Cisco.300-710.v2026-11-06.q181

Exam Code:	300-710
Exam Name:	Securing Networks with Cisco Firepower
Certification Provider:	Cisco
Free Question Number:	181
Version:	v2026-11-06
# of views:	108
# of Questions views:	1903
https://www.freecram.net/torrent/Cisco.300-710.v2026-11-06.q181.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 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 FQDN including the subdomain for the website
C. Specify the protocol to match (HTTP or HTTPS).
D. Use the subject common name from the website certificate
Answer: (SHOW ANSWER)

NEW QUESTION: 3
An administrator must use Cisco FMC to install a backup route within the Cisco FTD to route traffic in case of a routing failure with the primary route. Which action accomplishes this task?
A. Create the backup route and use route tracking on both routes to a destination IP address in the network.
B. Use a default route on the FMC instead of having multiple routes contending for priority.
C. Install the static backup route and modify the metric to be less than the primary route.
D. Configure EIGRP routing on the FMC to ensure that dynamic routes are always updated.
Answer: (SHOW ANSWER)

NEW QUESTION: 4
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. The Enable Spoke to Spoke Connectivity through Hub option is not selected on FTD.
C. FTD has no NAT policy that allows outside to outside communication
D. Split tunneling is enabled for the Remote Access VPN on FTD
Answer: (SHOW ANSWER)

NEW QUESTION: 5
A network administrator is seeing an unknown verdict for a file detected by Cisco FTD. Which malware policy configuration option must be selected in order to further analyse the file in the Talos cloud?
A. Dynamic analysis
B. Malware analysis
C. Spero analysis
D. Sandbox analysis
Answer: (SHOW ANSWER)

NEW QUESTION: 6
A security engineer manages a firewall console and an endpoint console and finds it challenging and the consuming to review events and modify blocking of specific files in both consoles. Which action must the engineer take to streamline this process?

A. From the Secure FMC. create a Cisco Secure Endpoint object and reference the object in the Cisco Secure Endpoint console.
B. From the Cisco Secure Endpoint console, Croats and copy an API key and paste into the Cisco Secure AMP tab
C. initiate the integration between Secure FMC and Cisco Secure Endpoint from the Secure FMC using the AMP tab
D. Within the Cisco Secure Endpoint console, copy the connector GUID and paste into the Cisco Secure Firewall Management Center (FMC) AMP tab.
Answer: (SHOW ANSWER)
To streamline the process of reviewing events and modifying blocking of specific files across both the firewall console and the endpoint console, the security engineer should initiate the integration between Secure FMC and Cisco Secure Endpoint (formerly AMP for Endpoints) from the Secure FMC using the AMP tab.
Steps:
* In the FMC, navigate to Devices > Device Management.
* Select the device and go to the AMP tab.
* Initiate the integration by configuring the necessary API credentials and linking the FMC to the Cisco Secure Endpoint console.
* This integration allows the security engineer to view endpoint events and apply blocking actions directly from the FMC, consolidating the management tasks.
This approach simplifies the workflow by providing a single interface to manage both network and endpoint security, reducing the time and effort required to maintain security across the organization.
References: Cisco Secure Firewall Management Center and Cisco Secure Endpoint Integration Guide.

NEW QUESTION: 7
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. dynamic analysis
C. Ethos
D. static analysis
Answer: (SHOW ANSWER)

NEW QUESTION: 8
What is a benefit of implementing Integrated Routing and Bridging (IRB) on a Cisco Secure Firewall device?
A. Multiple physical interfaces on the device can be on the same VLAN.
B. Uptime is increased by preventing the device from being a single point of failure.
C. Customers with different security policies can reside on the same device.
D. Threat information can be dynamically updated from Cisco Talos.
Answer: (SHOW ANSWER)
Integrated Routing and Bridging allows a Secure Firewall device operating in routed mode to contain bridge groups while also supporting routed interfaces. Multiple physical or logical interfaces can become members of one bridge group, placing them in the same Layer 2 broadcast domain, VLAN, and IP subnet. A Bridge Virtual Interface represents that bridge group at Layer 3 and functions as its gateway, permitting communication between the bridged network and routed interfaces or other bridge groups, subject to security policy. This can remove the need for an additional external Layer 2 switch when suitable firewall interfaces are available. IRB does not itself provide high availability, security-context separation, or Cisco Talos threat- intelligence updates. Those capabilities are implemented through separate features. Therefore, allowing multiple interfaces to participate in the same VLAN is the stated IRB benefit. Cisco IRB documentation

NEW QUESTION: 9

A network administrator wants to block traffic to a known malware site at https://www.badsite.com and all subdomains while ensuring no packets from any internal client are sent to that site. Which type of policy must the network administrator use to accomplish this goal?

A. SSL policy

B. DNS policy

C. Access Control policy with URL filtering

D. Prefilter policy

Answer: C (LEAVE A REPLY)

NEW QUESTION: 10

Which two types of objects are reusable and supported by Cisco FMC? (Choose two.)

A. dynamic key mapping objects that help link HTTP and HTTPS GET requests to Layer 7 application protocols.

B. reputation-based objects that represent Security Intelligence feeds and lists, application filters based on category and reputation, and file lists

C. network-based objects that represent IP address and networks, port/protocols pairs, VLAN tags, security zones, and origin/destination country

D. network-based objects that represent FQDN mappings and networks, port/protocol pairs, VXLAN tags, security zones and origin/destination country

E. reputation-based objects, such as URL categories

Answer: (SHOW ANSWER)

Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-config-guide-v62/reusable_objects.html#ID-2243-00000414

NEW QUESTION: 11

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

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

A. Configure the appliance to receive the time from an NTP server.

B. Configure the appliance to sync with its own internal clock.

C. Reset the appliance with a hard reboot.

D. Reestablish the connection to the timeserver.

Answer: (SHOW ANSWER)

NEW QUESTION: 12

An administrator receives reports that users cannot access a cloud-hosted web server. The access control policy was recently updated with several new policy additions and URL filtering. What must be done to troubleshoot the issue and restore access without sacrificing the organization's security posture?

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

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

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

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

Answer: (SHOW ANSWER)

NEW QUESTION: 13

An engineer must deploy a high-availability that includes two Cisco Secure Firewall Threat Defense devices configured as cluster. The deployment must have a mechanism that protects synchronization between cluster members Which action must the engineer take to meet the requirements?

A. Encrypt the synchronization traffic with SSL.

B. Configure an SSL VPN tunnel between units.

C. Clear the commit queue at the time of a sync.

D. Select the Key Generation method for IPsec.

Answer: (SHOW ANSWER)

To protect and encrypt the synchronization/failover traffic between Cisco Secure Firewall Threat Defense (FTD) high-availability or cluster units, the correct action is to encrypt the synchronization traffic with IPsec (via the failover/state link configuration) or choose the appropriate cryptographic authentication/key settings

NEW QUESTION: 14

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

* Configure the passive interface.

* Configure the ERSPAN IP address.

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

A. Source IP

B. Flow ID

C. TCP Intercept

D. Destination MAC

E. Bypass Mode

Answer: B,C (LEAVE A REPLY)

NEW QUESTION: 15

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

A. unavailable

B. unknown

C. clean

D. disconnected

Answer: (SHOW ANSWER)

NEW QUESTION: 16

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

A. Use packet capture to ensure that traffic is not being blocked by an access list.

B. Use packet-tracer to validate that the packet passes through the firewall and is NATed to the corrected IP address.

C. Use packet capture to validate that the packet passes through the firewall and is NATed to the corrected IP address.

D. Use packet-tracer to ensure that traffic is not being blocked by an access list.

Answer: (SHOW ANSWER)

Valid 300-710 Dumps shared by ExamDiscuss.com for Helping Passing 300-710 Exam! ExamDiscuss.com now offer the **newest 300-710 exam dumps**, the ExamDiscuss.com 300-710 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com 300-710 dumps with Test Engine here: https://www.examdiscuss.com/Cisco/exam/300-710/premium/ (**446** Q&As Dumps, **35%OFF** **Special Discount Code: freecram**)

NEW QUESTION: 17
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: 18
A large online retailer places Cisco Secure Firewall NGIPS Inline between core and edge firewalls. Seasonal promotions generate sudden traffic spikes that occasionally overwhelm the inspection engine. The device must automatically forward packets uninspected during the overload periods while resuming normal analysis and blocking afterward. Which configuration action must be done to meet the requirement?
A. configure LINA Failsafe
B. switch inline interface pair to tap mode
C. increase capture buffer size
D. enable Snort Fail Open
Answer: (SHOW ANSWER)

