Cisco.300-710.v2026-03-20.q190

Exam Code:	300-710
Exam Name:	Securing Networks with Cisco Firepower
Certification Provider:	Cisco
Free Question Number:	190
Version:	v2026-03-20
# of views:	109
# of Questions views:	2369
https://www.freecram.net/torrent/Cisco.300-710.v2026-03-20.q190.html	

NEW QUESTION: 1
A network administrator must create an EtherChannel Interface on a new Cisco Firepower 9300 appliance registered with an FMC tor 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)
An EtherChannel interface is a logical interface that consists of a bundle of individual Ethernet links that act as a single network link. An EtherChannel interface can increase the bandwidth and reliability of a network connection5.
On a Cisco Firepower 9300 appliance registered with an FMC for high availability, the network administrator must create the EtherChannel interface on the FXOS CLI. The FXOS is the operating system that runs on the Firepower 9300 chassis and provides hardware management functions such as interface configuration, power supply status, fan speed control, and so on6.
To create an EtherChannel interface on the FXOS CLI, the network administrator can follow these steps5:
* Connect to the FXOS CLI using SSH or console.
* Enter scope eth-uplink command to enter Ethernet uplink mode.
* Enter create port-channel command to create an EtherChannel interface.
* Enter a port-channel ID (1-48) and a mode (on or active) for the EtherChannel interface.
* Enter add interface command to add physical interfaces to the EtherChannel interface.
* Enter one or more interface IDs (for example, 1/1) for the physical interfaces.
* Enter commit-buffer command to save the changes.
The other options are incorrect because:

* The FMC CLI does not provide any commands to create an EtherChannel interface on a Firepower 9300 appliance. The FMC CLI is mainly used for managing FMC settings such as backup, restore, upgrade, troubleshoot, and so on7.
* The FTD CLI does not provide any commands to create an EtherChannel interface on a Firepower 9300 appliance. The FTD CLI is mainly used for managing FTD settings such as routing, NAT, VPN, access control, and so on8.
* The FMC GUI does not provide any options to create an EtherChannel interface on a Firepower 9300 appliance. The FMC GUI is mainly used for managing FTD policies such as access control, intrusion, file, malware, and so on9.

NEW QUESTION: 2
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)
When you configure the Cisco Firepower devices to bypass the access control policies for VPN traffic, the devices will not inspect the VPN traffic and thus will not waste resources on it. This is the best option to ensure that the VPN traffic is not wasting resources on the Cisco Firepower devices.
Reference:https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/219759-configure-bypass- policies-on-the-cisco-firepow.html

NEW QUESTION: 3
An engineer must replace a Cisco Secure Firewall high-availability device due to a failure. When the replacement device arrives, the engineer must separate the high-availability pair from Cisco Secure Firewall Management Center Which action must the engineer take first to restore high availability?
A. Register the secondary device
B. Force a break between the devices.
C. Unregister the secondary device.
D. Configure NTP time synchronization.
Answer: (SHOW ANSWER)
When replacing a Cisco Secure Firewall high-availability (HA) device due to a failure, the first step the engineer must take is to unregister the secondary (failed) device from the Cisco Secure Firewall Management Center (FMC). This action separates the HA pair and ensures that the new replacement device can be registered and configured correctly.

Steps:
* Access the FMC and navigate to the device management section.
* Unregister the failed secondary device to remove it from the HA pair.
* Register the replacement device to the FMC.
* Reconfigure the HA settings to restore the high-availability configuration.
By unregistering the failed device first, the engineer ensures a clean setup for the replacement device, avoiding potential conflicts or issues in the HA configuration.
References: Cisco Secure Firewall Management Center Administrator Guide, Chapter on High Availability Configuration.

NEW QUESTION: 4
An engineer is configuring a Cisco IPS to protect the network and wants to test a policy before deploying it. A copy of each incoming packet needs to be monitored while traffic flow remains constant. Which IPS mode should be implemented to meet these requirements?
A. Inline tap
B. passive
C. routed
D. transparent
Answer: (SHOW ANSWER)

NEW QUESTION: 5
An engineer must export a packet capture from Cisco Secure Firewall Management Center to assist in troubleshooting an issue an a Secure Firewall Threat Defense device. When the engineer navigates to URL for Secure Firewall Management Center at:
..<FMC IP>/capture/CAP/pcap/sample.pcap
An engineer receives a 403: Forbidden error instead of being provided with the PCAP file. Which action resolves the issue?
A. Disable the HTTPS server and use HTTP.
B. Enable the proxy setting in the device platform policy.
C. Enable HTTPS in the device platform policy.
D. Disable the proxy setting on the client browser.
Answer: (SHOW ANSWER)
If an engineer receives a 403: Forbidden error when attempting to download a packet capture file from Cisco Secure Firewall Management Center (FMC), the issue is likely due to HTTPS not being enabled in the device platform policy. To resolve this issue, the engineer must enable HTTPS in the platform policy.
Steps:
* In FMC, navigate to Policies > Device Management > Platform Settings.
* Edit the relevant platform policy.
* Enable HTTPS for the device.
* Deploy the changes to the FTD device.

This ensures that the FMC and FTD device can securely transfer the packet capture file over HTTPS, resolving the 403 error.
References: Cisco Secure Firewall Management Center Administrator Guide, Chapter on Platform Settings and HTTPS Configuration.

NEW QUESTION: 6
Which feature is supported by IRB on Cisco FTD devices?
A. redundant interface
B. high-availability cluster
C. dynamic routing protocol
D. EtherChannel interface
Answer: (SHOW ANSWER)

NEW QUESTION: 7
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_Send_Destination object to the configuration
B. Create a Security Intelligence object to send the data to Cisco Stealthwatch
C. Create a service identifier to enable the NetFlow service
D. Add the NetFlow_Add_Destination object to the configuration
Answer: (SHOW ANSWER)
Cisco Firepower uses FlexConfig objects to send NetFlow data. Here's the key point:
NetFlow_Set_Parameters object: Defines the parameters of the NetFlow data being exported (e.g., version, sampling rate).
NetFlow_Add_Destination object: Specifies the IP address and port of the flow collector (in this case, your Cisco Stealthwatch appliance) where the NetFlow data should be sent.

NEW QUESTION: 8
An administrator is configuring the interface of a Cisco Secure Firewall Threat Defense device in a passive IPS deployment. The device and interface have been identified. Which set of configuration steps of the administrator take next to complete the implementation?
A. Set the interface mode to passive. Associate the interface with a security zone. Set the MTU parameter.
Reset the interface.
B. Modify the interface to retransmit received traffic. Associate the interface with a security zone Enable the interface. Sat the MTU parameter.
C. Modify the interface to retransmit received traffic. Associate the interface with a security zone. Set the MTU parameter.
D. Set the interface mode to passive. Associate the interface with a security zone. Enable the interface. Set the MTU parameter.

Answer: (SHOW ANSWER)

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

Steps:

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

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

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

NEW QUESTION: 9

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

(Choose two.)

A. Directory password

B. Active directory primary domain

C. Active directory join password

D. Active directory join username

E. Directory username

Answer: (SHOW ANSWER)

NEW QUESTION: 10

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

C. Link-state propagation is enabled

D. The Cisco IPS is configured in detection mode

Answer: (SHOW ANSWER)

NEW QUESTION: 11
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: 12
An engineer is configuring Cisco Security Devices by using Cisco Secure Firewall Management Center.
Which configuration command must be run to compare the CA certificate bundle on the local system to the latest CA bundle from the Cisco server?
A. configure cert-update run-now
B. configure cert-update compare
C. configure cert-update auto-update enable
D. configure cert-update test
Answer: (SHOW ANSWER)

NEW QUESTION: 13
An engineer must integrate a thud-party security Intelligence teed with Cisco Secure Firewall Management Center. Secure Firewall Management Center is running Version 6.2 3 and has 8 GB of memory. Which two actions must be taken to implement Throat Intelligence Director? (Choose two.)

A. Upgrade to version 6.6.
B. Enable REST API access.
C. Add the URL of the TAXII server.
D. Add 7 GB of memory.
E. Add a TAXII server
Answer: (SHOW ANSWER)
To integrate a third-party security intelligence feed with Cisco Secure Firewall Management Center (FMC) using Threat Intelligence Director (TID), the following actions are necessary:
Upgrade to version 6.6:The FMC must be running at least version 6.6 to support Threat Intelligence Director.
Version 6.2.3 does not support the necessary features for this integration.
Add the URL of the TAXII server:Threat Intelligence Director uses TAXII (Trusted Automated eXchange of Indicator Information) to pull threat intelligence data from third-party sources. The URL of the TAXII server must be added to the TID configuration in FMC.
Steps:
Upgrade FMC to version 6.6 or later.
In FMC, navigate toIntegration > Threat Intelligence Director.
Add a new TAXII server by entering the URL of the TAXII server.
These actions enable the integration of third-party threat intelligence feeds, enhancing the security capabilities of the FMC.
References:Cisco Secure Firewall Management Center Administrator Guide, Chapter on Threat Intelligence Director.

NEW QUESTION: 14
An engineer is investigating connectivity problems on Cisco Firepower for a specific SGT. Which command allows the engineer to capture real packets that pass through the firewall using an SGT of 64?
A. capture CAP match 64 type inline-tag ip any any
B. capture CAP headers-only type inline-tag 64 match ip any any
C. capture CAP type inline-tag 64 match ip any any
D. capture CAP buffer 64 match ip any any
Answer: (SHOW ANSWER)

NEW QUESTION: 15
An analyst using the security analyst account permissions is trying to view the Correlations Events Widget but is not able to access it. However, other dashboards are accessible. Why is this occurring?
A. An API restriction within the Cisco FMC is preventing the widget from displaying.
B. The widget is configured to display only when active events are present.
C. The security analyst role does not have permission to view this widget.
D. The widget is not configured within the Cisco FMC.

Answer: (SHOW ANSWER)

NEW QUESTION: 16
Which command is entered in the Cisco FMC CLI to generate a troubleshooting file?
A. show running-config
B. show tech-support chassis
C. system support diagnostic-cli
D. sudo sf_troubleshoot.pl
Answer: (SHOW ANSWER)
Reference: https://www.cisco.com/c/en/us/support/docs/security/sourcefire-defense-center/117663-technote- SourceFire-00.html

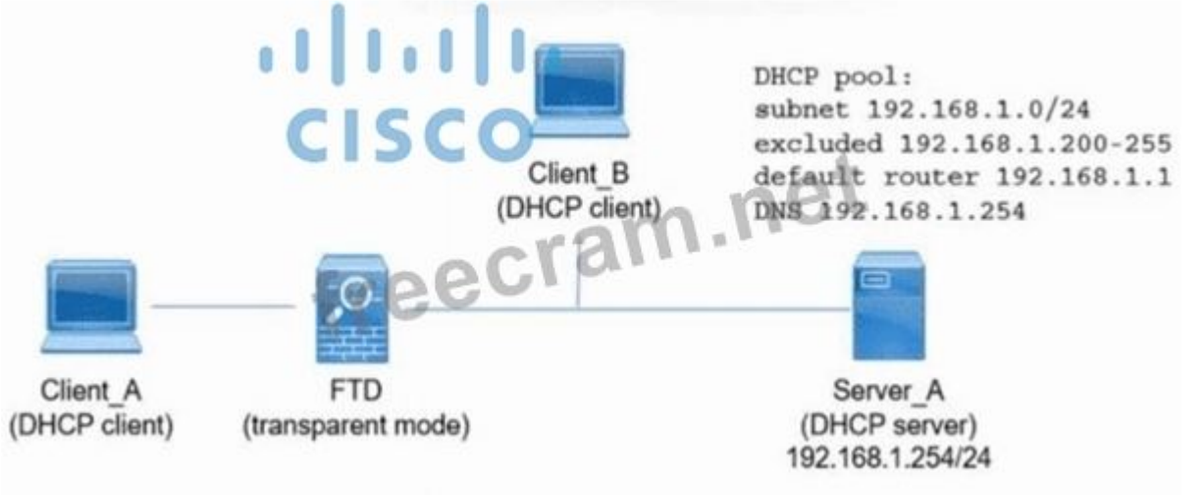
NEW QUESTION: 17
Which two statements about deleting and re-adding a device to Cisco FMC are true? (Choose two.)
A. An option to re-apply NAT and VPN policies during registration is available, so users do not need to re- apply the policies after registration is completed.
B. Before re-adding the device in Cisco FMC, you must add the manager back in the device.
C. No option to delete and re-add a device is available in the Cisco FMC web interface.
D. The Cisco FMC web interface prompts users to re-apply access control policies.
E. 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)
Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config- guide- v60/Device_Management_Basics.html

NEW QUESTION: 18
Refer to the exhibit.
A systems administrator conducts a connectivity test to their SCCM server from a host machine and gets no response from the server. Which action ensures that the ping packets reach the destination and that the host receives replies?
A. Create an ICMP allow list and add the ICMP destination to remove it from the implicit deny list.

