two additional settings must be configured to complete the configuration? (Choose two.)

A. TCP Intercept

B. Source IP

C. Flow ID

D. Destination MAC

E. Bypass Mode

Answer: A,C ([LEAVE A REPLY](#))

NEW QUESTION: 64

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 must allow traffic to the internal web server IP address.

C. The access policy rule must be configured for the action trust.

D. The NAT policy must be modified to translate the source IP address as well as destination IP address.

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 65

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. Link-state propagation is enabled

B. The Cisco IPS has been configured to be in fail-open mode

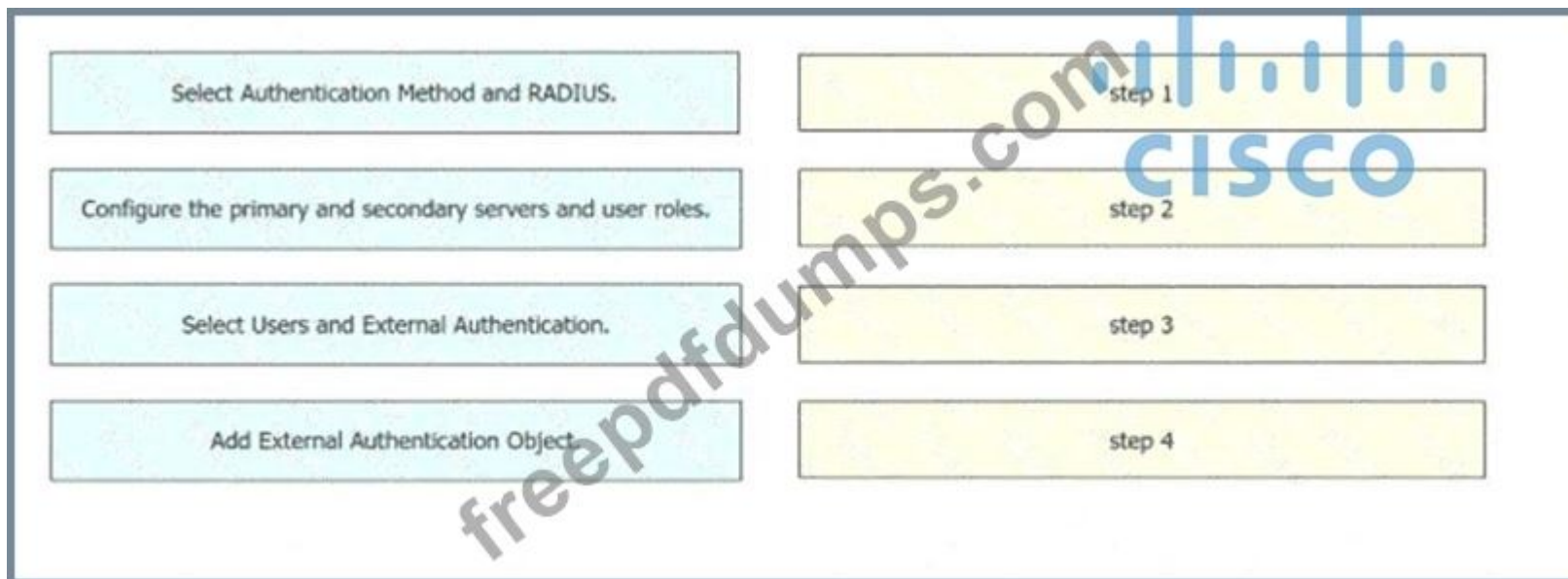
C. The upstream router has a misconfigured routing protocol

D. The Cisco IPS is configured in detection mode

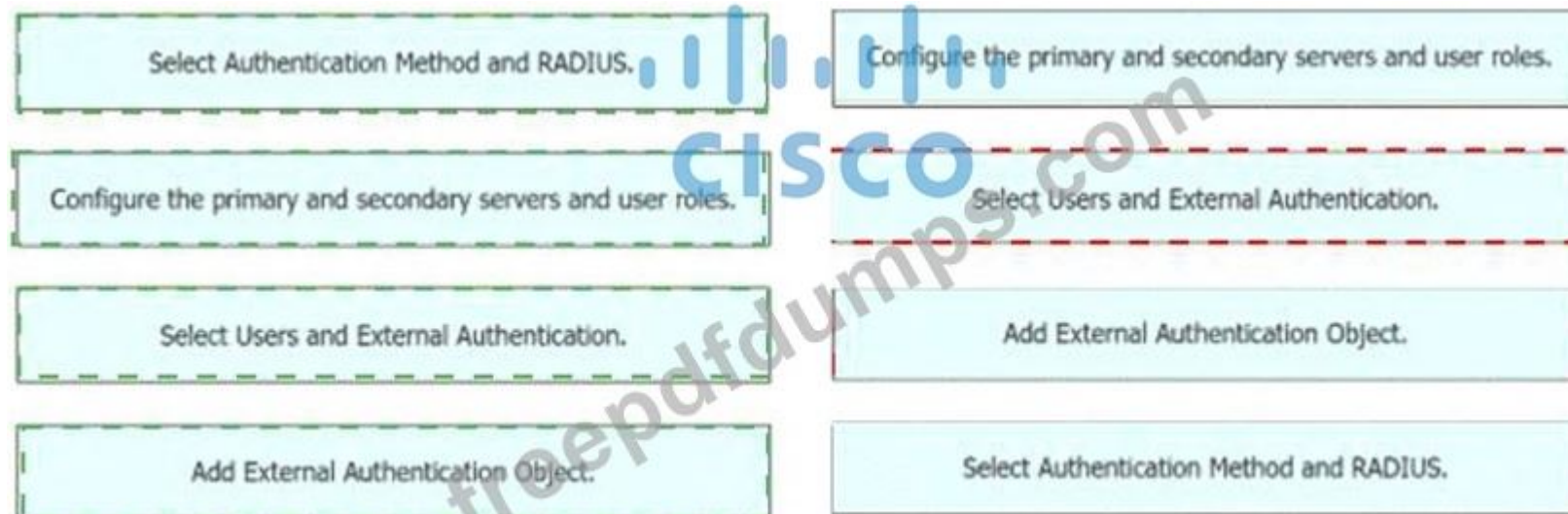
Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 66

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.



Answer:



Explanation:

4, 1, 2, 3

NEW QUESTION: 67

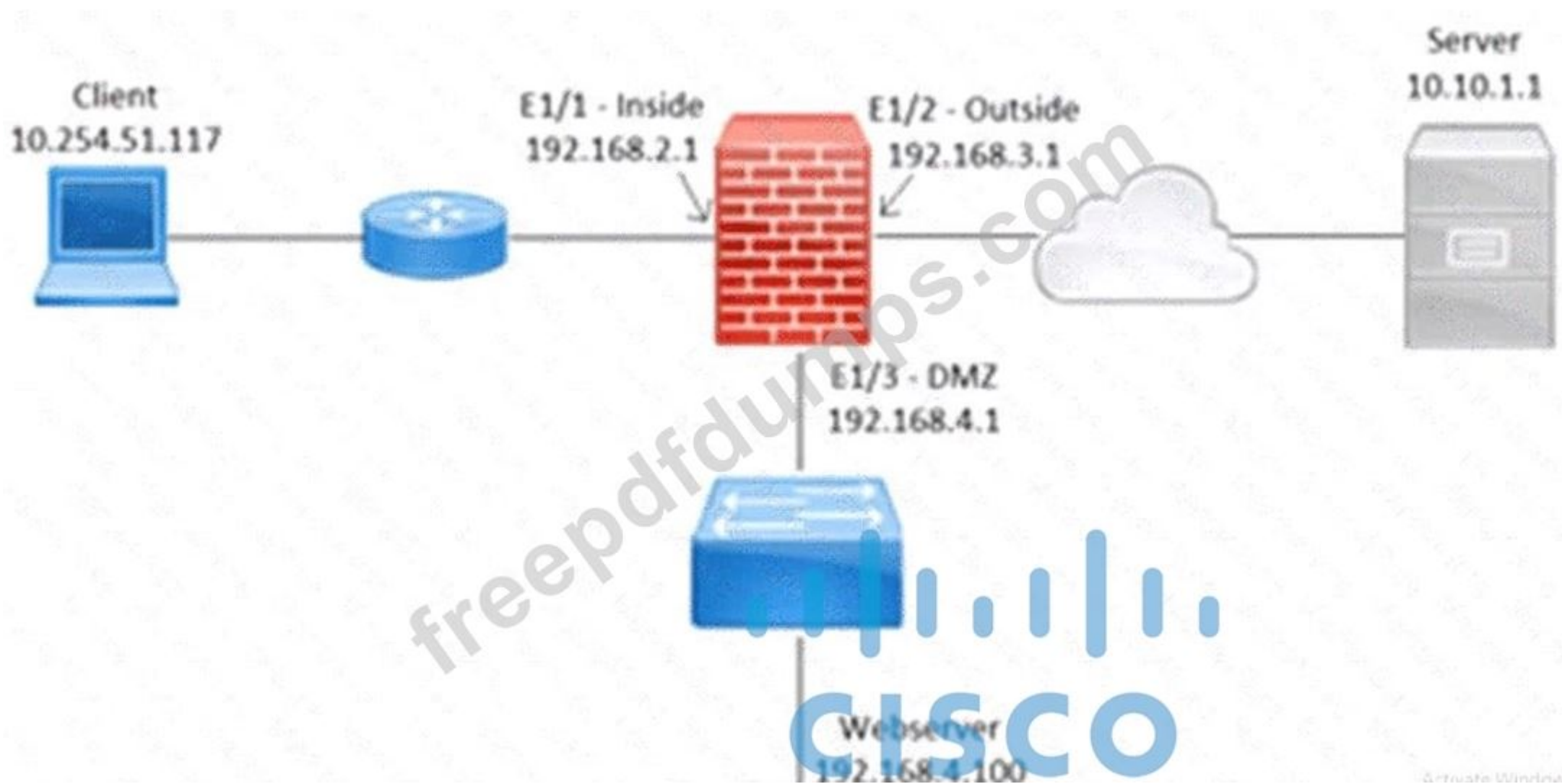
A network engineer is tasked with minimising traffic interruption during peak traffic times. When the SNORT inspection engine is overwhelmed, what must be configured to alleviate this issue?

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

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 68

Refer to the exhibit.



A client with IP address 10.254.51.117 connects through a Cisco Secure Firewall Threat Defense device toward a website at 10.10.1.1. The packet capture shows repeated TCP SYN packets from the client without completion of the three-way handshake. Which action must the engineer take to resolve the issue?

- A. Configure the inside interface to send ACK messages.
- B. Add a firewall rule that allows the web server to communicate with the DMZ.
- C. Add a firewall rule that allows ACK responses from the inside to the outside.
- D. Configure the outside interface to receive SYN-ACK messages.

Answer: D (LEAVE A REPLY)

The capture shows that the client repeatedly transmits a TCP SYN but does not receive the SYN-ACK required to advance the connection state. This indicates that the return portion of the TCP three-way handshake is not reaching the expected ingress interface or is not being processed there. The outside interface must therefore be configured or connected so that the returning SYN-ACK packets arrive through the interface where the firewall expects them. An access rule does not instruct an interface to generate TCP acknowledgement messages; ACK and SYN-ACK packets are produced by the communicating endpoints. Likewise, permitting communication "with the DMZ" does not address the missing return-handshake packet shown in the capture. Correcting the return path through the outside interface allows the firewall to observe both directions, establish state, and forward the subsequent packets.