NEW QUESTION: 19
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: 20

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

Freecram.net

A. Create an intrusion policy rule to have Snort allow port 443 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 intrusion policy rule to have Snort allow port 80 to only 172.1.1 50.
D. Create an access control policy rule to allow port 80 to only 172.1.1 50.
Answer: (SHOW ANSWER)

NEW QUESTION: 21
A company is in the process of deploying intrusion prevention with Cisco FTDs managed by a Cisco FMC.
An engineer must configure policies to detect potential intrusions but not block the suspicious traffic. Which action accomplishes this task?
A. Configure IPS mode when creating or editing a policy rule under the Cisco FMC Intrusion tab in Access Policies section by unchecking the "Drop when inline" option.
B. Configure 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.
C. 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.
D. 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.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 22
A network engineer is extending a user segment through an FTD device for traffic inspection without creating another IP subnet How is this accomplished on an FTD device in routed mode?
A. by leveraging the ARP to direct traffic through the firewall
B. by assigning an inline set interface
C. by using a BVI and create a BVI IP address in the same subnet as the user segment
D. by bypassing protocol inspection by leveraging pre-filter rules
Answer: (SHOW ANSWER)
https://www.cisco.com/c/en/us/td/docs/security/firepower/640/configuration/guide/fpmc-config-guide-v64
/transparent_or_routed_firewall_mode_for_firepower_threat_defense.html

NEW QUESTION: 23
An organization is migrating their Cisco ASA devices running in multicontext mode to Cisco FTD devices.
Which action must be taken to ensure that each context on the Cisco ASA is logically separated in the Cisco FTD devices?
A. Configure the Cisco FTD to use port channels spanning multiple networks.
B. Configure a container instance in the Cisco FTD for each context in the Cisco ASA.
C. Add the Cisco FTD device to the Cisco ASA port channels.
D. Add a native instance to distribute traffic to each Cisco FTD context.
Answer: (SHOW ANSWER)

NEW QUESTION: 24
A user within an organization opened a malicious file on a workstation which in turn caused a ransomware attack on the network. What should be configured within the Cisco FMC to ensure the file is tested for viruses on a sandbox system?

A. Local malware analysis
B. Dynamic analysis
C. Capacity handling
D. Spere analysis
Answer: (SHOW ANSWER)

NEW QUESTION: 25
A security engineer is configuring a remote Cisco FTD that has limited resources and internet bandwidth.
Which malware action and protection option should be configured to reduce the requirement for cloud lookups?
A. Block File action and local malware analysis
B. Malware Cloud Lookup and dynamic analysis
C. Block Malware action and dynamic analysis
D. Block Malware action and local malware analysis
Answer: (SHOW ANSWER)

NEW QUESTION: 26
A network engineer must provide a high-level statistical summary of a Cisco Secure Firewall Threat Defense device. The organization is approaching its peak season, so network downtime must be minimized. Which type of report must the network engineer use?
A. Malware
B. SNMP
C. Risk
D. Host
Answer: (SHOW ANSWER)
SNMP provides nonintrusive, read-only monitoring of Secure Firewall Threat Defense devices and is appropriate for collecting high-level device statistics without interrupting production traffic. An external network management system can poll supported Management Information Base objects to obtain CPU utilization, memory usage, interface statistics, Snort information, process status, high-availability state, and cluster health. SNMP traps can also report important events without requiring continuous manual access to the device. Malware reports focus on malicious files and malware events, while risk reports summarize security risks and attacks. Host reports describe discovered hosts, applications, operating systems, and vulnerabilities rather than overall device performance. Because the requirement concerns device-level statistics and minimizing operational disruption during peak season, SNMP monitoring is the most appropriate choice.
Cisco Secure Firewall SNMP monitoring

NEW QUESTION: 27
A Cisco FTD has two physical interfaces assigned to a BVI. Each interface is connected to a different VLAN on the same switch. Which firewall mode is the Cisco FTD set up to support?
A. routed
B. active/active failover
C. high availability clustering
D. transparent
Answer: (SHOW ANSWER)

NEW QUESTION: 28

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: 29

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: 30



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:

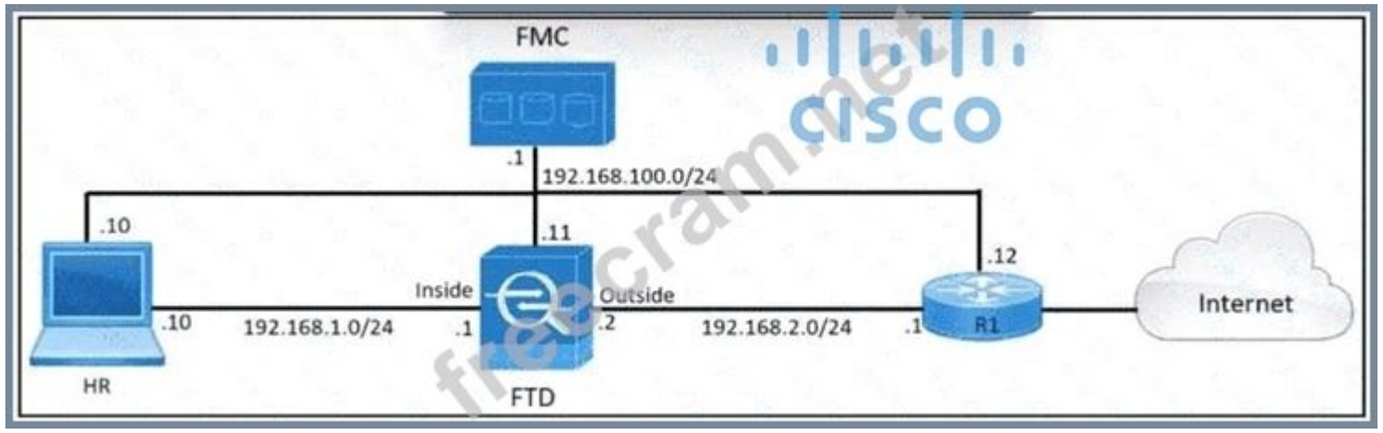


Explanation:

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



NEW QUESTION: 31
Refer to the exhibit.



An engineer must create a QoS policy in Cisco Secure Firewall Management Center to limit HTTP and HTTPS traffic originating from users in the HR department. The download and upload limits for HTTP and HTTPS traffic must both be set to 5 Mb/s. Drag and drop the values onto the corresponding QoS rule settings.



Answer:



Explanation:

Name # HTTP-HTTPS-QoS

Apply QoS On # Interfaces in Destination Interface Objects

Download/Upload Limit # 5 Mb/s

Source Interface Networks # 192.168.1.0/24

Destination Interface Networks # 192.168.2.0/24

Destination Ports # HTTP-HTTPS

The HR workstation resides on the inside 192.168.1.0/24 network, making that subnet the source-interface network. Internet-bound traffic exits through the 192.168.2.0/24 network, which must be configured as the destination-interface network. Because rate limiting must occur as traffic leaves toward the internet, QoS is applied to interfaces in the destination interface objects. The HTTP-HTTPS object identifies the destination ports for web traffic, while HTTP-HTTPS-QoS provides a descriptive rule name. Both download and upload limits are configured as 5 Mb/s. Cisco Secure Firewall applies a QoS limit independently on each selected interface and determines upload and

download direction based on the connection initiator. The Apply QoS On selection must correspond to a populated source or destination interface condition. Cisco Secure Firewall QoS configuration

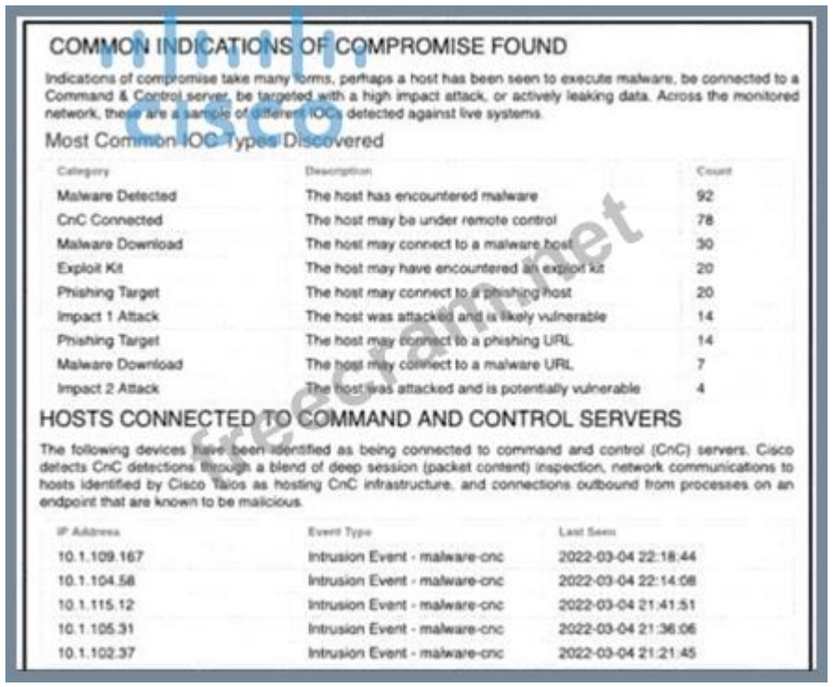
Valid 300-710 Dumps shared by ExamDiscuss.com for Helping Passing 300-710 Exam! ExamDiscuss.com now offer the **newest 300-710 exam dumps**, the ExamDiscuss.com 300-710 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com 300-710 dumps with Test Engine here: https://www.examdiscuss.com/Cisco/exam/300-710/premium/ (**446** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 32
Refer to the exhibit.