B. Modify the Snort rules to allow ICMP traffic.
C. Configure a custom Snort signature to allow ICMP traffic after Inspection.
D. Create an access control policy rule that allows ICMP traffic.
Answer: (SHOW ANSWER)

NEW QUESTION: 19
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. leaf domain
B. second-level domain
C. subdomain
D. global domain
Answer: (SHOW ANSWER)

NEW QUESTION: 20
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)
Reference: https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/212330-firepower- management-center-display-acc.html

NEW QUESTION: 21


Refer to the exhibit. An engineer is deploying a new instance of Cisco Secure Firewall Threat Defense. Which action must the engineer take next so that Client_A and Client_B receive an IP address via DHCP from Server_A?
A. Disable all the DHCP Snort rules by using Secure Firewall Device Manager.

B. Add access rules that allow DHCP traffic by using Cisco Secure Firewall Management Center.
C. Disable Option 82 in the DHCP relay configuration properties using Secure Firewall Management Center.
D. Add another DHCP pool on Server_A with DHCP relay on Secure Firewall Threat Defense.
Answer: (SHOW ANSWER)

NEW QUESTION: 22
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. Exclude the ports that must be skipped.
B. Set one common rule to override the reports in the multidomain environment.
C. Exclude the IP address that is used to communicate with the monitored host.
D. Add NetFlow monitoring for the network segment.
Answer: (SHOW ANSWER)

NEW QUESTION: 23
An engineer is troubleshooting an intermittent connectivity issue on a Cisco Secure Firewall Threat Defense appliance and must collect 24 hours worth of data. The engineer started a packet capture, however it stops prematurely during this time period. The engineer notices that the packet capture buffer size is set to the default of 32 MB. Which buffer size is the maximum that the engineer must set to enable the packet capture to run successfully?
A. 100 GB
B. 64 MB
C. 1 GB
D. 10 GB
Answer: (SHOW ANSWER)

NEW QUESTION: 24
A network administrator is configuring a site-to-site IPsec VPN to a router sitting behind a Cisco FTD. The administrator has configured an access policy to allow traffic to this device on UDP 500, 4500, and ESP VPN traffic is not working. Which action resolves this issue?
A. Change the access policy to allow all ports.
B. Set the allow action in the access policy to trust.
C. Enable IPsec inspection on the access policy.
D. Modify the NAT policy to use the interface PAT.
Answer: (SHOW ANSWER)

NEW QUESTION: 25
Which protocol is needed to exchange threat details in rapid threat containment on Cisco FMC?
A. pxGrid

B. SGT
C. SNMP v3
D. BFD
Answer: (SHOW ANSWER)

NEW QUESTION: 26
A network engineer is receiving reports of users randomly getting disconnected from their corporate applications which traverses the data center FTD appliance Network monitoring tools show that the FTD appliance utilization is peaking above 90% of total capacity. What must be done in order to further analyze this issue?
A. Use the Packet Tracer feature for traffic policy analysis
B. Use the Packet Export feature to save data onto external drives
C. Use the Packet Analysis feature for capturing network data
D. Use the Packet Capture feature to collect real-time network traffic
Answer: (SHOW ANSWER)

NEW QUESTION: 27
Which command-line mode is supported from the Cisco Firepower Management Center CLI?
A. privileged
B. user
C. configuration
D. admin
Answer: (SHOW ANSWER)
Reference:
https://www.cisco.com/c/en/us/td/docs/security/firepower/660/configuration/guide/fpmc-config-guide-v66/command_line_reference.pdf

NEW QUESTION: 28
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: (SHOW ANSWER)
Reference:
https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-config-guide-v62/troubleshooting_the_system.html

NEW QUESTION: 29
When packet capture is used on a Cisco Secure Firewall Threat Defense device and the packet flow is wailing on the malware query, which Snort verdict appears?

A. retry
B. replace
C. block
D. blocfcflow
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.
References: Cisco Secure Firewall Management Center Administrator Guide, Chapter on Packet Capture and Malware Inspection.

NEW QUESTION: 30
A network administrator is configuring an instance of Cisco Secure Firewall Threat Defense, which is registered to Cisco Secure Firewall Management Center, to prevent internal users from downloading executable files from the internet. What must be created and configured by the administrator to meet the requirement?

A. file policy that blocks downloads of all executable files and applies the file policy to the default action in the access policy
B. access policy rule that allows users to reach the internet with a second rule that blocks application executables
C. file policy rule that allows users to reach the internet with a second rule applied that blocks application use of FTP
D. access policy rule that allows users to reach the internet and assigns a file policy that blocks executable downloads to the rule
Answer: (SHOW ANSWER)

NEW QUESTION: 31
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 the 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: C (LEAVE A REPLY)

Reference:https://www.cisco.com/c/en/us/td/docs/security/firepower/640/fdm/fptd-fdm-config-guide-640/fptd- fdm-identity.html#concept_655B055575E04CA49B10186DEBDA301A

NEW QUESTION: 32
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. multi-instance
B. single-context
C. multiple deployment
D. single deployment
Answer: (SHOW ANSWER)

NEW QUESTION: 33
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. filter
C. title
D. results
Answer: (SHOW ANSWER)
When configuring a custom widget on a dashboard within Cisco Secure Firewall Management Center (FMC), it is mandatory to provide a title for the system to display the information correctly. The title helps in identifying and organizing the widget on the dashboard.
Steps:
* Navigate to the dashboard section in FMC.
* Add a new custom widget.
* Configure the widget settings and provide a title.
* Save and apply the widget to the dashboard.

Providing a title ensures that the widget is correctly displayed and easily identifiable on the dashboard.
References: Cisco Secure Firewall Management Center User Guide, Chapter on Dashboard and Custom Widgets.

NEW QUESTION: 34
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)
Reference:
https://www.cisco.com/c/en/us/td/docs/security/firepower/601/configuration/guide/fpmc-config-guide-v601/fpmc-config-guide-v60_chapter_01100011.html#ID-2101-0000000e

NEW QUESTION: 35
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. FTD has no NAT policy that allows outside to outside communication
C. The Enable Spoke to Spoke Connectivity through Hub option is not selected on FTD.
D. Split tunneling is enabled for the Remote Access VPN on FTD
Answer: (SHOW ANSWER)

NEW QUESTION: 36
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 network-options command to fine tune the policy.
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 application-identification-debug command to determine which rules the traffic matching and modify the rule accordingly
Answer: (SHOW ANSWER)

NEW QUESTION: 37
What is a characteristic of bridge groups on a Cisco FTD?
A. Routing between bridge groups is achieved only with a router-on-a-stick configuration on a connected router
B. In routed firewall mode, routing between bridge groups is supported.
C. In transparent firewall mode, routing between bridge groups is supported
D. In routed firewall mode, routing between bridge groups must pass through a routed interface.
Answer: (SHOW ANSWER)

NEW QUESTION: 38
With a recent summer time change, system logs are showing activity that occurred to be an hour behind real time Which action should be taken to resolve this issue?
A. Configure the system clock settings to use NTP with Daylight Savings checked
B. Configure the system clock settings to use NTP
C. Manually adjust the time to the correct hour on all managed devices
D. Manually adjust the time to the correct hour on the Cisco FMC.
Answer: (SHOW ANSWER)

NEW QUESTION: 39
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)
Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config- guide-v60/Access_Control_Using_Intrusion_and_File_Policies.html

NEW QUESTION: 40
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. ERSPAN Passive mode
B. Inline Pair mode
C. Passive mode
D. Inline Pair in Tap mode
Answer: C (LEAVE A REPLY)

NEW QUESTION: 41

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

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.

Answer:

Explanation:

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

NEW QUESTION: 42
An engineer must configure email notifications on Cisco Secure Firewall Management Center. TLS encryption must be used to protect the messages from unauthorized access. The engineer adds the IP address of the mail relay host and must set the port number. Which TCP port must the engineer use?
A. 587
B. 25
C. 389
D. 465
Answer: (SHOW ANSWER)

NEW QUESTION: 43
An organization is migrating their Cisco ASA devices running in multicontext mode to Cisco FTD devices.
Which action must be taken to ensure that each context on the Cisco ASA is logically separated in the Cisco FTD devices?
A. Configure a container instance in the Cisco FTD for each context in the Cisco ASA.
B. Add the Cisco FTD device to the Cisco ASA port channels.
C. Configure the Cisco FTD to use port channels spanning multiple networks.
D. Add a native instance to distribute traffic to each Cisco FTD context.
Answer: (SHOW ANSWER)

NEW QUESTION: 44
What is an attribute of the risk reporting capability in Cisco Secure Firewall Management Center?
A. Includes the current domain in a multidomain system
B. Includes all domains in a multidomain system
C. Uses the XML format to export all reporting
D. Uses the same templates available to standard reports
Answer: (SHOW ANSWER)

NEW QUESTION: 45
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 the firewall mode to transparent.
B. Set the firewall mode to routed.
C. Set interface configuration mode to passive.
D. Set interface configuration mode to none.
Answer: (SHOW ANSWER)

NEW QUESTION: 46
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. Security Intelligence Statistics dashboard set to Show the Last option to one day
C. Events by priority and classification and set a sliding time window of one day
D. Reports with a daily recurring task that generates based on the network risk report template
Answer: (SHOW ANSWER)

NEW QUESTION: 47
Which default action setting in a Cisco FTD Access Control Policy allows all traffic from an undefined application to pass without Snort Inspection?
A. Trust All Traffic
B. Inherit from Base Policy
C. Network Discovery Only
D. Intrusion Prevention
Answer: (SHOW ANSWER)
The default action setting in a Cisco FTD Access Control Policy determines how the system handles and logs traffic that is not handled by any other access control configuration. The default action can block or trust all traffic without further inspection, or inspect traffic for intrusions and discovery data3.
The Trust All Traffic option allows all traffic from an undefined application to pass without Snort inspection.
This option also disables Security Intelligence filtering, file and malware inspection, and URL filtering for all traffic handled by the default action. This option is useful when you want to minimize the performance impact of access control on your network3.
The other options are incorrect because:
* The Inherit from Base Policy option inherits the default action setting from the base policy. The base policy is the predefined access control policy that you use as a starting point for creating

your own policies. Depending on which base policy you choose, the inherited default action setting can be different3.
* The Network Discovery Only option inspects all traffic for discovery data only. This option enables Security Intelligence filtering for all traffic handled by the default action, but disables file and malware inspection, URL filtering, and intrusion inspection. This option is useful when you want to collect information about your network before you configure access control rules3.
* The Intrusion Prevention option inspects all traffic for intrusions and discovery data. This option enables Security Intelligence filtering, file and malware inspection, URL filtering, and intrusion inspection for all traffic handled by the default action. This option provides the most comprehensive protection for your network, but also has the most performance impact3.

NEW QUESTION: 48

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?
A. Verify that the proxy server can use HTTPS to communicate to the internet.
B. Bypass the proxy server for intelligence.sourcefire.com.
C. Ensure that proxy authentication is disabled for the Cisco Secure Firewall Management Center device.
D. Install a self-signed certificate on the proxy server for intelligence.sourcefire.com.
Answer: (SHOW ANSWER)

NEW QUESTION: 49
What is the role of the casebook feature in Cisco Threat Response?
A. sharing threat analysts
B. pulling data via the browser extension
C. triage automaton with alerting
D. alert prioritization
Answer: (SHOW ANSWER)
The casebook and pivot menu are widgets available in Cisco Threat Response. Casebook - It is used to record, organize, and share sets of observables of interest primarily during an investigation and threat analysis. You can use a casebook to get the current verdicts or dispositions on the observables.
https://www.cisco.com/c/en/us/td/docs/security/ces/user_guide/esa_user_guide_13-5-1/b_ESA_Admin_Guide_ces_13-5-1/b_ESA_Admin_Guide_13-0_chapter_0110001.pdf

NEW QUESTION: 50

Which license type is required on Cisco ISE to integrate with Cisco FMC pxGrid?