NEW QUESTION: 69

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

- A. Install the static backup route and modify the metric to be less than the primary route.

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

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 70

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

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 71

After a network security breach, an engineer must strengthen the security of the corporate network. Upper management must be regularly updated with a high-level overview of any occurring network threats. Which access must the engineer provide upper management to view the required data from Cisco Secure Firewall Management Center?

- A. Events by priority and classification and set a sliding time window of one day
- B. Analysis > Status with a sliding time window of one day
- C. Reports with a daily recurring task that generates based on the network risk report template
- D. Security Intelligence Statistics dashboard set to Show the Last option to one day

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 72

A network administrator is seeing an unknown verdict for a file detected by Cisco FTD. Which malware policy configuration option must be selected in order to further analyse the file in the Talos cloud?

- A. Dynamic analysis
- B. Sandbox analysis
- C. Malware analysis
- D. Spero analysis

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 73

A network administrator is configuring a site-to-site IPsec VPN to a router sitting behind a Cisco FTD. The administrator has configured an access policy to allow traffic to this device on UDP 500, 4500, and ESP VPN traffic is not working. Which action resolves this issue?

- A. Change the access policy to allow all ports.
- B. Modify the NAT policy to use the interface PAT.
- C. Set the allow action in the access policy to trust.
- D. Enable IPsec inspection on the access policy.

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 74

On the advanced tab under inline set properties, which allows interfaces to emulate a passive interface?

- A. transparent inline mode
- B. TAP mode
- C. strict TCP enforcement
- D. propagate link state

Answer: D (LEAVE A REPLY)

Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/640/configuration/guide/fpmc-config-guide-v64/inline_sets_and_passive_interfaces_for_firepower_threat_defense.html

NEW QUESTION: 75

Refer to the exhibit.



An engineer generates troubleshooting files in Cisco Secure Firewall Management Center (FMC). A successfully completed task is removed before the files are downloaded. Which two actions must be taken to determine the filename and obtain the generated troubleshooting files without regenerating them? (Choose two.)

- A. Use an FTP client in expert mode on Secure FMC to upload the files to the FTP server.
- B. Go to the same screen as shown in the exhibit, click Advanced Troubleshooting, enter the file name, and then start the download
- C. Connect to CU on the FTD67 and FTD66 devices and copy the files from flash to the PIP server.
- D. Go to expert mode on Secure FMC. list the contents of /var/common, and determine the correct filename from the output
- E. Click System Monitoring, then Audit to determine the correct filename from the line containing the Generate Troubleshooting Files string.

Answer: (SHOW ANSWER)

If a task to generate troubleshooting files in Cisco Secure Firewall Management Center (FMC) is completed successfully but removed before the files are downloaded, the following steps can be taken to determine the filename and obtain the generated troubleshooting files without regenerating them:

Go to expert mode on Secure FMC:

Access expert mode on the FMC via SSH or the console.

List the contents of the directory /var/common to locate the generated troubleshooting files. Use the command `ls /var/common`.

Use the System Monitoring Audit logs:

In FMC, navigate to `System > Monitoring > Audit`.

Find the line containing the "Generate Troubleshooting Files" string to determine the correct filename.

These actions help identify and retrieve the generated troubleshooting files without the need to regenerate them, saving time and resources.

References: Cisco Secure Firewall Management Center Administrator Guide, Chapter on Troubleshooting and File Management.

NEW QUESTION: 76

A network administrator reviews the attack risk report and notices several Low-Impact attacks. What does this type of attack indicate?

- A. All attacks are listed as low until manually categorized.
- B. The host is not vulnerable to those attacks.
- C. The attacks are not dangerous to the network.
- D. The host is not within the administrator's environment.

Answer: B (LEAVE A REPLY)

A low-impact attack indicates that the host is not vulnerable to those attacks. A low-impact attack is an attack that does not exploit any known vulnerability on the target host or does not match any signature or anomaly rule on the FTD device⁵. A low-impact attack does not mean that the attack is not dangerous to the network or that the host is not within the administrator's environment. It simply means that the attack did not succeed in compromising or affecting the host.

The other options are incorrect because:

- * All attacks are not listed as low until manually categorized. The FTD device automatically assigns an impact level to each attack based on various factors, such as vulnerability information, threat score, and confidence rating⁵. The impact level can be high, medium, or low, depending on how likely and how severe the attack is.
- * The attacks are not necessarily harmless to the network. A low-impact attack may still cause some damage or disruption to the network, such as consuming bandwidth, generating noise, or distracting attention from other attacks⁶. A low-impact attack may also indicate that the attacker is probing or scanning the network for potential vulnerabilities or weaknesses⁷.
- * The host is not necessarily outside the administrator's environment. A low-impact attack can target any host on the network, regardless of its location or ownership. A low-impact attack does not imply that the host is external or irrelevant to the administrator's environment.

Valid 300-710 Dumps shared by Actual4test.com for Helping Passing 300-710 Exam! Actual4test.com now offer the **newest 300-710 exam dumps**, the Actual4test.com 300-710 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com 300-710 dumps with Test Engine here: https://www.actual4test.com/300-710_examcollection.html (446 Q&As Dumps, **30%OFF Special Discount: Freepdfdumps**)

NEW QUESTION: 77

An engineer must determine the root cause of an incident. The engineer plans to run a packet capture on a Cisco Secure Firewall device but remembers that the device experienced performance problems when the packet-capture command was previously executed. Which packet-capture options must the engineer use to minimize the performance impact?

- A. -c 10000 host 10.10.10.10
- B. -s 1500 -c 1000 host 10.10.10.10
- C. -c 1000 host 10.10.10.10
- D. -w test -s 1518 -c 1000 host 10.10.10.10

Answer: D (LEAVE A REPLY)

Cisco warns that displaying captured packets directly on the screen can degrade system and network performance. The -w test option writes raw packets to a file instead of continuously parsing and displaying them on the terminal. The -s 1518 option sets the snapshot length to the default Ethernet maximum frame size so complete packets are captured, while -c 1000 automatically stops the capture after 1,000 packets. The BPF expression host 10.10.10.10 further reduces resource consumption by capturing only traffic involving the specified host. Options A, B, and C limit the captured traffic to varying degrees, but they omit -w and therefore continue sending decoded packet output to the screen. Consequently, Option D is the complete performance-conscious capture command. Cisco packet-capture procedure

NEW QUESTION: 78

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 QoS policy rate-limiting high bandwidth applications
- B. Create a VPN policy so that direct tunnels are established to the business applications
- C. Create a flexconfig policy to use WCCP for application aware bandwidth limiting
- D. Create a NAT policy so that the Cisco Firepower device does not have to translate as many addresses

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 79

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: A,E ([LEAVE A REPLY](#))

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

NEW QUESTION: 80

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

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 81

An engineer defines a new rule while configuring an Access Control Policy. After deploying the policy, the rule is not working as expected and the hit counters associated with the rule are showing zero. What is causing this error?

- A. An incorrect application signature was used in the rule.
- B. Logging is not enabled for the rule.
- C. The rule was not enabled after being created.
- D. The wrong source interface for Snort was selected in the rule.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 82



Refer to the exhibit. An engineer is configuring a high-availability solution that has the hardware devices and software versions:

two Cisco Secure Firewall 9300 Security Appliances with FXOS SW 2.0(1.23) software Cisco Secure Firewall Threat Defense 6.0.1.1 (build 1023) on both appliances one Cisco Secure Firewall Management Center with SW 6.0.1.1 (build 1023) Which condition must be met to complete the high-availability configuration?

- A. Both firewalls must be in transparent mode.
- B. Both firewalls must have the same number of interfaces.
- C. DHCP must be configured on at least one firewall interface.
- D. The version numbers must have the same patch number.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 83

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

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 84

Which two routing options are valid with Cisco Firepower Threat Defense? (Choose two.)

- A. BGPv6

- B. ECMP with up to three equal cost paths across multiple interfaces
- C. ECMP with up to three equal cost paths across a single interface
- D. BGPv4 in transparent firewall mode
- E. BGPv4 with nonstop forwarding

Answer: A,C (LEAVE A REPLY)

Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/601/configuration/guide/fpmc-config-guide-v601/fpmc-config-guide-v60_chapter_01100011.html#ID-2101-0000000e

NEW QUESTION: 85

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

Answer: (SHOW ANSWER)

NEW QUESTION: 86

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

Answer: A (LEAVE A REPLY)

NEW QUESTION: 87



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

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 88

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

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 89

An engineer is troubleshooting an intermittent connectivity issue on a Cisco Secure Firewall Threat Defense appliance and must collect 24 hours' worth of data. The engineer started a packet capture. Whenever it stops prematurely during this time period. The engineer notices that the packet capture buffer size is set to the default of 32 MB Which buffer size is the maximum that the engineer must set to allow the packet capture to run successfully?

- A. 64 MB
- B. 1 GB
- C. 10 GB
- D. 100 GB

Answer: ([SHOW ANSWER](#))

To collect 24 hours' worth of data using a packet capture on a Cisco Secure Firewall Threat Defense (FTD) appliance without prematurely stopping due to buffer size limitations, the engineer should increase the packet capture buffer size. The default buffer size is 32 MB, which is insufficient for extended captures. Steps:

- * Access the packet capture configuration on the FTD device.
- * Increase the buffer size to 1 GB, which provides a significantly larger capacity for capturing packets over a 24-hour period.

Setting the buffer size to 1 GB should accommodate a substantial amount of traffic and prevent the capture from stopping prematurely.

References: Cisco Secure Firewall Threat Defense Configuration Guide, Chapter on Packet Capture Configuration and Management.

NEW QUESTION: 90

Which two routing options are valid with Cisco FTD? (Choose Two)

- A. BGPv6
- B. ECMP with up to three equal cost paths across multiple interfaces
- C. ECMP with up to three equal cost paths across a single interface
- D. BGPv4 in transparent firewall mode
- E. BGPv4 with nonstop forwarding

Answer: ([SHOW ANSWER](#))

Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/601/configuration/guide/fpmc-config-guide-v601/fpmc-config-guide-v601_chapter_01100011.html#ID-2101-0000000e

NEW QUESTION: 91

Which policy rule is included in the deployment of a local DMZ during the initial deployment of a Cisco NGFW through the Cisco FMC GUI?

- A. deny ip any
- B. permit ip any
- C. no policy rule is included
- D. a default DMZ policy for which only a user can change the IP addresses.