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

NEW QUESTION: 33



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. Trend analysis

C. Network-based detection

D. IP address and URL blacklisting

Answer: (SHOW ANSWER)

NEW QUESTION: 34

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. reporting

D. enforcement

Answer: B (LEAVE A REPLY)

NEW QUESTION: 35

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

A. BFD

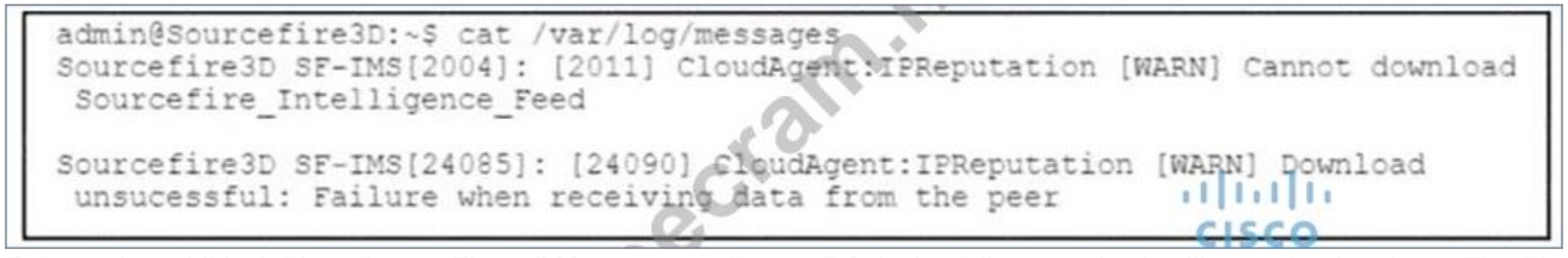
B. SGT

C. pxGrid

D. SNMP v3

Answer: (SHOW ANSWER)

NEW QUESTION: 36



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. Install a self-signed certificate on the proxy server for intelligence.sourcefire.com.

C. Bypass the proxy server for intelligence.sourcefire.com.

D. Ensure that proxy authentication is disabled for the Cisco Secure Firewall Management Center device.

Answer: (SHOW ANSWER)

NEW QUESTION: 37

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

A. Logging is not enabled for the rule.

B. The rule was not enabled after being created.

C. The wrong source interface for Snort was selected in the rule.

D. An incorrect application signature was used in the rule.

Answer: (SHOW ANSWER)

NEW QUESTION: 38

Which interface mode on the firewall must be deployed on a Cisco Secure Firewall Threat Defense when implementing an IPS using a SPAN port for traffic monitoring?

A. inline

B. passive

C. transparent

D. routed

Answer: (SHOW ANSWER)

NEW QUESTION: 39

Which two remediation options are available when Cisco FMC is integrated with Cisco ISE? (Choose two.)

A. dynamic null route configured

B. DHCP pool disablement

C. quarantine

D. port shutdown

E. host shutdown

Answer: (SHOW ANSWER)

Reference: https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/210524-configure- firepower-6-1-pxgrid-remediati.html

NEW QUESTION: 40

Which firewall design will allow It to forward traffic at layers 2 and 3 for the same subnet?

A. Cisco Firepower Threat Defense mode

B. routed mode

C. Integrated routing and bridging

D. transparent mode

Answer: (SHOW ANSWER)

Transparent mode is a firewall configuration in which the firewall acts as a "bump in the wire" or a "stealth firewall" and is not seen as a router hop to connected devices. In transparent mode, the firewall can forward traffic at both layer 2 and layer 3 for the same subnet, as it does not perform any address translation or routing. The firewall inspects the traffic and applies security policies based on the source and destination IP addresses, ports, and protocols. Transparent mode is useful when you want to deploy a firewall without changing the existing network topology or addressing scheme1.

NEW QUESTION: 41

Network users experience issues when accessing a server on a different network segment. An engineer investigates the issue by performing packet capture on Cisco Secure Firewall Threat Defense. The engineer expects more data and suspects that not all the traffic was collected during a 15-minute can't captured session.

Which action must the engineer take to resolve the issue?

A. Forward the captured data lo an FTP server

B. Increase the amount of RAM allocated for the capture.

C. Provide a file name to save the data.

D. Ensure that the allocated memory is sufficient.

Answer: (SHOW ANSWER)

When performing packet capture on a Cisco Secure Firewall Threat Defense (FTD) device, ensuring that the allocated memory is sufficient is crucial for capturing all necessary traffic during a specified capture session.

If users experience issues accessing a server and the engineer suspects not all traffic was collected, it indicates that the current memory allocation might not be enough to store the entire capture data for the 15-minute session.

Steps:

* Check the current memory allocation for packet captures on the FTD device.

* Increase the memory allocation if it is insufficient to handle the volume of traffic expected during the capture session.

This ensures that all relevant traffic is captured and can be analyzed to diagnose and resolve the network issue.

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

NEW QUESTION: 42

An engineer is configuring multiple Cisco FTD appliances (or use in the network. Which rule must the engineer follow while defining interface objects in Cisco FMC for use with interfaces across multiple devices?

A. Two security zones can contain the same interface

B. Interface groups can contain interfaces from many devices.

C. Interface groups can contain multiple interface types

D. An interface cannot belong to a security zone and an interface group

Answer: (SHOW ANSWER)

NEW QUESTION: 43

```
FMC: System > Monitor > [FTDv] > Advanced Troubleshooting > Packet Tracer

Interface: inside, Packet type: TCP, Source: 192.168.67.102, Source Port:
47381, Destination: 209.165.202.6, Destination Port: 443 (reduced output)


Phase: 1
Type: INPUT-ROUTE-LOOKUP, Subtype: Resolve Egress Interface, Result: ALLOW
Found next-hop 209.165.201.2 using egress ifc  public(vrfid:0)
Phase: 2
Type: ACCESS-LIST, Subtype: log, Result: ALLOW
Config: access-list CSM_FW_ACL_ remark rule-id 268434481: RULE: Allow_HTTPS
Phase: 3
Type: CONN-SETTINGS, Result: ALLOW
Phase: 4
Type: NAT, Result: ALLOW
Config:
object network NET67
 nat (inside,public) dynamic IP67
Additional Information: Dynamic translate 192.168.67.102/47381 to 192.168.67.67/
47381
Phase: 5 - 10
Result: ALLOW
Phase: 11
Type: ADJACENCY-LOOKUP, Subtype: Resolve Nexthop IP address to MAC, Result:
ALLOW
Additional Information: Found adjacency entry for Next-hop 209.165.201.2 on
interface  public
Adjacency :Active, MAC address 000c.296c.41c3 hits 5506 reference 2

Result:
input-interface: inside(vrfid:0)
input-status: up
input-line-status: up
output-interface: public(vrfid:0)
output-status: up
output-line-status: up
```



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. Unblock the access rule on FTDv.