A. mobility

B. apex

C. base

D. plus

Answer: D (LEAVE A REPLY)

NEW QUESTION: 51

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

A. integrated routing and bridging

B. interface-based VLAN switching

C. inter-chassis clustering VLAN

D. Cisco ISE Security Group Tag

Answer: (SHOW ANSWER)

NEW QUESTION: 52

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

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

What must do configured to meet the requirements"

A. capacity handling

B. Spero analysis

C. dynamic analysis

D. local malware analysis

Answer: (SHOW ANSWER)

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

Steps to configure local malware analysis:

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

* Apply the policy to the relevant access control policy.
This configuration ensures that the specified file types are analyzed locally, meeting the requirement to avoid sending them to Cisco Secure Malware Analytics.
References: Cisco Secure Firewall Management Center Configuration Guide, Chapter on Malware and File Policies

NEW QUESTION: 53
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 M 68.1.0/24 from its routing table when the cable between routed R1 and the Secure FTD device Is disconnected. Which action must the engineer take?
1
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.
References:Cisco Secure Firewall Threat Defense Configuration Guide, Chapter on Interface Settings and Link State Propagation.

NEW QUESTION: 54
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. Secure Endpoint Cloud Connection
B. security group tag
C. Smart Software Manager Satellite
D. internet connection
E. Cisco Success Network
Answer: (SHOW ANSWER)

NEW QUESTION: 55
What is the role of realms in the Cisco ISE and Cisco FMC integration?
A. AD definition
B. TACACS+ database
C. Cisco ISE context
D. Cisco Secure Firewall VDC
Answer: (SHOW ANSWER)
In the integration between Cisco Identity Services Engine (ISE) and Cisco Firewall Management Center (FMC), realms are used to define the Active Directory (AD) configuration. Realms in FMC specify the AD servers, domain, and other authentication settings necessary to authenticate and authorize users.
Steps to configure realms:
* In FMC, navigate to System > Integration > Realms and Directory.
* Add a new realm and configure the AD settings.
* Ensure the realm settings match the AD environment for seamless integration.
Realms are essential for integrating AD with FMC, allowing the firewall to use AD for user authentication and policy enforcement.
References: Cisco Secure Firewall Management Center Administrator Guide, Chapter on Realms and Directory Integration.

NEW QUESTION: 56
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. Define the path to the individual webpage that uses HTTPS.
B. Use the subject common name from the website certificate
C. Use the FQDN including the subdomain for the website
D. Specify the protocol to match (HTTP or HTTPS).
Answer: (SHOW ANSWER)

NEW QUESTION: 57

```
admin@FirePOWER:~$ ntpq -pn
     remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
 *198.51.100.200  .INIT.          16 u    -   1024    0     0.000    0.000   0.000
```

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

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

NEW QUESTION: 58
An engineer must configure a Cisco FMC dashboard in a child domain. Which action must be taken so that the dashboard is visible to the parent domain?
A. Add a separate widget.
B. Create a copy of the dashboard.
C. Adjust policy inheritance settings.
D. Add a separate tab.
Answer: (SHOW ANSWER)

NEW QUESTION: 59
An administrator needs to configure Cisco FMC to send a notification email when a data transfer larger than
10 MB is initiated from an internal host outside of standard business hours. Which Cisco FMC feature must be configured to accomplish this task?
A. intrusion policy
B. correlation policy
C. file and malware policy
D. application detector
Answer: (SHOW ANSWER)

NEW QUESTION: 60
An organization does not want to use the default Cisco Firepower block page when blocking HTTP traffic.
The organization wants to include information about its policies and procedures to help educate the users whenever a block occurs. Which two steps must be taken to meet these requirements? (Choose two.)

A. Edit the HTTP request handling in the access control policy to customized block.
B. Modify the system-provided block page result using Python.
C. Create HTML code with the information for the policies and procedures.
D. Write CSS code with the information for the policies and procedures.
E. Change the HTTP response in the access control policy to custom.
Answer: (SHOW ANSWER)

NEW QUESTION: 61
Refer to the exhibit.

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

NEW QUESTION: 62
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)
Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config- guide- v60/Working_with_Reports.html

NEW QUESTION: 63
Which two considerations must be made when deleting and re-adding devices while managing them via Cisco FMC (Choose two).
A. The Cisco FMC web interface prompts users to re-apply access control policies.
B. Before re-adding the device In Cisco FMC, the manager must be added back.
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)

NEW QUESTION: 64
An administrator is configuring their transparent Cisco FTD device to receive ERSPAN traffic from multiple switches on a passive port, but the Cisco FTD is not processing the traffic. What is the problem?
A. The switches were not set up with a monitor session ID that matches the flow ID defined on the Cisco FTD.
B. The Cisco FTD must be configured with an ERSPAN port not a passive port.
C. The switches do not have Layer 3 connectivity to the FTD device for GRE traffic transmission.
D. The Cisco FTD must be in routed mode to process ERSPAN traffic.
Answer: (SHOW ANSWER)

NEW QUESTION: 65
A network administrator reviews the file report for the last month and notices that all file types, except exe.
show a disposition of unknown. What is the cause of this issue?
A. The malware license has not been applied to the Cisco FTD.
B. The Cisco FMC cannot reach the Internet to analyze files.
C. A file policy has not been applied to the access policy.
D. Only Spero file analysis is enabled.
Answer: (SHOW ANSWER)
A file policy defines the actions that the Cisco Firepower Threat Defense (FTD) device should take when it encounters different types of files. The file policy is applied as part of an access control policy. If an access control policy does not include a file policy, the FTD device will not

take any action on the files it encounters, resulting in a disposition of "unknown" for all file types except exe.
Reference:https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/219759-configure-bypass- policies-on-the-cisco-firepow.html

NEW QUESTION: 66
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. Dereglster the FTD device from FMC and configure transparent mode via the CLI.
B. Assign an IP address to two physical interfaces.
C. Add a Bridge Group Interface to the FTD before transparent mode is configured.
D. Obtain an FTD model that supports transparent mode.
Answer: (SHOW ANSWER)

NEW QUESTION: 67
After using Firepower for some time and learning about how it interacts with the network, an administrator is trying to correlate malicious activity with a user Which widget should be configured to provide this visibility on the Cisco Firepower dashboards?
A. Current Status
B. Current Sessions
C. Correlation Events
D. Custom Analysis
Answer: (SHOW ANSWER)

NEW QUESTION: 68
Network users are experiencing Intermittent issues with internet access. An engineer ident med mat 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. Configure fallthrough to interface PAT on 'he Advanced tab.
C. Convert the dynamic auto NAT rule to dynamic manual NAT.
D. Add an identity NAT rule to handle the overflow of users.
Answer: (SHOW ANSWER)
Fallthrough to interface PAT is a feature that allows the dynamic NAT configuration to use the interface IP address as a last resort when the NAT pool is exhausted. This way, more users can access the internet without running out of resources. To enable this feature, the engineer must check the Enable PAT Fallback check box on the Advanced tab of the NAT rule editor1

NEW QUESTION: 69
An administrator receives reports that users cannot access a cloud-hosted web server. The access control policy was recently updated with several new policy additions and URL filtering.

What must be done to troubleshoot the issue and restore access without sacrificing the organization's security posture?

A. Download a PCAP of the traffic attempts to verify the blocks and use the flexconfig objects to create a rule that allows only the required traffic to the destination server.

B. Verify the blocks using the packet capture tool and create a rule with the action monitor for the traffic.

C. Identify the blocked traffic in the Cisco FMC connection events to validate the block, and modify the policy to allow the traffic to the web server.

D. Create a new access control policy rule to allow ports 80 and 443 to the FQDN of the web server.

Answer: (SHOW ANSWER)

NEW QUESTION: 70

A network engineer must monitor threat events from the console of Cisco Secure Firewall Management Center. The engineer integrates the Cisco Secure Firewall Malware Defense in Secure Firewall Management Center. Which action must the engineer take next?

A. Log in to Secure Endpoint, click Allow to authorize the Secure Firewall Malware Defense to Secure FMC connection, add a Secure Firewall Malware Defense cloud connection to Secure FMC, and select the Secure Firewall Malware Defense cloud for Secure Endpoint.

B. Log in to Cisco Secure Endpoint, click Allow to authorize the Secure Firewall Malware Defense to Secure FMC connection, and add a Secure Firewall Malware Defense cloud connection to Secure FMC.

C. Add a Secure Firewall Malware Defense cloud connection in Secure FMC, log in to Secure Endpoint, and click Allow to authorize the Secure Firewall Malware Defense to Secure FMC connection.

D. Add a Secure Firewall Malware Defense cloud connection in Secure FMC, select the Secure Firewall Malware Defense cloud for Secure Endpoint, log in to Secure Endpoint, and click Allow to authorize the Secure Firewall Malware Defense to Secure FMC connection.

Answer: (SHOW ANSWER)

NEW QUESTION: 71

An engineer is implementing a new Cisco Secure Firewall. The firewall must filler traffic between the three subnets:

* LAN 192.168.101.0724
* DMZ 192.168 200.0/24
* WAN 10.0.0.0/30

Which firewall mode must the engineer implement?

A. transparent

B. network

C. routed

D. gateway

Answer: (SHOW ANSWER)

To filter traffic between multiple subnets, the engineer must implement the firewall in routed mode. In routed mode, the firewall operates as a Layer 3 device, capable of routing traffic between different IP subnets. This mode is appropriate for filtering traffic between LAN, DMZ, and WAN subnets.

Steps to configure routed mode:

* Access the firewall's management interface.
* Configure interfaces for each subnet (LAN, DMZ, WAN) with appropriate IP addresses and network masks.
* Define security zones and apply access control policies to filter traffic as required.

This ensures that the firewall can inspect and route traffic between the different subnets, providing the necessary security and control.

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

NEW QUESTION: 72

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.

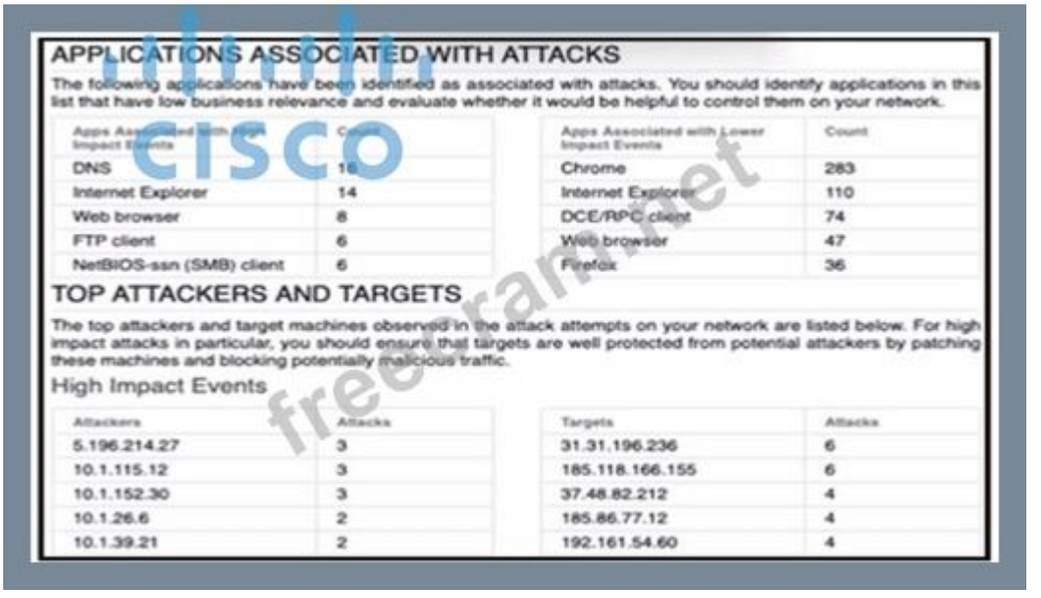
B. Ensure that both servers are in the same bridge domain.

C. Assign the same subnet to both servers.

D. Enable both servers to share the same VXLAN segment.

Answer: (SHOW ANSWER)

NEW QUESTION: 73



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	Apps Associated with Lower Impact Events	Count
DNS	16	Chrome	283
Internet Explorer	14	Internet Explorer	110
Web browser	8	DCE/RPC client	74
FTP client	6	Web browser	47
NetBIOS-ssn (SMB) client	6	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	Targets	Attacks
5.196.214.27	3	31.31.196.236	6
10.1.115.12	3	185.118.166.155	6
10.1.152.30	3	37.48.82.212	4
10.1.26.6	2	185.86.77.12	4
10.1.39.21	2	192.161.54.60	4

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?

A. Inspect DNS traffic

B. Block NetBIOS.

C. Block Internal Explorer

D. Inspect TCP port 80 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.

References:Cisco Secure Firewall Management Center Administrator Guide, Chapter on DNS Security and Traffic Inspection.