Answer: C ([LEAVE A REPLY](#))

Valid 300-710 Dumps shared by Actual4test.com for Helping Passing 300-710 Exam! Actual4test.com now offer the **newest 300-710 exam dumps**, the Actual4test.com 300-710 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com 300-710 dumps with Test Engine here: https://www.actual4test.com/300-710_examcollection.html (446 Q&As Dumps, **30%OFF** Special Discount: **Freepdfdumps**)

NEW QUESTION: 92

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

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 93

```

18 ASA# show interface | include ",|MAC|Member
19 Interface GigabitEthernet1/1 "inside", is up, line protocol is up
20     MAC address e4aa.5ae4.612e, MTU 1500
21 Interface GigabitEthernet1/2 "outside", is up, line protocol is up
22     MAC address e4aa.5ae4.612f, MTU 1500
23 Interface GigabitEthernet1/3 "", is up, line protocol is up
24     MAC address 500f.8000.bbb5, MTU 1500
25 Interface GigabitEthernet1/4 "", is up, line protocol is up
26     MAC address 500f.8000.bbb6, MTU 1500
27 Interface GigabitEthernet1/5 "", is up, line protocol is up
28     MAC address 500f.8000.bbb7, MTU 1500
29 Interface GigabitEthernet1/6 "", is up, line protocol is up
30     MAC address 500f.8000.bbb8, MTU 1500
31 Interface GigabitEthernet1/7 "", is up, line protocol is up
32     MAC address 500f.8000.bbb9, MTU 1500
33 Interface GigabitEthernet1/8 "", is up, line protocol is up
34     MAC address 500f.8000.bbba, MTU 1500
35 Interface Management1/1 "", is up, line protocol is up
36     MAC address 500f.8000.bbb2, MTU 1500
37 Interface Redundant1 "Redundant1", is up, line protocol is up
38     MAC address 500f.8000.bbb7, MTU 1500
39     Member GigabitEthernet1/5(Active), GigabitEthernet1/4

```

Refer to the exhibit. An engineer must configure a connection on a Cisco ASA Firewall with a Cisco Secure Firewall Services Module to ensure that the secondary interface takes over all the functions of the primary interface if the primary interface fails. Drag and drop the code snippets from the bottom onto the boxes in the CLI commands to configure the failover. Not all options are used.

```

1 ASA(config)#interface 
2 ASA(config-if)# 
3 ASA(config-if)# 
4 ASA(config-if)# nameif Redundant1
5 ASA(config-if)# security-level 20
6 ASA(config-if)# ip address 172.16.47.1
7 ASA(config-if)# end
8
9 ASA# show version | include Gigabit.*address is
10 1: Ext: GigabitEthernet1/1 : address is 500f.8000.bbb3, irq 255
11 2: Ext: GigabitEthernet1/2 : address is 500f.8000.bbb4, irq 255
12 3: Ext: GigabitEthernet1/3 : address is 500f.8000.bbb5, irq 255
13 4: Ext: GigabitEthernet1/4 : address is 500f.8000.bbb6, irq 255
14 5: Ext: GigabitEthernet1/5 : address is 500f.8000.bbb7, irq 255
15 6: Ext: GigabitEthernet1/6 : address is 500f.8000.bbb8, irq 255
16 7: Ext: GigabitEthernet1/7 : address is 500f.8000.bbb9, irq 255
17 8: Ext: GigabitEthernet1/8 : address is 500f.8000.bbba, irq 255

```

member-interface GigabitEthernet1/5

member-interface GigabitEthernet1/4

GigabitEthernet1/5

backup interface GigabitEthernet1/4

Redundant1

reactivation mode timed

failover link Redundant1 GigabitEthernet1/4

Answer:

```

1 ASA(config)#interface Redundant1
2 ASA(config-if)# GigabitEthernet1/5
3 ASA(config-if)# member-interface GigabitEthernet1/4
4 ASA(config-if)# nameif Redundant1
5 ASA(config-if)# security-level 20
6 ASA(config-if)# ip address 172.16.47.1
7 ASA(config-if)# end
8
9 ASA# show version | include Gigabit.*address is
10 1: Ext: GigabitEthernet1/1 : address is 500f.8000.bbb3, irq 255
11 2: Ext: GigabitEthernet1/2 : address is 500f.8000.bbb4, irq 255
12 3: Ext: GigabitEthernet1/3 : address is 500f.8000.bbb5, irq 255
13 4: Ext: GigabitEthernet1/4 : address is 500f.8000.bbb6, irq 255
14 5: Ext: GigabitEthernet1/5 : address is 500f.8000.bbb7, irq 255
15 6: Ext: GigabitEthernet1/6 : address is 500f.8000.bbb8, irq 255
16 7: Ext: GigabitEthernet1/7 : address is 500f.8000.bbb9, irq 255
17 8: Ext: GigabitEthernet1/8 : address is 500f.8000.bbba, irq 255

```

member-interface GigabitEthernet1/5

member-interface GigabitEthernet1/4

GigabitEthernet1/5

backup interface GigabitEthernet1/4

Redundant1

reactivation mode timed

failover link Redundant1 GigabitEthernet1/4

Explanation:

A screenshot of a computer AI-generated content may be incorrect.

```

1 ASA(config)#interface Redundant1
2 ASA(config-if)# GigabitEthernet1/5
3 ASA(config-if)# member-interface GigabitEthernet1/4
4 ASA(config-if)# nameif Redundant1
5 ASA(config-if)# security-level 20
6 ASA(config-if)# ip address 172.16.47.1
7 ASA(config-if)# end
8
9 ASA# show version | include Gigabit.*address is
10 1: Ext: GigabitEthernet1/1 : address is 500f.8000.bbb3, irq 25
11 2: Ext: GigabitEthernet1/2 : address is 500f.8000.bbb4, irq 25
12 3: Ext: GigabitEthernet1/3 : address is 500f.8000.bbb5, irq 25
13 4: Ext: GigabitEthernet1/4 : address is 500f.8000.bbb6, irq 25
14 5: Ext: GigabitEthernet1/5 : address is 500f.8000.bbb7, irq 25
15 6: Ext: GigabitEthernet1/6 : address is 500f.8000.bbb8, irq 25
16 7: Ext: GigabitEthernet1/7 : address is 500f.8000.bbb9, irq 25
17 8: Ext: GigabitEthernet1/8 : address is 500f.8000.bbba, irq 25

```

NEW QUESTION: 94

An engineer is investigating connectivity problems on Cisco Firepower for a specific SGT. Which command allows the engineer to capture real packets that pass through the firewall using an SGT of 64?

- A. capture CAP type inline-tag 64 match ip any any
- B. capture CAP buffer 64 match ip any any
- C. capture CAP match 64 type inline-tag ip any any
- D. capture CAP headers-only type inline-tag 64 match ip any any

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 95

A network engineer wants to disable the HTTP response page and interactive blocking of the entire access control policy in Cisco Secure Firewall Management Center. What must be selected in Block Response Page and Interactive Block Response Page?

- A. View
- B. System
- C. None
- D. Custom

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 96

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

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 97

A network engineer is deploying a Cisco Firepower 4100 appliance and must configure a multi-instance environment for high availability. Drag and drop the actions from the left into sequence on the right for this configuration.

The screenshot shows a configuration interface with two columns. The left column contains five actions: 'Add a MAC pool prefix and view the MAC addresses for the container instance interfaces', 'Configure interfaces', 'Add a high-availability pair', 'Add a resource profile for container instances', and 'Add a Standalone Firepower Threat Defense for Cisco Secure Firewall Management Center'. The right column contains five numbered slots: 1, 2, 3, 4, and 5. A large 'CISCO' watermark is visible across the center of the interface.

Answer:

The screenshot shows the same configuration interface as above, but with the actions rearranged to show the correct sequence for high availability. The sequence is: 'Add a resource profile for container instances', 'Add a MAC pool prefix and view the MAC addresses for the container instance interfaces', 'Configure interfaces', 'Add a Standalone Firepower Threat Defense for Cisco Secure Firewall Management Center', and 'Add a high-availability pair'. A large 'CISCO' watermark is visible across the center of the interface.

Explanation:

The correct sequence of actions for configuring a multi-instance environment for high availability on a Cisco Firepower 4100 appliance is as follows:

Add a resource profile for container instances. A resource profile defines the CPU, RAM, and disk space allocation for each container instance. You can create multiple resource profiles with different resource settings and assign them to different container instances¹.

Add a MAC pool prefix and view the MAC address for the container instance interfaces. A MAC pool prefix is a 24-bit prefix that is used to generate MAC addresses for the container instance interfaces. You can specify a custom MAC pool prefix or use the default one. You can also view the MAC addresses that are assigned to each container instance interface¹.

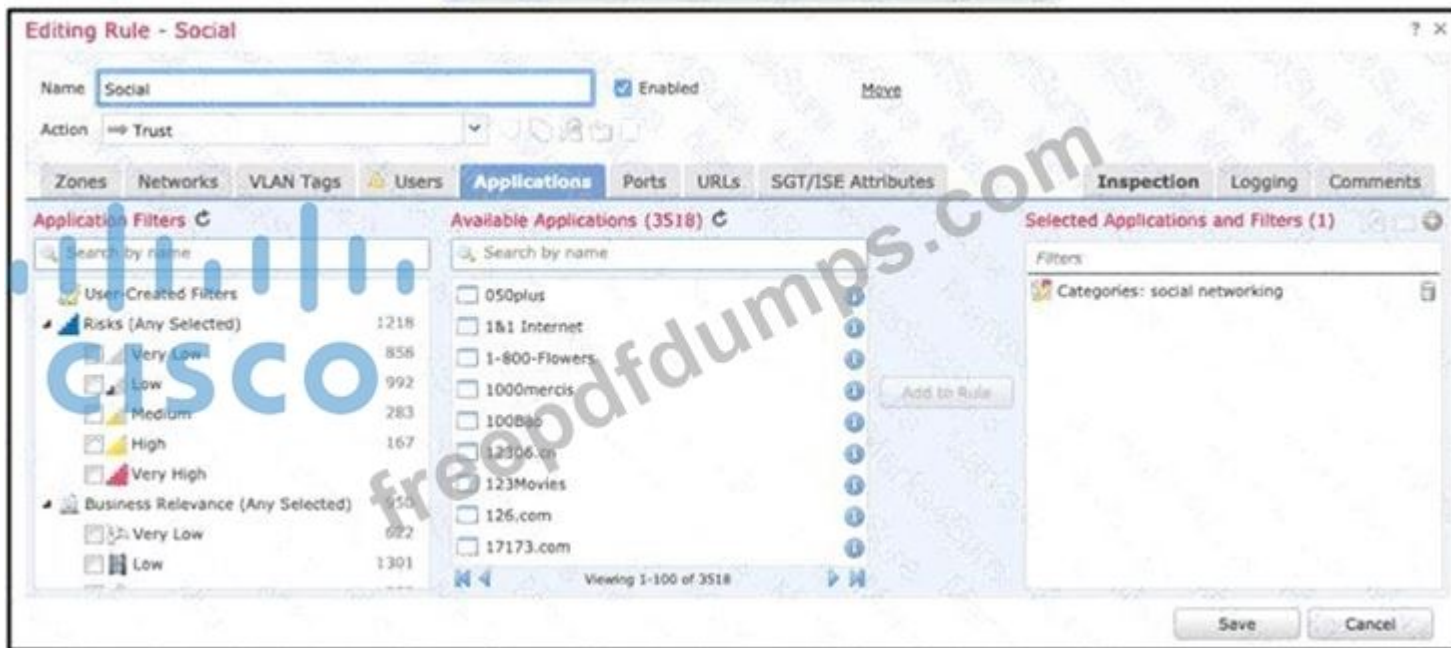
Configure interfaces. You need to configure the physical interfaces, EtherChannels, and VLAN subinterfaces that will be used by the container instances. You can also configure shared interfaces that can be used by multiple container instances on the same security module/engine¹.

Add a Standalone Firepower Threat Defense for Cisco Secure Firewall Management Center. You need to add a logical device that runs a standalone Firepower ThreatDefense (FTD) application instance and register it with the Cisco Secure Firewall Management Center (FMC). This logical device will act as the management interface for the container instances1.

