Cisco.300-710.v2026-06-20.q210

Exam Code:	300-710
Exam Name:	Securing Networks with Cisco Firepower
Certification Provider:	Cisco
Free Question Number:	210
Version:	v2026-06-20
# of views:	102
# of Questions views:	2100
https://www.freecram.net/torrent/Cisco.300-710.v2026-06-20.q210.html	

NEW QUESTION: 1
Refer to the exhibit. An engineer is analyzing a Network Risk Report from Cisco FMC. Which application must the engineer take immediate action against to prevent unauthorized network use?

HIGH BANDWIDTH APPLICATIONS

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

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

ENCRYPTED APPLICATIONS

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

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

EVASIVE APPLICATIONS

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

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

A. TOR
B. Chrome
C. Kerberos
D. YouTube
Answer: (SHOW ANSWER)

NEW QUESTION: 2
Due to an Increase in malicious events, a security engineer must generate a threat report to include intrusion events, malware events, and security intelligence events. How Is this information collected in a single report?
A. Run the default Firepower report.
B. Generate a malware report.
C. Create a Custom report.
D. Export the Attacks Risk report.
Answer: (SHOW ANSWER)

NEW QUESTION: 3
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. Implement a secondary route that has a higher precedence.
B. Enable the IP SLA Responder on the backup path interface.
C. Assign a tracking object to the static route and the IP SLA operation.
D. Enable an ICMP redirect message on the interface connected to the backup path.
Answer: (SHOW ANSWER)
Linking the IP SLA operation and its tracking object to the static route causes the route to be withdrawn automatically when the SLA probe fails.

NEW QUESTION: 4
While configuring FTD, a network engineer wants to ensure that traffic passing through the appliance does not require routing or Vlan rewriting.
Which interface mode should the engineer implement to accomplish this task?
A. passive
B. transparent
C. Inline tap
D. Inline set
Answer: (SHOW ANSWER)
Passive: traffic does not flow through the IPS.
Inline Tap: it gets a copy of the packets, traffic does not flow through the IPS.
Transparent: it is Transparent inline mode, then this can be an answer as well.
Inline set: it is called bump-on-wire mode. Traffic passes through the appliance, but it does not require routing and Vlan rewriting.
https://www.cisco.com/c/en/us/td/docs/security/firepower/630/configuration/guide/fpmc-config- guide-v63/inline_sets_and_passive_interfaces_for_firepower_threat_defense.html

NEW QUESTION: 5
A network engineer is configuring URL Filtering on Firepower Threat Defense. Which two port requirements on the Firepower Management Center must be validated to allow communication with the cloud service? (Choose two.)
A. outbound port TCP/443
B. inbound port TCP/80
C. outbound port TCP/8080
D. inbound port TCP/443
E. outbound port TCP/80

Answer: (SHOW ANSWER)
https://www.cisco.com/c/en/us/support/docs/security/firesight-management-center/118852- technote-firesight-00.html
https://community.cisco.com/t5/security-documents/ftd-url-filtering-how-it-works/ta-p/3347292

NEW QUESTION: 6
A network administrator is deploying a Cisco IPS appliance and needs it to operate initially without affecting traffic flows. It must also collect data to provide a baseline of unwanted traffic before being reconfigured to drop it. Which Cisco IPS mode meets these requirements?
A. inline tap
B. failsafe
C. promiscuous
D. bypass
Answer: A (LEAVE A REPLY)

NEW QUESTION: 7
Drag and Drop Question
Refer to the exhibit. An engineer must configure a connection on a Cisco ASA 5500-X Series 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.

```
ASA# show interface | include ",|MAC|Member
Interface GigabitEthernet1/1 "inside", is up, line protocol is up
        MAC address e4aa.5ae4.612e, MTU 1500
Interface GigabitEthernet1/2 "outside", is up, line protocol is up
        MAC address e4aa.5ae4.612f, MTU 1500
Interface GigabitEthernet1/3 "", is up, line protocol is up
        MAC address 500f.8000.bbb5, MTU 1500
Interface GigabitEthernet1/4 "", is up, line protocol is up
        MAC address 500f.8000.bbb6, MTU 1500
Interface GigabitEthernet1/5 "", is up, line protocol is up
        MAC address 500f.8000.bbb7, MTU 1500
Interface GigabitEthernet1/6 "", is up, line protocol is up
        MAC address 500f.8000.bbb8, MTU 1500
Interface GigabitEthernet1/7 "", is up, line protocol is up
        MAC address 500f.8000.bbb9, MTU 1500
Interface GigabitEthernet1/8 "", is up, line protocol is up
        MAC address 500f.8000.bbba, MTU 1500
Interface Management1/1 "", is up, line protocol is up
        MAC address 500f.8000.bbb2, MTU 1500
Interface Redundant1 "Redundant1", is up, line protocol is up
        MAC address 500f.8000.bbb7, MTU 1500
        Member GigabitEthernet1/5(Active), GigabitEthernet1/4
```

```
ASA(config)#interface [                                    ]
ASA(config-if)# [                                          ]
ASA(config-if)# [                                          ]
ASA(config-if)# nameif Redundant1
ASA(config-if)# security-level 20
ASA(config-if)# ip address 172.16.47.1
ASA(config-if)# end

ASA# show version | include Gigabit.*address is
 1: Ext: GigabitEthernet1/1  : address is 500f.8000.bbb3, irq 255
 2: Ext: GigabitEthernet1/2  : address is 500f.8000.bbb4, irq 255
 3: Ext: GigabitEthernet1/3  : address is 500f.8000.bbb5, irq 255
 4: Ext: GigabitEthernet1/4  : address is 500f.8000.bbb6, irq 255
 5: Ext: GigabitEthernet1/5  : address is 500f.8000.bbb7, irq 255
 6: Ext: GigabitEthernet1/6  : address is 500f.8000.bbb8, irq 255
 7: Ext: GigabitEthernet1/7  : address is 500f.8000.bbb9, irq 255
 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:

```
ASA(config)#interface Redundant1
ASA(config-if)# member-interface GigabitEthernet1/5
ASA(config-if)# member-interface GigabitEthernet1/4
ASA(config-if)# nameif Redundant1
ASA(config-if)# security-level 20
ASA(config-if)# ip address 172.16.47.1
ASA(config-if)# end

ASA# show version | include Gigabit.*address is
  1: Ext: GigabitEthernet1/1   : address is 500f.8000.bbb3, irq 255
  2: Ext: GigabitEthernet1/2   : address is 500f.8000.bbb4, irq 255
  3: Ext: GigabitEthernet1/3   : address is 500f.8000.bbb5, irq 255
  4: Ext: GigabitEthernet1/4   : address is 500f.8000.bbb6, irq 255
  5: Ext: GigabitEthernet1/5   : address is 500f.8000.bbb7, irq 255
  6: Ext: GigabitEthernet1/6   : address is 500f.8000.bbb8, irq 255
  7: Ext: GigabitEthernet1/7   : address is 500f.8000.bbb9, irq 255
  8: Ext: GigabitEthernet1/8   : address is 500f.8000.bbba, irq 255
```

GigabitEthernet1/5

backup interface GigabitEthernet1/4

reactivation mode timed

failover link Redundant1 GigabitEthernet1/4

Explanation:
ASA(config)# interface Redundant1
ASA(config-if)# member-interface GigabitEthernet1/5
ASA(config-if)# member-interface GigabitEthernet1/4
Redundant1command creates the redundant interface that will combine the primary and secondary interfaces into a failover pair. After this, you define the member-interface for each physical interface (GigabitEthernet1/5 and GigabitEthernet1/4) under the redundant interface configuration.

NEW QUESTION: 8
Remote users who connect via Cisco AnyConnect to the corporate network behind a Cisco FTD device report that they get no audio when calling between remote users using their softphones.
These same users can call internal users on the corporate network without any issues. What is the cause of this issue?
A. The hairpinning feature is not available on FTD.
B. Split tunneling is enabled for the Remote Access VPN on FTD
C. FTD has no NAT policy that allows outside to outside communication
D. The Enable Spoke to Spoke Connectivity through Hub option is not selected on FTD.
Answer: (SHOW ANSWER)
For remote users connected via AnyConnect VPN behind a Cisco FTD device, calls between remote users require the FTD to allow traffic between VPN clients, which is considered "outside to outside" traffic since VPN clients are logically on the outside interface.

Without a proper NAT exemption or NAT policy that permits this outside-to-outside communication, the traffic between remote users will be blocked or dropped, causing issues such as no audio during calls. Cisco FTD requires explicit NAT rules to allow such communication; otherwise, the default behavior blocks this traffic.
https://www.cisco.com/c/en/us/support/docs/security/anyconnect-secure-mobility-client/216180- troubleshoot-common-anyconnect-communica.pdf

NEW QUESTION: 9
An engineer must configure high availability for the Cisco Firepower devices. The current network topology does not allow for two devices to pass traffic concurrently.
How must the devices be implemented in this environment?
A. in active/active mode
B. in active/passive mode
C. in cluster interface mode
D. in a cluster span EtherChannel
Answer: (SHOW ANSWER)

NEW QUESTION: 10
An administrator is configuring a new report template off. of a saved search within Cisco Secure Firewall Management Centre. The goal is to use the malware analysis report template, but use a different type saved search as the basis. The report is not working. What must be considered when configuring this report template?

A. Saved searches can be used for the same report template only
B. Saved searches are available freely for all report templates within the same domain.
C. Saved searches from a different report template must be used.
D. Saved searches must be renamed before using for different report template.
Answer: (SHOW ANSWER)
When configuring a new report template based on a saved search in Cisco Secure Firewall Management Center (FMC), it is important to note that saved searches are specific to the report template they were created with. Saved searches cannot be freely used across different report templates.
To use a different type of saved search, you must ensure that it aligns with the specific report template being used.
This restriction ensures that the saved search parameters match the report's data requirements.

NEW QUESTION: 11
A network administrator wants to configure a default policy to block malicious sites based on the requested URL lookup. Which feature meets the requirement?
A. file policies
B. malware policies
C. DNS policies
D. URL filtering policies
Answer: (SHOW ANSWER)
URL filtering allows control over website access based on the URL's category and reputation, which includes blocking malicious or risky sites by inspecting the requested URL.
This feature can use category and reputation-based filtering to automatically block URLs classified as malicious or high risk, fulfilling the requirement for a default blocking policy.
URL filtering works by inspecting HTTP/HTTPS traffic and matching URLs against Cisco's URL database or manually configured URL lists.
https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/management-center/device- config/720/management-center-device-config-72/access-url-filtering.html

NEW QUESTION: 12

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

A. Change the base policy to Security over Connectivity.

B. Change the rule state within the policy being used.

C. Change the dynamic state of the rule within the policy.

D. Change the rules using the Generate and Use Recommendations feature.

Answer: (SHOW ANSWER)

NEW QUESTION: 13

A network engineer must configure IPS mode on a Secure Firewall Threat Defense device to inspect traffic and act as an IDS. The engineer already configured the passive-interface on the Secure Firewall Threat Defense device and SPAN on the switch. What must be configured next by the engineer?

A. intrusion policy on the Secure Firewall Threat Defense device

B. active SPAN port on the switch

C. DHCP on the switch

D. active interface on the Secure Firewall Threat Defense device

Answer: (SHOW ANSWER)

To configure IPS mode on a Cisco Secure Firewall Threat Defense (FTD) device to inspect traffic and act as an IDS, the network engineer must configure an intrusion policy on the FTD device.

The passive-interface and SPAN on the switch have already been configured, which means the traffic is being mirrored to the FTD. The next step is to set up an intrusion policy that defines the rules and actions for detecting and responding to malicious traffic.

Steps:

In FMC, navigate to Policies > Intrusion.

Create a new intrusion policy or edit an existing one.

Define the rules and actions for detecting threats.

Apply the intrusion policy to the relevant interfaces or access control policies. This configuration enables the FTD to inspect the mirrored traffic and take appropriate actions based on the defined intrusion policy.

NEW QUESTION: 14

In which two ways do access control policies operate on a Cisco Firepower system? (Choose two.)

A. Traffic inspection can be interrupted temporarily when configuration changes are deployed.

B. The system performs intrusion inspection followed by file inspection.

C. They can block traffic based on Security Intelligence data.

D. File policies use an associated variable set to perform intrusion prevention.

E. The system performs a preliminary inspection on trusted traffic to validate that it matches the trusted parameters.

Answer: (SHOW ANSWER)

When deploying changes SNORT can restart causing traffic interuptions.

https://www.cisco.com/c/en/us/td/docs/security/firepower/623/configuration/guide/fpmc-config- guide-v623/policy_management.html#reference_F11C552688424DEF85ED145FA97283B7

NEW QUESTION: 15

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

A. redundant interfaces

B. high availability active/standby firewalls

C. multi-instance firewalls
D. span EtherChannel clustering
Answer: (SHOW ANSWER)

NEW QUESTION: 16
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?