NEW QUESTION: 74

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. LUA script

D. Python program

Answer: (SHOW ANSWER)

A custom application detector is a user-defined script that can detect web applications, clients, and application protocols based on patterns in network traffic. Custom application detectors are written in LUA, which is a lightweight and embeddable scripting language. LUA scripts can use predefined functions and variables provided by the Firepower System to access packet data and metadata, and to specify the detection criteria and the application information1.

To import a custom application detector file that was provided by a third party, you need to follow these steps1:

* In the FMC web interface, navigate to Objects > Object Management > Application Detectors.
* Click Import.
* Browse to the location of the LUA script file and select it.

* Click Upload.
* Review the detector details and click Save.
The other options are incorrect because:
* Perl script is not a supported format for custom application detectors. Perl is a general-purpose programming language that is not embedded in the Firepower System.
* NBAR protocol is not a file type, but a feature of Cisco IOS routers that can classify and monitor network traffic based on application types. NBAR protocols are predefined and cannot be imported as custom application detectors.
* Python program is not a supported format for custom application detectors. Python is a general-purpose programming language that is not embedded in the Firepower System.

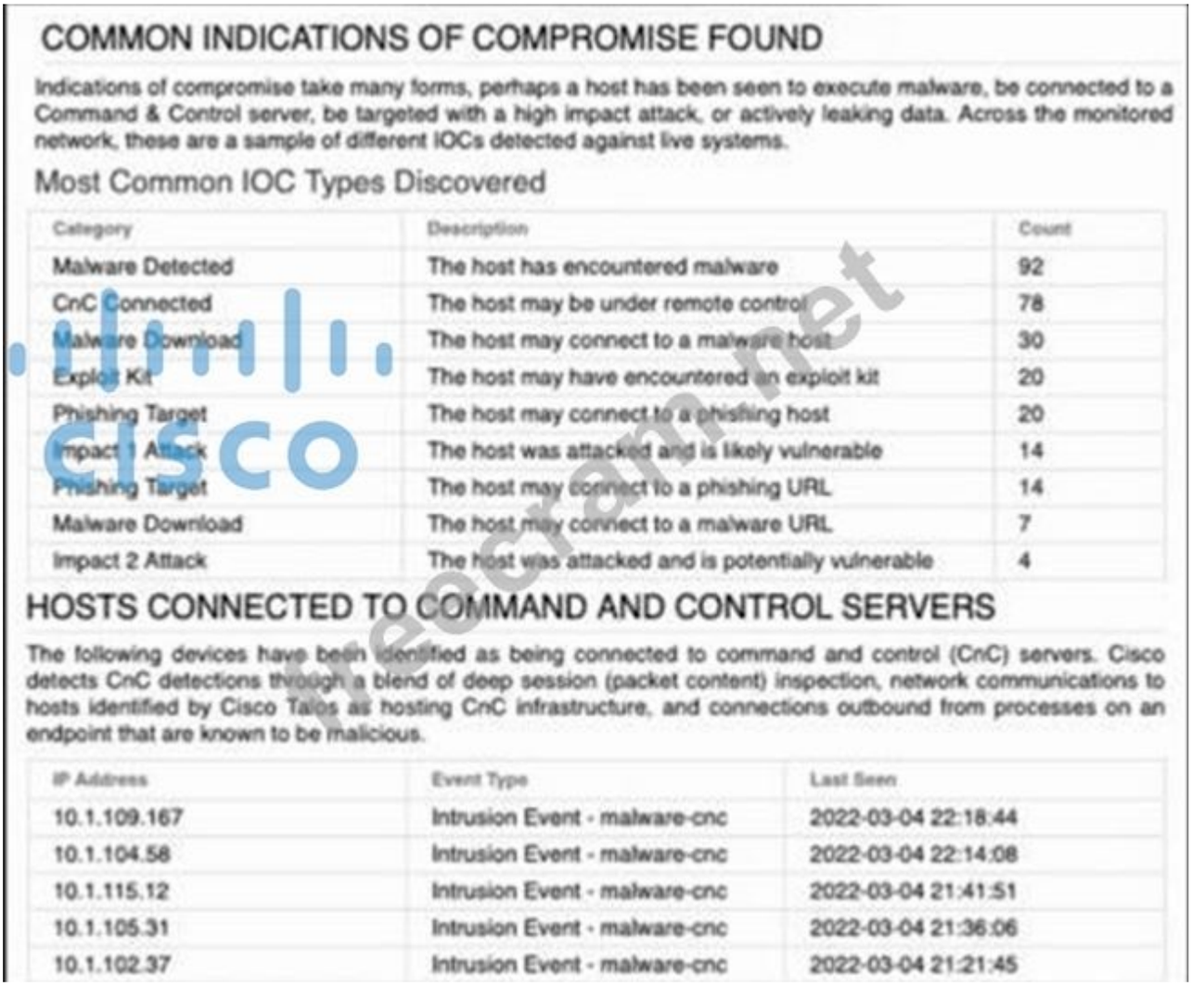
NEW QUESTION: 75

Refer to the exhibit. An engineer is configuring an instance of Cisco Secure Firewall Threat Defense with interfaces in IPS Inline Pair mode. What must be configured on interface e1/6 to accomplish the requirement?
A. propagate link state disabled
B. inline set MTU set to 1500
C. FailSafe disabled
D. security zone set to OUTSIDE_ZONE
Answer: (SHOW ANSWER)

NEW QUESTION: 76
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 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.
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 unchecking the "Drop when inline" option.

D. 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.
Answer: (SHOW ANSWER)

NEW QUESTION: 77



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

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?
A. Virtual protection
B. Network-based detection

C. Trend analysis
D. IP address and URL blacklisting
Answer: (SHOW ANSWER)

NEW QUESTION: 78
A network administrator is trying to configure an access rule to allow access to a specific banking site over HTTPS. Which method must the administrator use to meet the requirement?
A. Enable SSL decryption and specify the URL.
B. Define the URL to be blocked and set the application to HTTP.
C. Define the URL to be blocked and disable SSL inspection.
D. Block the category of banking and define the application of WWW.
Answer: (SHOW ANSWER)
To allow access to a specific banking site over HTTPS, the network administrator must use SSL decryption (also known as SSL/TLS inspection) and specify the URL. This is because HTTPS traffic is encrypted, and the firewall needs to decrypt the traffic to inspect the URL and enforce the access rule.
Steps:
* Enable SSL Decryption: Configure SSL policies to decrypt the HTTPS traffic.
* Specify the URL: Define the URL of the banking site in the access control policy, ensuring that the decrypted traffic is inspected and allowed based on the specified URL.
This method ensures that only the desired banking site is accessed over HTTPS, while other HTTPS traffic can be filtered or blocked according to the organization's security policies.
References: Cisco Secure Firewall Management Center Configuration Guide, Chapter on SSL Decryption.

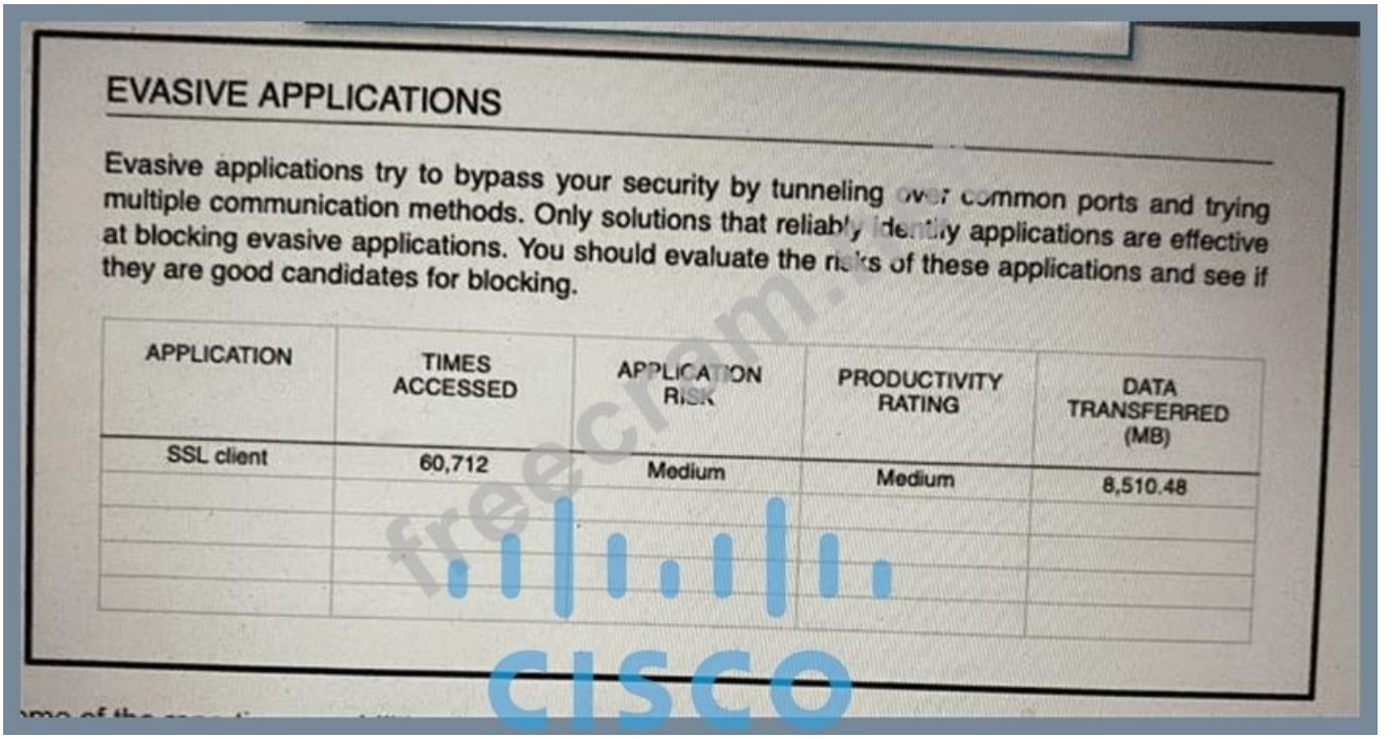
NEW QUESTION: 79
An administrator is optimizing the Cisco FTD rules to improve network performance, and wants to bypass inspection for certain traffic types to reduce the load on the Cisco FTD. Which policy must be configured to accomplish this goal?
A. identity
B. URL filtering
C. prefilter
D. intrusion
Answer: (SHOW ANSWER)

NEW QUESTION: 80
An administrator configures the interfaces of a Cisco Secure Firewall Threat Defence device in an inline IPS deployment. The administrator completes these actions:
* identifies the device and the interfaces
* sets the interface mode to inline
* enables the interlaces
Which configuration step must the administrator take next to complete the implementation?

A. Enable spanning-tree PortFast on the interfaces.
B. Configure an inline set
C. Set the interface to Transparent mode.
D. Set the interface to routed mode.
Answer: (SHOW ANSWER)
After setting the interface mode to inline and enabling the interfaces on a Cisco Secure Firewall Threat Defense (FTD) device in an inline IPS deployment, the next step is to configure an inline set. An inline set groups two interfaces that work together to inspect traffic passing between them.
Steps to configure an inline set:
* In FMC, navigate to Devices > Device Management.
* Select the FTD device and configure the interfaces.
* Create a new inline set, adding the relevant interfaces that have been set to inline mode.
* Deploy the configuration to the FTD device.
Configuring an inline set ensures that the traffic between the specified interfaces is inspected and processed according to the IPS policies, completing the implementation of the inline IPS deployment.
References: Cisco Secure Firewall Management Center Configuration Guide, Chapter on Inline Sets.

NEW QUESTION: 81
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. EtherChannel
B. Subinterface
C. Diagnostic
D. BVI
E. Physical
Answer: (SHOW ANSWER)

NEW QUESTION: 82
Refer to the exhibit.



EVASIVE APPLICATIONS

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

APPLICATION	TIMES ACCESSED	APPLICATION RISK	PRODUCTIVITY RATING	DATA TRANSFERRED (MB)
SSL client	60,712	Medium	Medium	8,510.48

An administrator is looking at some of the reporting capabilities for Cisco Firepower and noticed this section of the Network Risk report showing a lot of SSL activity that cloud be used for evasion. Which action will mitigate this risk?