B. Add the route to the destination.

C. Reconfigure NAT on FTDv.

D. Restart the client-side application.

Answer: (SHOW ANSWER)

NEW QUESTION: 44

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: 45
An administrator is attempting to add a new FTD device to their FMC behind a NAT device with a NAT ID of NAT001 and a password of Cisco0420l06525. The private IP address of the FMC server is 192.168.45.45.
which is being translated to the public IP address of 209.165.200.225/27. Which command set must be used in order to accomplish this task?
A. configure manager add 192.168.45,45 <reg_key> <nat_id>
B. configure manager add 209.165.200.225 <reg_key> <nat_id>
C. configure manager add 209.165.200.225/27 <reg_key> <nat_id>
D. configure manager add 209.165.200.225 255.255.255.224 <reg_key> <nat_id>
Answer: (SHOW ANSWER)

NEW QUESTION: 46
A security engineer is deploying a Cisco Secure Firewall Threat Defense device through Cisco Secure Firewall Management Center. The Threat license is installed, the Encrypted Visibility Engine is enabled in the access control policy Decryption policy is configured with the Decrypt - Resign action to inspect outbound TLS/SSL traffic. Users report that a banking applications repeatedly fails to load. The engineer confirms the endpoint performs certificate pinning to validate the server certificate. Engineer must allow the traffic to pass while all other outbound traffic continues to be inspected. The engineer created a rule that matches banking category and placed the rule above Decrypt - Resign policy. Which decryption rule action must be configured to meet the requirement?
A. Trust
B. Block
C. Do Not Decrypt
D. Decrypt - Known Key
Answer: (SHOW ANSWER)

Valid 300-710 Dumps shared by ExamDiscuss.com for Helping Passing 300-710 Exam! ExamDiscuss.com now offer the **newest 300-710 exam dumps**, the ExamDiscuss.com 300-710 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com 300-710 dumps with Test Engine here: https://www.examdiscuss.com/Cisco/exam/300-710/premium/ (**446** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 47
An engineer must define a URL object on Cisco FMC. What is the correct method to specify the URL without performing SSL inspection?
A. Specify all subdomains in the object group.
B. Include all URLs from CRL Distribution Points.
C. Use Subject Common Name value.
D. Specify the protocol in the object.
Answer: (SHOW ANSWER)

NEW QUESTION: 48
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 do not have Layer 3 connectivity to the FTD device for GRE traffic transmission.
B. The FTD must be configured with an ERSPAN port, not a passive port.
C. The switches were not set up with a monitor session ID (hat matches the flow ID defined on the FTD
D. The FTD must &e in routed mode to process ERSPAN traffic.
Answer: (SHOW ANSWER)

NEW QUESTION: 49
What acts as the remediation module for Rapid Threat Containment within Cisco Secure Firewall Management Center?
A. Adaptive Network Control
B. Cisco Secure Endpoint
C. Cisco Identity Services Engine
D. Network Protection Services
Answer: (SHOW ANSWER)
Cisco ISE Adaptive Network Control is the remediation module used for Rapid Threat Containment. Secure Firewall Management Center detects malicious activity or a correlation-policy violation and invokes an ANC remediation through the pxGrid integration. Cisco ISE then applies the specified ANC policy to the affected endpoint and can issue a RADIUS Change of Authorization to the relevant network-access device. The resulting action can quarantine the endpoint, restrict its authorization, or clear a previously applied ANC policy. Cisco ISE provides the policy and enforcement infrastructure, but the specific remediation module presented in Secure Firewall Management Center is Cisco ISE Adaptive Network Control. Cisco Secure Endpoint supplies endpoint detection and response telemetry but is not the RTC remediation module described. Network Protection Services is not the applicable Secure Firewall remediation component. Cisco Secure Firewall remediation modules

NEW QUESTION: 50
What is a valid Cisco AMP file disposition?
freecram.net
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: 51
Which action must be taken on the Cisco FMC when a packet bypass is configured in case the Snort engine is down or a packet takes too long to process?
A. Enable Inspect Local Router Traffic
B. Configure Fastpath rules to bypass inspection
C. Add a Bypass Threshold policy for failures
D. Enable Automatic Application Bypass
Answer: (SHOW ANSWER)

NEW QUESTION: 52
An engineer is configuring a Cisco Secure Firewall Management Center appliance. The company requires the use of a TAXII server in Threat Intelligence Director and requires the Action to be set to Block. On which two object types can the engineer configure the Block action? (Choose two.)
A. Observable
B. Element
C. Indicator
D. Complex indicator
E. Source
Answer: (SHOW ANSWER)
Threat Intelligence Director cannot apply Block directly to a TAXII source because STIX data obtained through TAXII can contain complex indicators. A managed device takes enforcement action based on individual observables, such as an IP address, URL, domain, or file hash. After the TAXII content has been ingested, an administrator can configure Block on an individual observable or on a simple indicator containing one actionable observable. Complex indicators combine multiple observables and therefore cannot be blocked directly; the administrator must instead block the appropriate individual observables within them.
An element is the managed device that receives published intelligence, not an intelligence object on which this action is configured. Consequently, the two supported object types are an observable and a simple indicator. Cisco Threat Intelligence Director documentation

NEW QUESTION: 53
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: (SHOW ANSWER)
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: 54

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

A. IPsec

B. SSH

C. MACsec

D. SSL

Answer: (SHOW ANSWER)

NEW QUESTION: 55

In a multi-tennent deployment where multiple domains are in use. which update should be applied outside of the Global Domain?

A. minor upgrade

B. Cisco Geolocation Database

C. local import of intrusion rules

D. local import of major upgrade

Answer: (SHOW ANSWER)

NEW QUESTION: 56

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: 57

An administrator is creating interface objects to better segment their network but is having trouble adding interfaces to the objects. What is the reason for this failure?

A. The interfaces are being used for NAT for multiple networks.

B. The administrator is adding interfaces of multiple types.

C. The administrator is adding an interface that is in multiple zones.

D. The interfaces belong to multiple interface groups.
Answer: (SHOW ANSWER)
https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-config-guide-v62/reusable_objects.html#ID-2243-000009b4
"All interfaces in an interface object must be of the same type: all inline, passive, switched, routed, or ASA FirePOWER. After you create an interface object, you cannot change the type of interfaces it contains."

NEW QUESTION: 58
A company is deploying intrusion protection on multiple Cisco FTD appliances managed by Cisco FMC.
Which system-provided policy must be selected if speed and detection are priorities?
A. Maximum Detection
B. Balanced Security and Connectivity
C. Connectivity Over Security
D. Security Over Connectivity
Answer: (SHOW ANSWER)

NEW QUESTION: 59
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. Modify the device's settings using the device management feature within Cisco FMC to force only secure protocols.
B. Enable the UCAPL/CC compliance on the device to support only the most secure protocols available.
C. Configure a FlexConfig object to disable any insecure TLS protocols on the Cisco FTD device.
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: 60
An engineer is troubleshooting an intermittent connectivity issue on a Cisco Secure Firewall Threat Defense appliance and must collect 24 hours' worth of data. The engineer started a packet capture. Whenever it stops prematurely during this time period. The engineer notices that the packet capture butter size is set to the default of 32 MB Which butter S170 is the maximum that the engineer must sot to able the packet capture to run successfully?
Freecram.net
A. 64 MB
B. 1 GB
C. 10 GB
D. 100 GB
Answer: (SHOW ANSWER)
To collect 24 hours' worth of data using a packet capture on a Cisco Secure Firewall Threat Defense (FTD) appliance without prematurely stopping due to buffer size limitations, the engineer should increase the packet capture buffer size. The default buffer size is 32 MB, which is insufficient for extended captures.
Steps:
* Access the packet capture configuration on the FTD device.
* Increase the buffer size to 1 GB, which provides a significantly larger capacity for capturing packets over a 24-hour period.

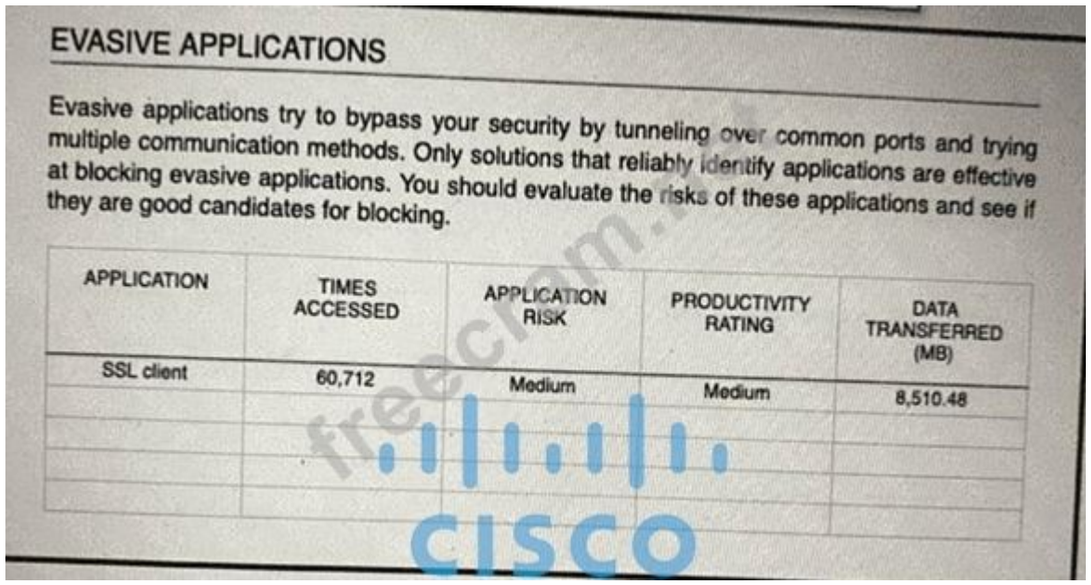
Setting the buffer size to 1 GB should accommodate a substantial amount of traffic and prevent the capture from stopping prematurely.
References: Cisco Secure Firewall Threat Defense Configuration Guide, Chapter on Packet Capture Configuration and Management.