```
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
```


A. Configure the appliance to receive the time from an NTP server.
B. Reestablish the connection to the timeserver.
C. Reset the appliance with a hard reboot.
D. Configure the appliance to sync with its own internal clock.
Answer: (SHOW ANSWER)
In the exhibit, the output of ntpq -pn shows the NTP server 198.51.100.200 with a reach value of
0 and a reference ID of .INIT., meaning no successful synchronization has occurred. The reach value of 0 indicates that the appliance cannot reach the NTP server.
Therefore, the issue is not with NTP configuration, but with network reachability to the timeserver.
The next action is to reestablish the connection to the NTP server - this may involve checking routing, firewall rules, or server availability.

NEW QUESTION: 17
An engineer is using the configure manager add <FMC IP> Cisc404225383 command to add a new Cisco FTD device to the Cisco FMC; however, the device is not being added. Why is this occurring?
A. The IP address used should be that of the Cisco FTD, not the Cisco FMC
B. The NAT ID is required since the Cisco FMC is behind a NAT device
C. DONOTRESOLVE must be added to the command
D. The registration key is missing from the command
Answer: (SHOW ANSWER)

NEW QUESTION: 18
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 son 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. IPFIX
B. NetFlow v5
C. PCAP
D. NetFlow v9
Answer: (SHOW ANSWER)

NEW QUESTION: 19
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. Set up Cisco Firepower in intrusion prevention mode
B. Configure Cisco Firepower in FXOS monitor only mode.
C. Set up Cisco Firepower as managed by Cisco FDM
D. Configure Cisco Firepower as a transparent firewall
Answer: (SHOW ANSWER)

NEW QUESTION: 20
A software development company hosts the website https://dev.company.com for contractors to share code for projects they are working on with internal developers. The web server is on premises and is protected by a Cisco Secure Firewall Threat Defense appliance. The network administrator is worried about someone trying to transmit infected files to internal users via this site. Which type of policy must be associated with an access control policy to enable Cisco Secure Firewall Malware Defense to detect and block malware?

A. SSL policy
B. file policy
C. network discovery policy
D. prefilter policy
Answer: B (LEAVE A REPLY)
To enable Cisco Secure Firewall Malware Defense to detect and block malware transmitted through a web server, you must associate a file policy with an access control policy.
A file policy is a set of configurations that the Secure Firewall uses to inspect files in network traffic for malware. By associating file policies with access control rules, the firewall inspects files before allowing them through, enabling detection and blocking of malware in transmitted files.
This is essential for controlling file-based threats coming from sources like web servers, email, or other vectors.
https://secure.cisco.com/secure-firewall/docs/malware-and-file-policy

NEW QUESTION: 21
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. Define the transport protocol and the mandatory port range.
C. Add the transport number and specify the type and code.
D. Add the corresponding IP protocol number for UDP and TCP.
Answer: (SHOW ANSWER)
When creating an access rule or object to block all UDP traffic to a server, specifying the transport protocol as UDP without defining any specific port number effectively matches all UDP ports. This means the rule will apply to all UDP traffic regardless of port number.

NEW QUESTION: 22
Which CLI command is used to register a Cisco FirePOWER sensor to Firepower Management Center?
A. configure system add <host><key>
B. configure manager <key> add host
C. configure manager delete
D. configure manager add <host><key>
Answer: (SHOW ANSWER)
http://www.cisco.com/c/en/us/support/docs/security/firesight-management-center/118596- configure-firesight-00.html

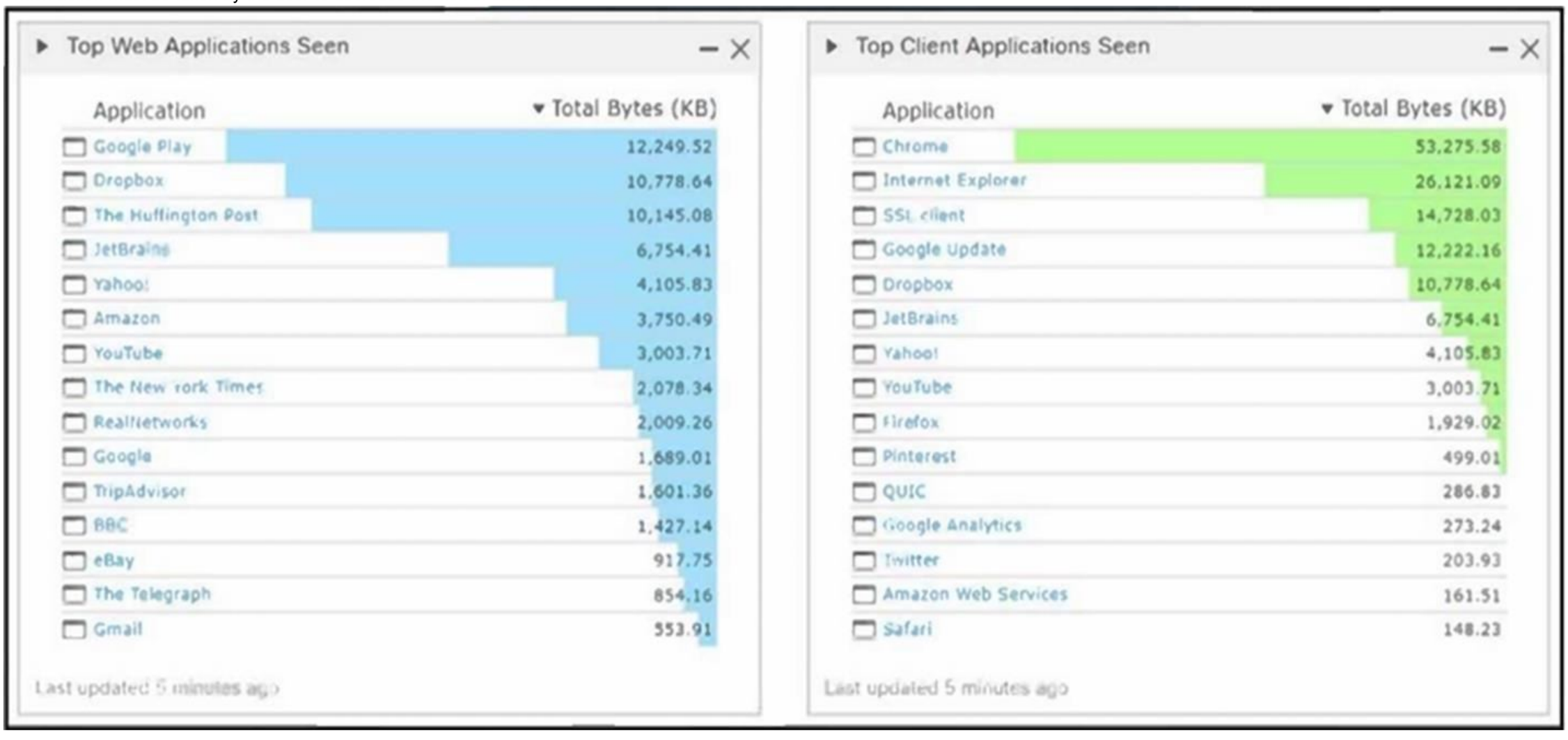
NEW QUESTION: 23
An administrator is attempting to add a Cisco Secure Firewall Threat Defence device to Cisco Secure Firewall Management Center with a password of Cisco0480846211 480846211. The private IP address of the FMC server is 192.168.75.201. Which command must be used in order to accomplish this task?
A. configure manager add 192.168.75.201/24 <reg_key>
B. configure manager add 192.168.75.201 <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: (SHOW ANSWER)
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>

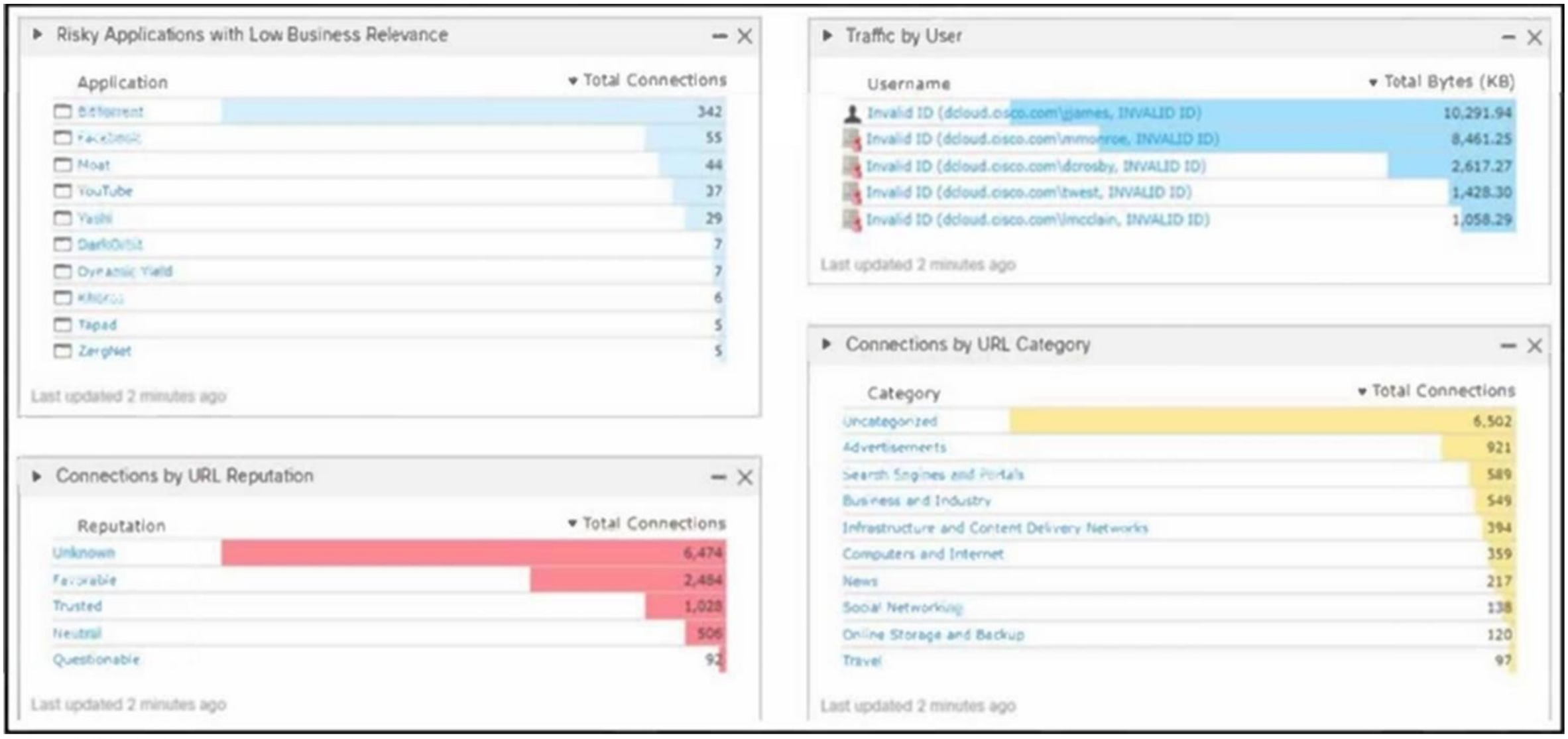
NEW QUESTION: 24
What is an advantage of adding multiple inline interface pairs to the same inline interface set when deploying an asynchronous routing configuration?
A. Allows the IPS to identify inbound and outbound traffic as part of the same traffic flow.
B. The interfaces disable autonegotiation and interface speed is hard coded set to 1000 Mbps.
C. Allows traffic inspection to continue without interruption during the Snort process restart.
D. The interfaces are automatically configured as a media-independent interface crossover.
Answer: (SHOW ANSWER)
https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config- guide-v60/fpmc-config-guide-v60_chapter_01011010.html

NEW QUESTION: 25
A network administrator is trying to convert from LDAP to LDAPS for VPN user authentication on a Cisco FTD. Which action must be taken on the Cisco FTD objects to accomplish this task?
A. Create a Certificate Enrollment object to get the LDAPS certificate needed.
B. Modify the Policy List object to define the session requirements for LDAPS.

C. Identify the LDAPS cipher suite and use a Cipher Suite List object to define the Cisco FTD connection requirements.
D. Add a Key Chain object to acquire the LDAPS certificate.
Answer: (SHOW ANSWER)

NEW QUESTION: 26
Refer to the exhibit. An engineer analyzes a Cisco Firepower Management Center dashboard.
Which action must be taken by the user to decrease the risk of data loss?





A. Stop all URLs that have an unknown reputation.
B. Block the use of Dropbox.
C. Stop all the URLs that are uncategorized.
D. Block all the BitTorrent applications.
Answer: (SHOW ANSWER)
BitTorrent traffic is the most active low-business-relevance, peer-to-peer protocol shown.
Blocking BitTorrent prevents high-volume, unmanaged file transfers and greatly reduces the risk of sensitive data exfiltration.

NEW QUESTION: 27
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)
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: 28
An engineer installs a Cisco FTD device and wants to inspect traffic within the same subnet passing through a firewall and inspect traffic destined to the Internet. Which configuration will meet this requirement?
A. transparent firewall mode with IRB only
B. routed firewall mode with BVI and routed interfaces
C. transparent firewall mode with multiple BVIs
D. routed firewall mode with routed interfaces only
Answer: (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: 29
How does Cisco Secure Cloud Analytics handle information about network traffic?
A. It stores the information in a database without any analysis.
B. It performs a heuristic analysis on events and network flow data.
C. It forwards the information to other devices without storing it.
D. It performs a behavioral analysis on events and network flow data.
Answer: (SHOW ANSWER)
Cisco Secure Cloud Analytics (formerly Stealthwatch Cloud) uses behavioral analysis to monitor events and network flow data. It builds a baseline of normal network behavior and then detects anomalies, such as data exfiltration or lateral movement, indicating potential threats.

NEW QUESTION: 30
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. Network Risk Report
B. User Risk Report
C. Advanced Malware Risk Report
D. Attacks Risk Report
Answer: (SHOW ANSWER)

NEW QUESTION: 31
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 the URL for Secure Firewall Management Center at:
https:///capture/CAPI/pcap/sample.pcap
The engineer receives a 403: Forbidden error instead of being provided with the PCAP file. Which action resolves the issue?

A. Disable the proxy setting on the client browser.
B. Disable the HTTPS server and use HTTP.
C. Enable HTTPS in the device platform policy.
D. Enable the proxy setting in the device platform policy.
Answer: (SHOW ANSWER)
The 403: Forbiddenerror indicates that the HTTPS server on the Secure Firewall Threat Defense (FTD) device is not properly configured or enabled, preventing access to the requested PCAP file. To resolve this, the engineer must enable the HTTPS service in the device platform policy applied to the FTD device in Cisco Secure Firewall Management Center (FMC). This allows the FTD to serve HTTPS requests, including access to PCAP files.

NEW QUESTION: 32
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 a prefilter policy defined
D. Set to none, and configure an access control policy with an intrusion policy and a file policy defined
Answer: (SHOW ANSWER)

NEW QUESTION: 33
An organization is using a Cisco FTD and Cisco ISE to perform identity-based access controls. A network administrator is analyzing the Cisco FTD events and notices that unknown user traffic is being allowed through the firewall. How should this be addressed to block the traffic while allowing legitimate user traffic?
A. Modify lhe Cisco ISE authorization policy to deny this access to the user.
B. Modify Cisco ISE to send only legitimate usernames to the Cisco FTD.
C. Add the unknown user in the Access Control Policy in Cisco FTD.
D. Add the unknown user in the Malware & File Policy in Cisco FTD.
Answer: (SHOW ANSWER)
Unkown is a special identity that can be used in a rule if you use identity policies.

NEW QUESTION: 34
An engineer must implement static route tracking on Cisco Secure Firewall Threat Defense and reroute traffic by using a backup path if the primary path fails. The engineer already defined the primary static route, and the primary path is already monitored. Which action must the engineer take to meet the requirement?
A. Establish an IP SLA ICMP echo request.
B. Configure a tracking object for the static route
C. Assign a unique tracking ID to the static route
D. Configure a secondary static route that has higher precedence

Answer: (SHOW ANSWER)
Create the backup static route that will be used if the primary route fails. This route must have a larger metric than the primary route. For example, if the primary route is 1, the backup route could be 10. You would also normally select a different interface for the backup route.
https://www.cisco.com/c/en/us/td/docs/security/firepower/70/fdm/fptd-fdm-config-guide-700/fptd- fdm- routing.html#:~:text=Create%20the%20backup%20static%20route%20that%20will%20be%20use d%20if%20the%20primary%20route%20fails.%20This%20route%20must%20have%20a%20larg er%20metric%20than%20the%20primary%20route.%20For%20example%2C%20if%20the%20pr imary%20route%20is%201%2C%20the%20backup%20route%20could%20be%2010

NEW QUESTION: 35
Which two features of Cisco AMP for Endpoints allow for an uploaded file to be blocked? (Choose two.)
A. application blocking
B. simple custom detection
C. file repository
D. exclusions
E. application whitelisting
Answer: (SHOW ANSWER)
Configure custom malware detection policies and profiles for your entire organization, as well as perform flash and full scans on all your users' files perform malware analysis, including view heat maps, detailed file information, network file trajectory, and threat root causes configure multiple aspects of outbreak control, including automatic quarantines, application blocking to stop non- quarantined executables from running, and exclusion lists.
https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config- guide-v60/Reference_a_wrapper_Chapter_topic_here.html#id_96014

NEW QUESTION: 36
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 selected to allow traffic to pass through uninterrupted when VDB updates are being applied?
A. Tap Mode
B. Strict TCP Enforcement
C. Propagate Link State
D. Snort Fail Open
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.

NEW QUESTION: 37
An engineer is configuring a custom application detector for HTTP traffic and wants to import a file that was provided by a third party. Which type of flies are advanced application detectors creates and uploaded as?
A. Perl script
B. NBAR protocol

C. Python program
D. LUA script
Answer: (SHOW ANSWER)

NEW QUESTION: 38
An administrator is configuring their transparent Cisco FTD device to receive ERSPAN traffic from multiple switches on a passive port, but the Cisco FTD is not processing the traffic. What is the problem?
A. The Cisco FTD must be configured with an ERSPAN port not a passive port.
B. The Cisco FTD must be in routed mode to process ERSPAN traffic.
C. The switches were not set up with a monitor session ID that matches the flow ID defined on the Cisco FTD.
D. The switches do not have Layer 3 connectivity to the FTD device for GRE traffic transmission.
Answer: (SHOW ANSWER)

NEW QUESTION: 39
What are 2 types or forms of suppression on a FirePower policy (or FTD)?
A. application
B. port
C. rule
D. protocol
E. source
Answer: (SHOW ANSWER)

NEW QUESTION: 40
A network engineer is planning on deploying a Cisco Secure Firewall Threat Defense Virtual appliance in transparent mode. Which two virtual environments support this configuration?
(Choose two.)

A. ESXi
B. AWS
C. GCP
D. OSI
E. KVM
Answer: (SHOW ANSWER)

NEW QUESTION: 41
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)

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

NEW QUESTION: 42
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: (SHOW ANSWER)
Integrated routing and bridging (IRB) is a feature of Cisco Firepower Threat Defense (FTD) that allows the firewall to forward traffic at both layers 2 and 3 for the same subnet. In this mode, the firewall can act as a switch or a bridge to forward traffic at layer 2 and as a router to forward traffic at layer 3. This allows the firewall to maintain full control over the traffic, while still allowing it to forward traffic at both layers.
https://www.cisco.com/c/en/us/td/docs/security/firepower/ftd-config-guide/FTD-Config-Guide-v6/Integrated-Routing-and-Bridging.html

NEW QUESTION: 43
A network engineer must provide redundancy between two Cisco FTD devices. The redundancy configuration must include automatic configuration, translation, and connection updates. After the initial configuration of the two appliances, which two steps must be taken to proceed with the redundancy configuration? (Choose two.)
A. Configure the virtual MAC address on the failover link.
B. Disable hellos on the inside interface.
C. Configure the standby IP addresses.
D. Ensure the high availability license is enabled.
E. Configure the failover link with stateful properties.
Answer: (SHOW ANSWER)
Configure the standby IP addresses
Standby IP addresses must be configured on the failover interfaces to enable communication and synchronization between the primary and secondary FTD devices. These IP addresses are used for the failover and stateful failover links that carry the synchronization and state information between the two units.
Configure the failover link with stateful properties
The failover link is a dedicated connection between the two FTD devices that carries failover communication, including unit state, hello messages, MAC address exchange, and configuration synchronization. Configuring the failover link with stateful properties ensures that connection state information is passed to the standby device, allowing active connections to be preserved during failover.
Note: You cannot configure a virtual MAC address for the failover or Stateful Failover links. The MAC and IP addresses for those links do not change during failover.
https://www.cisco.com/c/en/us/td/docs/security/asa/asa72/configuration/guide/conf_gd/failover.ht ml

NEW QUESTION: 44
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. Inspect Local Traffic Bypass
B. Fast-Path Rules Bypass
C. Automatic Application Bypass
D. Cisco ISE Security Group Tag
Answer: (SHOW ANSWER)

NEW QUESTION: 45
Upon detecting a flagrant threat on an endpoint, which two technologies instruct Cisco Identity Services Engine to contain the infected endpoint either manually or automatically? (Choose two.)
A. Cisco ASA 5500 Series
B. Cisco FMC
C. Cisco AMP
D. Cisco Stealthwatch
E. Cisco ASR 7200 Series
Answer: C,D (LEAVE A REPLY)
Cisco AMP provides endpoint threat detection and can send threat intelligence to Cisco ISE to trigger containment actions such as quarantine or restricted access based on detected malware or compromise.
Cisco Stealthwatch offers network traffic analysis and behavioral detection of threats, which can also integrate with ISE to initiate containment by identifying suspicious or malicious endpoint activity.
https://community.cisco.com/t5/network-access-control/cisco-ise-amp-for-endpoints- integration/td-p/4273949

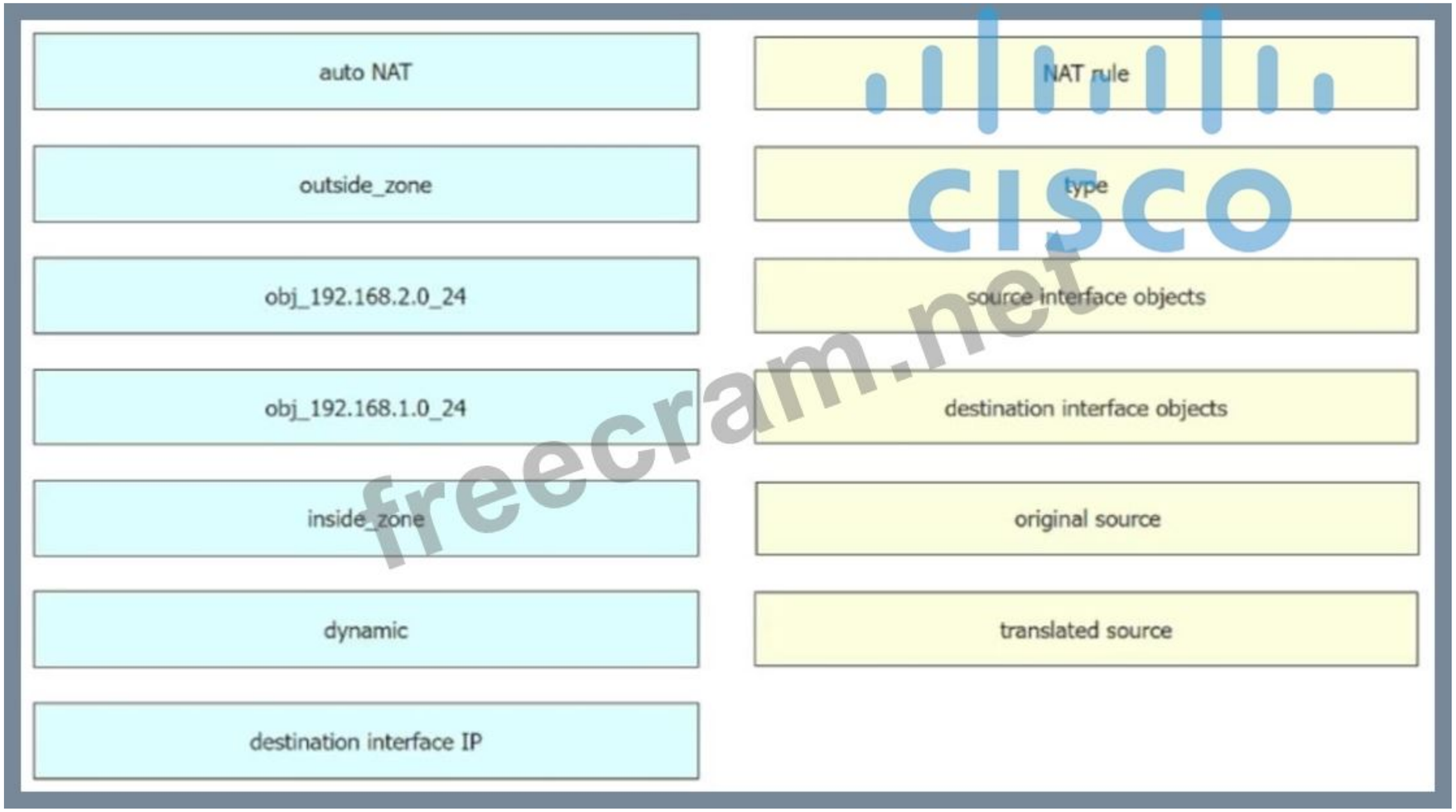
NEW QUESTION: 46
A company has many Cisco FTD devices managed by a Cisco FMC. The security model requires that access control rule logs be collected for analysis. The security engineer is concerned that the Cisco FMC will not be able to process the volume of logging that will be generated. Which configuration addresses concern this?
A. Send Cisco FTD connection events directly to a SIEM system and forward security events from Cisco FMC to the SIEM system for storage and analysis
B. Send Cisco FTD connection events and security events to a cluster of Cisco FMC devices for storage and analysis
C. Send Cisco FTD connection events and security events to Cisco FMC and configure it to forward logs to SIEM for storage and analysis
D. Send Cisco FTD connection events and security events directly to SIEM system for storage and analysis
Answer: (SHOW ANSWER)

NEW QUESTION: 47
Drag and Drop Question
Refer to the exhibit. An engineer configures a NAT rule allowing clients to use the internet only if clients are located on the directly connected internal network. Dynamic auto PAT must be configured. Drag and drop the NAT rules from the left onto the corresponding targets on the right.
Not all options are used.

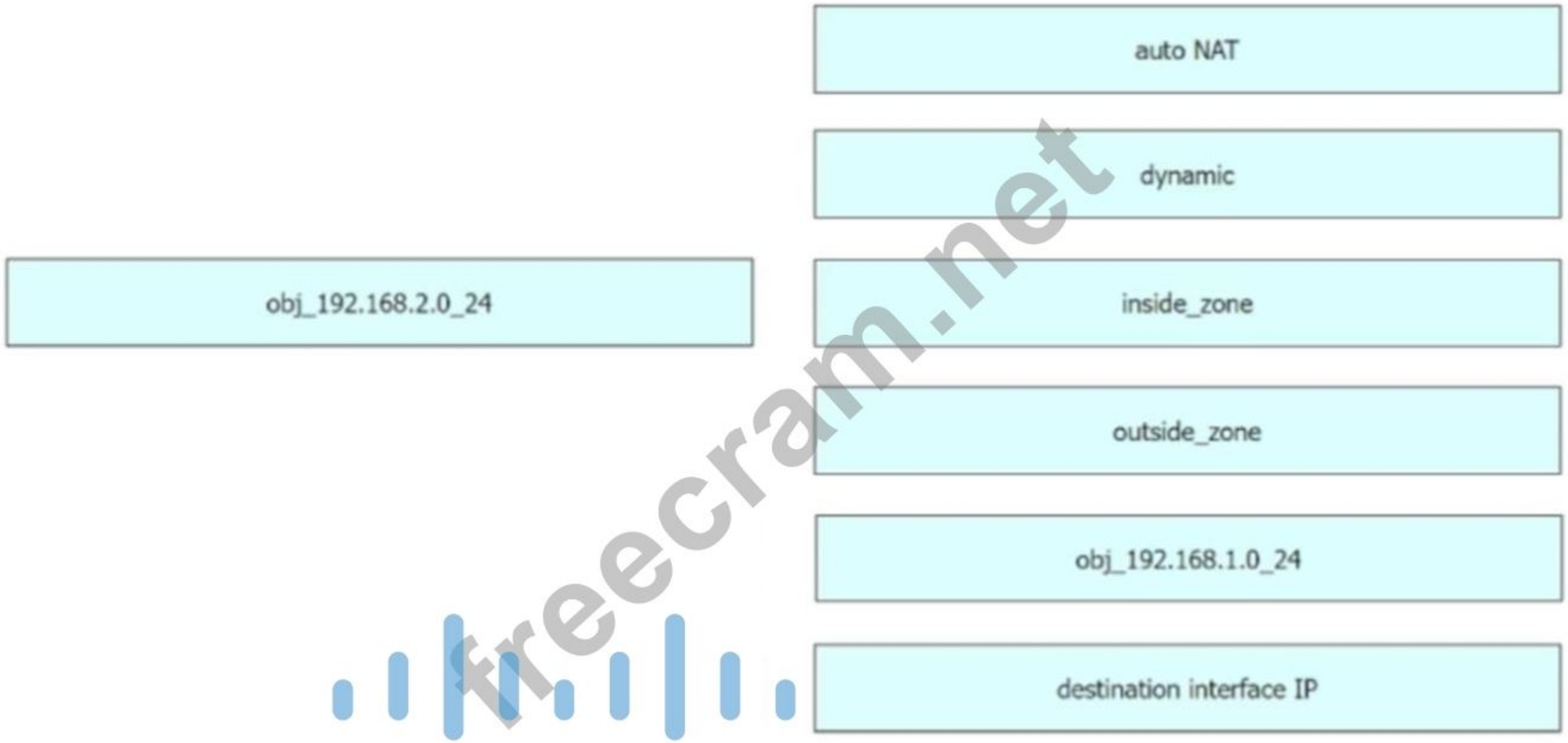
GigabitEthernet0/0	outside	Physical	outside_zone	209.165.201.2/30(Static)	Global
GigabitEthernet0/1	inside	Physical	inside_zone	192.168.1.1/24(Static)	Global
GigabitEthernet0/2	public	Physical	public_zone	209.165.201.5/30(Static)	Global

Name	Value	Type
obj_192.168.1.0_24	192.168.1.0/24	Network
obj_192.168.1.1_32	192.168.1.1	Host
obj_192.168.1.254_32	192.168.1.254	Host
obj_192.168.2.0_24	192.168.2.0/24	Network
obj_209.165.201.1_32	209.165.201.1	Host
obj_any	0.0.0.0/0	Network

Network ▲	Interface	Leaked from Virtual Router	Gateway
▼ IPv4 Routes			
obj_192.168.2.0_24	inside	Global	obj_192.168.1.254_32
any-ipv4	outside	Global	obj_209.165.201.1_32


auto NAT
NAT rule
outside_zone
type
obj_192.168.2.0_24
source interface objects
obj_192.168.1.0_24
destination interface objects
inside_zone
original source
dynamic
translated source
destination interface IP

Answer:



NEW QUESTION: 48
Which feature sets up multiple interfaces on a Cisco Secure Firewall Threat Defense to be on the same subnet?
A. EtherChannel
B. SVI
C. BVI
D. security levels
Answer: C (LEAVE A REPLY)
A Bridge-Group Virtual Interface (BVI) lets you bridge multiple physical interfaces into a single logical interface so they share the same IP subnet on Cisco Secure Firewall Threat Defense.

NEW QUESTION: 49
A company is deploying Cisco Secure Endpoint private cloud. The Secure Endpoint private cloud instance has already been deployed by the server administrator. The server administrator provided the hostname of the private cloud instance to the network engineer via email. What additional information does the network engineer require from the server administrator to be able to make the connection to Secure Endpoint private cloud in Cisco Secure Firewall Management Centre?
A. SSL certificate for the Secure Endpoint ornate cloud instance
B. Internet access for the Secure End point private cloud to reach the Secure Endpoint public cloud
C. Username and password to the Secure Endpoint private cloud instance
D. IP address and port number for the connection proxy
Answer: (SHOW ANSWER)
When integrating Cisco Secure Endpoint (formerly AMP for Endpoints) private cloud with Cisco Secure Firewall Management Center (FMC), the FMC needs to establish a secure HTTPS connection to the Secure Endpoint private cloud instance.
Even though the hostname has already been provided, the SSL certificate is also required for trust establishment during the connection setup. The certificate allows FMC to validate the identity of the Secure Endpoint private cloud instance and ensure that communication is encrypted and secure.

NEW QUESTION: 50
What is a valid Cisco AMP file disposition?
A. non-malicious
B. malware
C. known-good
D. pristine
Answer: (SHOW ANSWER)
Disposition: malware, clean or unknown
https://www.cisco.com/c/en/us/td/docs/security/firepower/623/configuration/guide/fpmc-config- guide-v623/file_malware_events_and_network_file_trajectory.html

NEW QUESTION: 51
There is an increased amount of traffic on the network and for compliance reasons, management needs visibility into the encrypted traffic.
What is a result of enabling TLS'SSL decryption to allow this visibility?
A. It prompts the need for a corporate managed certificate
B. It will fail if certificate pinning is not enforced
C. It is not subject to any Privacy regulations
D. It has minimal performance impact
Answer: (SHOW ANSWER)

NEW QUESTION: 52
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: (SHOW ANSWER)

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.

NEW QUESTION: 53
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?