A. Use encrypted traffic analytics to detect attacks

B. Use Cisco Tetration to track SSL connections to servers.

C. Use SSL decryption to analyze the packets.

D. Use Cisco AMP for Endpoints to block all SSL connection

Answer: (SHOW ANSWER)

NEW QUESTION: 83

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

A. Unregister the faulty Cisco FTD device from the Cisco FMC

B. Shut down the Cisco FMC before powering up the replacement unit.

C. Shut down the active Cisco FTD device before powering up the replacement unit.

D. Ensure that the faulty Cisco FTD device remains registered to the Cisco FMC.

Answer: (SHOW ANSWER)

NEW QUESTION: 84

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

A. MACsec

B. SSH

C. SSL

D. IPsec
Answer: (SHOW ANSWER)

NEW QUESTION: 85
What is a result of enabling Cisco FTD clustering?
A. For the dynamic routing feature, if the master unit fails, the newly elected master unit maintains all existing connections.
B. Integrated Routing and Bridging is supported on the master unit.
C. Site-to-site VPN functionality is limited to the master unit, and all VPN connections are dropped if the master unit fails.
D. All Firepower appliances can support Cisco FTD clustering.
Answer: (SHOW ANSWER)
Reference:
https://www.cisco.com/c/en/us/td/docs/security/firepower/640/configuration/guide/fpmc-config-guide-v64/clustering_for_the_firepower_threat_defense.html

NEW QUESTION: 86
Encrypted Visibility Engine (EVE) is enabled under which lab on an access control policy in Cisco Secure Firewall Management Centre?
A. Network Analysis Policy
B. Advanced
C. Security Intelligence
D. SSL
Answer: (SHOW ANSWER)
The Encrypted Visibility Engine (EVE) in Cisco Secure Firewall Management Center is enabled under the SSL tab of an access control policy. EVE provides visibility into encrypted traffic, allowing the firewall to detect threats even when traffic is encrypted.
Steps to enable EVE:
* Navigate to the access control policy in FMC.
* Go to the SSL tab.
* Enable Encrypted Visibility Engine (EVE) to analyze encrypted traffic.
This configuration helps in identifying and mitigating threats within encrypted traffic without the need for full decryption.
References: Cisco Secure Firewall Management Center Configuration Guide, Chapter on SSL and Encrypted Traffic Visibility.

NEW QUESTION: 87
A network administrator is deploying a new Cisco Secure Firewall Threat Defense (FTD) firewall After Cisco Secure FTD is deployed, inside clients nave intermittent connectivity to each other. When ... the packet capture on the Secure FTD firewall, the administrator sees that Secure FID is

responding to all the AW requests on the inside network. Which action must the network administrator e to resolve the issue"

A. Review NAT policy and disable incorrect proxy ARP configuration.

B. Hardcode the MAC address of the FTD to IP mapping on client machines.

C. Review the access policy and verify that ARP is allowed from inside to inside.

D. Convert the FTD to transparent mode to allow ARP requests.

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.

References: Cisco Secure Firewall Management Center Configuration Guide, Chapter on NAT and ARP Configuration.

NEW QUESTION: 88

A company has many Cisco FTD devices managed by a Cisco FMC. The security model requires that access control rule logs be collected for analysis. The security engineer is concerned that the Cisco FMC will not be able to process the volume of logging that will be generated. Which configuration addresses this concern?

A. Send Cisco FTD connection events and security events to Cisco FMC and configure it to forward logs to SIEM 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 directly to a SIEM system and forward security events from Cisco FMC to the SIEM system 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: 89

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 oy FMC tor nigh availability. The customer wants the configures 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 configured by hand into FMC before the devices are registered.
B. The current FDM configuration will be converted automatically into FMC when the device registers.
C. The current FDM configuration must be migrated to FMC using the Secure Firewall Migration Tool.
D. The FTD configuration must be converted to ASA command format, which can then be migrated to FMC.
Answer: (SHOW ANSWER)
When an FTD device that is managed by FDM is registered to FMC, the existing configuration is automatically converted and imported into FMC. The FMC then pushes the configuration back to the device.
This process preserves most of the FDM configuration, except for some features that are not supported by FMC, such as VPN wizards and certificates.

NEW QUESTION: 90
With Cisco Firepower Threat Defense software, which interface mode must be configured to passively receive traffic that passes through the appliance?

A. inline set
B. passive
C. routed
D. inline tap
Answer: (SHOW ANSWER)
Reference:
https://www.cisco.com/c/en/us/td/docs/security/firepower/640/configuration/guide/fpmc-config-guide-v64/interface_overview_for_firepower_threat_defense.html

NEW QUESTION: 91
Due to an Increase in malicious events, a security engineer must generate a threat report to include intrusion in events, malware events, and security intelligence events. How Is this information collected in a single report?
A. Create a Custom report.
B. Generate a malware report.
C. Export the Attacks Risk report.
D. Run the default Firepower report.
Answer: (SHOW ANSWER)

NEW QUESTION: 92
An engineer is deploying failover capabilities for a pair of Cisco Secure Firewall devices. The core switch keeps the MAC address of the previously active unit in the ARP table. Which action must the engineer take to minimize downtime and ensure that network users keep access to the internet after a Cisco Secure Firewall failover?
A. Add the MAC address to the switch ARP table.
B. Use a virtual MAC address on both units
C. Run a script to send gratuitous ARP after a failover.
D. Set the same MAC address on both units.
Answer: (SHOW ANSWER)

NEW QUESTION: 93
Which firewall design allows a firewall to forward traffic at layer 2 and layer 3 for the same subnet?
A. transparent mode
B. integrated routing and bridging
C. routed mode
D. Cisco Firepower Threat Defense mode
Answer: (SHOW ANSWER)

NEW QUESTION: 94
Refer to the exhibit.
What must be done to fix access to this website while preventing the same communication to all other websites?
A. Create an intrusion policy rule to have Snort allow port 80 to only 172.1.1 50.
B. Create an access control policy rule to allow port 443 to only 172.1.1 50
C. Create an access control policy rule to allow port 80 to only 172.1.1 50.
D. Create an intrusion policy rule to have Snort allow port 443 to only 172.1.1.50
Answer: (SHOW ANSWER)

NEW QUESTION: 95
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. Analysts > Files > Malware Events

C. Analysis > Hosts > Host Attributes
D. Analysis > Flies > Network File Trajectory
Answer: (SHOW ANSWER)
To determine if a host is infected with malware, the network administrator can look at the Indications of Compromise (IOC) feature in Cisco FMC. The IOC feature analyzes network and endpoint data collected by Firepower sensors and AMP for Endpoints connectors, and identifies hosts that exhibit signs of compromise or infection. The IOC feature uses predefined rules based on Cisco Talos intelligence and other sources to detect IOCs on hosts. One of these rules is CnC Connected, which indicates that a host has communicated with a command-and-control (CnC) server that is known to be associated with malware activity2.
To view the IOC information for a host, the network administrator can navigate to Analysis > Hosts > Indications of Compromise in Cisco FMC, and select a host from the table. The IOC Details page will show the IOC events for that host, including the CnC Connected event, along with other information such as severity, timestamp, source, destination, protocol, and rule name. The network administrator can also view more details about each IOC event by clicking on it2.
The other options are incorrect because:
* Analysis > Files > Malware Events shows information about files that have been detected as malware by Firepower sensors or AMP for Endpoints connectors. This does not show information about hosts that are infected with malware or have communicated with CnC servers3.
* Analysis > Hosts > Host Attributes shows information about hosts that have been discovered by Firepower sensors, such as IP address, MAC address, operating system, applications, users, vulnerabilities, and so on. This does not show information about IOCs or CnC connections on hosts4.
* Analysis > Files > Network File Trajectory shows information about files that have traversed your network and have been detected by Firepower sensors or AMP for Endpoints connectors. This allows you to track where a file came from, where it went, and what happened to it along the way. This does not show information about hosts that are infected with malware or have communicated with CnC servers5.

NEW QUESTION: 96
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. inline tap mode
C. strict TCP enforcement
D. Snort fail open
Answer: (SHOW ANSWER)

NEW QUESTION: 97

An engineer is configuring Cisco Secure Firewall Threat Defense managed by a Secure Firewall Management Center appliance. The company wants remote access VPN users to be reachable from the inside network.
What must the engineer configure to meet the requirements?
A. manual NAT exemption rule at the bottom of the NAT policy
B. auto NAT exemption rule at the top of the NAT policy
C. manual NAT exemption rule at the top of the NAT policy
D. auto NAT exemption rule at the bottom of the NAT policy
Answer: (SHOW ANSWER)

NEW QUESTION: 98
What is a valid Cisco AMP file disposition?
A. non-malicious
B. malware
C. known-good
D. pristine
Answer: (SHOW ANSWER)
Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config- guide- v60/Reference_a_wrapper_Chapter_topic_here.html

NEW QUESTION: 99
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. Configure an IPS policy and enable global logging.
C. Disable the default IPS policy and enable global logging.
D. Disable the default IPS policy and enable per-rule logging.
Answer: (SHOW ANSWER)

NEW QUESTION: 100
When using Cisco Threat Response, which phase of the Intelligence Cycle publishes the results of the investigation?

A. direction
B. dissemination
C. processing
D. analysis
Answer: (SHOW ANSWER)
Disseminate: The dissemination phase publishes the results of the investigation or threat hunt. This information is disseminated with a focus on the receivers of the information. At the tactical

level, this information feeds back into the beginning of the F3EAD model, Find. Figure 3 illustrates the F3EAD model.

NEW QUESTION: 101
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 none, 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 passive, and configure an access control policy with an intrusion policy and a file policy defined
D. Set to none, and configure an access control policy with a prefilter policy defined
Answer: (SHOW ANSWER)

NEW QUESTION: 102
An engineer wants to perform a packet capture on the Cisco FTD to confirm that the host using IP address
192 168.100.100 has the MAC address of 0042 7734.103 to help troubleshoot aconnectivity issue
What is the correct tcpdump command syntax to ensure that the MAC address appears in the packet capture output?
A. -nm src 192.168.100.100
B. -ne src 192.168.100.100
C. -w capture.pcap -s 1518 host 192.168.100.100 mac
D. -w capture.pcap -s 1518 host 192.168.100.100 ether
Answer: (SHOW ANSWER)
Reference:https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/212474-working-with- firepower-threat-defense-f.html

NEW QUESTION: 103
A network administrator has converted a Cisco FTD from using LDAP to LDAPS for VPN authentication.
The Cisco FMC can connect to the LDAPS server, but the Cisco FTD is not connecting. Which configuration must be enabled on the Cisco FTD?
A. DNS servers must be defined for name resolution.
B. The RADIUS server must be defined.
C. The LDAPS must be allowed through the access control policy.
D. SSL must be set to a use TLSv1.2 or lower.
Answer: (SHOW ANSWER)

NEW QUESTION: 104

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. Current Sessions
C. Correlation Information
D. Appliance Status
E. Network Compliance
Answer: (SHOW ANSWER)

NEW QUESTION: 105
The event dashboard within the Cisco FMC has been inundated with low priority intrusion drop events, which are overshadowing high priority events. An engineer has been tasked with reviewing the policies and reducing the low priority events. Which action should be configured to accomplish this task?

A. generate events
B. drop packet
C. drop connection
D. drop and generate
Answer: B (LEAVE A REPLY)
Reference"
https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-config-guide-v62/working_with_intrusion_events.html

NEW QUESTION: 106
An analyst is investigating a potentially compromised endpoint within the network and pulls a host report for the endpoint in question to collect metrics and documentation. What information should be taken from this report for the investigation?

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

NEW QUESTION: 107
Which feature within the Cisco FMC web interface allows for detecting, analyzing and blocking malware in network traffic?
A. Cisco AMP for Networks
B. file policies
C. intrusion and file events
D. Cisco AMP for Endpoints
Answer: (SHOW ANSWER)

NEW QUESTION: 108
An engineer wants to connect a single IP subnet through a Cisco FTD firewall and enforce policy. There is a requirement to present the internal IP subnet to the outside as a different IP address. What must be configured to meet these requirements?
A. Configure the Cisco FTD firewall in routed mode with NAT enabled.
B. Configure the downstream router to perform NAT.
C. Configure the Cisco FTD firewall in transparent mode with NAT enabled.
D. Configure the upstream router to perform NAT.
Answer: (SHOW ANSWER)

NEW QUESTION: 109
An engineer must change the mode of a Cisco Secure Firewall Threat Defense (FTD) firewall in the Cisco Secure Firewall Management Center (FMC) inventory. The engineer must take these actions:
* Register Secure FTD with Secure FMC.
* Change the firewall mode.
* Deregister the Secure FTD device from Secure FMC.
How must the engineer take FTD take the actions?
A. Reload the Secure FTD device.
B. Configure the management IP address.
C. Access the Secure FTD CLI from the console port.
D. Erase the Secure FTD configuration
Answer: (SHOW ANSWER)
To change the mode of a Cisco Secure Firewall Threat Defense (FTD) device in the Cisco Secure Firewall Management Center (FMC) inventory, the engineer must follow these steps:
* Register the Secure FTD with Secure FMC.
* Change the firewall mode.
* Deregister the Secure FTD device from Secure FMC.