NEW QUESTION: 61
An engineer has been tasked with using Cisco FMC to determine if files being sent through the network are malware. Which two configuration tasks must be performed to achieve this file lookup? (Choose two).
A. The Cisco FMC needs to include a SSL decryption policy.
B. The Cisco FMC needs to connect to the Cisco ThreatGrid service directly for sandboxing.
C. The Cisco FMC needs to include a file inspection policy for malware lookup.
D. The Cisco FMC needs to connect with the FireAMP Cloud.
E. The Cisco FMC needs to connect to the Cisco AMP for Endpoints service.
Answer: (SHOW ANSWER)

Valid 300-710 Dumps shared by ExamDiscuss.com for Helping Passing 300-710 Exam! ExamDiscuss.com now offer the **newest 300-710 exam dumps**, the ExamDiscuss.com 300-710 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com 300-710 dumps with Test Engine here: https://www.examdiscuss.com/Cisco/exam/300-710/premium/ (**446** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 62
An organization is configuring a new Cisco Firepower High Availability deployment. Which action must be taken to ensure that failover is as seamless as possible to end users?
A. Use a dedicated stateful link between chassis.
B. Load the same software version on both chassis.
C. Set up a virtual failover MAC address between chassis.
D. Set the same FQDN for both chassis.
Answer: (SHOW ANSWER)

NEW QUESTION: 63
Refer to the exhibit.



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 Cisco AMP for Endpoints to block all SSL connection

D. Use SSL decryption to analyze the packets.

Answer: (SHOW ANSWER)

NEW QUESTION: 64

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. Tetra

B. RBAC

C. Spero

D. Ethos

Answer: (SHOW ANSWER)

NEW QUESTION: 65

A network administrator wants to configure a new Secure Firewall Threat Defense instance, which is managed by Cisco Secure Firewall Management Center, to load balance internet-bound traffic across multiple zones. Secure Firewall is connected to upstream ISP devices in multiple Zones. Which action must be taken to meet the requirement?

A. Add multiple dynamic routes set up via flex configuration to multiple zones.

B. Configure multiple static default routes to multiple zones towards upstream ISP devices.

C. Implement OSPF and static route towards to upstream ISP devices.

D. Enable BGP and OSPF towards upstream ISP devices.

Answer: (SHOW ANSWER)

NEW QUESTION: 66

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

A. Inspect Local Traffic Bypass

B. Fast-Path Rules Bypass

C. Automatic Application Bypass

D. Cisco ISE Security Group Tag

Answer: (SHOW ANSWER)

NEW QUESTION: 67

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

A. BGPv6

B. ECMP with up to three equal cost paths across multiple interfaces

C. ECMP with up to three equal cost paths across a single interface

D. BGPv4 in transparent firewall mode

E. BGPv4 with nonstop forwarding

Answer: A,C (LEAVE A REPLY)

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

NEW QUESTION: 68

A network engineer sets up a secondary Cisco FMC that is integrated with Cisco Security Packet Analyzer What occurs when the secondary Cisco FMC synchronizes with the primary Cisco FMC?

A. The existing configuration for integration of the secondary Cisco FMC the Cisco Security Packet Analyzer is overwritten.

B. The synchronization between the primary and secondary Cisco FMC fails

C. The secondary Cisco FMC must be reintegrated with the Cisco Security Packet Analyzer after the synchronization

D. The existing integration configuration is replicated to the primary Cisco FMC

Answer: (SHOW ANSWER)

NEW QUESTION: 69

An engineer currently has a Cisco FTD device registered to the Cisco FMC and is assigned the address of 10 10.50.12. The organization is upgrading the addressing schemes and there is a requirement to convert the addresses to a format that provides an adequate amount of addresses on the network What should the engineer do to ensure that the new addressing takes effect and can be used for the Cisco FTD to Cisco FMC connection?

A. Update the IP addresses from IFV4 to IPv6 without deleting the device from Cisco FMC

B. Cisco FMC does not support devices that use IPv4 IP addresses.

C. Format and reregister the device to Cisco FMC.

D. Delete and reregister the device to Cisco FMC

Answer: (SHOW ANSWER)

NEW QUESTION: 70

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?

Freecram.net

A. creating an Access Control Policy with an INSIDE_NET network object and object overrides

B. utilizing a dynamic Access Control Policy that updates from Cisco Talos

C. utilizing policy inheritance

D. creating a unique Access Control Policy per device

Answer: (SHOW ANSWER)

NEW QUESTION: 71

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. Add a TAXII server.

C. Enable REST API access.

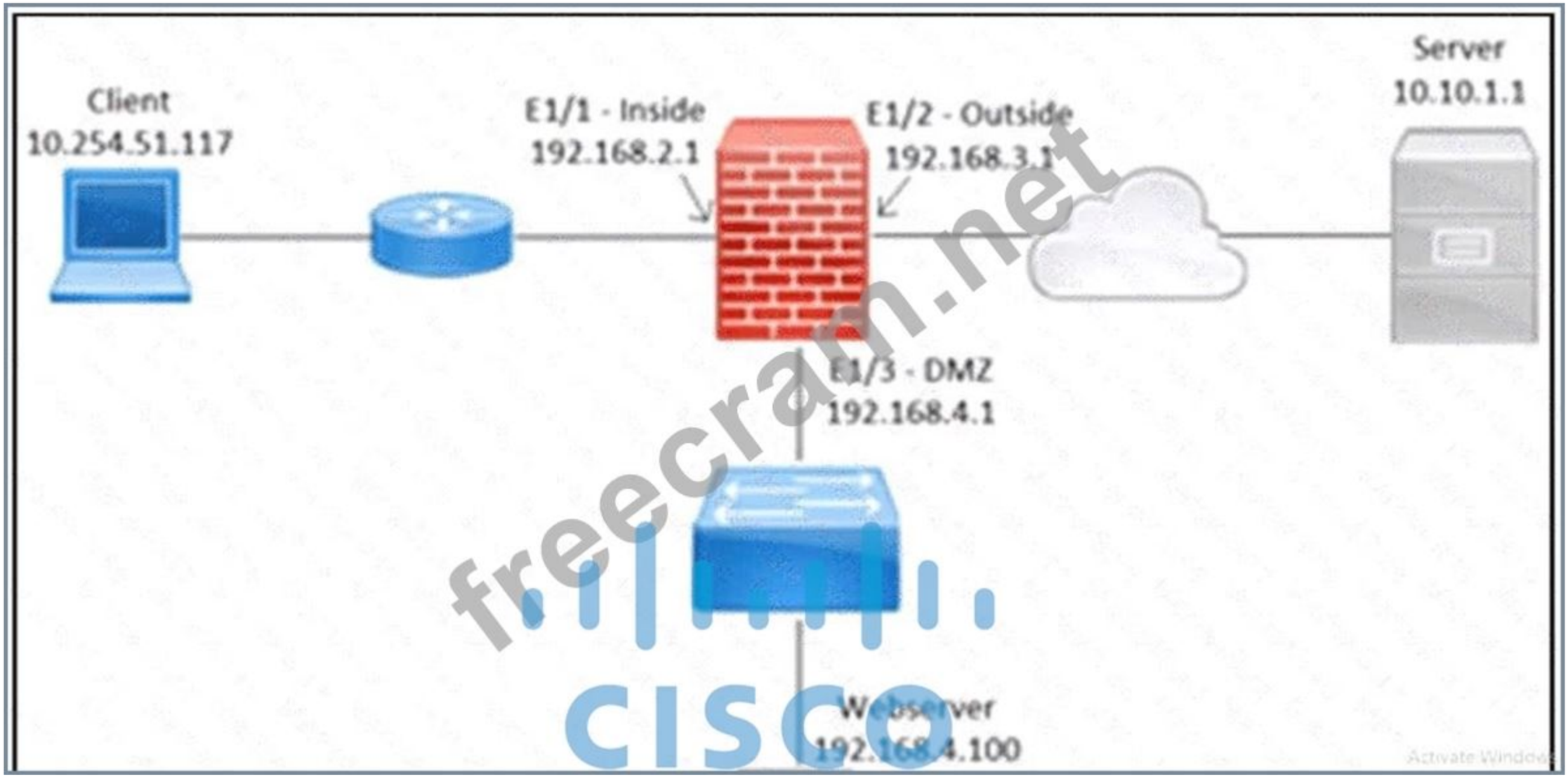
D. Add 7 GB of memory.