```
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;
```

A. NAME;DESCRIPTION;TYPE;VALUE;LOOKUP;
B. Name;Description;Type;Value;Lookup;
C. Name;Description;Type;Value;DN;
D. NAME;DESCRIPTION;TYPE;VALUE;DN;
Answer: (SHOW ANSWER)
Cisco FMC's CSV import for network objects requires exact uppercase headers - NAME, DESCRIPTION, TYPE, VALUE - plus the LOOKUP column to specify DNS-based (FQDN) versus IP-based objects.

NEW QUESTION: 54
Which two statements about bridge-group interfaces in Cisco FTD are true? (Choose two.)
A. The BVI IP address must be in a separate subnet from the connected network.
B. Bridge groups are supported in both transparent and routed firewall modes.
C. Bridge groups are supported only in transparent firewall mode.
D. Bidirectional Forwarding Detection echo packets are allowed through the FTD when using bridge- group members.
E. Each directly connected network must be on the same subnet.
Answer: (SHOW ANSWER)
https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-config- guide-v62/transparent_or_routed_firewall_mode_for_firepower_threat_defense.html

NEW QUESTION: 55
Which two types of objects are reusable and supported by Cisco FMC? (Choose two.)
A. dynamic key mapping objects that help link HTTP and HTTPS GET requests to Layer 7 application protocols.
B. reputation-based objects that represent Security Intelligence feeds and lists, application filters based on category and reputation, and file lists
C. network-based objects that represent IP address and networks, port/protocols pairs, VLAN tags, security zones, and origin/destination country
D. network-based objects that represent FQDN mappings and networks, port/protocol pairs, VXLAN tags, security zones and origin/destination country
E. reputation-based objects, such as URL categories
Answer: (SHOW ANSWER)
https://www.cisco.com/c/en/us/td/docs/security/firepower/670/configuration/guide/fpmc-config- guide-v67/reusable_objects.html

NEW QUESTION: 56
A network administrator manages a network with multiple firewalls in a data center. The administrator must change a next-generation firewall from routed to transparent mode. Which action must the administrator take to meet the requirement?
A. Deregister the firewall in Cisco Secure Firewall Management Center.
B. Enter the configure firewall transparent command from the CLI.
C. Manually delete the interface configuration from the CLI.
D. Create one or more bridge groups from the CLI.
Answer: (SHOW ANSWER)
Step 1. Deregister the Firepower Threat Defense device from the FMC.
Step 2. Access the Firepower Threat Defense device CLI, preferably from the console port.
Step 3. > configure firewall [routed | transparent]
Step 4. Re-register with the FMC
https://www.cisco.com/c/en/us/td/docs/security/firepower/70/configuration/guide/fpmc-config- guide-v70/transparent_or_routed_firewall_mode_for_firepower_threat_defense.html

NEW QUESTION: 57
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. No Rules Active
B. Connectivity Over Security
C. Balanced Security and Connectivity
D. Maximum Detection
Answer: (SHOW ANSWER)

NEW QUESTION: 58
An organization is migrating their Cisco ASA devices running in multicontext mode to Cisco FTD devices.
Which action must be taken to ensure that each context on the Cisco ASA is logically separated in the Cisco FTD devices?
A. Add a native instance to distribute traffic to each Cisco FTD context.
B. Add the Cisco FTD device to the Cisco ASA port channels.
C. Configure a container instance in the Cisco FTD for each context in the Cisco ASA.
D. Configure the Cisco FTD to use port channels spanning multiple networks.
Answer: (SHOW ANSWER)
On Cisco ASA, multi-context mode allows a single physical device to run multiple virtual firewalls, called "contexts," each with separate configurations and policies. The equivalent solution in Cisco FTD is the multi-instance (container instance) feature. This allows you to carve up the physical appliance into multiple FTD instances (or containers), each operating as an independent firewall with its own dedicated interfaces, resource allocation, and policy sets.
Each migrated ASA context maps to a separate FTD container instance to maintain isolation and separation of security policies and network segmentation. This setup ensures each virtual firewall from ASA becomes its own logically isolated FTD instance after migration.
https://community.cisco.com/t5/security-blogs/migrating-asa-multi-context-to-ftd-multi- instance/ba-p/3893465

NEW QUESTION: 59
What is a functionality of port objects in Cisco FMC?

A. to mix transport protocols when setting both source and destination port conditions in a rule
B. to represent protocols other than TCP, UDP, and ICMP
C. to represent all protocols in the same way
D. to add any protocol other than TCP or UDP for source port conditions in access control rules.
Answer: (SHOW ANSWER)
A port object can represent other protocols that do not use ports.
https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-config- guide-v62/reusable_objects.html
https://www.cisco.com/c/en/us/td/docs/security/firepower/630/configuration/guide/fpmc-config- guide-v63/reusable_objects.html#ID-2243-00000364

NEW QUESTION: 60
A network administrator must create an EtherChannel interface on a new Cisco Firepower 9300 appliance registered with an FMC for high availability. Where must the administrator create the EtherChannel interface?

A. FMC CLI
B. FTD CLI
C. FXOS CLI
D. FMC GUI
Answer: (SHOW ANSWER)

NEW QUESTION: 61
When a Cisco FTD device is configured in transparent firewall mode, on which two interface types can an IP address be configured? (Choose two.)
A. Physical
B. EtherChannel
C. BVI
D. Diagnostic
E. Subinterface
Answer: (SHOW ANSWER)

NEW QUESTION: 62
An engineer wants to add Cisco Secure Firewall Thread Defense to Cisco Secure Firewall Management Center with the real IP address hidden behind firewall. Engineer configured the command configure manager add Cisc0497926642 on Cisco Secure Firewall Thread Defense.
After the command is added the device is not being added to Cisco Secure Firewall Management Center. Which configuration must be added in the configuration command to accomplish the task?
A. NAT ID
B. Registration Key
C. Cisco FTD IP Address

D. DONOTRESOLVE
Answer: (SHOW ANSWER)
When the Cisco Secure Firewall Threat Defense (FTD) device is behind NAT and the real IP is hidden, a NAT ID must be used in the configure manager addcommand. This allows the FMC to uniquely identify and establish communication with the FTD device through NAT traversal. Without the NAT ID, the registration will fail.

NEW QUESTION: 63
A consultant is working on a project where the customer is upgrading from a single Cisco Firepower 2130 managed by FDM to a pair of Cisco Firepower 2130s managed by FMC for high availability. The customer wants the configuration of the existing device being managed by FDM to be carried over to FMC and then replicated to the additional device being added to create the high availability pair. Which action must the consultant take to meet this requirement?
A. The current FDM configuration must be migrated to FMC using the Secure Firewall Migration Tool.
B. The FTD configuration must be converted to ASA command format, which can then be migrated to FMC.
C. The current FDM configuration will be converted automatically into FMC when the device registers.
D. The current FDM configuration must be configured by hand into FMC before the devices are registered.
Answer: (SHOW ANSWER)

NEW QUESTION: 64
A network administrator is setting up a new highly available Cisco Secure Firewall Threat Defense (FTD) pair. The administrator wants to monitor that the interfaces on the secondary Secure FTD are reachable not just up. What must the administrator configure?
A. This happens by default when high availability is enabled.
B. secondary IP address
C. EUI 64 address on a high-availability link
D. separate high-availability and failover links
Answer: (SHOW ANSWER)
Although recommended, the standby address is not required. Without a standby IP address, the active unit cannot perform network tests to check the standby interface health; it can only track the link state. You also cannot connect to the standby unit on that interface for management purposes.
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: 65
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: (SHOW ANSWER)
https://www.cisco.com/c/en/us/td/docs/security/firepower/660/fdm/fptd-fdm-config-guide-660/fptd- fdm-bgp.html BGP IPv4 is supported both on global and user-defined virtual routers. However, only BGP IPv6 configuration is supported on a global virtual router.
https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/management-center/device- config/710/management-center-device-config-71/routing-ecmp.html You can have up to 8 equal cost static or dynamic routes across up to 8 interfaces within each zone.

NEW QUESTION: 66

An engineer is deploying a Cisco Secure Firewall Management Center appliance. The company must send data to Cisco Secure Network Analytics appliances. Which two actions must the engineer take? (Choose two.)

A. Create a service identifier to enable the NetFlow service.

B. Add the Netflow_Send_Destination object to the configuration.

C. Add the Netflow_Set_Parameters object to the configuration.

D. Add the Netflow_Add_Destination object to the configuration.

E. Security Intelligence object to send data to Cisco Secure Network Analytics

Answer: (SHOW ANSWER)

https://www.cisco.com/c/en/us/support/docs/quality-of-service-qos/netflow/216126-configure- netflow-secure-event-logging- o.html#:~:text=The%20four%20predefined%20objects%20are%20listed%20in%20the%20table%

3A

NEW QUESTION: 67

Which function is the primary function of Cisco AMP threat Grid?

A. automated email encryption

B. monitoring network traffic

C. automated malware analysis

D. applying a real-time URI blacklist

Answer: (SHOW ANSWER)

NEW QUESTION: 68

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

A. Add members to the Cisco FMC, configure Cisco FTD interfaces, create the cluster in Cisco FMC, and configure cluster members in Cisco FMC

B. Add members to Cisco FMC, configure Cisco FTD interfaces in Cisco FMC, configure cluster members in Cisco FMC, create cluster in Cisco FMC, and configure cluster members in Cisco FMC

C. Configure the Cisco FTD interfaces, add members to FMC, configure cluster members in FMC, and create cluster in Cisco FMC

D. Configure the Cisco FTD interfaces and cluster members, add members to Cisco FMC, and create the cluster in Cisco FMC

Answer: (SHOW ANSWER)

In Chassis manager, you (STEP1) config the interfaces, create the cluster and add nodes, then you (STEP2) switch to FMC to add the units to FMC and build the cluster there.

https://www.cisco.com/c/en/us/td/docs/security/firepower/fxos/clustering/ftd-4100-9300- cluster.html#task_tqm_ghj_qgb

NEW QUESTION: 69

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

A. when capture packets are less than 16 MB

B. when capture packets are restricted from the secondary memory

C. when capture packets exceed 10 GB

D. when capture packets exceed 32 MB

Answer: D (LEAVE A REPLY)

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

NEW QUESTION: 70

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

A. The destination MAC address is optional if a VLAN ID value is entered
B. Only the UDP packet type is supported
C. The output format option for the packet logs unavailable
D. The VLAN ID and destination MAC address are optional
Answer: (SHOW ANSWER)
https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-config- guide-v62/troubleshooting_the_system.html

NEW QUESTION: 71
An engineer is configuring a multidomain instance of Cisco Secure Firewall Management Center.
The instance must be integrated with Cisco Secure Endpoint. What must the engineer configure to allow multiple domains to have hosts with the same IP-MAC address pairs?
A. subdomain
B. leaf domain
C. second-level domain
D. global domain
Answer: (SHOW ANSWER)

NEW QUESTION: 72
Which two field can be used to create a new email alert within the Cisco Firepower Management center under Policies > Actions > Alerts tab? (Choose two.)
A. From
B. Device
C. Source
D. Destination
E. Relay Host
Answer: (SHOW ANSWER)

NEW QUESTION: 73
Which report template field format is available in Cisco FMC?
A. box lever chart
B. arrow chart
C. bar chart
D. benchmark chart
Answer: (SHOW ANSWER)
https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config- guide-v60/Working_with_Reports.html

NEW QUESTION: 74
An engineer must integrate Cisco Secure Endpoint with Cisco Secure Firewall Management Center. The company deploys Secure Endpoint to the public cloud and plans to use the same public cloud provider for Cisco Secure Firewall Malware Defense. What must the engineer configure to meet these requirements?

A. file and malware policy
B. Secure Endpoint for Secure Firewall
C. proxy for Secure Firewall connection
D. SSL encryption certificate
Answer: (SHOW ANSWER)
To integrate Cisco Secure Endpoint with Cisco Secure Firewall Management Center and leverage public cloud-based Secure Firewall Malware Defense, the engineer must configure "Secure Endpoint for Secure Firewall". This establishes the connection between FMC and Secure Endpoint for sharing malware event data.

NEW QUESTION: 75
A network security engineer must export packet captures from the Cisco FMC web browser while troubleshooting an issue. When navigating to the address https://<FMC IP>/capture/CAPI/pcap/test.pcap, an error 403: Forbidden is given instead of the PCAP file.
Which action must the engineer take to resolve this issue?
A. Use the Cisco FTD IP address as the proxy server setting on the browser
B. Enable the HTTPS server for the device platform policy
C. Disable the HTTPS server and use HTTP instead
D. Disable the proxy setting on the browser
Answer: (SHOW ANSWER)

NEW QUESTION: 76
administrator is configuring SNORT 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 device in question.
B. A "show tech" file for the device in question
C. A "show tech" for the Cisco FMC.
D. A "troubleshoot" file for the Cisco FMC
Answer: (SHOW ANSWER)
https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-config- guide-v62/troubleshooting_the_system.html

NEW QUESTION: 77
An organization has a Cisco FTD that uses bridge groups to pass traffic from the inside interfaces to the outside interfaces. They are unable to gather information about neighbouring Cisco devices or use multicast in their environment. What must be done to resolve this issue?
A. Create a firewall rule to allow CDP traffic.
B. Create a bridge group with the firewall interfaces.
C. Change the firewall mode to transparent.
D. Change the firewall mode to routed.

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

NEW QUESTION: 78
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 HTTPS and SNMP under the Access List section.
D. Enable SSH and define an access list.
Answer: (SHOW ANSWER)

NEW QUESTION: 79
An administrator needs to configure Cisco FMC to send a notification email when a data transfer larger than 10 MB is initiated from an internal host outside of standard business hours. Which Cisco FMC feature must be configured to accomplish this task?
A. file and malware policy
B. application detector
C. intrusion policy
D. correlation policy
Answer: (SHOW ANSWER)
Correlation policies allow you to correlate security events based on various criteria, including time of day, user, source/destination IP address, and more. When the specified criteria are met, the correlation policy can trigger a response action, such as sending an email notification.

NEW QUESTION: 80
An administrator is setting up Cisco Firepower to send data to the Cisco Stealthwatch appliances. The NetFlow_Set_Parameters object is already created, but NetFlow is not being sent to the flow collector. What must be done to prevent this from occurring?

A. Add the NetFlow_Add_Destination object to the configuration
B. Add the NetFlow_Send_Destination object to the configuration
C. Create a service identifier to enable the NetFlow service
D. Create a Security Intelligence object to send the data to Cisco Stealthwatch
Answer: (SHOW ANSWER)

NEW QUESTION: 81
Which interface type allows packets to be dropped?
A. passive
B. inline
C. ERSPAN
D. TAP

Answer: (SHOW ANSWER)
https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/200908-configuring- firepower-threat-defense-int.html

NEW QUESTION: 82
An engineer integrates Cisco FMC and Cisco ISE using pxGrid. Which role is assigned for Cisco FMC?
A. server
B. client
C. controller
D. publisher
Answer: (SHOW ANSWER)

NEW QUESTION: 83
Which feature is supported by IRB on Cisco FTD devices?
A. redundant interface
B. dynamic routing protocol
C. EtherChannel interface
D. high-availability cluster
Answer: (SHOW ANSWER)
https://www.cisco.com/c/en/us/td/docs/security/firepower/70/configuration/guide/fpmc-config- guide-v70/transparent_or_routed_firewall_mode_for_firepower_threat_defense.html#id_40010

NEW QUESTION: 84
An engineer needs to configure remote storage on Cisco FMC. Configuration backups must be available from a secure location on the network for disaster recovery. Reports need to back up to a shared location that auditors can access with their Active Directory logins. Which strategy must the engineer use to meet these objectives?
A. Use SMB for backups and NFS for reports.
B. Use NFS for both backups and reports.
C. Use SMB for both backups and reports.