To perform these actions, accessing the Secure FTD CLI from the console port is necessary. This allows the engineer to execute the required commands to change the firewall mode and manage the registration status of the FTD device.
Steps:
* Connect to the Secure FTD device via the console port.
* Access the CLI and execute the command to change the firewall mode (configure firewall-mode).
* Deregister the device from FMC if needed.
* Register or re-register the device with FMC as required.
References: Cisco Secure Firewall Threat Defense Configuration Guide, Chapter on Device Management and CLI Access.

NEW QUESTION: 110

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 "show tech" for the Cisco FMC.
D. A "troubleshoot" file for the Cisco FMC.
Answer: (SHOW ANSWER)

NEW QUESTION: 111
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. Advanced Malware Risk Report
B. User Risk Report
C. Attacks Risk Report
D. Network Risk Report
Answer: D (LEAVE A REPLY)

NEW QUESTION: 112
An engineer configures an access control rule that deploys file policy configurations to security zones or tunnel zones, and it causes the device to restart. What is the reason for the restart?
A. The source tunnel zone in the rule does not match a tunnel zone that is assigned to a tunnel rule in the source policy.
B. Source or destination security zones in the access control rule matches the security zones that are associated with interfaces on the target devices.
C. The source tunnel zone in the rule does not match a tunnel zone that is assigned to a tunnel rule in the destination policy.

D. 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.
Answer: (SHOW ANSWER)

NEW QUESTION: 113
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)
Reference: https://www.cisco.com/c/en/us/td/docs/security/firesight/541/firepower-module-user-guide/asa- firepower-module-user-guide-v541/Intrusion-Global-Threshold.html

NEW QUESTION: 114
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. Enter the configure transparent firewall command from the CLI.
B. Deregister the firewall in Cisco Secure Firewall Management Center.
C. Create one or more bridge groups from the CLI.
D. Manually delete the interface configuration from the CLI.
Answer: (SHOW ANSWER)

NEW QUESTION: 115
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 Centre (FMC), the network administrator sees an error in the Cisco Duo AAA server has been marked as tailed. What is the root cause of the Issue?
A. Multifactor authentication Is not supported on Secure FMC managed devices.
B. Duo trust certificates are missing from the Secure FTD device.
C. The internal AD server is unreachable from the Secure FTD device.
D. AD 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.
References: Cisco Secure Firewall Management Center Administrator Guide, Chapter on Certificate Management.

NEW QUESTION: 116
What is a behavior of a Cisco FMC database purge?
A. User login and history data are removed from the database if the User Activity check box is selected.
B. Data can be recovered from the device.
C. The appropriate process is restarted.
D. The specified data is removed from Cisco FMC and kept for two weeks.
Answer: (SHOW ANSWER)
Reference:
https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-config-guide-v62/management_center_database_purge.pdf

NEW QUESTION: 117
An engineer runs the command restore remote-manager-backup location 2.2.2.2 admin /Volume/home/admin FTD408566513.zip on a Cisco FMC. After connecting to the repository, the Cisco FTD device is unable to accept the backup file. What is the reason for this failure?
A. The backup file is not in .cfg format.
B. The wrong IP address is used.
C. The backup file extension was changed from .tar to .zip.
D. The directory location is incorrect.
Answer: (SHOW ANSWER)
Reference: https://www.ciscolive.com/c/dam/r/ciscolive/emea/docs/2019/pdf/BRKSEC-3455.pdf

NEW QUESTION: 118
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)
Reference: https://www.cisco.com/c/en/us/support/docs/security/firepower-management-center/212699- configure-ftd-high-availability-on-firep.html

NEW QUESTION: 119
A network administrator is trying to configure a previously created file policy on a new access policy. Which action must the administrator take before applying the file policy?
A. Apply an application to an access control rule.
B. Set up an inspection policy.
C. Assign the file policy to the default action.
D. Create a new access control rule.
Answer: (SHOW ANSWER)

NEW QUESTION: 120
An engineer has been tasked with performing an audit of network projects to determine which objects are duplicated across the various firewall models (Cisco Secure Firewall Threat Defense Cisco Secure firewall ASA, and Meraki MX Series) deployed throughout the company Which tool will assist the engineer in performing that audit?

A. Cisco Firepower Device Manager
B. Cisco SecureX
C. Cisco Defense Orchestrator
D. Cisco Secure Firewall Management Center
Answer: (SHOW ANSWER)
Cisco Defense Orchestrator (CDO) is the tool that assists engineers in performing an audit of network projects to determine which objects are duplicated across various firewall models, including Cisco Secure Firewall Threat Defense, Cisco Secure Firewall ASA, and Meraki MX Series. CDO provides a unified management interface for managing multiple security devices and can identify duplicate objects across these devices.
Steps:
* Access Cisco Defense Orchestrator.
* Connect and synchronize all relevant firewall devices (FTD, ASA, Meraki MX).
* Use the audit and reporting features in CDO to identify and manage duplicate objects.
This helps ensure consistency and efficient management across the organization's firewall deployments.
References: Cisco Defense Orchestrator Documentation, Chapter on Device Management and Object Auditing.

NEW QUESTION: 121
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 HTTPS and SNMP under the Access List section.
B. Enable SCP under the Access List section.
C. Enable HTTP and define an access list.
D. Enable SSH and define an access list.
Answer: (SHOW ANSWER)

NEW QUESTION: 122
An organization recently implemented a transparent Cisco FTD in their network.
They must ensure that the device does not respond to insecure SSL/TLS protocols.
Which action accomplishes the task?
A. Enable the UCAPL/CC compliance on the device to support only the most secure protocols available.
B. Configure a FlexConfig object to disable any insecure TLS protocols on the Cisco FTD device.
C. Modify the device's settings using the device management feature within Cisco FMC to force only secure protocols.
D. Use the Cisco FTD platform policy to change the minimum SSL version on the device to TLS 1.2.
Answer: (SHOW ANSWER)

NEW QUESTION: 123
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. routed firewall mode with BVI and routed interfaces
B. routed firewall mode with routed interfaces only
C. transparent firewall mode with multiple BVIs
D. transparent firewall mode with IRB only

Answer: (SHOW ANSWER)

NEW QUESTION: 124
Which limitation applies to Cisco Firepower Management Center dashboards in a multidomain environment?
A. Child domains can view but not edit dashboards that originate from an ancestor domain.
B. Child domains have access to only a limited set of widgets from ancestor domains.
C. Only the administrator of the top ancestor domain can view dashboards.
D. Child domains cannot view dashboards that originate from an ancestor domain.
Answer: (SHOW ANSWER)
Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config- guide- v60/Using_Dashboards.html

NEW QUESTION: 125
What is a feature of Cisco AMP private cloud?
A. It disables direct connections to the public cloud.
B. It supports security intelligence filtering.
C. It performs dynamic analysis
D. It supports anonymized retrieval of threat intelligence
Answer: (SHOW ANSWER)

NEW QUESTION: 126
A network engineer is logged into the Cisco AMP for Endpoints console and sees a malicious verdict for an identified SHA-256 hash. Which configuration is needed to mitigate this threat?
A. Add the hash from the infected endpoint to the network block list.
B. Use regular expressions to block the malicious file.
C. Add the hash to the simple custom detection list.
D. Enable a personal firewall in the infected endpoint.
Answer: (SHOW ANSWER)

NEW QUESTION: 127
A security engineer is configuring an Access Control Policy for multiple branch locations. These locations share a common rule set and utilize a network object called INSIDE_NET which contains the locally significant internal network subnets at each location. Which technique will retain the policy consistency at each location but allow only the locally significant network subnet within the applicable rules?
A. utilizing policy inheritance
B. utilizing a dynamic Access Control Policy that updates from Cisco Talos
C. creating an Access Control Policy with an INSIDE_NET network object and object overrides
D. creating a unique Access Control Policy per device
Answer: (SHOW ANSWER)

NEW QUESTION: 128
Which object type supports object overrides?
A. time range
B. security group tag
C. network object
D. DNS server group
Answer: (SHOW ANSWER)
Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config- guide- v60/Reusable_Objects.html#concept_8BFE8B9A83D742D9B647A74F7AD50053

NEW QUESTION: 129
What is the disadvantage of setting up a site-to-site VPN in a clustered-units environment?
A. VPN connections can be re-established only if the failed master unit recovers.
B. Smart License is required to maintain VPN connections simultaneously across all cluster units.
C. VPN connections must be re-established when a new master unit is elected.
D. Only established VPN connections are maintained when a new master unit is elected.
Answer: (SHOW ANSWER)
Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/fxos/clustering/ftd-cluster-solution.
html#concept_g32_yml_y2b

NEW QUESTION: 130
An engineer has been tasked with using Cisco FMC to determine if files being sent through the network are malware. Which two configuration tasks must be performed to achieve this file lookup? (Choose two).

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

NEW QUESTION: 131
A network administrator needs to create a policy on Cisco Firepower to fast-path traffic to avoid Layer 7 inspection. The rate at which traffic is inspected must be optimized. What must be done to achieve this goal?
A. Configure a prefilter policy.
B. Configure modular policy framework.
C. Enable lhe FXOS for multi-instance.
D. Disable TCP inspection.

Answer: (SHOW ANSWER)

NEW QUESTION: 132
Which action should you take when Cisco Threat Response notifies you that AMP has identified a file as malware?
A. Add the malicious file to the block list.
B. Send a snapshot to Cisco for technical support.
C. Forward the result of the investigation to an external threat-analysis engine.
D. Wait for Cisco Threat Response to automatically block the malware.
Answer: (SHOW ANSWER)

NEW QUESTION: 133
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. The output format option for the packet logs is unavailable.
C. Only the UDP packet type is supported.
D. The VLAN ID and destination MAC address are optional.
Answer: (SHOW ANSWER)

NEW QUESTION: 134
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. Enable the IP SLA Responder on the backup path interface.
B. Implement a secondary route that has a higher precedence.
C. Enable an ICMP redirect message on the interface connected to the backup path.
D. Assign a tracking object to the static route and the IP SLA operation.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 135
A security engineer must integrate an external feed containing STIX/TAXII data with Cisco FMC. Which feature must be enabled on the Cisco FMC to support this connection?
A. Cisco Secure Endpoint Integration
B. Security Intelligence Feeds
C. Threat Intelligence Director
D. Cisco Success Network
Answer: C (LEAVE A REPLY)

NEW QUESTION: 136

Refer to the exhibit. Users attempt to connect to numerous external resources on various TCP ports. If the users mistype the port, their connection closes immediately, and it takes more than one minute before the connection is torn down. An engineer manages to capture both types of connections as shown in the exhibit.

What must the engineer configure to lower the timeout values for the second group of connections and resolve the user issues?