Add a high-availability pair. You need to add another logical device that runs a standalone FTD application instance and register it with the FMC as well. Then, you need to configure high availability (HA) between the two standalone FTD logical devices. This will enable HA for the container instances that are associated with them1.

NEW QUESTION: 98

Refer to the exhibit.



An organization has an access control rule with the intention of sending all social media traffic for inspection. After using the rule for some time, the administrator notices that the traffic is not being inspected, but is being automatically allowed. What must be done to address this issue?

- A. Modify the selected application within the rule
- B. Add the social network URLs to the block list
- C. Change the intrusion policy to connectivity over security.
- D. Modify the rule action from trust to allow

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 99

A network engineer is extending a user segment through an FTD device for traffic inspection without creating another IP subnet. How is this accomplished on an FTD device in routed mode?

- A. by leveraging the ARP to direct traffic through the firewall
- B. by assigning an inline set interface
- C. by using a BVI and create a BVI IP address in the same subnet as the user segment
- D. by bypassing protocol inspection by leveraging pre-filter rules

Answer: (SHOW ANSWER)

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

NEW QUESTION: 100

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: (SHOW ANSWER)

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

NEW QUESTION: 101

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

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

Answer: C (LEAVE A REPLY)

NEW QUESTION: 102

An administrator configures a Cisco Secure Firewall Threat Defense device in transparent mode. To configure the BVI (Bridge Virtual Interface), the administrator must:

Add a bridge-group interface

Configure a bridge-group ID

Configure the bridge-group interface description

Add bridge-group member interfaces

How must the engineer perform these actions?

- A. Set a security zone for the bridge-group interface
- B. Configure an IP address for the bridge-group interface
- C. Set the bridge-group interface mode to transparent
- D. Configure a name for the bridge-group interface

Answer: B (LEAVE A REPLY)

NEW QUESTION: 103

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: B,E (LEAVE A REPLY)

<https://www.cisco.com/c/en/us/support/docs/security/firepower-management-center/212699-configure-ftd-high-availability-on-firep.html> Conditions In order to create an HA between 2 FTD devices, these conditions must be met:

Same model

Same version (this applies to FXOS and to FTD - (major (first number), minor (second number), and maintenance (third number) must be equal)) Same number of interfaces Same type of interfaces Both devices as part of same group/domain in FMC Have identical Network Time Protocol (NTP) configuration Be fully deployed on the FMC without uncommitted changes Be in the same firewall mode: routed or transparent.

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

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

NEW QUESTION: 104

An administrator is configuring the interface of a Cisco Secure Firewall Threat Defense device in a passive IPS deployment. The device and interface have been identified. Which set of configuration steps of the administrator take next to complete the implementation?

A. Set the interface mode to passive. Associate the interface with a security zone. Set the MTU parameter.

Reset the interface.

B. Modify the interface to retransmit received traffic. Associate the interface with a security zone Enable the interface. Set the MTU parameter.

C. Modify the interface to retransmit received traffic. Associate the interface with a security zone. Set the MTU parameter.

D. Set the interface mode to passive. Associate the interface with a security zone. Enable the interface. Set the MTU parameter.

Answer: D (LEAVE A REPLY)

In a passive IPS deployment for a Cisco Secure Firewall Threat Defense (FTD) device, the administrator must configure the interface to operate in passive mode. This involves setting the interface mode, associating it with a security zone, enabling the interface, and setting the MTU parameter.

Steps:

- * Set the interface mode to passive:
- * In FMC, navigate to Devices > Device Management.
- * Select the FTD device and configure the relevant interface.
- * Set the interface mode to "Passive."
- * Associate the interface with a security zone:
- * Create or select an appropriate security zone.
- * Assign the passive interface to this security zone.
- * Enable the interface:
- * Ensure the interface is enabled to receive traffic.
- * Set the MTU parameter:
- * Configure the Maximum Transmission Unit (MTU) parameter as required.

This ensures that the FTD device can inspect traffic passively without impacting the network flow.

References: Cisco Secure Firewall Management Center Device Configuration Guide, Chapter on Interface Settings

NEW QUESTION: 105

An administrator is attempting to remotely log into a switch in the data centre using SSH and is unable to connect. How does the administrator confirm that traffic is reaching the firewall?

A. by performing a packet capture on the firewall.

- B. by running a packet tracer on the firewall.
- C. by running Wireshark on the administrator's PC
- D. by attempting to access it from a different workstation.

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 106

Refer to the exhibit.

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. Configure a custom Snort signature to allow ICMP traffic after Inspection.
- B. Create an access control policy rule that allows ICMP traffic.
- C. Create an ICMP allow list and add the ICMP destination to remove it from the implicit deny list.
- D. Modify the Snort rules to allow ICMP traffic.

Answer: B ([LEAVE A REPLY](#))

Valid 300-710 Dumps shared by Actual4test.com for Helping Passing 300-710 Exam! Actual4test.com now offer the **newest 300-710 exam dumps**, the Actual4test.com 300-710 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com 300-710 dumps with Test Engine here: https://www.actual4test.com/300-710_examcollection.html (446 Q&As Dumps, **30%OFF** Special Discount: **Freepdfdumps**)

NEW QUESTION: 107

A security engineer must add a new policy to block UDP traffic to one server. The engineer adds a new object. Which action must the engineer take next to identify all the UDP ports?

- A. Specify the transport protocol and leave the port number empty.
- B. Add the corresponding IP protocol number for UDP and TCP.
- C. Add the transport number and specify the type and code.
- D. Define the transport protocol and the mandatory port range.

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 108

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

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 109

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

Answer: (SHOW ANSWER)

NEW QUESTION: 110

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. Inspect Local Traffic Bypass
- C. Cisco ISE Security Group Tag
- D. Automatic Application Bypass

Answer: D (LEAVE A REPLY)

NEW QUESTION: 111

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 (LEAVE A REPLY)

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

NEW QUESTION: 112

Which type of certificate must be exported from Cisco ISE to integrate Cisco Secure Firewall Management Center with pxGrid?

- A. A self-signed SAML certificate from the domain controller
- B. The certificate authority certificate of the pxGrid server node
- C. A self-signed certificate authority certificate signed by a third party
- D. The public-key certificate of the domain

Answer: (SHOW ANSWER)

Secure Firewall Management Center must trust the certificate presented by the Cisco ISE pxGrid server.

Therefore, the certificate authority certificate that signed the pxGrid node's server certificate must be exported from ISE and imported into Management Center as a trusted CA object. If primary and secondary pxGrid nodes are deployed, Cisco requires their certificates to be signed by the same trusted certificate authority.

Depending on the integration design, the engineer might also need the monitoring-node CA certificate and a pxGrid client certificate with its private key for Management Center. However, the question specifically asks which certificate establishes trust with the pxGrid server node. SAML and domain-controller

certificates are unrelated, and a certificate cannot simultaneously be self-signed and signed by a third-party CA. Cisco ISE and Secure Firewall certificate integration

NEW QUESTION: 113

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

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

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 114

An engineer must change the mode of a Cisco Secure Firewall Threat Defense (FTD) firewall in the Cisco Secure Firewall Management Center (FMC) inventory. The engineer must take these actions:

- * Register Secure FTD with Secure FMC.
- * Change the firewall mode.
- * Deregister the Secure FTD device from Secure FMC.

How must the engineer take FTD take the actions?

- A. Reload the Secure FTD device.
- B. Configure the management IP address.
- C. Access the Secure FTD CLI from the console port.
- D. Erase the Secure FTD configuration

Answer: C ([LEAVE A REPLY](#))

To change the mode of a Cisco Secure Firewall Threat Defense (FTD) device in the Cisco Secure Firewall Management Center (FMC) inventory, the engineer must follow these steps:

- * Register the Secure FTD with Secure FMC.
- * Change the firewall mode.
- * Deregister the Secure FTD device from Secure FMC.

To perform these actions, accessing the Secure FTD CLI from the console port is necessary. This allows the engineer to execute the required commands to change the firewall mode and manage the registration status of the FTD device.

Steps:

- * Connect to the Secure FTD device via the console port.
- * Access the CLI and execute the command to change the firewall mode (configure firewall-mode).
- * Deregister the device from FMC if needed.
- * Register or re-register the device with FMC as required.

References: Cisco Secure Firewall Threat Defense Configuration Guide, Chapter on Device Management and CLI Access.

NEW QUESTION: 115

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

- A. VPN connections can be re-established only if the failed master unit recovers.
- B. Smart License is required to maintain VPN connections simultaneously across all cluster units.

- C. VPN connections must be re-established when a new master unit is elected.
- D. Only established VPN connections are maintained when a new master unit is elected.

Answer: C (LEAVE A REPLY)

Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/fxos/clustering/ftd-cluster-solution.html#concept_g32_yml_y2b

NEW QUESTION: 116

Which protocol establishes network redundancy in a switched Firepower device deployment?

- A. STP
- B. HSRP
- C. GLBP
- D. VRRP

Answer: A (LEAVE A REPLY)

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

NEW QUESTION: 117

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)

The screenshot shows the 'Add Capture' configuration window in Cisco FTD. The settings are as follows:

- Name: Server1_Capture
- Interface: Inside
- Match Criteria:
 - Protocol: IP
 - Source Host: 10.0.1.100
 - Destination Host: 10.20.10.20
 - Source Network: (empty)
 - Destination Network: (empty)
 - SGT number: (0-65533)
- Buffer:
 - Packet Size: 1518 (range 14-1522 bytes)
 - Buffer Size: 524288 (range 1534-33554432 bytes)
 - Continuous Capture (selected)
 - Stop when full (unselected)
 - Trace Count: 50

Buttons: Save, Cancel

B)

C)

Add Capture ? x

Name*: Server1_Capture Interface*: diagnostic

Match Criteria:

Protocol*: IP

Source Host*: 10.20.10.20 Source Network: 10.20.10.0/24

Destination Host*: 10.0.1.100 Destination Network: 10.0.1.0/24

☐ SGT number: (0-65533)

Buffer:

Packet Size: 1518 14-1522 bytes

Buffer Size: 524288 1534-33554432 bytes

☒ Continuous Capture ☒ Trace

☐ Stop when full Trace Count: 50

CISCO Save Cancel

D)

A. Option C

B. Option B

C. Option A

D. Option D

Answer: B (LEAVE A REPLY)

NEW QUESTION: 118

An engineer is configuring a Cisco Secure Firewall Management Center appliance. The company requires the use of a TAXII server in Threat Intelligence Director and requires the Action to be set to Block. On which two object types can the engineer configure the Block action? (Choose two.)

A. Observable

B. Element

C. Indicator

D. Complex indicator

E. Source

Answer: A,C (LEAVE A REPLY)

Threat Intelligence Director cannot apply Block directly to a TAXII source because STIX data obtained through TAXII can contain complex indicators. A managed device takes enforcement action based on individual observables, such as an IP address, URL, domain, or file hash. After the TAXII content has been ingested, an administrator can configure Block on an individual observable or on a simple indicator containing one actionable observable. Complex indicators combine multiple observables and therefore cannot be blocked directly; the administrator must instead block the appropriate individual observables within them.