E. Add the URL of the TAXII server.

Answer: (SHOW ANSWER)

NEW QUESTION: 72

Refer to the exhibit.



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

A. Configure the inside interface to send ACK messages.

B. Add a firewall rule that allows the web server to communicate with the DMZ.

C. Add a firewall rule that allows ACK responses from the inside to the outside.

D. Configure the outside interface to receive SYN-ACK messages.

Answer: (SHOW ANSWER)

The capture shows that the client repeatedly transmits a TCP SYN but does not receive the SYN-ACK required to advance the connection state. This indicates that the return portion of the TCP three-way handshake is not reaching the expected ingress interface or is not being processed there. The outside interface must therefore be configured or connected so that the returning SYN-ACK packets arrive through the interface where the firewall expects them. An access rule does not instruct an interface to generate TCP acknowledgement messages; ACK and SYN-ACK packets are produced by the communicating endpoints.

Likewise, permitting communication "with the DMZ" does not address the missing return-handshake packet shown in the capture. Correcting the return path through the outside interface allows the firewall to observe both directions, establish state, and forward the subsequent packets.

NEW QUESTION: 73

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: 74
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: 75
A hospital network needs to upgrade their Cisco FMC managed devices and needs to ensure that a disaster recovery process is in place. What must be done in order to minimize downtime on the network?
A. Configure a second circuit to an ISP for added redundancy
B. Configure the Cisco FMC managed devices for clustering.
C. Keep a copy of the current configuration to use as backup
D. Configure the Cisco FMCs for failover
Answer: (SHOW ANSWER)

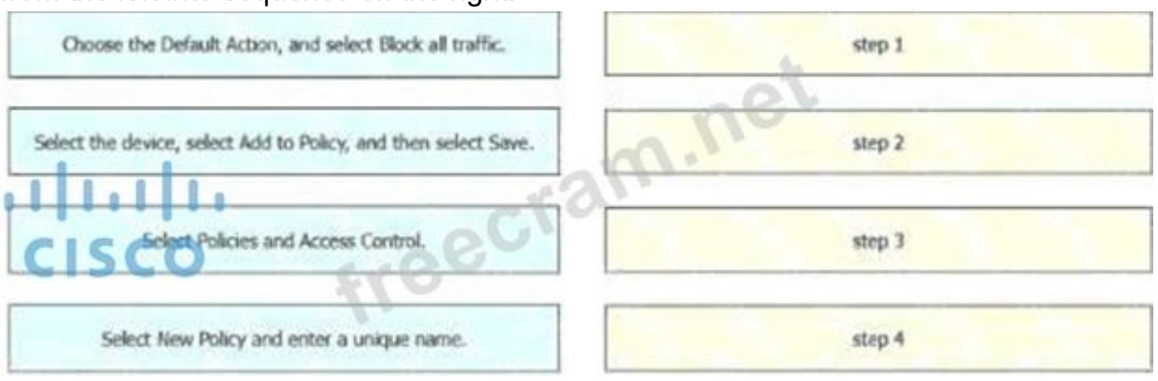
NEW QUESTION: 76
An engineer is configuring a cisco FTD appliance in IPS-only mode and needs to utilize fail-to-wire interfaces. Which interface mode should be used to meet these requirements?
A. transparent
B. routed
C. passive
D. inline set
Answer: (SHOW ANSWER)

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

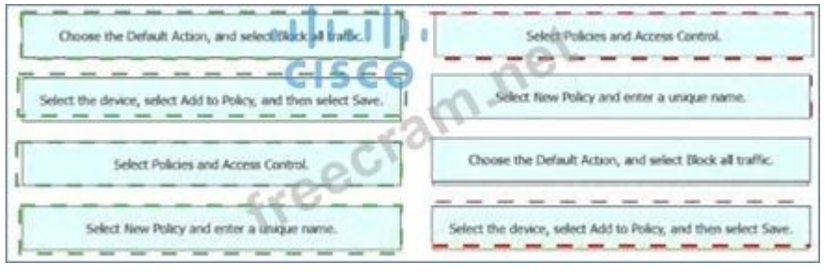
Valid 300-710 Dumps shared by ExamDiscuss.com for Helping Passing 300-710 Exam! ExamDiscuss.com now offer the **newest 300-710 exam dumps**, the ExamDiscuss.com 300-710 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com 300-710 dumps with Test Engine here: https://www.examdiscuss.com/Cisco/exam/300-710/premium/ (**446** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 77
Which feature within the Cisco FMC web interface allows for detecting, analyzing and blocking malware in network traffic?
A. intrusion and file events
B. file policies
C. Cisco AMP for Endpoints
D. Cisco AMP for Networks
Answer: (SHOW ANSWER)

NEW QUESTION: 78
An engineer must create a basic access control policy in the Cisco Secure Firewall Management Center to block all traffic by default. Drag and drop the configuration actions from the left into sequence on the right.



Answer:





NEW QUESTION: 79
A network engineer must configure an existing firewall to have a NAT configuration. The now configuration must support more than two interlaces per context. The firewall has previously boon operating transparent mode. The Cisco Secure Firewall Throat Defense (FTD) device has been deregistered from Cisco Secure Firewall Management Center (FMC). Which set of configuration actions must the network engineer take next to meet the requirements?
A. Run the configure manager add routed command from the Secure FTD device CL1, and reregister with Secure FMC.
B. Run the configure firewall routed command from the Secure FTD device CD, and reregister with Secure FMC.
C. Run the configure manager add routed command from the Secure FMC CLI. and reregister with Secure FMC.
D. Run the configure firewall routed command from the Secure FMC CLI. and reregister with Secure FMC.
Answer: (SHOW ANSWER)
To support more than two interfaces per context and enable NAT configurations, the firewall must operate in routed mode. Since the firewall was previously in transparent mode, the network engineer needs to change it to routed mode.
Steps:
Access the CLI of the Secure FTD device.
Run the commandconfigure firewall routedto switch the firewall from transparent mode to routed mode.
Reregister the FTD device with the FMC by running theconfigure manager add < FMC_IP > < Registration_Key > command from the FTD device CLI.
This will ensure that the firewall can support the required NAT configurations and more than two interfaces per context.
References:Cisco Secure Firewall Management Center Device Configuration Guide, Chapter on Routed Mode Configuration.

NEW QUESTION: 80
A network administrator is implementing an active/passive high availability Cisco FTD pair. When adding the high availability pair, the administrator cannot select the secondary peer. What is the cause?
A. The second Cisco FTD is not the same model as the primary Cisco FTD.
B. An high availability license must be added to the Cisco FMC before adding the high availability pair.
C. The failover link must be defined on each Cisco FTD before adding the high availability pair.
D. Both Cisco FTD devices are not at the same software Version
Answer: (SHOW ANSWER)

NEW QUESTION: 81
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. inline tap mode
B. propagate link state