A. Outbound access rule with the Block with reset action

B. Inbound access rule that allows TCP reset packets from outside

C. Outbound access rule that allows the entire ICMP protocol suite

Answer: (SHOW ANSWER)

NEW QUESTION: 137

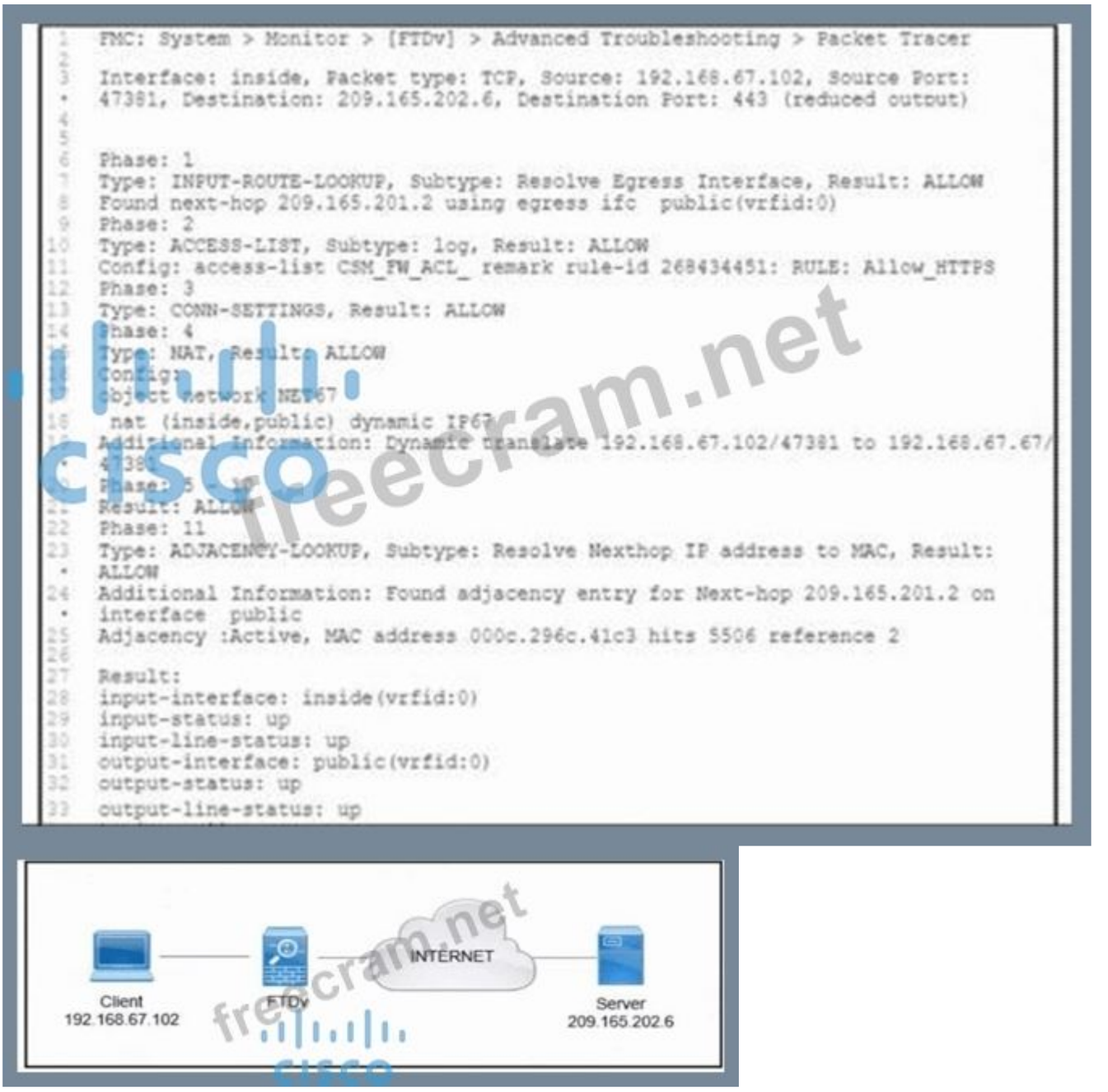
A Cisco FMC administrator wants to configure fastpathing of trusted network traffic to increase performance.

In which type of policy would the administrator configure this feature?
A. Prefilter policy
B. Identity policy
C. Network Analysis policy
D. Intrusion policy
Answer: (SHOW ANSWER)

NEW QUESTION: 138
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. KVM
B. Azure
C. ESXi
D. AWS
E. Openstack
Answer: (SHOW ANSWER)
Cisco Secure Firewall Threat Defense Virtual (FTDv) appliances support High Availability (HA) configurations in specific virtual environments. The supported environments for HA setups include:
* ESXi: VMware's ESXi is a widely supported platform for deploying FTDv appliances in HA configurations.
* AWS: Amazon Web Services (AWS) supports FTDv appliances and allows for HA configurations to ensure redundancy and reliability in cloud deployments.
These environments provide the necessary infrastructure and capabilities to support the high availability requirements for FTDv appliances.
References: Cisco Secure Firewall Threat Defense Virtual Configuration Guide, Chapter on High Availability and Supported Platforms.

NEW QUESTION: 139
When creating a report template, how can the results be limited to show only the activity of a specific subnet?
A. Create a custom search in Firepower Management Center and select it in each section of the report.
B. Add an Input Parameter in the Advanced Settings of the report, and set the type to Network/IP.
C. Add a Table View section to the report with the Search field defined as the network in CIDR format.
D. Select IP Address as the X-Axis in each section of the report.
Answer: (SHOW ANSWER)
Reference: https://www.cisco.com/c/en/us/td/docs/security/firesight/541/user-guide/FireSIGHT-System- UserGuide-v5401/Reports.html#87267

NEW QUESTION: 140



Refer to the exhibit. A client that has IP address 192.168.67.102 reports issues when connecting to a remote server. Based on the topology and output of packet tracer tool, which action resolves the connectivity issue?

A. Restart the client-side application.

B. Add the route to the destination.

C. Unblock the access rule on FTDv.

D. Reconfigure NAT on FTDv.

Answer: (SHOW ANSWER)

NEW QUESTION: 141

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

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

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

A. TOR

B. Chrome

C. YouTube

D. Kerberos

Answer: (SHOW ANSWER)

NEW QUESTION: 142

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

(Choose two.)

A. EIGRP

B. OSPF

C. static routing

D. IS-IS

E. BGP

Answer: (SHOW ANSWER)

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

/fptd- fdm-routing.html

NEW QUESTION: 143

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

A. Ethos

B. RBAC

C. Tetra

D. Spero
Answer: (SHOW ANSWER)

NEW QUESTION: 144
An engineer attempts to pull the configuration for a Cisco FTD sensor to review with Cisco TAC but does not have direct access to the CU for the device. The CLI for the device is managed by Cisco FMC to which the engineer has access. Which action in Cisco FMC grants access to the CLI for the device?
A. Download the configuration file within the File Download section of Cisco FMC.
B. Create a backup of the configuration within the Cisco FMC.
C. Use the show run all command in the Cisco FTD CLI feature within Cisco FMC.
D. Export the configuration using the Import/Export tool within Cisco FMC.
Answer: (SHOW ANSWER)

NEW QUESTION: 145
An administrator is adding a QoS policy to a Cisco FTD deployment. When a new rule is added to the policy and QoS is applied on 'Interfaces in Destination Interface Objects", no interface objects are available What is the problem?
A. The FTD is out of available resources lor use. so QoS cannot be added
B. QoS is available only on routed interfaces, and this device is in transparent mode.
C. A conflict exists between the destination interface types that is preventing QoS from being added
D. The network segments that the interfaces are on do not have contiguous IP space
Answer: (SHOW ANSWER)

NEW QUESTION: 146
An engineer must integrate a third-party security intelligence feed with Cisco Secure Firewall Management Center. Secure Firewall Management Center is running Version 6.2.3 and has 8 GB of memory. Which two actions must be taken to implement Threat Intelligence Director? (Choose two.)
A. Upgrade to version 6.6.
B. Enable REST API access.
C. Add a TAXII server.
D. Add the URL of the TAXII server.
E. Add 7 GB of memory.
Answer: (SHOW ANSWER)

NEW QUESTION: 147
Which command is run on an FTD unit to associate the unit to an FMC manager that is at IP address
10.0.0.10, and that has the registration key Cisco123?

A. configure manager local 10.0.0.10 Cisco123
B. configure manager add Cisco123 10.0.0.10
C. configure manager local Cisco123 10.0.0.10
D. configure manager add 10.0.0.10 Cisco123
Answer: (SHOW ANSWER)
Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/misc/fmc-ftd-mgmt-nw/fmc-ftd-mgmt-nw.html#id_106101

NEW QUESTION: 148
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. Add the port number being used for PAT on the router to the device's IP address in the Cisco FMC.
B. Reconfigure the Cisco FMC lo use the device's private IP address instead of the WAN address.
C. Reconfigure the Cisco FMC to use the device's hostname instead of IP address.
D. Remove the IP address defined for the device in the Cisco FMC.
E. Configure a NAT ID on both the Cisco FMC and the device.
Answer: (SHOW ANSWER)

NEW QUESTION: 149
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. multi-instance firewalls
C. high availability active/standby firewalls
D. span EtherChannel clustering
Answer: (SHOW ANSWER)

NEW QUESTION: 150
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
Passing Traffic Not Allowed in Routed Mode
In routed mode, some types of traffic cannot pass through the ASA even if you allow it in an access rule. The bridge group, however, can allow almost any traffic through using either an access rule (for IP traffic) or an EtherType rule (for non-IP traffic):
IP traffic-In routed firewall mode, broadcast and "multicast traffic is blocked even if you allow it in an access rule," including unsupported dynamic routing protocols and DHCP (unless you configure DHCP relay). Within a bridge group, you can allow this traffic with an access rule (using an extended ACL).
Non-IP traffic-AppleTalk, IPX, BPDUs, and MPLS, for example, can be configured to go through using an EtherType rule.
Note
"The bridge group does not pass CDP packets packets, or any packets that do not have a valid EtherType greater than or equal to 0x600. An exception is made for BPDUs and IS-IS, which are supported. "

NEW QUESTION: 151
An engineer is setting up a remote access VPN on a Cisco FTD device and wants to define which traffic gets sent over the VPN tunnel. Which named object type in Cisco FMC must be used to accomplish this task?
A. access list
B. crypto map
C. split tunnel
D. route map
Answer: (SHOW ANSWER)

NEW QUESTION: 152

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)

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: 153

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

A. Cisco AMP for Networks is unable to contact Cisco Threat Grid on premise.

B. The user agent status is set to monitor.

C. Cisco AMP for Networks is unable to contact Cisco Threat Grid Cloud.

D. There is a host limit set.

Answer: (SHOW ANSWER)

NEW QUESTION: 154

How many report templates does the Cisco Firepower Management Center support?

A. 20

B. 10

C. 5

D. unlimited

Answer: (SHOW ANSWER)

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

NEW QUESTION: 155

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

A. The switches were not set up with a monitor session ID (hat matches the flow ID defined on the FTD

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

C. The FTD must be configured with an ERSPAN port, not a passive port.

D. The FTD must &e in routed mode to process ERSPAN traffic.

Answer: D (LEAVE A REPLY)

NEW QUESTION: 156
A network administrator cannot select the link to be used for failover when configuring an active/passive HA Cisco FTD pair.
Which configuration must be changed before setting up the high availability pair?
A. The interface name must be removed from the interface on each Cisco FTD.
B. The interface must be configured as part of a LACP Active/Active EtherChannel.
C. An IP address in the same subnet must be added to each Cisco FTD on the interface.
D. The name Failover must be configured manually on the interface on each cisco FTD.
Answer: (SHOW ANSWER)

NEW QUESTION: 157
A network engineer detects a connectivity issue between Cisco Secure Firewall Management Center and Cisco Secure Firewall Threat Defense. Initial troubleshooting indicates that heartbeats and events are not being received. The engineer re-establishes the secure channels between both peers. Which two commands must the engineer run to resolve the issue? (Choose two.)
A. sudo stats_unified.pl
B. show history
C. show disk-manager
D. manage_procs.pl
E. sudo perfstats -Cq < /var/sf/rna/correlator-stats/now
Answer: (SHOW ANSWER)

NEW QUESTION: 158
An engineer is attempting to add a new FTD device to their FMC behind a NAT device with a NAT ID of ACME001 and a password of Cisco388267669. Which command set must be used in order to accomplish this?
A. configure manager add <FMC IP> registration key> ACME001
B. configure manager add <FMC IP> ACME0O1 <registration key>
C. configure manager add ACME001 <registration key> <FMC IP>
D. configure manager add DONTRESOLVE <FMC IP> AMCE001 <registration key>
Answer: A (LEAVE A REPLY)

NEW QUESTION: 159
A network engineer must configure IPS mode on a Cisco 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 Defence 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 Interface on me Secure Firewall threat Defense device
C. DHCP on the switch
D. active SPAN port on the switch

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 toPolicies > 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.

References:Cisco Secure Firewall Management Center Administrator Guide, Chapter on Intrusion Policies.

NEW QUESTION: 160

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

A. FTD RTC

B. ISEGrid

C. pxGrid

D. FMC RTC

Answer: (SHOW ANSWER)

NEW QUESTION: 161

Which process should be checked when troubleshooting registration issues between Cisco FMC and managed devices to verify that secure communication is occurring?

A. fpcollect

B. sftunnel

C. dhclient

D. sfmgr

Answer: (SHOW ANSWER)

NEW QUESTION: 162

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

A. Configure Cisco Firepower as a transparent firewall

B. Set up Cisco Firepower as managed by Cisco FDM

C. Set up Cisco Firepower in intrusion prevention mode

D. Configure Cisco Firepower in FXOS monitor only mode.

Answer: (SHOW ANSWER)

NEW QUESTION: 163
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. transparent
B. passive
C. Inline tap
D. Inline set
Answer: (SHOW ANSWER)

NEW QUESTION: 164
Which Cisco Rapid Threat Containment mitigation action is enabled by integrating pxGrid Adaptive Network Control with Cisco ISE and Cisco Secure Firewall Management Center?
A. Suspend
B. Block
C. Reject
D. Terminate
Answer: (SHOW ANSWER)

NEW QUESTION: 165
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.
References: Cisco Threat Response Documentation, Browser Plug-in Section.