D. Use SSH for backups and NFS for reports.
Answer: (SHOW ANSWER)
You cannot send backups to one remote system and reports to another, but you can choose to send either to a remote system and store the other on the Firepower Management Center.
https://www.cisco.com/c/en/us/td/docs/security/firepower/640/configuration/guide/fpmc-config- guide-v64/system_configuration.html#ID-2241-00000551

NEW QUESTION: 85
An administrator is creating interface objects to better segment their network but is having trouble adding interfaces to the objects. What is the reason for this failure?
A. The interfaces are being used for NAT for multiple networks.
B. The administrator is adding interfaces of multiple types.
C. The administrator is adding an interface that is in multiple zones.
D. The interfaces belong to multiple interface groups.
Answer: (SHOW ANSWER)
All interfaces in an interface object must be of the same type: all inline, passive, switched, routed, or ASA FirePOWER. After you create an interface object, you cannot change the type of interfaces it contains.
https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-config- guide-v62/reusable_objects.html#ID-2243-000009b4

NEW QUESTION: 86
An engineer must deploy a Cisco Secure Firewall Threat Defense instance. The company wants the Secure Firewall Threat Defense deployment to allow business traffic in the event of any type of failure, and there must be no connectivity issues caused by the IPS in the perimeter of its data center. Which implementation mode must the engineer use?
A. hardware bypass
B. Snort fail open
C. inline set
D. passive
Answer: (SHOW ANSWER)
The Snort fail open mode is used in Cisco Secure Firewall Threat Defense to ensure that business traffic is allowed to pass through the firewall even if there is a failure in the IPS functionality. This is particularly useful when an organization prioritizes uninterrupted traffic flow over security inspection during failures.
When Snort (the intrusion prevention system) fails or becomes unavailable, fail-open mode bypasses the IPS processing, ensuring that legitimate business traffic continues to flow without interruption.

NEW QUESTION: 87
When packet capture is used on a Cisco Secure Firewall Threat Defense device and the packet flow is waiting on the malware query, which Snort verdict appears?
A. block
B. retry
C. replace
D. blockflow
Answer: (SHOW ANSWER)
When packet capture is used on a Cisco Secure Firewall Threat Defense (FTD) device and the packet flow is waiting on the malware query, the Snort verdict appears as "retry." This indicates that the device is still processing the malware analysis and has not yet determined the final action for the packet.
The "retry" verdict signifies that the packet is in a holding state while awaiting the result of the malware inspection, which helps in maintaining the security posture until a definitive decision is made.

NEW QUESTION: 88
Which two considerations must be made when deleting and re-adding devices while managing them via Cisco FMC? (Choose two).
A. Before re-adding the device In Cisco FMC, the manager must be added back.
B. The Cisco FMC web interface prompts users to re-apply access control policies.
C. Once a device has been deleted, It must be reconfigured before it is re-added to the Cisco FMC.
D. An option to re-apply NAT and VPN policies during registration is available, so users do not need to re-apply the polices after registration is completed.
E. There is no option to re-apply NAT and VPN policies during registration is available, so users need to re-apply the policies after registration is completed.
Answer: (SHOW ANSWER)
When a device is deleted and then re-added, the Firepower Management Center web interface prompts you to re-apply your access control policies. However, there is no option to re-apply the NAT and VPN policies during registration. Any previously applied NAT or VPN configuration will be removed during registration and must be re-applied after registration is complete.
https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config- guide-v60/Device_Management_Basics.html

NEW QUESTION: 89
Network users are experiencing intermittent issues with internet access. An engineer identified that the issue is being caused by NAT exhaustion. How must the engineer change the dynamic NAT configuration to provide internet access for more users without running out of resources?
A. Define an additional static NAT for the network object in use.
B. Add an identity NAT rule to handle the overflow of users.
C. Configure fallthrough to interface PAT on the Advanced tab.

D. Convert the dynamic auto NAT rule to dynamic manual NAT.
Answer: (SHOW ANSWER)

NEW QUESTION: 90
Users report that Cisco Duo 2FA fails when they attempt to connect to the VPN on a Cisco Secure Firewall Threat Defense (FTD) device. IT staff have VPN profiles that do not require multifactor authentication and they can connect to the VPN without any issues. When viewing the VPN troubleshooting log in Cisco Secure Firewall Management Center (FMC), the network administrator sees an error that the Cisco Duo AAA server has been marked as failed. What is the root cause of the issue?

A. AD Trust certificates are missing from the Secure FTD device.
B. Multifactor authentication is not supported on Secure FMC managed devices.
C. The internal AD server is unreachable from the Secure FTD device.
D. Duo trust certificates are missing from the Secure FTD device.
Answer: (SHOW ANSWER)
If users report that Cisco Duo 2FA fails when attempting to connect to the VPN on a Cisco Secure Firewall Threat Defense (FTD) device, and the VPN troubleshooting log in FMC shows an error indicating that the Cisco Duo AAA server has been marked as failed, the root cause is likely missing Duo trust certificates on the FTD device. Trust certificates are essential for establishing a secure and trusted connection between the FTD and the Duo authentication service.
Steps:
Obtain the necessary Duo trust certificates.
Install the certificates on the FTD device.
Verify the configuration to ensure that the FTD device can properly communicate with the Duo AAA server.
This resolves the authentication failure by ensuring that the FTD device can trust the Duo server.

NEW QUESTION: 91
An engineer currently has a Cisco FTD device registered to the Cisco FMC and is assigned the address of 10 10.50.12. The organization is upgrading the addressing schemes and there is a requirement to convert the addresses to a format that provides an adequate amount of addresses on the network.
What should the engineer do to ensure that the new addressing takes effect and can be used for the Cisco FTD to Cisco FMC connection?
A. Delete and reregister the device to Cisco FMC
B. Update the IP addresses from IFV4 to IPv6 without deleting the device from Cisco FMC
C. Format and reregister the device to Cisco FMC.
D. Cisco FMC does not support devices that use IPv4 IP addresses.
Answer: (SHOW ANSWER)
If you registered a FMC and a device using IPv4 and want to convert them to IPv6, you must delete and reregister the device.
https://www.cisco.com/c/en/us/td/docs/security/firepower/70/configuration/guide/fpmc-config- guide-v70/device_management_basics.html

NEW QUESTION: 92
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. a default DMZ policy for which only a user can change the IP addresses.
B. deny ip any
C. no policy rule is included
D. permit ip any
Answer: (SHOW ANSWER)
No policy rule is included in the deployment of a local DMZ during the initial deployment of a Cisco NGFW through the Cisco FMC GUI. The administrator must create the necessary policy rules to allow traffic to and from the DMZ.

NEW QUESTION: 93
Refer to the exhibit. An engineer is configuring an instance of Cisco Secure Firewall Threat Defense with a Secure Firewall Threat Defense interface in IPS Inline Pair mode. What must the engineer configure on interface e1/6?

A. FailSafe disabled
B. propagate link state disabled
C. inline set MTU set to 1500
D. security zone set to OUTSIDE_ZONE
Answer: (SHOW ANSWER)
When configuring an Inline Pair mode as shown in the diagram (e1/6 as INSIDE and e1/8 as OUTSIDE), "propagate link state" must be disabled on the interfaces. This ensures that if one link goes down, the other interface doesn't go down as well, which is important during intrusion prevention testing or tuning.

NEW QUESTION: 94
What is a limitation to consider when running a dynamic routing protocol on a Cisco Secure Firewall Threat Defense device in IRB mode?
A. Only link-state routing protocols are supported.
B. Only EtherChannel interfaces are supported.
C. Only nonbridge interfaces are supported.
D. Only distance vector routing protocols are supported.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 95
Refer to the exhibit. An engineer is modifying an access control pokey to add a rule to inspect all DNS traffic that passes through the firewall.
After making the change and deploying the pokey they see that DNS traffic is not bang inspected by the Snort engine. What is the problem?

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

NEW QUESTION: 96
A network administrator notices that inspection has been interrupted on all non-managed interfaces of a device. What is the cause of this?
A. The value of the highest MTU assigned to any non-management interface was changed.
B. The value of the highest MSS assigned to any non-management interface was changed.
C. A passive interface was associated with a security zone.
D. Multiple inline interface pairs were added to the same inline interface.
Answer: (SHOW ANSWER)

Changing the highest MTU value among all non-management interfaces on the device restarts the Snort process when you deploy configuration changes, temporarily interrupting traffic inspection. Inspection is interrupted on all non-management interfaces, not just the interface you modified. Whether this interruption drops traffic or passes it without further inspection depends on the model of the managed device and the interface type. See Snort® Restart Traffic Behavior for more information.
https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config- guide-v60/fpmc-config-guide-v60_chapter_01101010.html

NEW QUESTION: 97
A network administrator is deploying a new Cisco Secure Firewall Threat Defense (FTD) firewall.
After Cisco Secure FTD is deployed, inside clients have intermittent connectivity to each other.
When reviewing the packet capture on the Secure FTD firewall, the administrator sees that Secure FTD is responding to all the ARP requests on the inside network. Which action must the network administrator take to resolve the issue?
A. Review the access policy and verify that ARP is allowed from inside to inside.
B. Review NAT policy and disable incorrect proxy ARP configuration.
C. Convert the FTD to transparent mode to allow ARP requests.
D. Hardcode the MAC address of the FTD to IP mapping on client machines.
Answer: (SHOW ANSWER)
If inside clients have intermittent connectivity issues and the Cisco Secure FTD is responding to all ARP requests on the inside network, it indicates that there may be an incorrect proxy ARP configuration in the NAT policy. Proxy ARP can cause the FTD to respond to ARP requests on behalf of other devices, leading to connectivity issues.
Steps to resolve:
Review the NAT policy on the FTD to identify any incorrect proxy ARP configurations. Disable the proxy ARP setting for the relevant NAT rules that are causing the issue. This ensures that the FTD only responds to ARP requests as needed, preventing it from interfering with normal ARP traffic on the inside network.

NEW QUESTION: 98
Refer to the exhibit. What is the effect of the existing Cisco FMC configuration?

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

NEW QUESTION: 99
A security engineer is adding three Cisco FTD devices to a Cisco FMC. Two of the devices have successfully registered to the Cisco FMC. The device that is unable to register is located behind a router that translates all outbound traffic to the router's WAN IP address. Which two steps are required for this device to register to the Cisco FMC? (Choose two.)
A. Remove the IP address defined for the device in the Cisco FMC.
B. Configure a NAT ID on both the Cisco FMC and the device.
C. Reconfigure the Cisco FMC lo use the device's private IP address instead of the WAN address.
D. Add the port number being used for PAT on the router to the device's IP address in the Cisco FMC.
E. Reconfigure the Cisco FMC to use the device's hostname instead of IP address.
Answer: (SHOW ANSWER)

NEW QUESTION: 100
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. Custom
C. System
D. None
Answer: (SHOW ANSWER)
In Cisco Secure Firewall Management Center, to disable the HTTP response page and interactive blocking of the entire access control policy, the engineer must select None for both the Block Response Page and Interactive Block Response Page settings. This configuration prevents the firewall from displaying any HTTP response page or offering interactive blocking features when a policy action is triggered, such as blocking traffic based on access control rules.

NEW QUESTION: 101
Which two remediation options are available when Cisco FMC is integrated with Cisco ISE?
(Choose two.)
A. dynamic null route configured
B. DHCP pool disablement
C. quarantine
D. port shutdown
E. host shutdown
Answer: (SHOW ANSWER)
Firepower 6.1 Remediation module allows Firepower system to use ISE EPS capabilities (quarantine, unquarantine, port shutdown) as a remediation when correlation rule is matched.
https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/210524-configure-firepower-6-1-pxgrid-remediati.html

NEW QUESTION: 102
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. inter-chassis clustering VLAN
B. Cisco ISE Security Group Tag
C. integrated routing and bridging

D. interface-based VLAN switching
Answer: (SHOW ANSWER)

NEW QUESTION: 103
What is a method used by Cisco Rapid Threat Containment to contain the threat in the network?
A. change of authentication
B. TACACS+
C. trusted segmentation
D. share context data
Answer: (SHOW ANSWER)
Cisco Rapid Threat Containment leverages technology like Cisco TrustSec to implement software-defined segmentation, effectively isolating compromised devices or portions of the network from the rest, thus containing the spread of a threat.
https://blogs.cisco.com/security/cisco-rapid-threat-containment

NEW QUESTION: 104
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: (SHOW ANSWER)
https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/212330-firepower- management-center-display-acc.html

NEW QUESTION: 105
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. -w capture.pcap -s 1518 host 192.168.100.100 mac
B. -nm src 192.168.100.100
C. -w capture.pcap -s 1518 host 192.168.100.100 ether
D. -ne src 192.168.100.100
Answer: (SHOW ANSWER)
To capture packets on a Cisco Secure Firewall Threat Defense (formerly Firepower Threat Defense) device and ensure that the MAC address appears in the tcpdump output, you need the following:
- Use the -n option to prevent name resolution (makes output clearer).
- Use the -e option to include the link-layer header in the output, which shows MAC addresses.
- Filter by the source IP address (or host IP).
So, the correct tcpdump command should include -ne and a filter for the IP address.

NEW QUESTION: 106
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. Configure the same default gateway for both servers.

B. Ensure that both servers are in the same bridge domain.
C. Enable both servers to share the same VXLAN segment.
D. Assign the same subnet to both servers.
Answer: (SHOW ANSWER)
In transparent mode, Cisco Secure Firewall Threat Defense (FTD) operates as a Layer 2 firewall, acting as a "bump in the wire" without performing routing functions. This mode allows devices on either side of the firewall to communicate as if they were on the same network. To achieve this, the firewall typically uses bridge domains or similar configurations to group devices.
A bridge domain groups interfaces in transparent mode so that devices on each side of the firewall can communicate directly. Ensuring that both servers are in the same bridge domain allows traffic to pass through the firewall transparently, enabling communication between the two servers as if the firewall were not there.

NEW QUESTION: 107
A network administrator is concerned about the high number of malware files affecting users' machines. What must be done within the access control policy in Cisco FMC to address this concern?
A. Create an intrusion policy and set the access control policy to block.
B. Create an intrusion policy and set the access control policy to allow.
C. Create a file policy and set the access control policy to allow.
D. Create a file policy and set the access control policy to block.
Answer: (SHOW ANSWER)
Access control rules:
Rule 3: Block evaluates traffic third. Matching traffic is blocked without further inspection. Traffic that does not match continues to the final rule.
Rule 4: Allow is the final rule. For this rule, matching traffic is allowed; however, prohibited files, malware, intrusions, and exploits within that traffic are detected and blocked. Remaining non- prohibited, non-malicious traffic is allowed to its destination, though it is still subject to identity requirements and rate limiting. You can configure Allow rules that perform only file inspection, or only intrusion inspection, or neither.