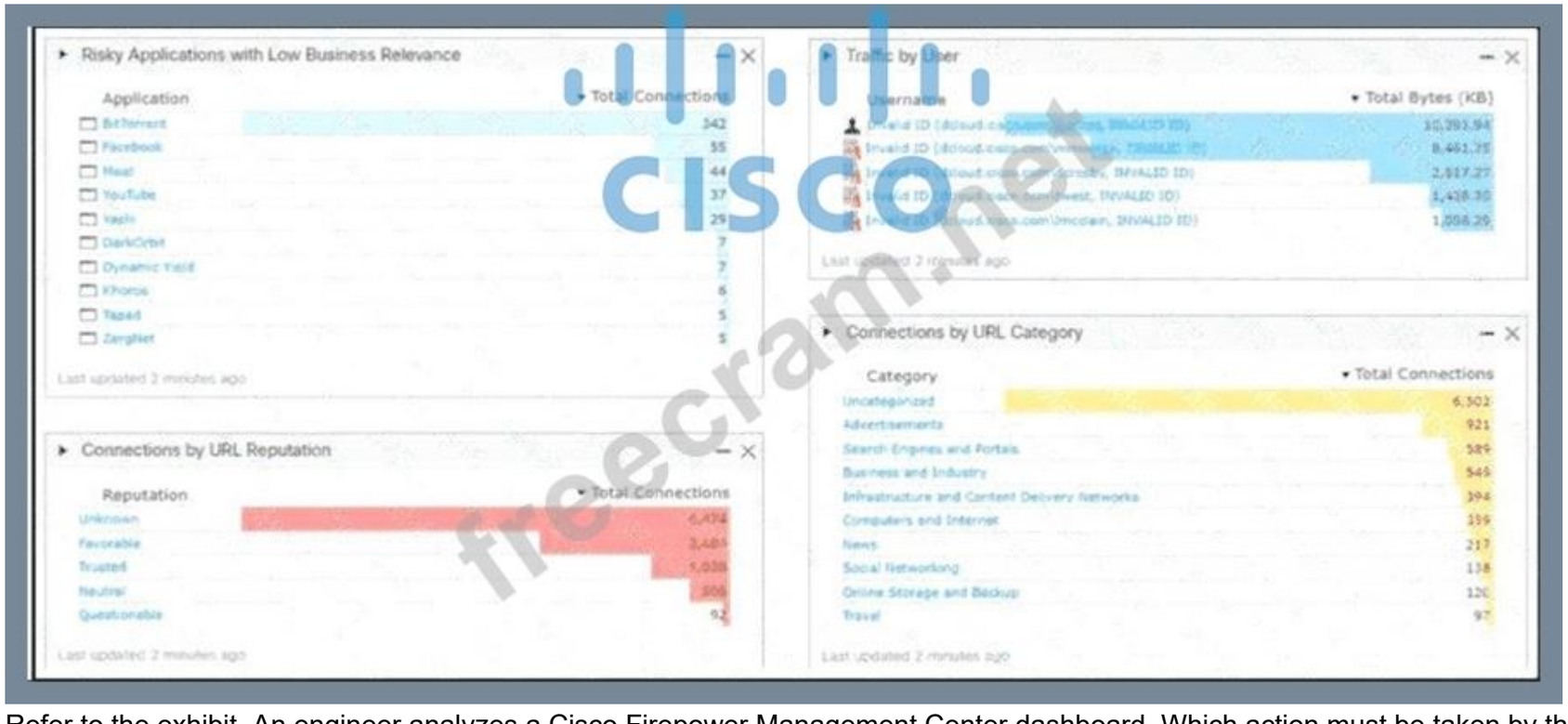
C. Snort fail open

D. strict TCP enforcement

Answer: (SHOW ANSWER)

NEW QUESTION: 82





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

A. Block the use of Dropbox.

B. Block all the BitTorrent applications.

C. Stop all the URLs that are uncategorized.

D. Stop all URLs that have an unknown reputation.

Answer: (SHOW ANSWER)

NEW QUESTION: 83

Which interface type allows packets to be dropped?

A. passive

B. inline

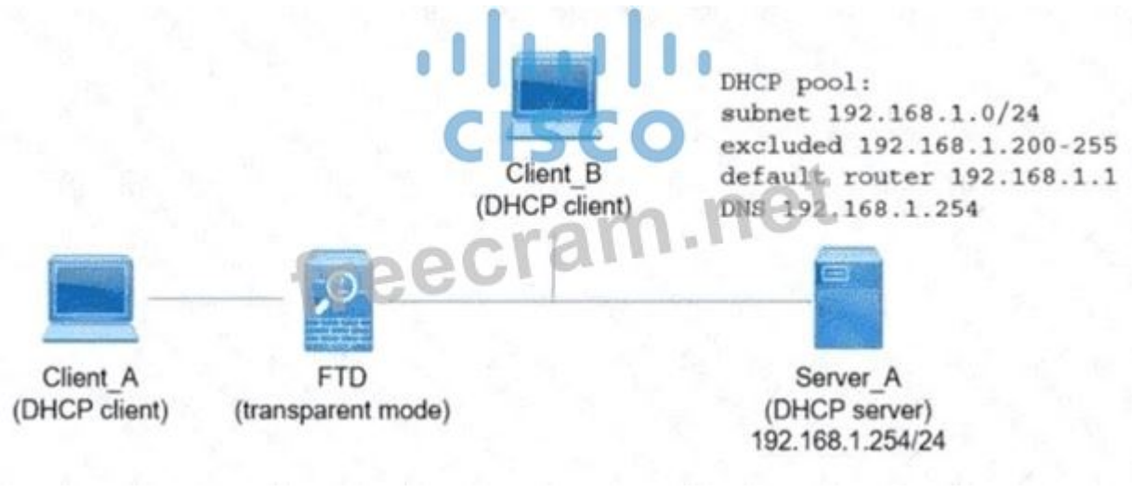
C. ERSPAN

D. TAP

Answer: (SHOW ANSWER)

Reference: https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/200908-configuring- firepower- threat-defense-int.html

NEW QUESTION: 84



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. Add access rules that allow DHCP traffic by using Cisco Secure Firewall Management Center.

B. Disable all the DHCP Snort rules by using Secure Firewall Device Manager.

C. Add another DHCP pool on Server_A with DHCP relay on Secure Firewall Threat Defense.

D. Disable Option 82 in the DHCP relay configuration properties using Secure Firewall Management Center.

Answer: (SHOW ANSWER)

NEW QUESTION: 85



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 that allows the entire ICMP protocol suite

B. Outbound access rule with the Block with reset action

C. Inbound access rule that allows TCP reset packets from outside
Answer: (SHOW ANSWER)

NEW QUESTION: 86
What is needed to start a threat investigation in Cisco XDR?
A. indicator of attack
B. indicator of compromise
C. user name
D. local IP address
Answer: (SHOW ANSWER)

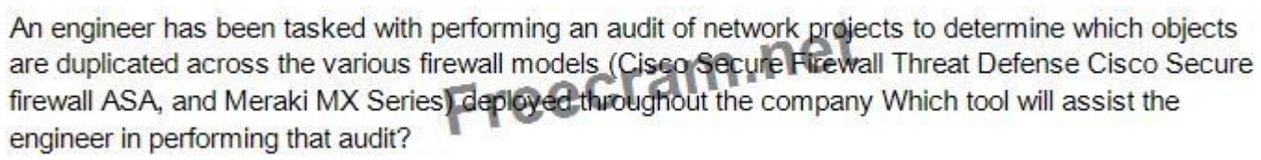
NEW QUESTION: 87
An engineer must implement Cisco Secure Firewall transparent mode due to a new server recently being added that must communicate with an existing server that is currently separated by the firewall. Which implementation action must be taken next by the engineer to accomplish the goal?
A. Configure the same default gateway for both servers.
B. Assign the same subnet to both servers.
C. Enable both servers to share the same VXLAN segment.
D. Ensure that both servers are in the same bridge domain.
Answer: (SHOW ANSWER)

NEW QUESTION: 88
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: 89
An engineer needs to configure remote storage on Cisco FMC. Configuration backups must be available from a secure location on the network for disaster recovery. Reports need to back up to a shared location that auditors can access with their Active Directory logins. Which strategy must the engineer use to meet these objectives?
A. Use SMB for backups and NFS for reports.
B. Use NFS for both backups and reports.
C. Use SMB for both backups and reports.
D. Use SSH for backups and NFS for reports.
Answer: (SHOW ANSWER)

https://www.cisco.com/c/en/us/td/docs/security/firepower/640/configuration/guide/fpmc-config-guide-v64/system_configuration.html#ID-2241-00000551
"You cannot send backups to one remote system and reports to another, but you can choose to send either to a remote system and store the other on the Firepower Management Center."

NEW QUESTION: 90



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: 91
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: (SHOW ANSWER)
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

Valid 300-710 Dumps shared by ExamDiscuss.com for Helping Passing 300-710 Exam! ExamDiscuss.com now offer the **newest 300-710 exam dumps**, the ExamDiscuss.com 300-710 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com 300-710 dumps with Test Engine here: https://www.examdiscuss.com/Cisco/exam/300-710/premium/ (**446** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 92
When deploying a Cisco ASA Firepower module, an organization wants to evaluate the contents of the traffic without affecting the network. It is currently configured to have more than one instance of the same device on the physical appliance Which deployment mode meets the needs of the organization?
A. inline tap monitor-only mode
B. passive monitor-only mode
C. passive tap monitor-only mode
D. inline mode
Answer: (SHOW ANSWER)
https://www.cisco.com/c/en/us/td/docs/security/asa/asa910/configuration/firewall/asa-910-firewall-config
/access-sfr.html
Inline tap monitor-only mode (ASA inline)-In an inline tap monitor-only deployment, a copy of the traffic is sent to the ASA FirePOWER module, but it is not returned to the ASA. Inline tap mode lets you see what the ASA FirePOWER module would have done to traffic, and lets you evaluate the content of the traffic, without impacting the network. However, in this mode, the ASA does apply its policies to the traffic, so traffic can be dropped due to access rules, TCP normalization, and so forth.