NEW QUESTION: 166
A company is deploying intrusion protection on multiple Cisco FTD appliances managed by Cisco FMC.
Which system-provided policy must be selected if speed and detection are priorities?
A. Security Over Connectivity
B. Balanced Security and Connectivity
C. Connectivity Over Security
D. Maximum Detection
Answer: (SHOW ANSWER)

NEW QUESTION: 167
An administrator is adding a new URL-based category feed to the Cisco FMC for use within the policies. The intelligence source does not use STIX. but instead uses a .txt file format. Which action ensures that regular updates are provided?
A. Convert the .txt file to STIX and upload it to the Cisco FMC.
B. Upload the .txt file and configure automatic updates using the embedded URL.
C. Add a TAXII feed source and input the URL for the feed.
D. Add a URL source and select the flat file type within Cisco FMC.
Answer: (SHOW ANSWER)

NEW QUESTION: 168
An engineer is configuring URL filtering for a Cisco FTD device in Cisco FMC. Users must receive a warning when they access http:/'www.Dac'additstte.corn with the option of continuing to the website if they choose to. No other websites should be blacked. Which two actions must the engineer lake to meet these requirements? (Choose two.)
A. On the HTTP Responses tab of the access control policy editor, set the Block Response Page to Custom.
B. On the HTTP Responses tab of the access control policy editor, sot the Interactive Block Response Page to system-provided.
C. Configure the default action for the access control policy to Interactive Block.
D. Configure an access control rule that matches the Adult URL category and se: the action to interactive Block.

E. Configure an access control rule that matches an URL object for http://www.badaduitslte.com; and set the action to interactive Block.

Answer: (SHOW ANSWER)

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

On the HTTP Responses tab of the access control policy editor, set the Interactive Block Response Page to system-provided. This will enable the system to display a warning page to the users when they try to access a blocked URL, and give them the option to continue or cancel. The system-provided page is a default page that contains a generic message and a logo1.

Configure

an access control rule that matches an URL object for http://www.badadultsite.com; and set the action to Interactive Block. This will apply the interactive block action to the specific URL that is defined in the URL object. The interactive block action will trigger the interactive block response page that was configured in the previous step1.

The other options are incorrect because:

On the HTTP Responses tab of the access control policy editor, setting the Block Response Page to Custom will not affect the interactive block action. The block response page is used when the action is set to Block, not Interactive Block1.

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

Configuring

an access control rule that matches the Adult URL category and sets the action to Interactive Block will apply the interactive block action to all URLs that belong to the Adult category. This will not meet the requirement of blocking only http://www.badadultsite.com1.

NEW QUESTION: 169

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. System

B. View

C. Custom

D. None

Answer: (SHOW ANSWER)

NEW QUESTION: 170

A network engineer is deploying a pair of Cisco Secure Firewall Threat Defense devices managed by Cisco Secure Firewall Management Center tor High Availability Internet access is a high priority for the business and therefore they have invested in internet circuits from two different ISPs. The requirement from the customer Is that Internet access must do available to their user's oven if one of the ISPs is down. Which two features must be deployed to achieve this requirement? (Choose two.)

A. EtherChannel interfaces
B. Route Tracking
C. SLA Monitor
D. Redundant interfaces
E. BGP
Answer: (SHOW ANSWER)
To ensure high availability of internet access when deploying a pair of Cisco Secure Firewall Threat Defense (FTD) devices managed by Cisco Secure Firewall Management Center (FMC), the following features must be deployed:
* Route Tracking: This feature monitors the reachability of a specified target (such as an external IP address) through the configured routes. If the route to the target is lost, the FTD can dynamically adjust the routing to use an alternate path, ensuring continuous internet access.
* SLA Monitor: Service Level Agreement (SLA) monitoring works alongside route tracking to continuously verify the status and performance of the internet links. If the SLA for one of the ISP links fails (indicating the link is down or underperforming), the FTD can switch traffic to the secondary ISP link.
Steps to configure:
* In FMC, navigate to Devices > Device Management.
* Select the FTD device and configure route tracking to monitor the ISP links.
* Configure SLA monitors to continuously check the health and performance of the internet circuits.
These configurations ensure that internet access remains available to users even if one of the ISPs goes down.
References: Cisco Secure Firewall Management Center Configuration Guide, Chapter on High Availability and SLA Monitoring.

NEW QUESTION: 171
Which two features of Cisco AMP for Endpoints allow for an uploaded file to be blocked? (Choose two.)
A. application whitelisting
B. exclusions
C. file repository
D. application blocking
E. simple custom detection
Answer: (SHOW ANSWER)

NEW QUESTION: 172
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 internal IP 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. Malware

B. Network discovery

C. Intrusion Impact Alert

D. Connection tracker

Answer: (SHOW ANSWER)

NEW QUESTION: 173

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

A. investigate

B. REST

C. enforcement

D. reporting

Answer: (SHOW ANSWER)

NEW QUESTION: 174

Refer to the exhibit.

An engineer is modifying an access control policy to add a rule to Inspect all DNS traffic that passes it making the change and deploying the policy, they see that DNS traffic Is not being Inspected by the Snort engine. What is.....

A. The rule must define the source network for inspection as well as the port.

B. The rule Is configured with the wrong setting for the source port.

C. The rule must specify the security zone that originates the traffic.

D. The action of the rule is set to trust instead of allow.

Answer: (SHOW ANSWER)

NEW QUESTION: 175

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

A. Permit BPDU packets to prevent loops.

B. Assign an IP address to the Bridge Virtual Interface.

C. Add a separate bridge group for each segment.

D. Specify a name for the bridge group.

Answer: (SHOW ANSWER)

NEW QUESTION: 176

Which firewall mode is Cisco Secure Firewall Threat Defense in when two physical interfaces are assigned to a named BVI?

A. IPS only

B. in-line

C. transparent

D. routed

Answer: (SHOW ANSWER)

NEW QUESTION: 177

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)

https://www.cisco.com/c/en/us/support/docs/security/firepower-management-center/212702-configure-and-verify-nat-on-ftd.html

NEW QUESTION: 178

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

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

A. Both firewalls must be in transparent mode.

B. Both firewalls must have the same number of interfaces.

C. The version numbers must have the same patch number.

D. DHCP must be configured on at least one firewall interface.

Answer: (SHOW ANSWER)

NEW QUESTION: 179

A network engineer must configure the cabling between a Cisco Secure Firewall Threat Defense appliance and a network so the Secure Firewall Threat Defense appliance performs inline to analyze and tune generated intrusion events before going live. Which Secure Firewall Threat Defense interface mode must the engineer use?

A. strict TCP enforcement

B. link state propagation

C. tap mode

D. bypass

Answer: (SHOW ANSWER)

NEW QUESTION: 180

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 failover link with stateful properties.

B. Ensure the high availability license is enabled.

C. Configure the standby IP addresses.

D. Configure the virtual MAC address on the failover link.

E. Disable hellos on the inside interface.

Answer: (SHOW ANSWER)

NEW QUESTION: 181

A network administrator is configuring a transparent Cisco Secure Firewall Threat Defense registered to a Cisco Secure Firewall Management Center. The administrator wants to configure the Secure Firewall Threat Defense to allow ARP traffic to pass between two interfaces of a bridge group. What must be configured?

A. An access policy must allow MAC address 0100.0CCC.CCCD.

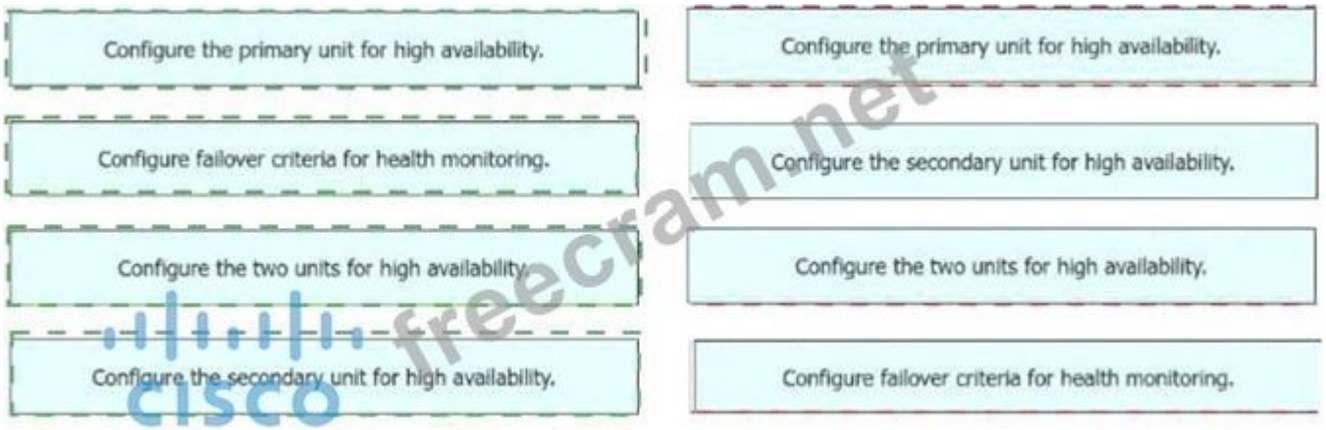
B. ARP inspection must be disabled.

C. Use the default configuration on the devices.

D. An access policy must allow MAC address FFFF.FFFF.FFFF.
Answer: (SHOW ANSWER)

NEW QUESTION: 182
An engineer must configure high availability on two Cisco Secure Firewall Threat Defense appliances. Drag and drop the configuration steps from the left into the sequence on the right.

Answer:



Explanation:
Step 1(Configure the primary unit for high availability),
Step 2(Configure the secondary unit for high availability),
Step 3(Configure the two units for high availability),
Step 4(Configure failover criteria for health monitoring)

NEW QUESTION: 183

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 DONTRESOLVE <FMC IP> AMCE001 <registration key>

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

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

Answer: (SHOW ANSWER)

NEW QUESTION: 184

What is the role of realms in the Cisco ISE and Cisco Secure Firewall Management Center integration?

A. TACACS+ database

B. (Option not provided - please confirm or provide)

C. Cisco ISE context

D. AD definition

E. Cisco Secure Firewall VDC

Answer: (SHOW ANSWER)

NEW QUESTION: 185

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

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

C. Force failover for the secondary Cisco FMC to synchronize the rule updates from the primary.

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

Answer: (SHOW ANSWER)

NEW QUESTION: 186

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

A. Spero

B. Ethos

C. dynamic analysis

D. static analysis

Answer: (SHOW ANSWER)

NEW QUESTION: 187

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

A. switch virtual

B. bridge group member

C. bridge virtual

D. subinterface

Answer: C (LEAVE A REPLY)

Reference: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: 188

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

A. Cisco ISE instructs Cisco FMC to contain the infected endpoint.

B. Cisco AMP instructs Cisco FMC to contain the infected endpoint.

C. Cisco ISE instructs Cisco AMP to contain the infected endpoint.

D. Cisco FMC instructs Cisco ISE to contain the infected endpoint.

Answer: (SHOW ANSWER)

NEW QUESTION: 189

A network administrator wants to configure a Cisco Secure Firewall Threat Defense instance managed by Cisco Secure Firewall Management Center to block traffic to known cryptomning networks. Which system settings must the administrator configure in Secure Firewall Management Center to meet the requirement?

A. Access Policy. Security Intelligence

B. Malware Policy.

C. Rules Intrusion Policy. Security Intelligence

D. Access Policy. Rules

Answer: (SHOW ANSWER)

To block traffic to known cryptomining networks using Cisco Secure Firewall Threat Defense (FTD) managed by Cisco Secure Firewall Management Center (FMC), the network administrator needs to configure Security Intelligence in an Access Control Policy. Security Intelligence allows administrators to block traffic based on threat intelligence feeds, which include known malicious IP addresses, domains, and URLs.

Steps:

* Navigate to Policies > Access Control > Access Control Policy in FMC.
* Edit or create an Access Control Policy.
* Go to the Security Intelligence tab.
* Enable the relevant threat intelligence feeds that include cryptomining networks.
* Apply the policy to the FTD device.

This configuration ensures that traffic to known cryptomining networks is blocked, enhancing the network's security posture against cryptomining threats.

References: Cisco Secure Firewall Management Center Configuration Guide, Chapter on Security Intelligence.

NEW QUESTION: 190

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)

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