An element is the managed device that receives published intelligence, not an intelligence object on which this action is configured. Consequently, the two supported object types are an observable and a simple indicator. Cisco Threat Intelligence Director documentation

NEW QUESTION: 119

An organization is setting up two new Cisco FTD devices to replace their current firewalls and cannot have any network downtime During the setup process, the synchronization between the two devices is failing What action is needed to resolve this issue?

- A. Confirm that both devices have the same flash memory sizes
- B. Confirm that both devices have the same port-channel numbering
- C. Confirm that both devices are running the same software version
- D. Confirm that both devices are configured with the same types of interfaces

Answer: (SHOW ANSWER)

NEW QUESTION: 120

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

Answer: B (LEAVE A REPLY)

NEW QUESTION: 121

An engineer must implement static route tracking on a Cisco Secure Firewall Threat Defense appliance. Static route and IP SLA operation has already been configured. Static route must be removed from the routing table if the tracked object is unreachable. Which action must the engineer take next to meet the requirement?

- A. Assign a tracking object to the static route and the IP SLA operation.
- B. Enable the IP SLA Responder on the backup path interface.
- C. Enable an ICMP redirect message on the interface connected to the backup path.
- D. Implement a secondary route that has a higher precedence.

Answer: A (LEAVE A REPLY)

Valid 300-710 Dumps shared by Actual4test.com for Helping Passing 300-710 Exam! Actual4test.com now offer the **newest 300-710 exam dumps**, the Actual4test.com 300-710 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com 300-710 dumps with Test Engine here: https://www.actual4test.com/300-710_examcollection.html (446 Q&As Dumps, **30%OFF** Special Discount: **Freepdfdumps**)

NEW QUESTION: 122

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 (LEAVE A REPLY)

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: 123

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

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 124

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

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 125

What is the result when two users modify a VPN policy at the same time on a Cisco Secure Firewall Management Center managed device?

- A. Both users can edit the policy and the last saved configuration persists.
- B. The first user locks the configuration when selecting edit on the policy.
- C. The changes from both users will be merged together into the policy.
- D. The system prevents modifications to the policy by multiple users.

Answer: B ([LEAVE A REPLY](#))

In Cisco Secure Firewall Management Center (FMC), when two users attempt to modify a VPN policy simultaneously, the system implements a locking mechanism to prevent conflicts. The first user who selects edit on the policy locks the configuration, preventing other users from making changes until the lock is released.

Steps:

- * When the first user selects edit on the VPN policy, FMC locks the policy for editing.
- * The lock ensures that only the first user can make changes.
- * Once the first user saves or cancels their changes, the lock is released.
- * Other users can then edit the policy.

This locking mechanism ensures that configuration conflicts are avoided and only one set of changes is applied at a time.

References: Cisco Secure Firewall Management Center Configuration Guide, Chapter on Policy Management and User Permissions.

NEW QUESTION: 126

An engineer is configuring two new Cisco Secure Firewall Threat Defense appliances as a high-availability pair. The high-availability pair must detect a failure on the failover link and trigger failover more quickly.

Which two settings must the engineer decrease? (Choose two.)

- A. Interface poll time
- B. Peer hold time
- C. Interface failure limit
- D. Peer poll time
- E. Interface hold time

Answer: [\(SHOW ANSWER\)](#)

Peer poll time controls how frequently one high-availability unit sends hello or polling messages to determine whether its peer remains responsive. Peer hold time specifies how long the appliance waits without receiving the expected peer communication before declaring that peer unavailable. Decreasing both values causes the appliances to test peer availability more frequently and wait less time before initiating failover. Interface- oriented timers are used to evaluate monitored data-interface failures and do not specifically accelerate detection of a failed failover link. Although shorter peer timers improve failover speed, excessively aggressive values can cause false failovers during congestion or high CPU utilization. Cisco explains that threat defense appliances monitor peer health through hello messages on the failover link and begin additional testing after consecutive messages are missed. Cisco Secure Firewall high-availability monitoring

NEW QUESTION: 127

An engineer has been tasked with performing an audit of network projects to determine which objects are duplicated across the various firewall models (Cisco Secure Firewall Threat Defense Cisco Secure firewall ASA, and Meraki MX Series) deployed throughout the company Which tool will assist the engineer in performing that audit?

- A. Cisco Firepower Device Manager
- B. Cisco SecureX
- C. Cisco Defense Orchestrator
- D. Cisco Secure Firewall Management Center

Answer: [C \(LEAVE A REPLY\)](#)

Cisco Defense Orchestrator (CDO) is the tool that assists engineers in performing an audit of network projects to determine which objects are duplicated across various firewall models, including Cisco Secure Firewall Threat Defense, Cisco Secure Firewall ASA, and Meraki MX Series. CDO provides a unified management interface for managing multiple security devices and can identify duplicate objects across these devices.

Steps:

- * Access Cisco Defense Orchestrator.
- * Connect and synchronize all relevant firewall devices (FTD, ASA, Meraki MX).
- * Use the audit and reporting features in CDO to identify and manage duplicate objects.

This helps ensure consistency and efficient management across the organization's firewall deployments.

References: Cisco Defense Orchestrator Documentation, Chapter on Device Management and Object Auditing.

NEW QUESTION: 128

A security engineer manages a firewall console and an endpoint console and finds it challenging and the consuming to review events and modify blocking of specific files in both consoles. Which action must the engineer take to streamline this process?

- A. From the Secure FMC. create a Cisco Secure Endpoint object and reference the object in the Cisco Secure Endpoint console.
- B. From the Cisco Secure Endpoint console, Create and copy an API key and paste into the Cisco Secure AMP tab

C. initiate the integration between Secure FMC and Cisco Secure Endpoint from the Secure FMC using the AMP tab

D. Within the Cisco Secure Endpoint console, copy the connector GUID and paste into the Cisco Secure Firewall Management Center (FMC) AMP tab.

Answer: C ([LEAVE A REPLY](#))

To streamline the process of reviewing events and modifying blocking of specific files across both the firewall console and the endpoint console, the security engineer should initiate the integration between Secure FMC and Cisco Secure Endpoint (formerly AMP for Endpoints) from the Secure FMC using the AMP tab.

Steps:

* In the FMC, navigate to Devices > Device Management.

* Select the device and go to the AMP tab.

* Initiate the integration by configuring the necessary API credentials and linking the FMC to the Cisco Secure Endpoint console.

* This integration allows the security engineer to view endpoint events and apply blocking actions directly from the FMC, consolidating the management tasks.

This approach simplifies the workflow by providing a single interface to manage both network and endpoint security, reducing the time and effort required to maintain security across the organization.

References: Cisco Secure Firewall Management Center and Cisco Secure Endpoint Integration Guide.

NEW QUESTION: 129

A network administrator is trying to configure an access rule to allow access to a specific banking site over HTTPS. Which method must the administrator use to meet the requirement?

A. Enable SSL decryption and specify the URL.

B. Define the URL to be blocked and set the application to HTTP.

C. Define the URL to be blocked and disable SSL inspection.

D. Block the category of banking and define the application of WWW.

Answer: ([SHOW ANSWER](#)**)**

To allow access to a specific banking site over HTTPS, the network administrator must use SSL decryption (also known as SSL/TLS inspection) and specify the URL. This is because HTTPS traffic is encrypted, and the firewall needs to decrypt the traffic to inspect the URL and enforce the access rule.

Steps:

* Enable SSL Decryption: Configure SSL policies to decrypt the HTTPS traffic.

* Specify the URL: Define the URL of the banking site in the access control policy, ensuring that the decrypted traffic is inspected and allowed based on the specified URL.

This method ensures that only the desired banking site is accessed over HTTPS, while other HTTPS traffic can be filtered or blocked according to the organization's security policies.

References: Cisco Secure Firewall Management Center Configuration Guide, Chapter on SSL Decryption.

NEW QUESTION: 130

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: A,B ([LEAVE A REPLY](#))

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: 131

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. Restore the primary Cisco FMC backup configuration to the secondary Cisco FMC device when the primary device fails
- D. Place the active Cisco FMC device on the same trusted management network as the standby device

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 132

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

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

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 133

What is an attribute of the risk reporting capability in Cisco Secure Firewall Management Center?

- A. Uses the XML format to export all reporting
- B. Includes the current domain in a multidomain system
- C. Uses the same templates available to standard reports
- D. Includes all domains in a multidomain system

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 134

Which feature is supported by IRB on Cisco FTD devices?

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

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 135

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 ([LEAVE A REPLY](#))

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: 136

A network administrator is configuring a Cisco Secure Firewall Threat Defense device managed by Cisco Secure Firewall Management Center to exchange routing information with an upstream BGP router. The administrator must verify which networks the device is advertising to the upstream router. Which action must the administrator take?

A. Run the show bgp neighbors NEIGHBOR-IP advertised-routes command from Advanced Troubleshooting.

B. Select Route Inject under the Device Routing configuration of the Secure Firewall Threat Defense device.

C. Select Route Inject under the Device Routing configuration of Secure Firewall Management Center.

D. Run the show route command from the Secure Firewall Management Center CLI.

Answer: (SHOW ANSWER)

The show bgp neighbors NEIGHBOR-IP advertised-routes command displays the prefixes that the Secure Firewall Threat Defense device is advertising to a specific BGP neighbor. It must be executed against the managed threat defense device through the Advanced Troubleshooting interface. The ordinary show route command displays routes installed in the local routing table, not the specific prefixes advertised to a neighbor.

Route injection is a configuration capability and does not provide the required verification output. Cisco's command reference confirms that the advertised-routes keyword displays all routes advertised to the specified BGP peer, including the network, next hop, metric, weight, and AS path. Therefore, option A directly verifies the routes being shared with the upstream router. Cisco Secure Firewall Threat Defense Command Reference

Valid 300-710 Dumps shared by Actual4test.com for Helping Passing 300-710 Exam! Actual4test.com now offer the **newest 300-710 exam dumps**, the Actual4test.com 300-710 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com 300-710 dumps with Test Engine here: https://www.actual4test.com/300-710_examcollection.html (446 Q&As Dumps, **30%OFF** Special Discount: **Freepdfdumps**)

NEW QUESTION: 137

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 passive.

B. Set the firewall mode to routed.

C. Set the firewall mode to transparent.

D. Set interface configuration mode to none.

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 138

What is the maximum bit size that Cisco FMC supports for HTTPS certificates?

A. 1024

B. 8192

C. 4096

D. 2048

Answer: ([SHOW ANSWER](#))

Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/610/configuration/guide/fpmc-config-guide-v61/system_configuration.html

NEW QUESTION: 139

An administrator is working on a migration from Cisco ASA to the Cisco FTD appliance and needs to test the rules without disrupting the traffic. Which policy type should be used to configure the ASA rules during this phase of the migration?

A. identity

B. Intrusion

C. Access Control

D. Prefilter

Answer: ([SHOW ANSWER](#))

Reference:

https://www.cisco.com/c/en/us/td/docs/security/firepower/migration-tool/migration-guide/ASA2FTD-with-FP-Migration-Tool/b_Migration_Guide_ASA2FTD_chapter_01011.html

NEW QUESTION: 140

An engineer must configure a SPAN to monitor traffic by using a Cisco Secure IPS device in passive mode.