NEW QUESTION: 108
An organization has a compliancy requirement to protect servers from clients, however, the clients and servers all reside on the same Layer 3 network.
Without readdressing IP subnets for clients or servers, how is segmentation achieved?
A. Deploy a firewall in transparent mode between the clients and servers.
B. Change the IP addresses of the clients, while remaining on the same subnet.
C. Deploy a firewall in routed mode between the clients and servers
D. Change the IP addresses of the servers, while remaining on the same subnet
Answer: (SHOW ANSWER)
Traditionally, a firewall is a routed hop and acts as a default gateway for hosts that connect to one of its screened subnets. A transparent firewall, on the other hand, is a Layer 2 firewall that acts like a "bump in the wire," or a "stealth firewall," and is not seen as a router hop to connected devices. However, like any other firewall, access control between interfaces is controlled, and all of the usual firewall checks are in place. Layer 2 connectivity is achieved by using a "bridge group" where you group together the inside and outside interfaces for a network, and the Firepower Threat Defense device uses bridging techniques to pass traffic between the interfaces.
Each bridge group includes a Bridge Virtual Interface (BVI) to which you assign an IP address on the network. You can have multiple bridge groups for multiple networks. In transparent mode, these bridge groups cannot communicate with each other.

NEW QUESTION: 109
A Cisco FTD has two physical interfaces assigned to a BVI. Each interface is connected to a different VLAN on the same switch.
Which firewall mode is the Cisco FTD set up to support?
A. active/active failover
B. routed
C. transparent
D. high availability clustering
Answer: (SHOW ANSWER)

NEW QUESTION: 110
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. security group tag
B. Secure Endpoint Cloud Connection
C. Smart Software Manager Satellite
D. internet connection
E. Cisco Success Network
Answer: (SHOW ANSWER)
Secure Endpoint Cloud Connection must be configured on each FMC peer to enable integration with Cisco Secure Endpoint and receive malware events.
Internet connection is required on both high availability peers to communicate with cloud-based services, including Cisco Secure Endpoint. Each peer manages its own cloud connection and must be configured independently.

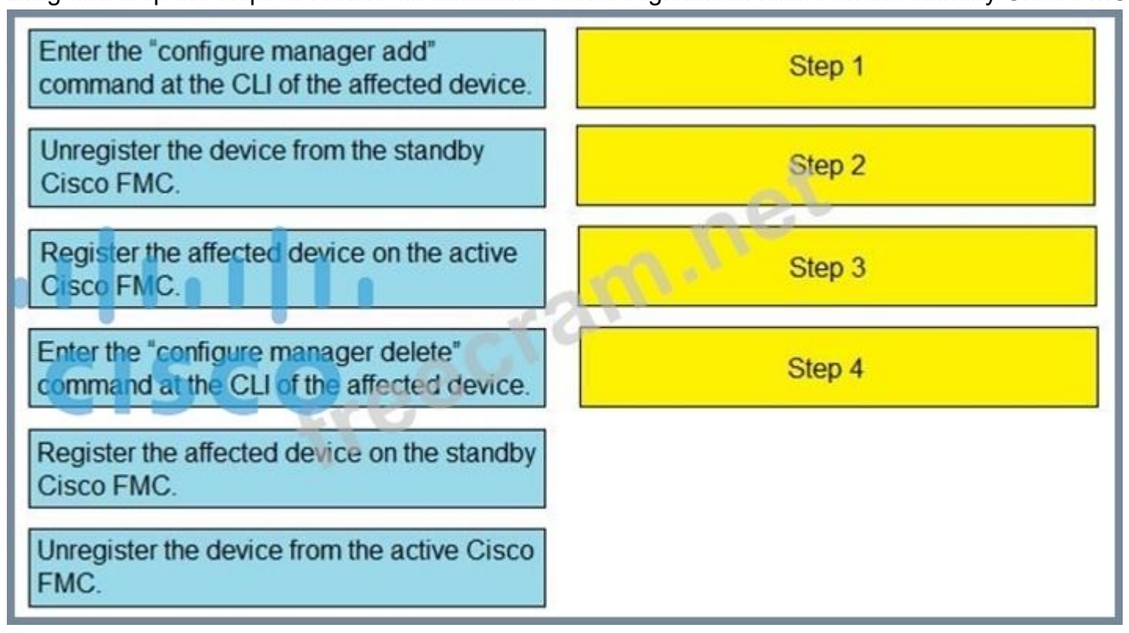
NEW QUESTION: 111
A network administrator is seeing an unknown verdict for a file detected by Cisco FTD.
Which malware policy configuration option must be selected in order to further analyse the file in the Talos cloud?
A. Spero analysis
B. Malware analysis
C. Dynamic analysis
D. Sandbox analysis
Answer: (SHOW ANSWER)
https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config- guide-v60/Reference_a_wrapper_Chapter_topic_here.html

NEW QUESTION: 112
Which action must be taken on the Cisco FMC when a packet bypass is configured in case the Snort engine is down or a packet takes too long to process?
A. Enable Inspect Local Router Traffic
B. Configure Fastpath rules to bypass inspection
C. Add a Bypass Threshold policy for failures
D. Enable Automatic Application Bypass

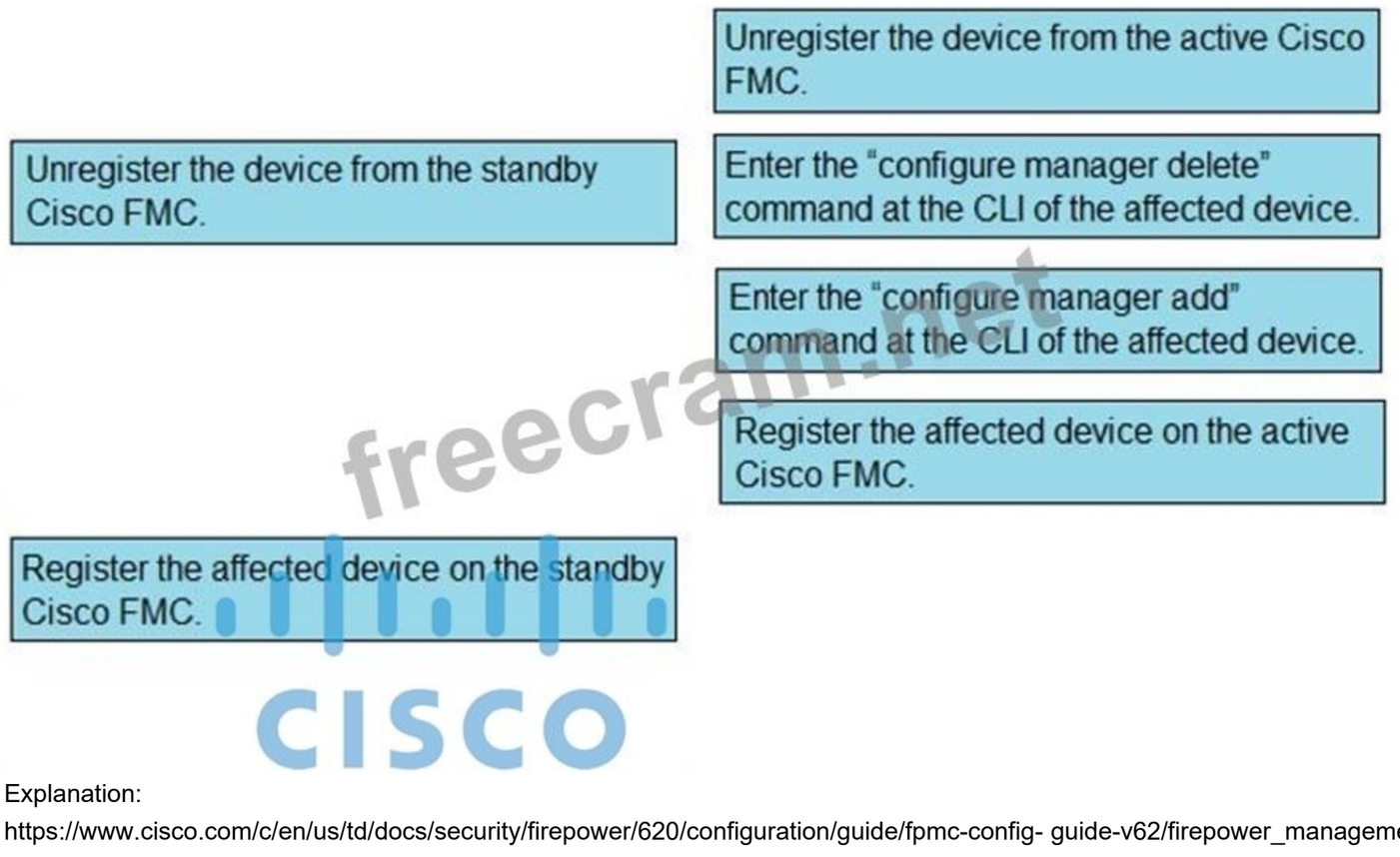
Answer: (SHOW ANSWER)

NEW QUESTION: 113
An engineer is configuring a Cisco Secure Firewall Threat Defense device and wants to create a new intrusion rule based on the detection of a specific pattern in the data payload for a new zero- day exploit.
Which keyword type must be used to add a line that identifies the author of the rule and the date it was created?
A. gtp_info
B. metadata
C. reference
D. content
Answer: (SHOW ANSWER)
When creating a new intrusion rule in a Cisco Secure Firewall Threat Defense (FTD) device, the keyword type "metadata" must be used to add a line that identifies the author of the rule and the date it was created. The metadata keyword is used to store additional information about the rule, such as authorship and creation date.
Steps:
In FMC, navigate to Policies > Intrusion > Rules.
Create a new rule or edit an existing one.
Use the "metadata" keyword to add information about the author and date.
Example:
metadata: created_at 2023-06-15, author "John Doe";
By using the metadata keyword, you ensure that the rule contains relevant information for tracking its creation and authorship, which is essential for maintaining rule documentation and accountability.

NEW QUESTION: 114
Drag and Drop Question
Drag and drop the steps to restore an automatic device registration failure on the standby Cisco FMC from the left into the correct order on the right. Not all options are used.



Answer:



Explanation:
https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-config- guide-v62/firepower_management_center_high_availability.html#id_32288

NEW QUESTION: 115
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 transparent mode and enable the DHCP Server feature.
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 routed mode and allow DHCP traffic in the access control policies.
Answer: (SHOW ANSWER)
For example, by using an access rule, you can allow DHCP traffic (instead of the unsupported DHCP relay feature) or multicast traffic such as that created by IP/TV. You can also establish routing protocol adjacencies through a transparent firewall; you can allow OSPF, RIP, EIGRP, or BGP traffic through based on an access rule. Likewise, protocols like HSRP or VRRP can pass through the FTD device.

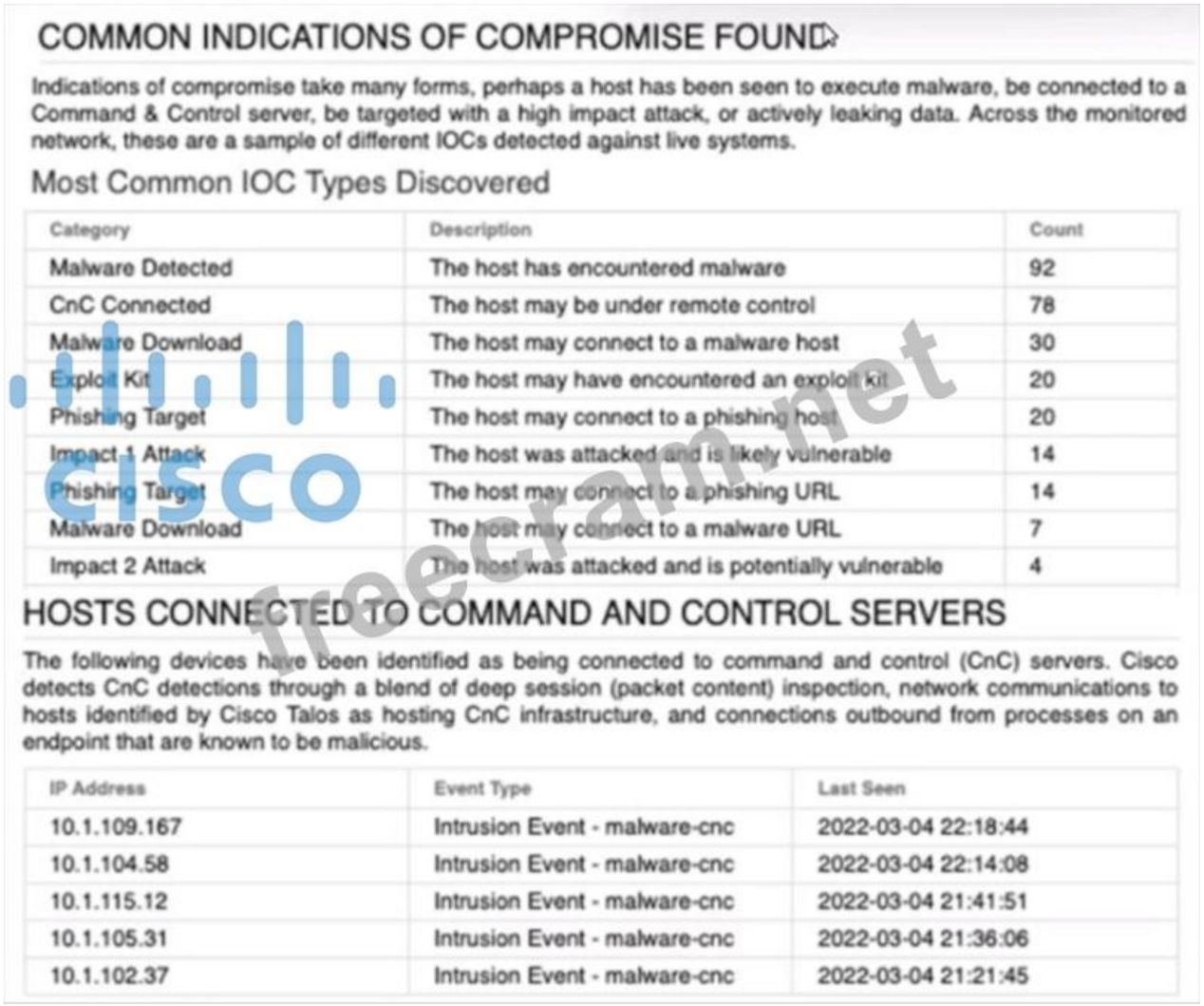
NEW QUESTION: 116
An engineer configures an access control rule that deploys file policy configurations to security zone or tunnel zones, and it causes the device to restart. What is the reason for the restart?
A. Source or destination security zones in the access control rule matches the security zones that are associated with interfaces on the target devices.
B. The source tunnel zone in the rule does not match a tunnel zone that is assigned to a tunnel rule in the destination policy.
C. Source or destination security zones in the source tunnel zone do not match the security zones that are associated with interfaces on the target devices.

D. The source tunnel zone in the rule does not match a tunnel zone that is assigned to a tunnel rule in the source policy.
Answer: (SHOW ANSWER)
Note that access control rules that deploy these file policy configurations to security zones or tunnel zones cause a restart only when your configuration meets the following conditions:
Source or destination security zones in your access control rule must match the security zones associated with interfaces on the target devices.
Unless the destination zone in you access control rule is any, a source tunnel zone in the rule must match a tunnel zone assigned to a tunnel rule in the prefilter policy.
https://www.cisco.com/c/en/us/td/docs/security/firepower/623/configuration/guide/fpmc-config- guide-v623/policy_management.html

NEW QUESTION: 117
An engineer is troubleshooting connectivity to the DNS servers from hosts behind a new Cisco FTD device. The hosts cannot send DNS queries to servers in the DMZ. Which action should the engineer take to troubleshoot this issue using the real DNS packets?
A. Use the packet capture tool to check where the traffic is being blocked and adjust the access control or intrusion policy as needed
B. Use the Connection Events dashboard to check the block reason and adjust the inspection policy as needed
C. Use the packet tracer tool to determine at which hop the packet is being dropped
D. Use the show blocks command in the Threat Defense CLI tool and create a policy to allow the blocked traffic
Answer: (SHOW ANSWER)
Packet capture on the FTD allows the engineer to observe the actual DNS query packets flowing through the device, identifying if and where the traffic is dropped or blocked.
This helps determine whether access control policies or intrusion policies are preventing DNS queries from reaching the servers in the DMZ.
https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/212474-working-with-firepower-threat-defense-f.html#anc34

NEW QUESTION: 118
A mid-sized company is experiencing higher network bandwidth utilization due to a recent acquisition. The network operations team is asked to scale up their one Cisco FTD appliance deployment to higher capacities due to the increased network bandwidth.
Which design option should be used to accomplish this goal?
A. Deploy multiple Cisco FTD appliances in firewall clustering mode to increase performance.
B. Deploy multiple Cisco FTD appliances using VPN load-balancing to scale performance.
C. Deploy multiple Cisco FTD HA pairs to increase performance
D. Deploy multiple Cisco FTD HA pairs in clustering mode to increase performance
Answer: (SHOW ANSWER)
https://www.cisco.com/c/en/us/td/docs/security/firepower/fxos/clustering/ftd-cluster- solution.html#concept_C8502505F840451C9E600F1EED9BC18E

NEW QUESTION: 119
Refer to the exhibit. An engineer analyzes a Network Risk Report from Cisco Secure Firewall Management Center. What should the engineer recommend implementing to mitigate the risk?



COMMON INDICATIONS OF COMPROMISE FOUND

Indications of compromise take many forms, perhaps a host has been seen to execute malware, be connected to a Command & Control server, be targeted with a high impact attack, or actively leaking data. Across the monitored network, these are a sample of different IOCs detected against live systems.

Most Common IOC Types Discovered

Category	Description	Count
Malware Detected	The host has encountered malware	92
CnC Connected	The host may be under remote control	78
Malware Download	The host may connect to a malware host	30
Exploit Kit	The host may have encountered an exploit kit	20
Phishing Target	The host may connect to a phishing host	20
Impact 1 Attack	The host was attacked and is likely vulnerable	14
Phishing Target	The host may connect to a phishing URL	14
Malware Download	The host may connect to a malware URL	7
Impact 2 Attack	The host was attacked and is potentially vulnerable	4

HOSTS CONNECTED TO COMMAND AND CONTROL SERVERS

The following devices have been identified as being connected to command and control (CnC) servers. Cisco detects CnC detections through a blend of deep session (packet content) inspection, network communications to hosts identified by Cisco Talos as hosting CnC infrastructure, and connections outbound from processes on an endpoint that are known to be malicious.

IP Address	Event Type	Last Seen
10.1.109.167	Intrusion Event - malware-cnc	2022-03-04 22:18:44
10.1.104.58	Intrusion Event - malware-cnc	2022-03-04 22:14:08
10.1.115.12	Intrusion Event - malware-cnc	2022-03-04 21:41:51
10.1.105.31	Intrusion Event - malware-cnc	2022-03-04 21:36:06
10.1.102.37	Intrusion Event - malware-cnc	2022-03-04 21:21:45

A. trend analysis
B. network-based detection
C. virtual protection
D. IP address and URL blacklisting
Answer: D (LEAVE A REPLY)
The report indicates that hosts in the network are connecting to known Command and Control (C&C) servers, which are commonly used by attackers to exfiltrate data or execute malicious commands on compromised systems. Implementing IP address and URL blacklisting is an effective mitigation strategy in this scenario, as it directly blocks communications with known malicious IPs and URLs, thereby preventing further exploitation and reducing the risk.

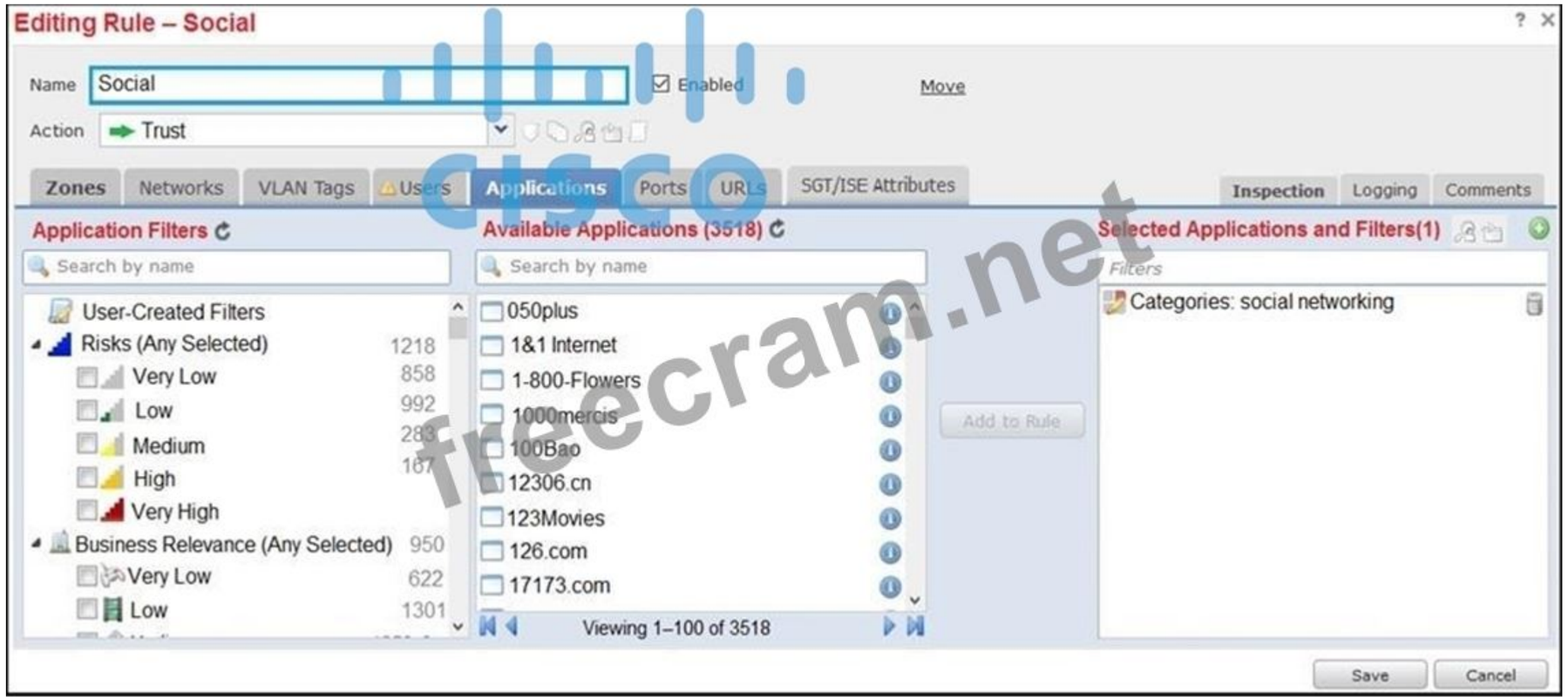
NEW QUESTION: 120
When creating a report template, how can the results be limited to show only the activity of a specific subnet?

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

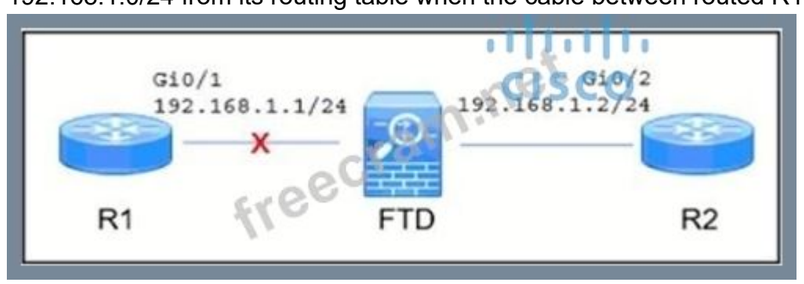
NEW QUESTION: 121
With Cisco FirePOWER Threat Defense software, which interface mode do you configure for an IPS deployment, where traffic passes through the appliance but does not require VLAN rewriting?
A. inline set
B. passive
C. inline tap
D. routed
E. transparent
Answer: A (LEAVE A REPLY)
Inline set (also known as bump-on-wire mode) allows traffic to flow through the appliance transparently without the need for routing or VLAN rewriting. It simply passes the traffic through IPS inspection inline.

NEW QUESTION: 122
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. Change the intrusion policy to connectivity over security.
C. Modify the rule action from trust to allow
D. Add the social network URLs to the block list
Answer: (SHOW ANSWER)
Rule 4: Allow is the final rule. For this rule, matching traffic is allowed; however, prohibited files, malware, intrusions, and exploits within that traffic are detected and blocked. Remaining non- prohibited, non-malicious traffic is allowed to its destination, though it is still subject to identity requirements and rate limiting. You can configure Allow rules that perform only file inspection, or only intrusion inspection, or neither.
https://www.cisco.com/c/en/us/td/docs/security/firepower/660/configuration/guide/fpmc-config- guide-v66/access_control_rules.html

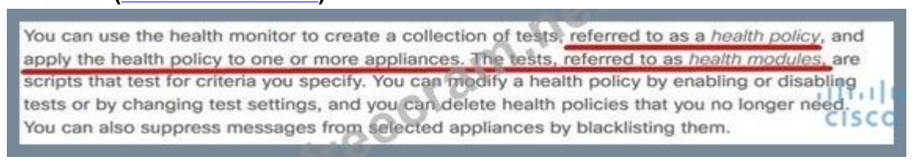
NEW QUESTION: 123
Refer to the exhibit. A Cisco Secure Firewall Threat Defense (FTD) device is deployed in inline mode with an inline set. The network engineer wants router R2 to remove the directly connected route 192.168.1.0/24 from its routing table when the cable between routed R1 and the Secure FTD device Is disconnected. Which action must the engineer take?



A. Implement the Propagate Link Stale option on the Secure FTD device

B. Establish a routing protocol between R1 and R2.
C. Disable hardware bypass on the Secure FTD device.
D. Implement autostate functionality on the Gi0/2 interface of R2
Answer: (SHOW ANSWER)
To ensure that router R2 removes the directly connected route for 192.168.1.0/24 from its routing table when the cable between router R1 and the Secure FTD device is disconnected, the network engineer must implement the "Propagate Link State" option on the Secure FTD device. This option allows the FTD to propagate the link state changes to adjacent devices, ensuring that the disconnection is recognized and the routing table is updated accordingly.
Steps:
Access the FTD device configuration via FMC.
Navigate to the interface settings for the relevant interfaces.
Enable the "Propagate Link State" option for the interfaces connected to R1 and R2.
Deploy the changes to the FTD device.
This configuration ensures that the link state changes are communicated to router R2, prompting it to remove the disconnected route from its routing table.

NEW QUESTION: 124
On Cisco Firepower Management Center, which policy is used to collect health modules alerts from managed devices?
A. health policy
B. system policy
C. correlation policy
D. access control policy
E. health awareness policy
Answer: (SHOW ANSWER)



NEW QUESTION: 125
An engineer must deny ICMP traffic to the networks of separate departments that use Cisco Secure Firewall Management Center. The engineer must use the same object on the relevant device for each network. What must be configured in Secure Firewall Management Center?
A. Allow Overrides check box
B. IP address
C. Deny ICMP check box
D. IP range
Answer: (SHOW ANSWER)
In Cisco Secure Firewall Management Center (FMC), if an engineer needs to apply the same object across multiple devices or networks but may want to configure specific settings for each device or network, they can use the "Allow Overrides" option. When the Allow Overrides checkbox is selected, it enables flexibility by allowing the object to have different configurations or values on different devices while still being centrally managed. This is useful when a single object is applied across multiple networks, as it lets the engineer tailor the settings for each department while maintaining consistency in object management.

NEW QUESTION: 126

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. Create one or more bridge groups from the CLI.

B. Manually delete the interface configuration from the CLI.

C. Deregister the firewall in Cisco Secure Firewall Management Center.

D. Enter the configure transparent firewall command from the CLI.

Answer: C (LEAVE A REPLY)

NEW QUESTION: 127

An engineer is attempting to add a new FTD device to their FMC behind a NAT device with a NAT ID of ACME001 and a password of Cisco388267669.

Which command set must be used in order to accomplish this?

A. configure manager add ACME001 <registration key> <FMC IP>

B. configure manager add <FMC IP> ACME0O1 <registration key>

C. configure manager add DONTRESOLVE <FMC IP> AMCE001 <registration key>

D. configure manager add <FMC IP> registration key> ACME001

Answer: D (LEAVE A REPLY)

https://www.cisco.com/c/en/us/support/docs/security/firesight-management-center/118596-configure-firesight-00.html

NEW QUESTION: 128

An engineer is troubleshooting the upgrade of a Cisco Secure Firewall Threat Defense device on the Secure Firewall Management Center 7.0 GUI. The engineer wants to collect the upgrade data and logs.

Which two actions must the engineer take? (Choose two.)

A. View the system and troubleshooting details.

B. Select the Secure Firewall Threat Defense device properties.

C. Select the Secure Firewall Management Center device.

D. Access the Health Events page.

E. Access the Health Monitor page.

Answer: (SHOW ANSWER)

In FMC you go to Health > Monitor, select your FTD device, then open its System & Troubleshooting details to download the upgrade logs and data bundle.

NEW QUESTION: 129

An engineer is attempting to create a new dashboard within the Cisco FMC to have a single view with widgets from many of the other dashboards. The goal is to have a mixture of threat and security related widgets along with Cisco Firepower device health information.

Which two widgets must be configured to provide this information? (Choose two.)

A. Intrusion Events

B. Correlation Information

C. Appliance Status

D. Current Sessions

E. Network Compliance

Answer: A,C (LEAVE A REPLY)

https://www.cisco.com/c/en/us/td/docs/security/firepower/640/configuration/guide/fpmc-config- guide-v64/dashboards.html#ID-2206-00000283

NEW QUESTION: 130

How is IRB on next-generation firewall running in transparent mode supported?

A. IPv4 routes must be configured on the physical interface.

B. IRB requires an external switch.

C. IPv4 routes must be configured on the BVI.

D. IRB is supported only in routed mode.

Answer: (SHOW ANSWER)

When using Integrated Routing and Bridging (IRB) on a next-generation firewall in transparent mode, IPv4 routes must be configured on the BVI (Bridge Virtual Interface).

The BVI acts as the routed interface for the bridged traffic, enabling Layer 3 connectivity within a transparent deployment.

NEW QUESTION: 131

An engineer is implementing Cisco FTD in the network and is determining which Firepower mode to use. The organization needs to have multiple virtual Firepower devices working separately inside of the FTD appliance to provide traffic segmentation.

Which deployment mode should be configured in the Cisco Firepower Management Console to support these requirements?

A. multiple deployment

B. single-context

C. single deployment

D. multi-instance

Answer: (SHOW ANSWER)

https://www.cisco.com/c/en/us/td/docs/security/firepower/fxos/multi-instance/multi- instance_solution.html#concept_vc4_2lh_3hb

NEW QUESTION: 132

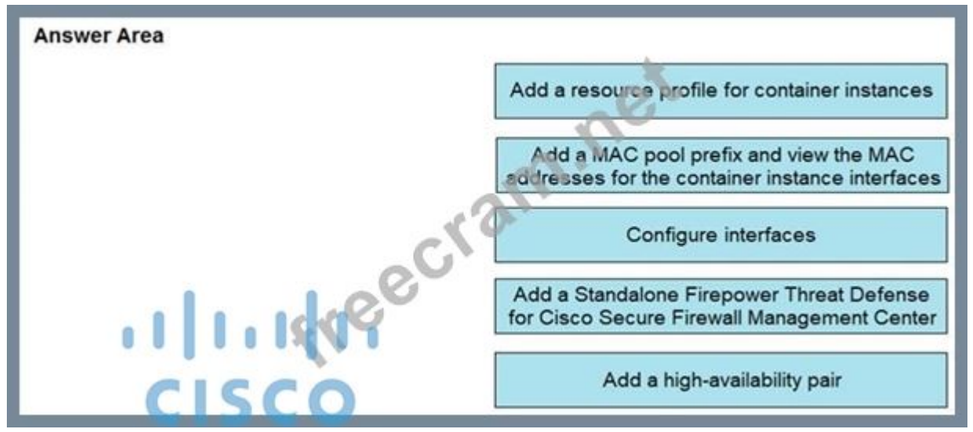
Drag and Drop Question

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.

Answer Area

Add a MAC pool prefix and view the MAC addresses for the container instance interfaces	1
Configure interfaces	2
Add a high-availability pair	3
Add a resource profile for container instances	4
Add a Standalone Firepower Threat Defense for Cisco Secure Firewall Management Center	5

Answer:



NEW QUESTION: 133
An engineer is configuring two new Cisco Secure Firewall Threat Defense devices to replace the existing firewalls. Network traffic must be analyzed for intrusion events without impacting the traffic. What must the engineer implement next to accomplish the goal?
A. Passive mode
B. Inline Pair in Tap mode
C. ERSPAN Passive mode
D. Inline Pair mode
Answer: (SHOW ANSWER)
Passive mode allows the Cisco Secure Firewall Threat Defense device to analyze traffic for intrusion events without impacting or altering the traffic flow. This is ideal for monitoring environments where traffic inspection is needed but enforcement is not required.

NEW QUESTION: 134
Network traffic coining from an organization's CEO must never be denied.
Which access control policy configuration option should be used if the deployment engineer is not permitted to create a rule to allow all traffic?
A. Change the intrusion policy from security to balance.
B. Create a NAT policy just for the CEO.
C. Configure a trust policy for the CEO.
D. Configure firewall bypass.
Answer: (SHOW ANSWER)

NEW QUESTION: 135
Which two statements are valid regarding the licensing model used on Cisco Secure Firewall Threat Defense Virtual appliances? (Choose two.)
A. All licenses require 500G of available storage for the VM
B. Licenses can be used on both physical and virtual appliances
C. All licenses support a maximum of 250 VPN peers
D. Licenses can be used on any supported cloud platform
E. All licenses support up to 16 vCPUs
Answer: (SHOW ANSWER)

NEW QUESTION: 136
An engineer must investigate a connectivity issue from an endpoint behind a Cisco FTD device and a public DNS server. The endpoint cannot perform name resolution queries. Which action must the engineer perform to troubleshoot the issue by simulating real DNS traffic on the Cisco FTD while verifying the Snort verdict?
A. Use the Capture w/Trace wizard in Cisco FMC.
B. Run the system support firewall-engine-debug command from the FTD CLI.
C. Create a Custom Workflow in Cisco FMC.
D. Perform a Snort engine capture using tcpdump from the FTD CLI.
Answer: (SHOW ANSWER)
To trace a real packet is very useful to troubleshoot connectivity issues. It allows you to see all the internal checks that a packet goes through. Add the trace detail keywords and specify the number of packets that you want to be traced. By default, the FTD traces the first 50 ingress packets.
In this case, enable capture with trace detail for the first 100 packets that FTD receives on the INSIDE interface:
> capture CAPI2 interface INSIDE trace detail trace-count 100 match icmp host 192.168.103.1 host 192.168.101.1

NEW QUESTION: 137
A network engineer sets up a secondary Cisco FMC that is integrated with Cisco Security Packet Analyzer.
What occurs when the secondary Cisco FMC synchronizes with the primary Cisco FMC?
A. The existing integration configuration is replicated to the primary Cisco FMC
B. The existing configuration for integration of the secondary Cisco FMC the Cisco Security Packet Analyzer is overwritten.
C. The synchronization between the primary and secondary Cisco FMC fails
D. The secondary Cisco FMC must be reintegrated with the Cisco Security Packet Analyzer after the synchronization
Answer: (SHOW ANSWER)
Note that any existing configurations on the intended secondary Firepower Management Center for integrations with Cisco Security Packet Analyzer will be overwritten when synchronization occurs. If necessary, recreate any such configurations on the intended primary Firepower Management Center.
https://www.cisco.com/c/en/us/td/docs/security/firepower/640/configuration/guide/fpmc-config- guide-v64/firepower_management_center_high_availability.html#id_32288

NEW QUESTION: 138
An administrator must fix a network problem whereby traffic from the inside network to a webserver is not getting through an instance of Cisco Secure Firewall Threat Defense. Which command must the administrator use to capture packets to the webserver that are dropped by Secure Firewall Threat Defense and resolve the issue?
A. capture CAP int INSIDE match ip any host WEBSERVERIP
B. capture CAP int OUTSIDE match ip any host WEBSERVERIP
C. capture CAP int INSIDE match tcp any 80 host WEBSERVERIP 80
D. capture CAP type asp-drop all headers-only
Answer: (SHOW ANSWER)
To capture packets that are dropped by Cisco Secure Firewall Threat Defense (FTD) and troubleshoot the issue of traffic from the inside network to a webserver not getting through, the administrator should use the command to capture packets dropped by the accelerated security path (ASP) engine.

The correct command is:
capture CAP type asp-drop all headers-only
This command captures all packets dropped by the ASP engine, which includes packets that are being blocked by access control policies, NAT issues, or other security checks.
Steps:
Access the FTD CLI.
Run the command capture CAP type asp-drop all headers-only to capture dropped packets.
Analyze the captured data to identify the cause of the drops. This command provides detailed information on why packets are being dropped, helping the administrator resolve the issue.

NEW QUESTION: 139
An engineer must define a URL object on Cisco FMC.
What is the correct method to specify the URL without performing SSL inspection?
A. Use Subject Common Name value.
B. Specify all subdomains in the object group.
C. Specify the protocol in the object.
D. Include all URLs from CRL Distribution Points.
Answer: (SHOW ANSWER)
HTTPS filtering, unlike HTTP filtering, disregards subdomains within the subject common name.
Do not include subdomain information when manually filtering HTTPS URLs.
https://www.cisco.com/c/en/us/td/docs/security/firepower/670/fdm/fptd-fdm-config-guide-670/fptd-fdm-access.html

NEW QUESTION: 140
Which group within Cisco does the Threat Response team use for threat analysis and research?
A. Cisco Deep Analytics
B. OpenDNS Group
C. Cisco Network Response
D. Cisco Talos
Answer: (SHOW ANSWER)
https://www.cisco.com/c/en/us/products/security/threat-response.html#~benefits

NEW QUESTION: 141
A security analyst must create a new report within Cisco FMC to show an overview of the daily attacks, vulnerabilities, and connections. The analyst wants to reuse specific dashboards from other reports to create this consolidated one. Which action accomplishes this task?
A. Copy the Malware Report and modify the sections to pull components from other reports.
B. Modify the Custom Workflows within the Cisco FMC to feed the desired data into the new report.
C. Use the import feature in the newly created report to select which dashboards to add.
D. Create a new dashboard object via Object Management to represent the desired views.
Answer: (SHOW ANSWER)

NEW QUESTION: 142
An organization must be able to ingest NetFlow traffic from their Cisco FTD device to Cisco Stealthwatch for behavioral analysis.
What must be configured on the Cisco FTD to meet this requirement?

A. flexconfig object for NetFlow
B. interface object to export NetFlow
C. security intelligence object for NetFlow
D. variable set object for NetFlow
Answer: (SHOW ANSWER)
Step 4. Configure the Netflow Destination
In order to configure the Netflow Destination, navigate to Objects > FlexConfig > FlexConfig Objects
https://www.cisco.com/c/en/us/support/docs/quality-of-service-qos/netflow/216126-configure- netflow-secure-event-logging-o.html#anc14

NEW QUESTION: 143
An engineer must configure a Cisco FMC dashboard in a child domain.
Which action must be taken so that the dashboard is visible to the parent domain?
A. Create a copy of the dashboard.
B. Add a separate tab.
C. Adjust policy inheritance settings.
D. Add a separate widget.
Answer: (SHOW ANSWER)

NEW QUESTION: 144
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 firewall-engine-dump-user-f density-data command to change the policy and allow the application through the firewall.
C. Use the system support firewall-engine-debug command to determine which rules the traffic matching and modify the rule accordingly
D. Use the system support network-options command to fine tune the policy.
Answer: (SHOW ANSWER)

NEW QUESTION: 145
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. propagate link state
B. Snort fail open
C. inline tap mode
D. strict TCP enforcement
Answer: (SHOW ANSWER)
In Cisco Secure Firewall Threat Defense deployments, propagate link state is a feature designed to manage interface behavior in inline sets. When inline sets are used, the network often requires that both interfaces in the set behave consistently; if one interface in the pair goes down, the other should automatically go down to prevent asymmetric routing or network issues. The Propagate Link State setting ensures that when one interface in an inline set experiences a failure, the paired interface automatically reflects that down status. This is critical in setups where symmetry and failover are essential, especially in high-availability or redundant network designs.

NEW QUESTION: 146

A network engineer is planning on replacing an Active/Standby pair of physical Cisco Secure Firewall ASAs with a pair of Cisco Secure Firewall Threat Defense Virtual appliances. Which two virtual environments support the current High Availability configuration? (Choose two.)

A. ESXi

B. Azure

C. Openstack

D. KVM

E. AWS

Answer: (SHOW ANSWER)

https://www.cisco.com/c/en/us/products/collateral/security/firepower-ngfw-virtual/threat-defense- virtual-ngfwv-ds.html

NEW QUESTION: 147

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

A. Set up a virtual failover MAC address between chassis.

B. Use a dedicated stateful link between chassis.

C. Load the same software version on both chassis.

D. Set the same FQDN for both chassis.

Answer: (SHOW ANSWER)

Configuring virtual MAC addresses on an FTD HA pair is beneficial to the availability of a network. Virtual MAC addresses allow the primary and secondary FTD to maintain consistent MAC addresses which prevents certain traffic disruptions.

https://www.cisco.com/c/en/us/support/docs/security/secure-firewall-threat-defense- virtual/222235-configure-virtual-mac-addresses-for-ftd.html

NEW QUESTION: 148

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. Obtain an FTD model that supports transparent mode.

B. Assign an IP address to two physical interfaces.

C. Deregister the FTD device from FMC and configure transparent mode via the CLI.

D. Add a Bridge Group Interface to the FTD before transparent mode is configured.

Answer: (SHOW ANSWER)

NEW QUESTION: 149

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. Configure the secondary Cisco FMC so that it receives updates from Cisco Talos.

C. Manually import rule updates onto the secondary Cisco FMC device.

D. Configure the primary Cisco FMC so that the rules are updated.

Answer: (SHOW ANSWER)

If your deployment includes a high availability pair of Firepower Management Centers, import the update on the primary only. The secondary Firepower Management Center receives the rule update as part of the regular synchronization process.

https://www.cisco.com/c/en/us/td/docs/security/firepower/670/configuration/guide/fpmc-config- guide-v67/system_software_updates.html

NEW QUESTION: 150

An engineer is implementing clustering in Cisco Secure Firewall Management Center. The configuration must ensure that the cluster has a designated control unit node with more resources than the other nodes. What must the engineer set for the priority value of the node?

A. value lower than the other units in the cluster
B. value higher than the other units in the cluster
C. 0
D. 255
Answer: (SHOW ANSWER)
In a Cisco Secure Firewall clustering deployment, the node with the highest priority value becomes the control unit. To ensure a specific node with more resources takes the control role, the engineer must assign it a priority higher than all other nodes in the cluster.

NEW QUESTION: 151
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)
Virtual Port Channels (vPC) are common EtherChannel deployments, especially in the data center, and allow multiple devices to share multiple interfaces EtherChannel Interface requires stack, VSS or vPC when connected to multiple switches.

NEW QUESTION: 152
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: (SHOW ANSWER)
https://www.cisco.com/c/en/us/support/docs/security/firepower-management-center/212699- configure-ftd-high-availability-on-firep.html

NEW QUESTION: 153
An organization has a Cisco IPS running in inline mode and is inspecting traffic for malicious activity. When traffic is received by the Cisco IRS, if it is not dropped, how does the traffic get to its destination?
A. It is retransmitted from the Cisco IPS inline set.

B. The packets are duplicated and a copy is sent to the destination.
C. It is transmitted out of the Cisco IPS outside interface.
D. It is routed back to the Cisco ASA interfaces for transmission.
Answer: (SHOW ANSWER)
Inline interfaces receive all traffic unconditionally, but all traffic received on these interfaces is retransmitted out of an inline set unless explicitly dropped.
https://www.cisco.com/c/en/us/td/docs/security/firepower/601/configuration/guide/fpmc-config- guide-v601/fpmc-config-guide-v60_chapter_01011010.pdf

NEW QUESTION: 154
An administrator configures new threat intelligence sources and must validate that the feeds are being downloaded and that the intelligence is being used within the Cisco Secure Firewall system. Which action accomplishes the task?
A. View the threat intelligence observables to see the downloaded data
B. Look at the access control policy to validate that the intelligence is being used
C. Use the source status indicator to validate the usage
D. Look at the connection security intelligence events
Answer: (SHOW ANSWER)

NEW QUESTION: 155
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: (SHOW ANSWER)
https://www.cisco.com/c/en/us/td/docs/security/firepower/640/fdm/fptd-fdm-config-guide-640/fptd- fdm-ravpn.html

NEW QUESTION: 156
An external vendor is reporting that they are unable to access an ordering website hosted behind a Cisco Secure Firewall Threat Defense device. The administrator of the device wants to verify that the access policy and NAT policy are configured correctly to allow traffic from the public IP of the external vendor to TCP port 443 on the web server. Which two Cisco Secure Firewall Management Center tools must the administrator use to verify which rules the traffic from the external vendor is matching? (Choose two.)
A. Packet Capture
B. Threat Defense CLI
C. Packet Tracer
D. Generate Troubleshooting File
E. File Download
Answer: (SHOW ANSWER)

NEW QUESTION: 157
An engineer has been asked to show application usages automatically on a monthly basis and send the information to management.
What mechanism should be used to accomplish this task?
A. event viewer

B. reports
C. context explorer
D. dashboards
Answer: B (LEAVE A REPLY)

NEW QUESTION: 158
Refer to the exhibit. A Cisco Secure Firewall Management Center, 7.0 device fails to receive intelligence feed updates. The Cisco Secure Firewall Management Center is configured to use a proxy server that performs SSL inspection. Which action allows the Cisco Secure Firewall Management Center device to download the intelligence feed updates?