The Cisco Secure IPS interface Gi0/1 is connected to Cisco Catalyst Switch interface Gi0/3. Which SPAN configuration meets the requirement?

```
Switch> enable
Switch# configure terminal
Switch(config)# monitor session 1 source interface Gi0/3
Switch(config)# monitor session 1 destination interface Gi0/3
Switch(config)# end
```

A.

```
Switch> enable
Switch# configure terminal
Switch(config)# monitor source interface Gi0/1
Switch(config)# monitor destination interface Gi0/3
Switch(config)# end
```

B.

```
Switch> enable
Switch# configure terminal
Switch(config)# monitor source interface Gi0/1
Switch(config)# monitor destination interface Gi0/1
Switch(config)# end
```

C.

```
Switch> enable
Switch# configure terminal
Switch(config)# monitor session 1 source interface Gi0/1
Switch(config)# monitor session 1 destination interface Gi0/3
Switch(config)# end
```

D.

Answer: D ([LEAVE A REPLY](#))

In a local SPAN configuration, the source is the switch interface whose traffic must be copied, while the destination is the interface connected to the passive monitoring device. Therefore, switch interface Gi0/1 must be configured as the SPAN source, and switch interface Gi0/3, which connects to the Cisco Secure IPS sensor, must be the destination. Both commands must also reference the same SPAN session number. Option D satisfies all these requirements. Options B and C omit the mandatory session number, while Option A incorrectly assigns Gi0/3 as both the source and destination. A SPAN destination cannot simultaneously be a source in the same session. The passive IPS receives the mirrored packets for inspection but does not retransmit or directly block them. Cisco SPAN configuration documentation

NEW QUESTION: 141

An engineer must deploy a Cisco FTD appliance via Cisco FMC to span a network segment to detect malware and threats. When setting the Cisco FTD interface mode, which sequence of actions meets this requirement?

- A. Set to passive, and configure an access control policy with an intrusion policy and a file policy defined
- B. Set to passive, and configure an access control policy with a prefilter policy defined
- C. Set to none, and configure an access control policy with an intrusion policy and a file policy defined
- D. Set to none, and configure an access control policy with a prefilter policy defined

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 142

A security engineer must integrate an external feed containing STIX/TAXII data with Cisco FMC. Which feature must be enabled on the Cisco FMC to support this connection?

- A. Security Intelligence Feeds
- B. Cisco Success Network
- C. Cisco Secure Endpoint Integration
- D. Threat Intelligence Director

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 143

An engineer must investigate a connectivity issue by using Cisco Secure Firewall Management Center to access the Packet Capture feature on a Cisco Secure Firewall Threat Defense device. The engineer must see a real packet going through the Secure Firewall Threat Defense device and the Snort detection actions. While reviewing the packet capture, the engineer discovers that the Snort detection actions are missing. Which action must the engineer take to resolve the issue?

- A. Enable the Continuous Capture option.
- B. Specify the packet size.
- C. Specify the buffer size.
- D. Enable the Trace option.

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 144

What is the purpose of the IRB feature in next-generation firewall?

- A. To enable transparent bridging between two Layer 2 interfaces
- B. To configure NAT in transparent mode
- C. To block routing between two Layer 3 interfaces
- D. To allow multiple physical interfaces to be part of the same VLAN

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 145

A network administrator cannot select the link to be used for failover when configuring an active/passive HA Cisco FTD pair.

Which configuration must be changed before setting up the high availability pair?

- A. An IP address in the same subnet must be added to each Cisco FTD on the interface.
- B. The interface must be configured as part of a LACP Active/Active EtherChannel.
- C. The name Failover must be configured manually on the interface on each cisco FTD.
- D. The interface name must be removed from the interface on each Cisco FTD.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 146

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

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 147

What is a method used by Cisco Rapid Threat Containment to contain the threat in the network?

- A. trustsec segmentation
- B. change of authentication
- C. share context data
- D. TACACS+

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 148

A network administrator is configuring Short inspection policies and is seeing failed deployment messages in Cisco FMC. What information should the administrator generate for Cisco TAC to help troubleshoot?

- A. A "troubleshoot" file for the Cisco FMC.
- B. A "show tech" file for the device in question.

- C. A "show tech" for the Cisco FMC.
- D. A "troubleshoot" file for the device in question.

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 149

A company is in the process of deploying intrusion protection with Cisco FTDs managed by a Cisco FMC.

Which action must be selected to enable fewer rules detect only critical conditions and avoid false positives?

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

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 150

Encrypted Visibility Engine (EVE) is enabled under which tab on an access control policy in Cisco Secure Firewall Management Centre?

- A. Network Analysis Policy
- B. Advanced
- C. Security Intelligence
- D. SSL

Answer: D ([LEAVE A REPLY](#))

The Encrypted Visibility Engine (EVE) in Cisco Secure Firewall Management Center is enabled under the SSL tab of an access control policy. EVE provides visibility into encrypted traffic, allowing the firewall to detect threats even when traffic is encrypted.

Steps to enable EVE:

- * Navigate to the access control policy in FMC.
- * Go to the SSL tab.
- * Enable Encrypted Visibility Engine (EVE) to analyze encrypted traffic.

This configuration helps in identifying and mitigating threats within encrypted traffic without the need for full decryption.

References: Cisco Secure Firewall Management Center Configuration Guide, Chapter on SSL and Encrypted Traffic Visibility.

NEW QUESTION: 151

A network administrator discovers that a user connected to a file server and downloaded a malware file. The Cisco FMC generated an alert for the malware event, however the user still remained connected. Which Cisco APM file rule action within the Cisco FMC must be set to resolve this issue?

- A. Malware Cloud Lookup
- B. Local Malware Analysis
- C. Detect Files
- D. Reset Connection

Answer: D ([LEAVE A REPLY](#))

Valid 300-710 Dumps shared by Actual4test.com for Helping Passing 300-710 Exam! Actual4test.com now offer the **newest 300-710 exam dumps**, the Actual4test.com 300-710 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com 300-710 dumps with Test Engine here: https://www.actual4test.com/300-710_examcollection.html (446 Q&As Dumps, **30%OFF** Special Discount: **Freepdfdumps**)

NEW QUESTION: 152

An engineer is deploying Cisco Secure Endpoint for the first time and on endpoint with MAC address 50:54:15:04:0:AB. The engineer must make sure that during the testing phase no files are isolated and network connections must not be blocked. Which policy type must be configured to accomplish the task?

- A. Audit
- B. Triage
- C. Protect
- D. Quarantine

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 153

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. SSL
- C. SSH
- D. MACsec

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 154

An engineer must perform a packet capture on a Cisco Secure Firewall Threat Defense device to confirm the MAC address of the host using IP address 192.168.100.100 while troubleshooting an ARP issue. What is the correct tcpdump command syntax to ensure that the MAC address appears in the packet capture output?

- A. -ne src 192.168.100.100
- B. -nm 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: A ([LEAVE A REPLY](#))

NEW QUESTION: 155

A network administrator is configuring an instance of Cisco Secure Firewall Threat Defense, which is registered to Cisco Secure Firewall Management Center, to prevent internal users from downloading executable files from the internet. What must be created and configured by the administrator to meet the requirement?

- A. access policy rule that allows users to reach the internet and assigns a file policy that blocks executable downloads to the rule
- B. file policy rule that allows users to reach the internet with a second rule applied that blocks application use of FTP
- C. access policy rule that allows users to reach the internet with a second rule that blocks application executables

D. file policy that blocks downloads of all executable files and applies the file policy to the default action in the access policy

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 156

Refer to the exhibit.



An engineer must configure a static route on the Cisco Catalyst switch to reach 192.168.10.0/24 through the 192.168.20.1 next hop. The route must use an administrative distance of 2. Which command meets the requirements?

- A. ip route 192.168.10.0 255.255.255.0 192.168.20.1 1
- B. ip route 192.168.20.0 255.255.255.0 192.168.10.1 1
- C. ip route 192.168.10.0 255.255.255.0 192.168.20.1 2
- D. ip route 192.168.20.0 255.255.255.0 192.168.10.1 2

Answer: C ([LEAVE A REPLY](#))

A static-route command follows the structure ip route destination-network subnet-mask next-hop administrative-distance. The required destination is 192.168.10.0/24, which corresponds to subnet mask 255.255.255.0. The next-hop address must be 192.168.20.1, and the routing-table exhibit confirms that the 192.168.20.0/24 network is directly connected through VLAN 10. The final value must be 2 because the question explicitly requires an administrative distance of 2. Option A uses the correct destination and next hop but sets the distance to 1. Options B and D incorrectly reverse the destination and next-hop networks. Consequently, only option C contains all four required elements and installs the route through the connected 192.168.20.0/24 network with the specified preference.

NEW QUESTION: 157

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: (SHOW ANSWER)

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

NEW QUESTION: 158

An engineer must configure email notifications on Cisco Secure Firewall Management Center. TLS encryption must be used to protect the messages from unauthorized access. The engineer adds the IP address of the mail relay host and must set the port number. Which TCP port must the engineer use?

- A. 465
- B. 25
- C. 389

D. 587

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 159

A Cisco Secure Firewall Threat Defense device is configured in inline IPS mode to inspect all traffic that passes through the interfaces in the inline set. Which setting in the inline set configuration must be connected to allow traffic to pass through uninterrupted when VDB updates are being applied?

- A. Propagate Link State
- B. Short Fall Open
- C. Strict TCP Enforcement
- D. Tap Mode

Answer: ([SHOW ANSWER](#))

In inline IPS mode, to ensure that traffic passes through uninterrupted when VDB (Vulnerability Database) updates are being applied, the "Short Fall Open" setting must be configured. This setting allows traffic to continue to flow through the firewall even if there are issues with the inspection process, such as during updates or if the inspection engine fails.

Steps:

- * In FMC, navigate to the inline set configuration.
- * Enable the "Short Fall Open" option.
- * Deploy the configuration to the FTD device.

This ensures that network traffic is not disrupted during updates or other issues with the inspection process.

References: Cisco Secure Firewall Threat Defense Configuration Guide, Chapter on Inline IPS Mode Configuration.

NEW QUESTION: 160

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

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

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 161

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

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 162

When an engineer captures traffic on a Cisco FTD to troubleshoot a connectivity problem, they receive a large amount of output data in the GUI tool. The engineer found that viewing the Captures this way is time-consuming and difficult to sort and filter. Which file type must the engineer export the data in so that it can be reviewed using a tool built for this type of analysis?

- A. NetFlow v9
- B. PCAP
- C. NetFlow v5
- D. IPFIX

Answer: B (LEAVE A REPLY)

When capturing traffic on a Cisco FTD device to troubleshoot a connectivity problem, a file type that can be exported for reviewing using a tool built for this type of analysis is PCAP. PCAP stands for Packet Capture and it is a file format used to store network packet data captured from a network interface⁸. PCAP files contain the raw data of network packets, including the headers and payloads of each packet⁸.

PCAP files are widely used in network analysis and troubleshooting tasks. They enable network administrators, analysts, and researchers to inspect and analyze network traffic for various purposes, such as diagnosing network issues, detecting malicious activity, measuring network performance, and understanding network protocols⁸. PCAP files can be read by applications that understand that format, such as Wireshark, tcpdump, CA NetMaster, or Microsoft Network Monitor⁸.