```
admin@Sourcefire3D:~$ cat /var/log/messages
Sourcefire3D SF-IMS[2004]: [2011] CloudAgent:IPReputation [WARN] Cannot download
 Sourcefire_Intelligence_Feed

Sourcefire3D SF-IMS[24085]: [24090] CloudAgent:IPReputation [WARN] Download
 unsucessful: Failure when receiving data from the peer
```

A. Install a self-signed certificate on the proxy server for intelligence.sourcefire.com.
B. Verify that the proxy server can use HTTPS to communicate to the internet.
C. Ensure that proxy authentication is disabled for the Cisco Secure Firewall Management Center device.
D. Bypass the proxy server for intelligence.sourcefire.com.
Answer: (SHOW ANSWER)
Bypassing the proxy for the Cisco threat-intelligence endpoint ensures the FMC connects directly using a trusted certificate chain, avoiding SSL-inspection breaks that prevent feed downloads.

NEW QUESTION: 159
An engineer must configure a correlation policy in Cisco Secure Firewall Management Center to detect when an IP address from an internal network communicates with a known malicious host. Connections made by the internalIP addresses must be tracked, and an external dynamic list must be used for the condition. Which type of event must the engineer configure on the correlation policy?
A. network discovery
B. malware
C. connection tracker
D. Intrusion Impact Alert
Answer: (SHOW ANSWER)
To detect when internal IP addresses initiate connections to known malicious hosts using an external dynamic list, the engineer must configure a connection tracker event in the correlation policy. This allows the policy to monitor traffic flows and correlate them with the external threat intelligence source.

NEW QUESTION: 160
A security engineer needs to configure a network discovery policy on a Cisco FMC appliance and prevent excessive network discovery events from overloading the FMC database? Which action must be taken to accomplish this task?
A. Change the network discovery method to TCP/SYN.
B. Exclude load balancers and NAT devices in the policy.
C. Monitor only the default IPv4 and IPv6 network ranges.
D. Configure NetFlow exporters for monitored networks.

Answer: (SHOW ANSWER)

NEW QUESTION: 161
What is a characteristic of bridge groups on a Cisco FTD?
A. In routed firewall mode, routing between bridge groups must pass through a routed interface.
B. In routed firewall mode, routing between bridge groups is supported.
C. In transparent firewall mode, routing between bridge groups is supported
D. Routing between bridge groups is achieved only with a router-on-a-stick configuration on a connected router
Answer: (SHOW ANSWER)
In routed mode: The BVI acts as the gateway between the bridge group and other routed interfaces. To route between bridge groups/routed interfaces, you must name the BVI. For some interface-based features, you can use the BVI itself.
https://www.cisco.com/c/en/us/td/docs/security/asa/asa97/configuration/general/asa-97-general- config/intro-fw.pdf

NEW QUESTION: 162
What is a limitation to consider when running a dynamic routing protocol on a Cisco FTD device in IRB mode?
A. Only link-stale routing protocols are supported.
B. Only nonbridge interfaces are supported.
C. Only distance vector routing protocols are supported.
D. Only EtherChannel interfaces are supposed.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 163
A security engineer is configuring an Access Control Policy for multiple branch locations.
These locations share a common rule set and utilize a network object called INSIDE_NET which contains the locally significant internal network subnets at each location.
What technique will retain the policy consistency at each location but allow only the locally significant network subnet within the applicable rules?
A. creating an ACP with an INSIDE_NET network object and object overrides
B. creating a unique ACP per device
C. utilizing policy inheritance
D. utilizing a dynamic ACP that updates from Cisco Talos
Answer: A (LEAVE A REPLY)

NEW QUESTION: 164
An administrator is attempting to add a new FTD device to their FMC behind a NAT device with a NAT ID of NAT001 and a password of Cisco0420l06525. The private IP address of the FMC server is 192.168.45.45. which is being translated to the public IP address of
209.165.200.225/27. Which command set must be used in order to accomplish this task?
A. configure manager add 192.168.45.45 <reg_key> <nat_id>
B. configure manager add 209.165.200.225 <reg_key> <nat_id>
C. configure manager add 209.165.200.225/27 <reg_key> <nat_id>
D. configure manager add 209.165.200.225 255.255.255.224 <reg_key> <nat_id>
Answer: (SHOW ANSWER)

NEW QUESTION: 165
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. Destination MAC
B. TCP Intercept
C. Bypass Mode
D. Flow Id
E. Source IP
Answer: (SHOW ANSWER)
To complete the configuration of an ERSPAN passive interface on a Cisco Secure IPS using Cisco Secure Firewall Management Center, the following additional settings are required:
- Destination MAC: Needed to identify the intended recipient of the ERSPAN traffic.
- Flow ID: Uniquely identifies the ERSPAN session, which is essential for processing mirrored traffic correctly.

NEW QUESTION: 166
How many report templates does the Cisco Firepower Management Center support?
A. 20
B. 10
C. 5
D. unlimited
Answer: (SHOW ANSWER)
https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config- guide-v60/Working_with_Reports.html

NEW QUESTION: 167
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: (SHOW ANSWER)
Log the detection: In this mode, the identified malicious process is not blocked by MAP, but the detection is logged in the AMP for Endpoints console. (This is Audit mode, where no blocking or quarantine action happens, but the detection is logged.)
https://www.cisco.com/c/en/us/products/collateral/security/amp-for-endpoints/white-paper-c11-740980.html

NEW QUESTION: 168
Which Firepower feature allows users to configure bridges in routed mode and enables devices to perform Layer 2 switching between interfaces?
A. FlexConfig
B. BDI
C. SGT
D. IRB
Answer: D (LEAVE A REPLY)
Integrated Routing and Bridging (IRB) : Customers often want to have multiple physical interfaces configured to be part of the same VLAN. The IRB feature meets this demand by allowing users to configure bridges in routed mode, and enables the devices to perform L2 switching between interfaces (including subinterfaces).
https://www.cisco.com/c/en/us/td/docs/security/firepower/620/relnotes/Firepower_System_Releas e_Notes_Version_620/new_features_and_functionality.html

NEW QUESTION: 169
What Software can be installed on the Cisco 4100 series appliance? (Choose two)
A. FTD
B. ASA
C. ASAv
D. FMC
Answer: (SHOW ANSWER)
Cisco Firepower Threat Defense (FTD): This is the core security software that provides firewall, intrusion prevention, malware protection, and URL filtering capabilities.
Cisco Firepower Management Center (FMC): This software is used to centrally manage and configure FTD instances. It provides a unified management interface for firewalls, application control, intrusion prevention, URL filtering, and advanced malware protection.
The Cisco 4100 series appliance is designed to run these two software components together to provide a comprehensive security solution.

NEW QUESTION: 170
An organization has seen a lot of traffic congestion on their links going out to the internet There is a Cisco Firepower device that processes all of the traffic going to the internet prior to leaving the enterprise. How is the congestion alleviated so that legitimate business traffic reaches the destination?

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

NEW QUESTION: 171
A network engineer implements a new Cisco Firepower device on the network to take advantage of its intrusion detection functionality. There is a requirement to analyze the traffic going across the device, alert on any malicious traffic, and appear as a bump in the wire How should this be implemented?
A. Specify the BVI IP address as the default gateway for connected devices.
B. Enable routing on the Cisco Firepower
C. Add an IP address to the physical Cisco Firepower interfaces.
D. Configure a bridge group in transparent mode.

Answer: (SHOW ANSWER)
Traditionally, a firewall is a routed hop and acts as a default gateway for hosts that connect to one of its screened subnets. A transparent firewall, on the other hand, is a Layer 2 firewall that acts like a "bump in the wire," or a "stealth firewall," and is not seen as a router hop to connected devices. However, like any other firewall, access control between interfaces is controlled, and all of the usual firewall checks are in place.
Layer 2 connectivity is achieved by using a "bridge group" where you group together the inside and outside interfaces for a network, and the ASA uses bridging techniques to pass traffic between the interfaces. Each bridge group includes a Bridge Virtual Interface (BVI) to which you assign an IP address on the network. You can have multiple bridge groups for multiple networks.
In transparent mode, these bridge groups cannot communicate with each other.
https://www.cisco.com/c/en/us/td/docs/security/asa/asa97/configuration/general/asa-97-general- config/intro-fw.html

NEW QUESTION: 172
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: (SHOW ANSWER)
FMC High Availability. High Availability is available on physical Firepower Management Center appliances (and FMCv since 6.7. 0).
Before configuring FMC HA make sure that:
* Hardware is identical (no mix and match between virtual and/or physical form factors)
* Software release is identical on both FMCs
* There are no sensors registered to the secondary FMC
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: 173
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: (SHOW ANSWER)
Link state propagation automatically brings down the second interface in the inline interface pair when one of the interfaces in an inline set goes down.
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 With tap mode, the FTD is deployed inline, but the network traffic flow is undisturbed.
https://www.cisco.com/c/en/us/td/docs/security/firepower/650/configuration/guide/fpmc-config- guide- v65/interface_overview_for_firepower_threat_defense.html#concept_DB45E8BBB07946728427F F98DB2DC56D

NEW QUESTION: 174
An engineer is configuring a new dashboard within Cisco Secure Firewall Management Center and is having trouble implementing a custom widget. When a custom analysis widget is configured, which option is mandatory for the system to display the information?
A. table

B. title
C. filter
D. results
Answer: (SHOW ANSWER)
The following items are required:
- Table (required): The table of events or assets that contains the data the widget displays.
- Field (required): The specific field of the event type you want to display. To show data over time (line graphs), choose Time. To show relative occurrences of events (bar graphs), choose another option.
- Aggregate (required): The aggregation method configures how the widget groups the data it displays. For most event types, the default option is Count.
https://www.cisco.com/c/en/us/td/docs/security/firepower/623/configuration/guide/fpmc-config- guide-v623/dashboards.html

NEW QUESTION: 175
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)
You can Have here BVI with no name and in that way the BVI acts as transparent firewall. So with that you have extended LAN network, the Gateway stays the same (ex. GW is 192.168.1.1 and BVI is 192.168.1.2) so nothing changes for users. If you go with Inline, you do not extend network, Inline only has inline par interfaces and that does not extend the LAN.

NEW QUESTION: 176
A company is in the process of deploying intrusion prevention with Cisco FTDs managed by a Cisco FMC. An engineer must configure policies to detect potential intrusions but not block the suspicious traffic.
Which action accomplishes this task?
A. Configure IPS mode when creating or editing a policy rule under the Cisco FMC Intrusion tab in Access Policies section by unchecking the "Drop when inline" option.
B. Configure IPS mode when creating or editing a policy rule under the Cisco FMC Intrusion tab in Access Policies section by checking the "Drop when inline" option.
C. Configure IDS mode when creating or editing a policy rule under the Cisco FMC Intrusion tab in Access Policies section by checking the "Drop when inline" option.
D. Configure IDS mode when creating or editing a policy rule under the Cisco FMC Intrusion tab in Access Policies section by unchecking the "Drop when inline" option.
Answer: (SHOW ANSWER)

NEW QUESTION: 177
An organization recently implemented a transparent Cisco FTD in their network. They must ensure that the device does not respond to insecure SSL/TLS protocols. Which action accomplishes this task?
A. Configure a FlexConfig object to disable any insecure TLS protocols on the Cisco FTD device.
B. Enable the UCAPL/CC compliance on the device to support only the most secure protocols available.
C. Use the Cisco FTD platform policy to change the minimum SSL version on the device to TLS 1.2.
D. Modify the device's settings using the device management feature within Cisco FMC to force only secure protocols.
Answer: (SHOW ANSWER)

NEW QUESTION: 178
A security engineer manages a firewall console and an endpoint console and finds it challenging and time consuming to review events and modify blocking of specific files in both consoles. Which action must the engineer take to streamline this process?

A. Within the Cisco Secure Endpoint console, copy the connector GUID and paste into the Cisco Secure Firewall Management Center (FMC) AMP tab.
B. From the Cisco Secure Endpoint console, create and copy an API key and paste into the Cisco Secure AMP tab.
C. From the Secure FMC, create a Cisco Secure Endpoint object and reference the object in the Cisco Secure Endpoint console.
D. Initiate the integration between Secure FMC and Cisco Secure Endpoint from the Secure FMC using the AMP tab.
Answer: (SHOW ANSWER)
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.

NEW QUESTION: 179
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: (SHOW ANSWER)
https://www.cisco.com/c/en/us/td/docs/security/firepower/610/fdm/fptd-fdm-config-guide-610/fptd-fdm- interfaces.html

NEW QUESTION: 180
An engineer is deploying the Cisco Firepower NGIPSv for VMware.
Which two aspects are unsupported during this deployment? (Choose two.)

A. vCenter
B. restoring a backup
C. vCloud Director
D. vMware tool
E. cloning a virtual machine
Answer: (SHOW ANSWER)
https://www.cisco.com/c/en/us/td/docs/security/firepower/60/quick_start/ngips_virtual/NGIPSv- quick/intro-ngipsv.html

NEW QUESTION: 181
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. Analysis > Status with a sliding time window of one day
B. Events by priority and classification and set 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: (SHOW ANSWER)
Scheduled reports using the network risk report template provide executives with a concise, high- level summary of emerging threats and overall network risk. Automating it on a daily cadence ensures upper management receives consistent updates without manual intervention.

NEW QUESTION: 182
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 FMC to contain the infected endpoint.
C. Cisco ISE instructs Cisco AMP to contain the infected endpoint.
D. Cisco AMP instructs Cisco FMC to contain the infected endpoint.
Answer: (SHOW ANSWER)

NEW QUESTION: 183
Which component simplifies incident investigation with Cisco Threat Response?
A. Cisco AMP client
B. local CVE database
C. Cisco Secure Firewall appliance
D. browser plug-in
Answer: (SHOW ANSWER)

Cisco Threat Response (CTR) is a security solution that helps simplify incident investigation and threat hunting. One of its components that significantly simplifies the investigation process is the browser plug-in. The browser plug-in integrates with CTR to provide contextual information directly within the browser, allowing security analysts to quickly view threat details, pivot to related information, and take appropriate actions without switching between multiple tools.
Features of the browser plug-in:
Provides real-time threat intelligence and context from various Cisco security products.
Allows security analysts to investigate incidents directly from web-based consoles.
Enhances efficiency by streamlining the workflow and reducing the time needed to gather and correlate information.

NEW QUESTION: 184
Refer to the exhibit. A security engineer must improve security in an organization and is producing a risk mitigation strategy to present to management for approval. Which action must the security engineer take based on this Attacks Risk Report?