The other options are incorrect because:

- * NetFlow v9 is not a file type, but a protocol for collecting and exporting information about network flows. A network flow is a sequence of packets that share common attributes such as source and destination IP addresses, ports, and protocols⁹. NetFlow v9 records contain summary information about network flows, such as start and end times, byte counts, packet counts, and so on⁹. NetFlow v9 records do not contain the raw data of network packets.
- * NetFlow v5 is not a file type, but an earlier version of the NetFlow protocol for collecting and exporting information about network flows. NetFlow v5 records contain similar information as NetFlow v9 records, but with fewer fields and less flexibility¹⁰. NetFlow v5 records do not contain the raw data of network packets.
- * IPFIX is not a file type, but a protocol for collecting and exporting information about network flows. IPFIX stands for IP Flow Information Export and it is based on NetFlow v9, but with some extensions and improvements¹¹. IPFIX records contain similar information as NetFlow v9 records, but with more fields and more flexibility¹¹. IPFIX records do not contain the raw data of network packets.

NEW QUESTION: 163

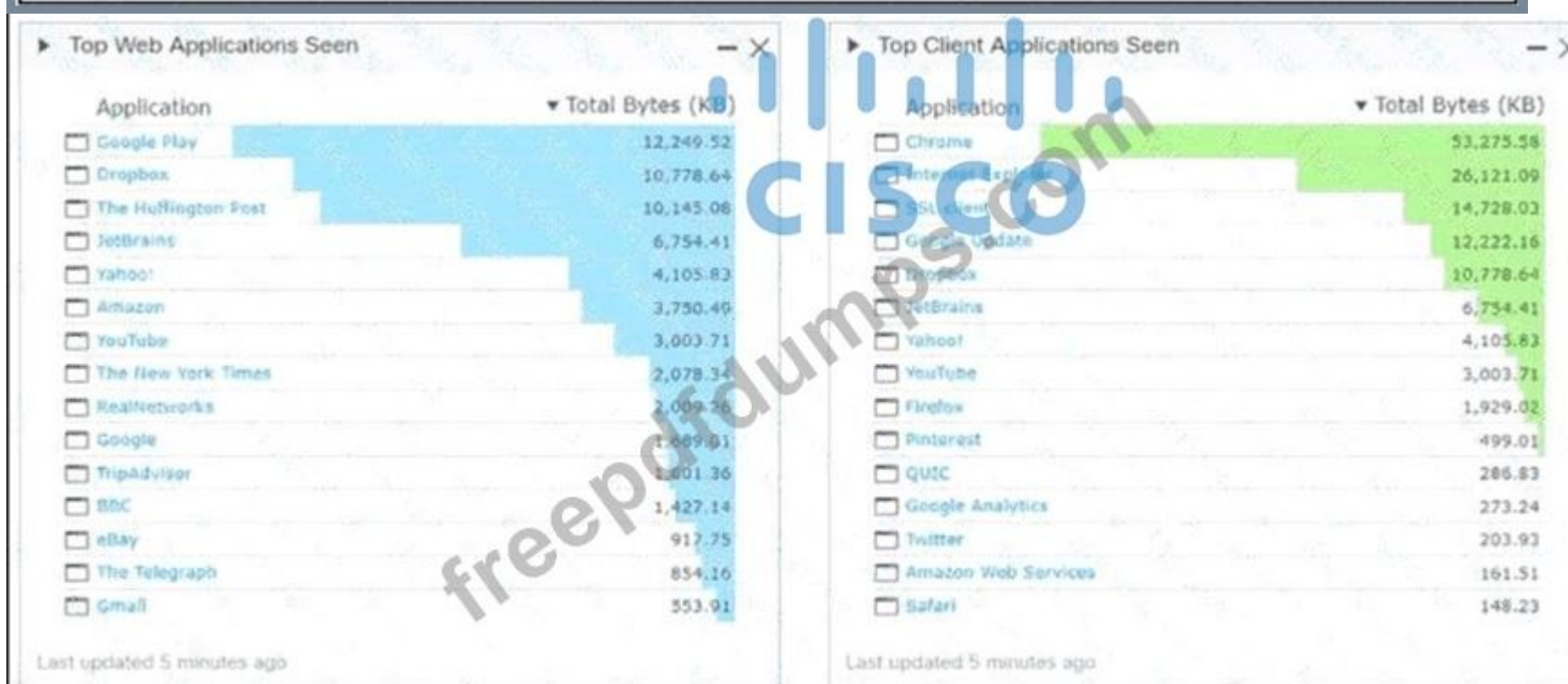
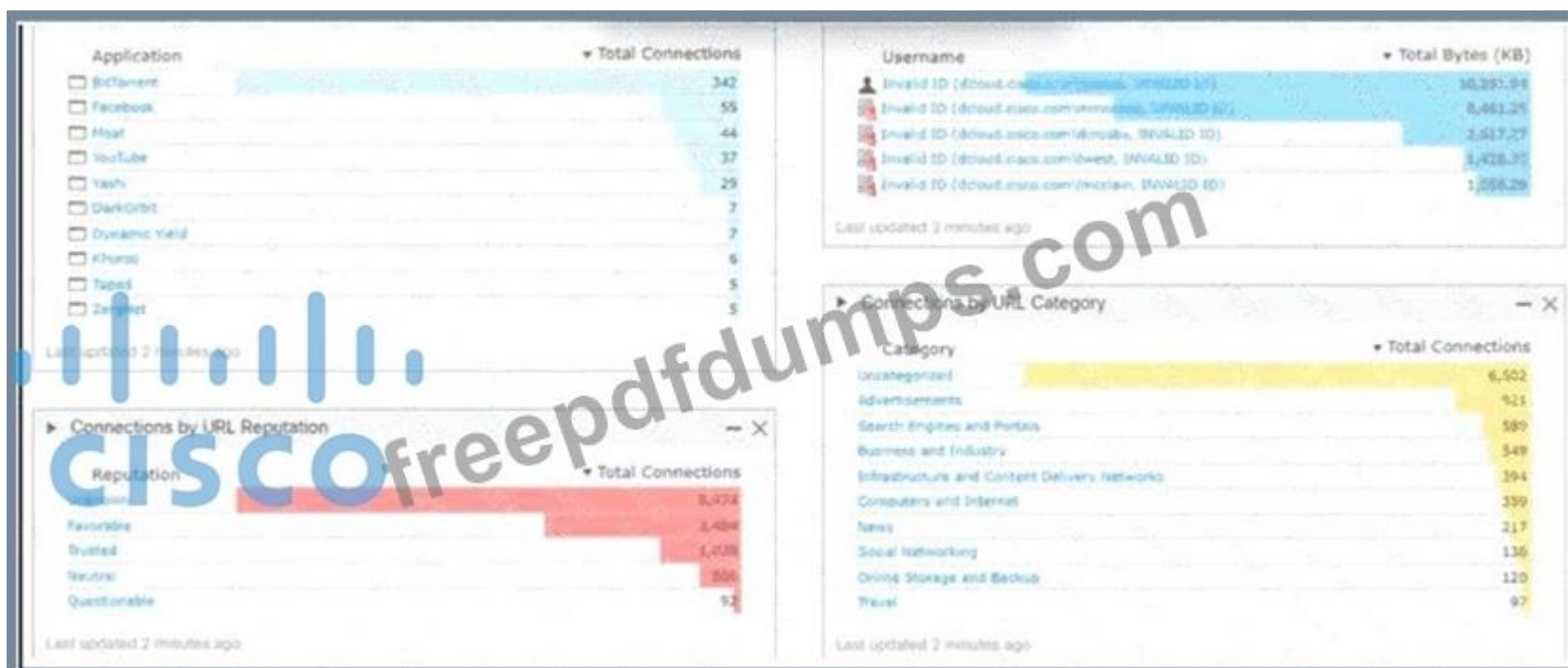
Which Cisco Firepower feature is used to reduce the number of events received in a period of time?

- A. rate-limiting
- B. suspending
- C. correlation
- D. thresholding

Answer: D (LEAVE A REPLY)

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

NEW QUESTION: 164



- C. system support ssl-client-hello-tuning
- D. system support ssl-client-hello-display

Answer: ([SHOW ANSWER](#))

Valid 300-710 Dumps shared by Actual4test.com for Helping Passing 300-710 Exam! Actual4test.com now offer the **newest 300-710 exam dumps**, the Actual4test.com 300-710 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com 300-710 dumps with Test Engine here: https://www.actual4test.com/300-710_examcollection.html (446 Q&As Dumps, **30%OFF** Special Discount: **Freepdfdumps**)

NEW QUESTION: 167

Refer to the exhibit.



What is the effect of the existing Cisco FMC configuration?

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

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 168

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: C,E ([LEAVE A REPLY](#))

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

NEW QUESTION: 169

In which two places can thresholding settings be configured? (Choose two.)

- A. on each IPS rule
- B. globally, within the network analysis policy

- C. globally, per intrusion policy
- D. on each access control rule
- E. per preprocessor, within the network analysis policy

Answer: A,C ([LEAVE A REPLY](#))

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

NEW QUESTION: 170

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 Tracer feature for traffic policy analysis
- C. Use the Packet Capture feature to collect real-time network traffic
- D. Use the Packet Analysis feature for capturing network data

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 171

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. 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.
- B. Verify the blocks using the packet capture tool and create a rule with the action monitor for the traffic.
- C. 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.
- D. Create a new access control policy rule to allow ports 80 and 443 to the FQDN of the web server.

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 172

An engineer is configuring a Cisco FTD device to place on the Finance VLAN to provide additional protection for company financial data. The device must be deployed without requiring any changes on the end user workstations, which currently use DHCP to obtain an IP address. How must the engineer deploy the device to meet this requirement?

- A. Deploy the device in routed mode and allow DHCP traffic in the access control policies.
- B. Deploy the device in routed mode and enable the DHCP Relay feature.
- C. Deploy the device in transparent mode and allow DHCP traffic in the access control policies
- D. Deploy the device in transparent mode and enable the DHCP Server feature.

Answer: C ([LEAVE A REPLY](#))

Transparent mode allows the FTD device to act as a "bump in the wire" that does not affect the IP addressing of the network. The end user workstations will not need any changes to their configuration, as they will still receive an IP address from the same DHCP server. However, the FTD device must allow DHCP traffic in the access control policies, otherwise it will block the DHCP requests and replies.

NEW QUESTION: 173

An engineer must export a packet capture from Cisco Secure Firewall Management Center to assist in troubleshooting an issue on a Secure Firewall Threat Defense device. When the engineer navigates to URL for Secure Firewall Management Center at:

..[FMC IP](#)/capture/CAP/pcap/sample.pcap

An engineer receives a 403: Forbidden error instead of being provided with the PCAP file. Which action resolves the issue?

- A.** Disable the HTTPS server and use HTTP.
- B.** Enable the proxy setting in the device platform policy.
- C.** Enable HTTPS in the device platform policy.
- D.** Disable the proxy setting on the client browser.

Answer: [\(SHOW ANSWER\)](#)

If an engineer receives a 403: Forbidden error when attempting to download a packet capture file from Cisco Secure Firewall Management Center (FMC), the issue is likely due to HTTPS not being enabled in the device platform policy. To resolve this issue, the engineer must enable HTTPS in the platform policy.

Steps:

- * In FMC, navigate to Policies > Device Management > Platform Settings.
- * Edit the relevant platform policy.
- * Enable HTTPS for the device.
- * Deploy the changes to the FTD device.

This ensures that the FMC and FTD device can securely transfer the packet capture file over HTTPS, resolving the 403 error.

References: Cisco Secure Firewall Management Center Administrator Guide, Chapter on Platform Settings and HTTPS Configuration.

NEW QUESTION: 174

An engineer is configuring URL filtering for a Cisco FTD device in Cisco FMC. Users must receive a warning when they access <http://www.Badadultsite.com> with the option of continuing to the website if they choose to. No other websites should be blocked. Which two actions must the engineer take to meet these requirements? (Choose two.)

- A.** On the HTTP Responses tab of the access control policy editor, set the Block Response Page to Custom.
- B.** On the HTTP Responses tab of the access control policy editor, set the Interactive Block Response Page to system-provided.
- C.** Configure the default action for the access control policy to Interactive Block.
- D.** Configure an access control rule that matches the Adult URL category and set the action to interactive Block.
- E.** Configure an access control rule that matches an URL object for <http://www.badadultsite.com>; and set the action to interactive Block.

Answer: **B,E** [\(LEAVE A REPLY\)](#)

To configure URL filtering for a Cisco FTD device in Cisco FMC, and to meet the requirements of the question, the engineer must do the following:

On the HTTP Responses tab of the access control policy editor, set the Interactive Block Response Page to system-provided. This will enable the system to display a warning page to the users when they try to access a blocked URL, and give them the option to continue or cancel. The system-provided page is a default page that contains a generic message and a logo.

Configure

an access control rule that matches an URL object for <http://www.badadultsite.com>; and set the action to Interactive Block. This will apply the interactive block action to the specific URL that is defined in the URL object. The interactive block action will trigger the interactive block response page that was configured in the previous step.

The other options are incorrect because:

On the HTTP Responses tab of the access control policy editor, setting the Block Response Page to Custom will not affect the interactive block action. The block response page is used when the action is set to Block, not Interactive Block.

Configuring the default action for the access control policy to Interactive Block will apply the interactive block action to all URLs that are not matched by any access control rule. This will not meet the requirement of blocking no other websites1.

Configuring

an access control rule that matches the Adult URL category and sets the action to Interactive Block will apply the interactive block action to all URLs that belong to the Adult category. This will not meet the requirement of blocking only <http://www.badadultsite.com>1.

NEW QUESTION: 175

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

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 176

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

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 177

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.** Routing between bridge groups is achieved only with a router-on-a-stick configuration on a connected router
- D.** In transparent firewall mode, routing between bridge groups is supported

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 178

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

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 179

What is the difference between inline and inline tap on Cisco Firepower?

- A. Inline tap mode does full packet capture.
- B. Inline tap mode can send a copy of the traffic to another device.
- C. Inline mode cannot do SSL decryption.
- D. Inline mode can drop malicious traffic.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 180

An organization is installing a new Cisco FTD appliance in the network. An engineer is tasked with configuring access between two network segments within the same IP subnet. Which step is needed to accomplish this task?

- A. Permit BPDU packets to prevent loops.
- B. Assign an IP address to the Bridge Virtual Interface.
- C. Specify a name for the bridge group.
- D. Add a separate bridge group for each segment.

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 181

Which two dynamic routing protocols are supported in Firepower Threat Defense without using FlexConfig?

(Choose two.)

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

Answer: ([SHOW ANSWER](#))

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

Valid 300-710 Dumps shared by Actual4test.com for Helping Passing 300-710 Exam! Actual4test.com now offer the **newest 300-710 exam dumps**, the Actual4test.com 300-710 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com 300-710 dumps with Test Engine here: https://www.actual4test.com/300-710_examcollection.html (446 Q&As Dumps, **30%OFF** Special Discount: **Freepdfdumps**)

NEW QUESTION: 182

Which component is needed to perform rapid threat containment with Cisco FMC?

- A. ISE
- B. RESTful API
- C. SIEM
- D. DDI

Answer: ([SHOW ANSWER](#))

To perform rapid threat containment with Cisco FMC, the necessary component is Cisco Identity Services Engine (ISE). ISE integrates with FMC to provide dynamic network access control and enforcement, allowing for quick isolation of compromised endpoints based on security events detected by FMC.

Steps:

- * Integrate FMC with ISE by configuring the necessary settings in both platforms.
- * Define security policies in FMC that trigger rapid threat containment actions via ISE.
- * When a threat is detected, FMC can instruct ISE to isolate the affected endpoint, limiting its access to the network.

This integration enables automated and efficient threat containment, reducing the response time and mitigating the impact of security incidents.

References: Cisco Secure Firewall Management Center Integration Guide, Chapter on ISE Integration for Rapid Threat Containment.

NEW QUESTION: 183

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: ([SHOW ANSWER](#))

Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/integrations/CTR/Firepower_and_Cisco_Threat_Response_Integration_Guide.pdf

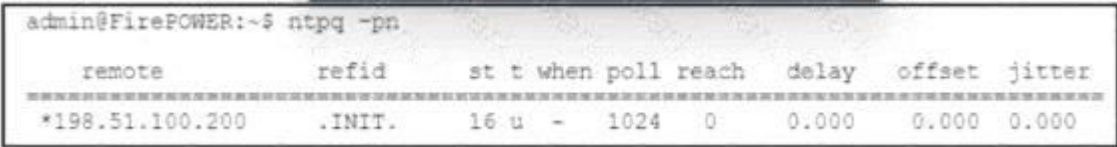
NEW QUESTION: 184

A network administrator notices that SI events are not being updated The Cisco FTD device is unable to load all of the SI event entries and traffic is not being blocked as expected. What must be done to correct this issue?

- A. Manually update the SI event entries to that the appropriate traffic is blocked
- B. Redeploy configurations to affected devices so that additional memory is allocated to the SI module
- C. Restart the affected devices in order to reset the configurations
- D. Replace the affected devices with devices that provide more memory

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 185



```
admin@FirePOWER:~$ ntpq -pn
```

remote	refid	st	t	when	poll	reach	delay	offset	jitter
*198.51.100.200	.INIT.	16	u	-	1024	0	0.000	0.000	0.000

Refer to the exhibit. A security engineer views the health alerts in Cisco Secure Firewall Management Center by using the Health Monitor in the web interface. One of the alerts shows an appliance as critical because the Time Synchronization module status is out of sync. To troubleshoot the issue, the engineer runs the ntpq command in Secure Firewall Management Center. The output is shown in the exhibit. Which action must the security engineer take next to resolve the issue?

- A. Configure the appliance to receive the time from an NTP server.
- B. Configure the appliance to sync with its own internal clock.
- C. Reestablish the connection to the timeserver.
- D. Reset the appliance with a hard reboot.

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 186

An engineer is setting up a new Cisco Secure Firewall Threat Defense appliance to replace the current firewall. The company requests that inline sets be used and that when one interface in an inline set goes down, the second interface in the inline set goes down. What must the engineer configure to meet the deployment requirements?

- A. strict TCP enforcement
- B. propagate link state
- C. inline tap mode
- D. Snort fail open

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 187

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

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 188

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 ([LEAVE A REPLY](#))

Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/630/configuration/guide/fpmc-config-guide-v63/reusable_objects.html

NEW QUESTION: 189

An organization is migrating their Cisco ASA devices running in multicontext mode to Cisco FTD devices.

Which action must be taken to ensure that each context on the Cisco ASA is logically separated in the Cisco FTD devices?

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

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 190

A security engineer is deploying a pair of primary and secondary Cisco FMC devices. The secondary must also receive updates from Cisco Talos. Which action achieves this goal?

- A. Force failover for the secondary Cisco FMC to synchronize the rule updates from the primary.
- B. Manually import rule updates onto the secondary Cisco FMC device.
- C. Configure the primary Cisco FMC so that the rules are updated.
- D. Configure the secondary Cisco FMC so that it receives updates from Cisco Talos.

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 191

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

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 192

Which Cisco Secure Firewall Threat Defense interface mode must be deployed when implementing an IPS that uses a SPAN port for traffic monitoring?

- A. Routed
- B. Passive
- C. Transparent
- D. Inline

Answer: B ([LEAVE A REPLY](#))

A passive interface is specifically designed to monitor copied network traffic received from a switch SPAN or mirror port. Because the Secure Firewall Threat Defense device is not physically placed in the traffic path, it receives a copy of the packets for inspection but does not retransmit them. This provides network and intrusion visibility without affecting production traffic. The trade-off is that a passive deployment cannot directly block, shape, or modify the monitored traffic because the original packets continue through the switch independently. An inline deployment, by comparison, places paired interfaces directly in the forwarding path and can drop malicious traffic. Routed and transparent describe firewall forwarding modes and are not the appropriate SPAN-based IPS interface type. Therefore, a SPAN-port monitoring deployment requires a passive interface. Cisco passive-interface documentation

NEW QUESTION: 193

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 ([LEAVE A REPLY](#))

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-cisco-firepow.html>

NEW QUESTION: 194

An engineer is configuring a file policy on a Cisco Secure Firewall Management Center appliance. Files with an Unknown disposition must be analyzed by Cisco Secure Malware Analytics. What must be configured on the Secure Firewall Management Center appliance?

- A.** Sandbox Analysis
- B.** Spero Analysis
- C.** Malware Analysis
- D.** Dynamic Analysis

Answer: [\(SHOW ANSWER\)](#)

Dynamic Analysis submits eligible files with an Unknown or Unavailable malware-cloud disposition to Cisco Secure Malware Analytics, formerly Cisco Threat Grid. The service executes and observes the file in a controlled environment, examines its behavior, and returns a threat score and detailed analysis report. Secure Firewall Management Center can use the returned threat score and the threshold configured in the file policy to determine whether the file should be treated as malware. Spero Analysis is different because it examines structural characteristics and generates a signature primarily for executable files. It does not provide the comprehensive sandbox-based behavioral examination described in the question. Therefore, when unknown files must be submitted to Secure Malware Analytics for deeper investigation, Dynamic Analysis is the required configuration. Cisco file-policy documentation

NEW QUESTION: 195

A network administrator is trying to configure Active Directory authentication for VPN authentication to a Cisco Secure Firewall Threat Defence instance that is registered with Cisco Secure Firewall Management Center. Which system settings must be configured first in Secure Firewall Management Center to accomplish the goal?

- A.** Device, Remote Access VPN
- B.** System, Realms
- C.** Policies, Authentication
- D.** Authentication, Device

Answer: **B** [\(LEAVE A REPLY\)](#)

To configure Active Directory authentication for VPN authentication on a Cisco Secure Firewall Threat Defense (FTD) instance registered with Cisco Secure Firewall Management Center (FMC), the administrator needs to configure Realms in the System settings of the FMC. Realms in FMC are used to define the directory servers (e.g., Active Directory) and how they are used for user authentication.

Steps to configure this in FMC:

- * Navigate to System > Integration > Realms and Directory.
- * Add a new realm and configure the necessary details such as the directory server type (e.g., Active Directory), server address, and bind credentials.
- * Test the connection to ensure it works correctly.

This setup allows the FMC to authenticate VPN users against the Active Directory, thereby enabling secure access control for VPN connections.

References: Cisco Secure Firewall Management Center Administrator Guide, Chapter on Realms Configuration.

Valid 300-710 Dumps shared by Actual4test.com for Helping Passing 300-710 Exam! Actual4test.com now offer the **newest 300-710 exam dumps**, the Actual4test.com 300-710 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com 300-710 dumps with Test Engine here: https://www.actual4test.com/300-710_examcollection.html (**446** Q&As Dumps, **30%OFF** Special Discount: **Freepdfdumps**)