APPLICATIONS ASSOCIATED WITH ATTACKS

The following applications have been identified as associated with attacks. You should identify applications in this list that have low business relevance and evaluate whether it would be helpful to control them on your network.

Apps Associated with High Impact Events	Count
DNS	16
Internet Explorer	14
Web browser	8
FTP client	6
NetBIOS-ssn (SMB) client	6

Apps Associated with Low Impact Events	Count
Chrome	283
Internet Explorer	110
DCE/RPC client	74
Web browser Firefox	47
Firefox	36

TOP ATTACKERS AND TARGETS

The top attackers and target machines observed in the attack attempts on your network are listed below. For high impact attacks in particular, you should ensure that targets are well protected from potential attackers by patching these machines and blocking potentially malicious traffic.

High Impact Events

Attackers	Attacks
5.196.214.27	3
10.1.115.12	3
10.1.115.12	3
10.1.26.6	2
10.1.39.21	2

Targets	Attacks
31.31.196.236	6
185.118.166.155	6
37.48.82.212	4
185.86.77.12	4
192.161.54.60	4

A. Block NetBIOS.
B. Inspect TCP port 80 traffic.
C. Block Internet Explorer.
D. Inspect DNS traffic.
Answer: (SHOW ANSWER)
Based on the Attacks Risk Report, DNS is associated with a high number of impact events (16).
DNS traffic is critical for network operations but can also be exploited for malicious activities such as DNS tunneling, DDoS attacks, and data exfiltration. To improve security, the security engineer should focus on inspecting DNS traffic. This involves deploying DNS security solutions and monitoring DNS traffic for anomalies to detect and mitigate potential threats.
Steps:
Implement DNS security tools such as DNS filtering, DNSSEC, and DNS anomaly detection.
Configure the firewall to inspect DNS traffic for malicious activities. Regularly analyze DNS logs to identify and respond to threats. This action addresses a significant risk identified in the report and helps to mitigate potential attacks exploiting DNS.

NEW QUESTION: 185
A security engineer is reviewing a Cisco Secure Endpoint public cloud instance. The engineer discovers a malicious verdict for a SHA-256 hash of 689efc1ecdc23ec0b0885a80663e30ea013d493f8e88224b570a1234567890.
Which configuration action must be done in Secure Endpoint console to mitigate the threat?
A. Add the hash to the custom detection list.
B. Set access control policy and deny files with the hash.
C. Configure correlation policy to block the hash.
D. Apply regular expression to block the malicious file.
Answer: (SHOW ANSWER)
To mitigate a known malicious file in Cisco Secure Endpoint, the security engineer can add the hash (SHA-256) to the custom detection list. This action ensures that Cisco Secure Endpoint will automatically block or quarantine any file matching this hash in the environment, preventing it from executing or spreading further.

NEW QUESTION: 186
An engineer must configure the encrypted visibility engine for a Cisco Secure Firewall Threat Defense device in Cisco Secure Firewall Management Center. The engineer already configured an access control policy, Cisco vulnerability database updates, and the Cisco Success Network.
Which two actions must be taken to complete the Secure Firewall Threat Defense device configuration? (Choose two.)
A. Configure an SSL/TLS policy.
B. Enable encrypted traffic inspection.
C. Enable Snort 3.

D. Install a Threat license.
E. Configure an identity policy.
Answer: (SHOW ANSWER)
To complete the configuration of the encrypted visibility engine on a Cisco Secure Firewall Threat Defense device via FMC, the engineer must:
- Configure an SSL/TLS policy: This is required to define how encrypted traffic is handled (e.g., detection, decryption).
- Enable encrypted traffic inspection: This activates the engine that analyzes encrypted traffic to detect threats without full decryption.

NEW QUESTION: 187
An engineer is tasked with configuring a custom intrusion rule on Cisco Secure Firewall Management Center to detect and block the malicious traffic pattern with specific payload containing string "|04 68 72 80 87 ff ed cq fg he qm pn|". Which action must the Engineer configure on the IPS policy?
A. disable
B. quarantine
C. reset
D. drop
E. alert
Answer: (SHOW ANSWER)

NEW QUESTION: 188
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. Enable the Trace option.
C. Specify the packet size.
D. Specify the buffer size.
Answer: (SHOW ANSWER)
Select Trace if you want to capture the details for each packet.
https://www.cisco.com/c/en/us/td/docs/security/firepower/70/configuration/guide/fpmc-config- guide-v70/troubleshooting_the_system.html

NEW QUESTION: 189
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)
https://www.cisco.com/c/en/us/td/docs/security/asa/asa96/configuration/general/asa-96-general- config/intro-fw.html

NEW QUESTION: 190
An engineer is creating an URL object on Cisco FMC. How must it be configured so that the object will match for HTTPS traffic in an access control policy?

A. Specify the protocol to match (HTTP or HTTPS).
B. Use the FQDN including the subdomain for the website
C. Define the path to the individual webpage that uses HTTPS.
D. Use the subject common name from the website certificate
Answer: (SHOW ANSWER)
The subject common name from the website certificate is used to match HTTPS traffic without performing SSL inspection. This allows the system to identify and match the URLs without decrypting the traffic, hence avoiding SSL inspection.

NEW QUESTION: 191
An engineer is building a new access control policy using Cisco FMC. The policy must inspect a unique IPS policy as well as log rule matching.
Which action must be taken to meet these requirements?
A. Configure an IPS policy and enable per-rule logging.
B. Disable the default IPS policy and enable global logging.
C. Configure an IPS policy and enable global logging.
D. Disable the default IPS policy and enable per-rule logging.
Answer: (SHOW ANSWER)
To meet the requirements of inspecting a unique IPS policy as well as logging rule matching in a new access control policy using Cisco FMC, the engineer should configure an IPS policy and enable per-rule logging. Therefore, the correct answer is A: Configure an IPS policy and enable per-rule logging.

NEW QUESTION: 192
A network administrator is reviewing a monthly advanced malware risk report and notices a host that is listed as CnC Connected. Where must the administrator look within Cisco FMC to further determine if this host is infected with malware?
A. Analysis > Hosts > Indications of Compromise
B. Analysis > Files > Malware Events
C. Analysis > Hosts > Host Attributes
D. Analysis > Files > Network File Trajectory
Answer: (SHOW ANSWER)

NEW QUESTION: 193
What is an attribute of the risk reporting capability in Cisco Secure Firewall Management Center?
A. Includes all domains in a multidomain system
B. Uses the same templates available to standard reports
C. Includes the current domain in a multidomain system
D. Uses the XML format to export all reporting
Answer: (SHOW ANSWER)
Risk reports in FMC are generated per domain context and only cover the objects and events within the active (current) domain, not the entire multidomain hierarchy.

NEW QUESTION: 194
An engineer is reviewing an existing custom server fingerprint on a Cisco Secure Firewall because the current information is inaccurate. Which action must the engineer take to improve the accuracy of the network discovery rules?
A. Add NetFlow monitoring for the network segment

B. Exclude the ports that must be skipped.
C. Set one common rule to override the reports in the multidomain environment.
D. Exclude the IP address that is used to communicate with the monitored host.
Answer: (SHOW ANSWER)
To improve the accuracy of a custom server fingerprint in Cisco Secure Firewall, the engineer should exclude ports that may lead to false positives or are not representative of the actual services on the host. This helps the system focus only on relevant traffic, ensuring more precise network discovery and fingerprinting.

NEW QUESTION: 195
A network administrator notices that remote access VPN users are not reachable from inside the network. It is determined that routing is configured correctly, however return traffic is entering the firewall but not leaving it.
What is the reason for this issue?
A. A manual NAT exemption rule does not exist at the top of the NAT table.
B. An external NAT IP address is not configured.
C. An external NAT IP address is configured to match the wrong interface.
D. An object NAT exemption rule does not exist at the top of the NAT table.
Answer: (SHOW ANSWER)
NAT exemptions can only be done with manual rules before Auto/Object NAT.
https://www.cisco.com/c/en/us/support/docs/security/firepower-management-center/212702-configure-and-verify-nat-on-ftd.html

NEW QUESTION: 196
A network administrator is configuring Snort 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 "show tech" file for the device in question.
B. A "troubleshoot" file for the device in question.
C. A "troubleshoot" file for the Cisco FMC.
D. A "show tech" for the Cisco FMC.
Answer: (SHOW ANSWER)
https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-config- guide-v62/troubleshooting_the_system.html

NEW QUESTION: 197
What is a feature of Cisco AMP private cloud?
A. It supports anonymized retrieval of threat intelligence
B. It supports security intelligence filtering.
C. It disables direct connections to the public cloud.
D. It performs dynamic analysis

Answer: (SHOW ANSWER)
Connecting a Firepower Management Center to an AMP private cloud disables existing direct connections to the public AMP cloud.
https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-config- guide-v62/file_policies_and_amp_for_firepower.html

NEW QUESTION: 198
An engineer is working on a LAN switch and has noticed that its network connection to the mime Cisco IPS has gone down.
Upon troubleshooting it is determined that the switch is working as expected. What must have been implemented for this failure to occur?
A. The upstream router has a misconfigured routing protocol
B. Link-state propagation is enabled
C. The Cisco IPS has been configured to be in fail-open mode
D. The Cisco IPS is configured in detection mode
Answer: (SHOW ANSWER)
If link-state propagation is enabled on a switch, it can cause the switch to incorrectly detect a link failure, which can lead to network connectivity issues. In the case of the inline Cisco IPS, the switch may detect a link failure due to the IPS not responding to certain types of traffic, even though the IPS is functioning properly.

NEW QUESTION: 199
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: (SHOW ANSWER)
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: 200
An organization is implementing Cisco FTD using transparent mode in the network. Which rule in the default Access Control Policy ensures that this deployment does not create a loop in the network?

A. ARP inspection is enabled by default.
B. Multicast and broadcast packets are denied by default.
C. STP BPDU packets are allowed by default.
D. ARP packets are allowed by default.
Answer: (SHOW ANSWER)
https://www.cisco.com/c/en/us/td/docs/security/firepower/630/configuration/guide/fpmc-config- guide-v63/transparent_or_routed_firewall_mode_for_firepower_threat_defense.html

NEW QUESTION: 201
A security engineer is deploying Cisco Secure Endpoint to detect a zero day malware attack with an SHA-256 hash of 47ea931f3e9dc23ec0b0885a80663e30ea013d493f8e88224b570a0464084628. What must be configured in Cisco Secure Endpoint to enable the application to take action based on this hash?
A. custom detection list
B. access control rule
C. transform set
D. correlation policy

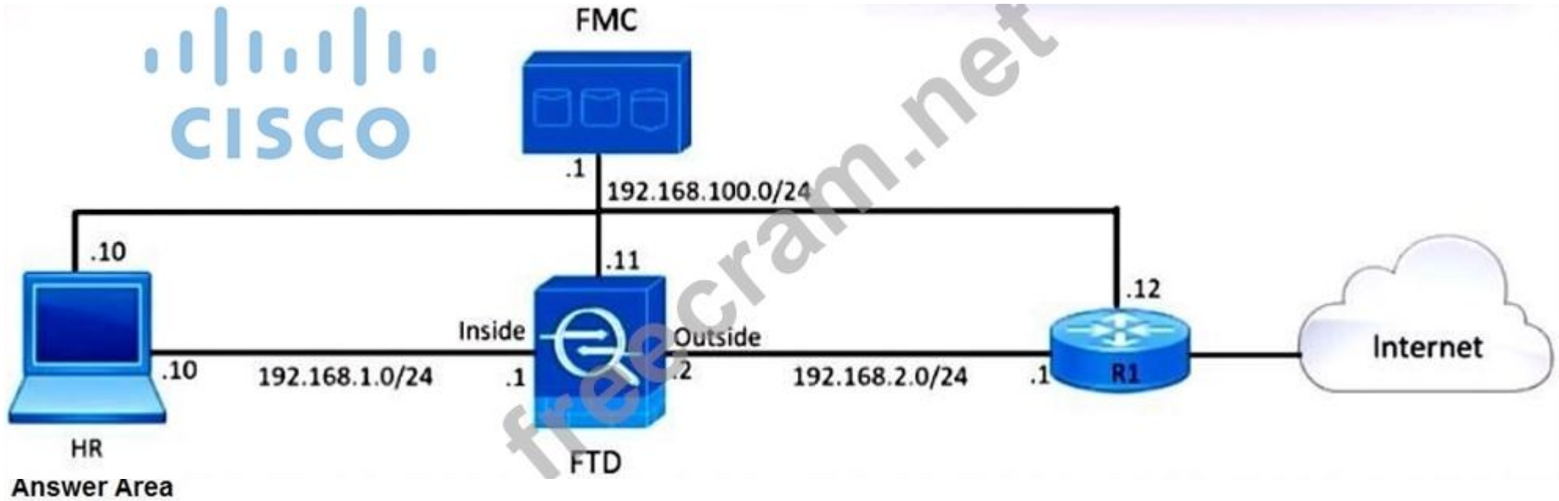
Answer: (SHOW ANSWER)

NEW QUESTION: 202
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. Update the IP addressing so that each segment is a unique IP subnet.
B. Assign a unique VLAN ID for the interface in each segment.
C. Deploy inbound ACLs on each interface to allow traffic between the segments.
D. Configure a NAT rule so that traffic between the segments is exempt from NAT.
Answer: (SHOW ANSWER)

NEW QUESTION: 203
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. prevalence
C. vulnerable software
D. file analysis
Answer: (SHOW ANSWER)

NEW QUESTION: 204
A security engineer must configure a Cisco FTD appliance to inspect traffic coming from the internet. The Internet traffic will be mirrored from the Cisco Catalyst 9300 Switch.
Which configuration accomplishes the task?
A. Set interface configuration mode to none.
B. Set the firewall mode to routed.
C. Set the firewall mode to transparent.
D. Set interface configuration mode to passive.
Answer: (SHOW ANSWER)

NEW QUESTION: 205
Drag and Drop Question
Refer to the exhibit. An engineer must create a QoS policy in Cisco Firepower Management Center to limit HTTP and HTTPS traffic from users in the HR department. The upload and download limit of the HTTP and HTTPS traffic must be set to 5 Mb/s. Drag and drop the values from the left onto the corresponding settings on the right.



Answer Area

192.168.1.0/24

192.168.2.0/24

HTTP-HTTPS

HTTP-HTTPS-QoS

5 Mb/s

Interfaces in Destination Interface Objects

Name

Apply QoS On

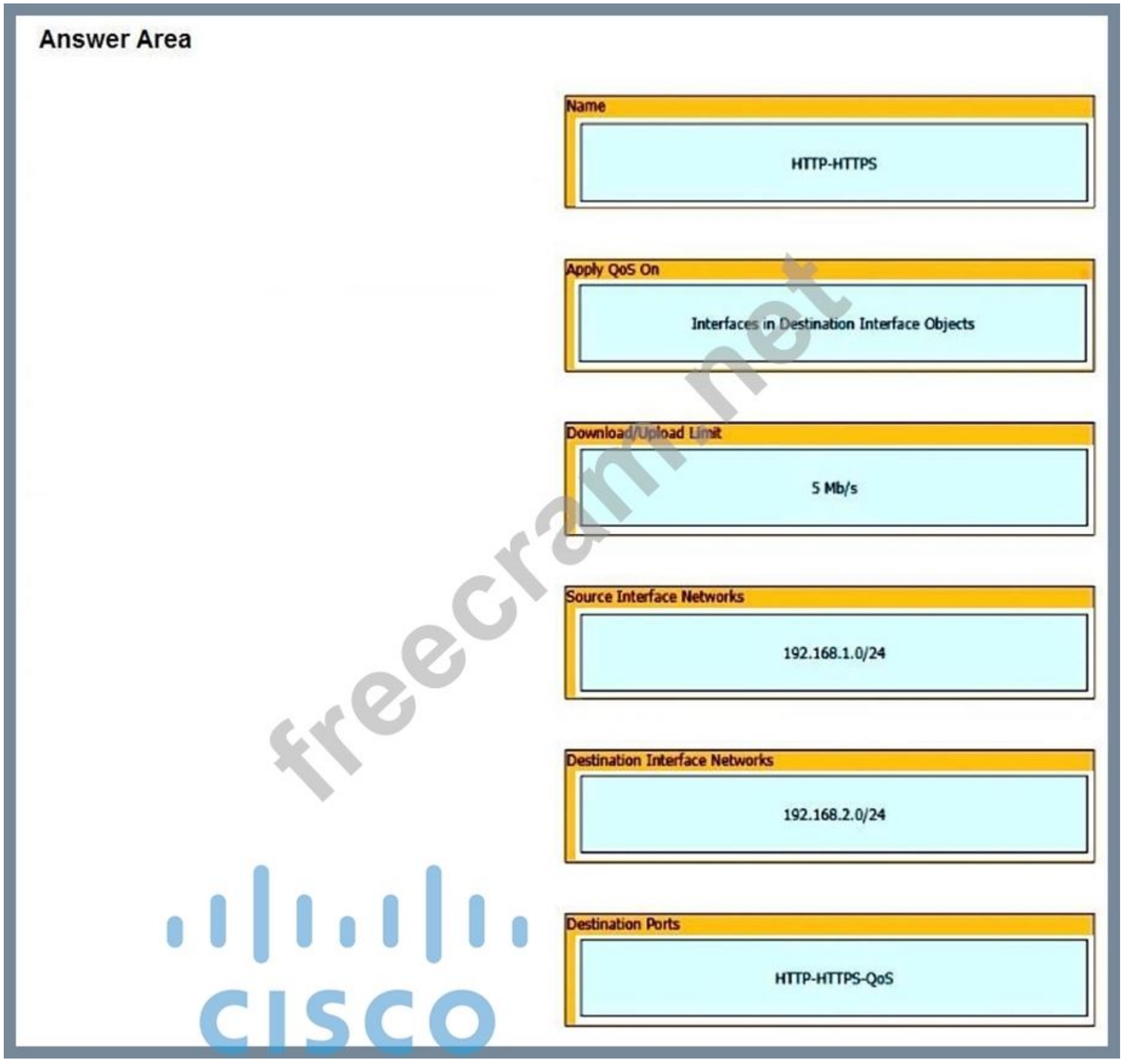
Download/Upload Limit

Source Interface Networks

Destination Interface Networks

Destination Ports

Answer:



NEW QUESTION: 206

A network administrator configured a NAT policy that translates a public IP address to an internal web server IP address.
An access policy has also been created that allows any source to reach the public IP address on port 80.

The web server is still not reachable from the Internet on port 80.
Which configuration change is needed?
A. The intrusion policy must be disabled for port 80.
B. The access policy rule must be configured for the action trust.
C. The NAT policy must be modified to translate the source IP address as well as destination IP address.
D. The access policy must allow traffic to the internal web server IP address.
Answer: (SHOW ANSWER)

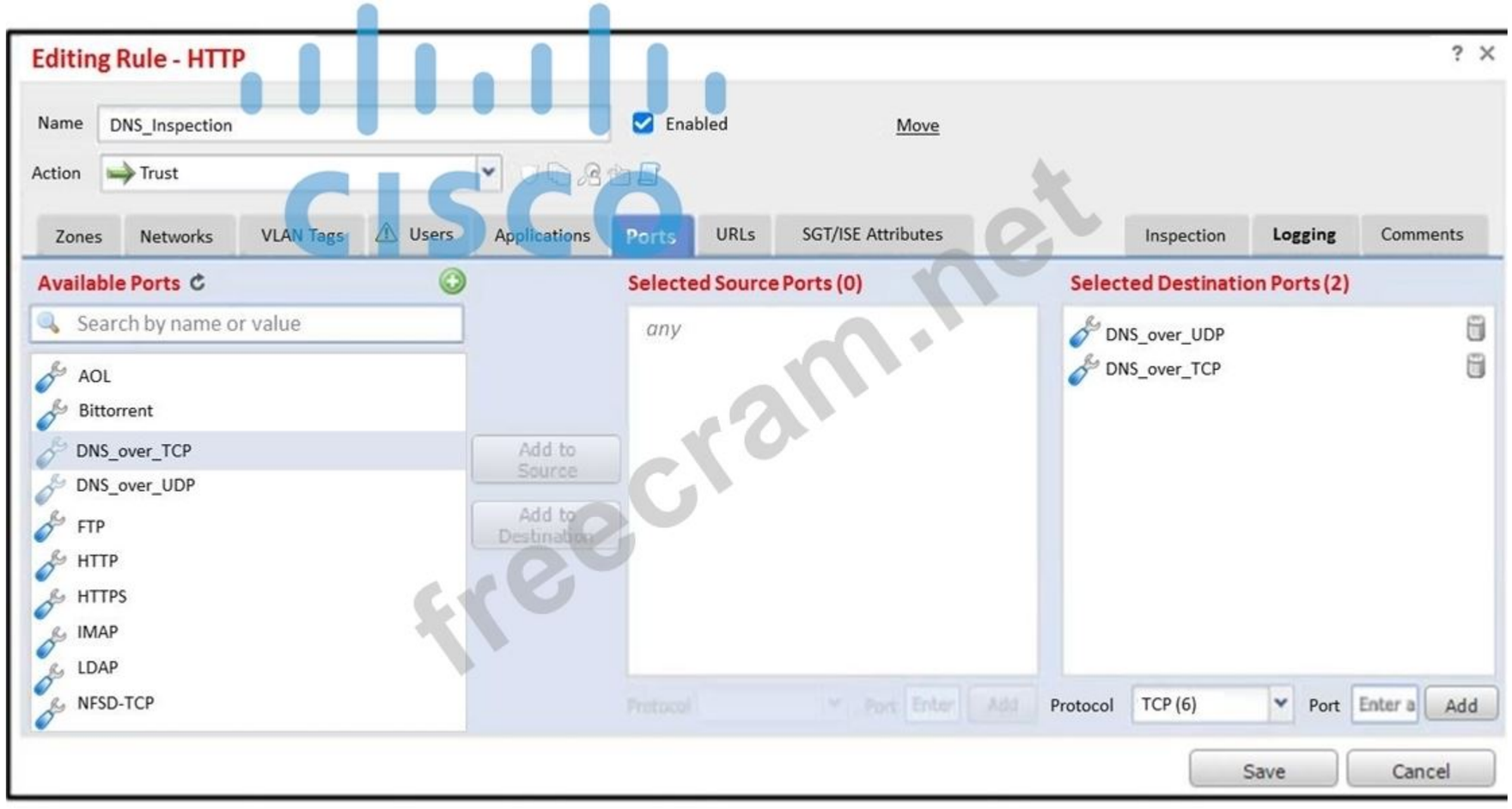
NEW QUESTION: 207
An engineer is analyzing a risk report generated by using Cisco Secure Firewall Management Center. The report contains these fields:
- Total Attacks
- Events Requiring Attention
- Hosts Targeted
- Hosts Connected to CnC Servers
Which type of risk report is the engineer analyzing-
A. attacks
B. network
C. events
D. hosts
Answer: (SHOW ANSWER)
The presence of fields like "Hosts Targeted" and "Hosts Connected to CnC Servers" indicates that this is a hosts risk report. This report focuses on host-level security posture, showing which internal systems are being attacked, are compromised, or are behaving suspiciously based on threat intelligence and traffic analysis.

NEW QUESTION: 208
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 two switch stacks without causing any interruption to network traffic? (Choose two.)
A. Set the MTU to 9198 on all interfaces to support jumbo frames.
B. Add separate routes for data and management traffic.
C. Exempt BPDUs from advanced inspection
D. Configure a BVI interface for VLAN 10.
E. Configure at least one bridge group.
Answer: (SHOW ANSWER)
In transparent mode, a Cisco Secure Firewall Threat Defense (FTD) device must be configured with:
- A Bridge Virtual Interface (BVI) for management access (e.g., VLAN 10) since it does not participate in IP routing.
- At least one bridge group to enable traffic forwarding between interfaces (i.e., the switch stacks), as transparent mode uses bridging at Layer 2 to inspect traffic.
These two actions allow the device to inspect traffic without disrupting the Layer 2 forwarding behavior of the existing network.

NEW QUESTION: 209
What is the advantage of having Cisco Firepower devices send events to Cisco Threat Response via the security services exchange portal directly as opposed to using syslog?
A. All types of Cisco Firepower devices are supported.
B. Supports all devices that are running supported versions of Cisco Firepower.

C. An on-premises proxy server does not need to be set up and maintained.
D. Cisco Firepower devices do not need to be connected to the Internet.
Answer: (SHOW ANSWER)

NEW QUESTION: 210
Refer to the exhibit. An engineer is modifying an access control policy to add a rule to inspect all DNS traffic that passes through the firewall. After making the change and deploying the policy, they see that DNS traffic is not being inspected by the Snort engine. What is the problem?



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