NEW QUESTION: 93
An engineer must import three port objects into the Cisco Secure Firewall Management Center by using a CSV file. Which file content must be imported to meet the requirement?
A.
```
Name;Protocol;Port;ICMPCode;ICMPType;
port1;tcp;;;;
mail;smptp;;;
EchoRequest;icmp;;;;
```
B.
```
NAME;PROTOCOL;PORT;
port1;tcp;4154;;;
mail;smptp;;;
EchoRequest;icmp;;
```
C.
```
Name;Protocol;Port;ICMPCode;ICMPType;
port1;tcp;4154;;;
mail;smptp;;;
Echo;ip;;8;0;
```
D.
```
NAME;PROTOCOL;PORT;ICMPCODE;ICMPTYPE;
port1;tcp;4154;;;
mail;tcp;25;;;
EchoRequest;icmp;;8;0;
```
Answer: (SHOW ANSWER)

NEW QUESTION: 94
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: 95
Which feature is supported by IRB on Cisco FTD devices?
A. EtherChannel interface
B. dynamic routing protocol
C. high-availability cluster
D. redundant interface
Answer: (SHOW ANSWER)

NEW QUESTION: 96
An administrator is configuring a new report template off. of a saved search within Cisco Secure Firewall Management Centre. The goal is to use the malware analysis report template, but use a different type saved search as the basis. The report is not working. What must be considered when configuring this report template?
A. Saved searches can be used for the same report template only
B. Saved searches are available freely for all report templates within the same domain.
C. Saved searches from a different report template must be used.
D. Saved searches must be renamed before using for different report template.
Answer: (SHOW ANSWER)
When configuring a new report template based on a saved search in Cisco Secure Firewall Management Center (FMC), it is important to note that saved searches are specific to the report template they were created with. Saved searches cannot be freely used across different report templates.
To use a different type of saved search, you must ensure that it aligns with the specific report template being used. This restriction ensures that the saved search parameters match the report's data requirements.

References:Cisco Secure Firewall Management Center Administrator Guide, Chapter on Reporting and Saved Searches.

NEW QUESTION: 97
A VPN administrator converted an instance of Cisco Secure Firewall Threat Defense, which is managed by Cisco Secure Firewall Management Center, from using LDAP to LDAPS for remote access VPN authentication. Which certificate must be added to allow for remote users to authenticate over the VPN?
A. Secure Firewall Management Center certificate must be added to the LDAPS server.
B. LDAPS server certificate must be added to Secure Firewall Management Center realms.
C. Secure Firewall Threat Defense certificate must be added to the LDAPS server.
D. LDAPS server certificate must be added to Secure Firewall Threat Defense.
Answer: (SHOW ANSWER)

NEW QUESTION: 98
An engineer wants to convert a Cisco Secure Firewall Threat Defense device that is currently managed by Cisco Secure Firewall Management Center from routed mode to transparent mode. Which CLI command must the engineer execute first to perform this conversion?
A. no configure manager
B. no configure firewall routed
C. configure manager delete
D. configure firewall transparent
Answer: (SHOW ANSWER)
The Threat Defense device cannot change its firewall mode while it has an active manager configuration.
After unregistering the device from Management Center, the engineer must execute configure manager delete to remove the manager association and place the device in No Manager Mode. The engineer can then execute configure firewall transparent to change the operating mode. Changing firewall modes clears the device configuration because routed-mode and transparent-mode interface configurations are incompatible. After completing the conversion, the engineer must configure the Management Center association again with configure manager add and register the device. Options A and B are not valid Threat Defense CLI commands.
Option D performs the actual mode conversion, but it is not the first required CLI command while the manager association remains configured. Cisco Threat Defense command reference

NEW QUESTION: 99
An engineer must configure a Cisco FMC dashboard in a child domain. Which action must be taken so that the dashboard is visible to the parent domain?
A. Add a separate tab.
B. Adjust policy inheritance settings.
C. Add a separate widget.
D. Create a copy of the dashboard.
Answer: (SHOW ANSWER)

NEW QUESTION: 100
What is a characteristic of bridge groups on a Cisco FTD?
A. In routed firewall mode, routing between bridge groups is supported.
B. Routing between bridge groups is achieved only with a router-on-a-stick configuration on a connected router
C. In routed firewall mode, routing between bridge groups must pass through a routed interface.
D. In transparent firewall mode, routing between bridge groups is supported

Answer: (SHOW ANSWER)

NEW QUESTION: 101
An engineer must configure a passive interface on a Cisco Secure IPS by using the Cisco Secure Firewall Management Center. These configurations have been performed already:
*Set the interface mode to Passive.
*Configure the MTU.
*Set the speed and duplex. Which action completes the configuration?
A. Reset the NGIPS
B. Reregister the NGIPS.
C. Enable the bridge virtual interface.
D. Enable the interface.
Answer: (SHOW ANSWER)

NEW QUESTION: 102
An engineer is configuring a new Cisco Secure Firewall Management Center appliance. Secure Firewall Management Center must report on peer-to-peer applications used on the network and identify which applications pose the greatest risk to the network. Which template must the engineer configure to generate the report?
A. Attacks Risk Report
B. Network Risk Report
C. User Risk Report
D. Advanced Malware Risk Report
Answer: (SHOW ANSWER)

NEW QUESTION: 103
An engineer must build redundancy into the network and traffic must continuously flow if a redundant switch in front of the firewall goes down. What must be configured to accomplish this task?
A. redundant interfaces on the firewall cluster mode and switches
B. redundant interfaces on the firewall noncluster mode and switches
C. vPC on the switches to the interface mode on the firewall duster
D. vPC on the switches to the span EtherChannel on the firewall cluster
Answer: (SHOW ANSWER)
Reference: https://www.ciscolive.com/c/dam/r/ciscolive/us/docs/2018/pdf/BRKSEC-2020.pdf

NEW QUESTION: 104
After deploying a network-monitoring tool to manage and monitor networking devices in your organization, you realize that you need to manually upload an MIB for the Cisco FMC. In which folder should you upload the MIB file?
A. /etc/sf/DCMIB.ALERT
B. /sf/etc/DCEALERT.MIB
C. /etc/sf/DCEALERT.MIB
D. system/etc/DCEALERT.MIB
Answer: (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-External-Responses.pdf

NEW QUESTION: 105
Which two solutions are used to access and view aggregated log data from the firewalls using Cisco Security Analytics and Logging? (Choose two.)
A. Secure Cloud Analytics
B. Cisco Prime Infrastructure
C. Cisco Secure Network Analytics
D. Cisco Defense Orchestrator
E. Cisco Catalyst Center
Answer: (SHOW ANSWER)

NEW QUESTION: 106


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. inline set MTU set to 1500
B. propagate link state disabled
C. FailSafe disabled
D. security zone set to OUTSIDE_ZONE
Answer: (SHOW ANSWER)

Valid 300-710 Dumps shared by ExamDiscuss.com for Helping Passing 300-710 Exam! ExamDiscuss.com now offer the **newest 300-710 exam dumps**, the ExamDiscuss.com 300-710 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com 300-710 dumps with Test Engine here: https://www.examdiscuss.com/Cisco/exam/300-710/premium/ (**446** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 107
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. The widget is configured to display only when active events are present.
B. The security analyst role does not have permission to view this widget.

C. The widget is not configured within the Cisco FMC.
D. An API restriction within the Cisco FMC is preventing the widget from displaying.
Answer: (SHOW ANSWER)

NEW QUESTION: 108
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: 109
A security administrator must configure Cisco Secure Firewall Management Center so that certain intrusion rules are active only during specified times. Which action must the administrator take?
A. Assign a time range directly to every intrusion rule in the intrusion policy.
B. Configure a time-based trigger in the intrusion policy to enable the rules at defined times.
C. Create time-based access control rules that apply the intrusion policy at the scheduled intervals.
D. Create a scheduled task that activates and deactivates the intrusion rules at the required times.
Answer: (SHOW ANSWER)
Individual intrusion rules do not support direct time-range conditions or scheduled activation triggers. Instead, the administrator creates a time-range object and uses it as a condition in an access control rule. The required intrusion policy is then associated with that access control rule. During the specified time range, matching traffic invokes the intrusion policy and its enabled intrusion rules; outside the range, the access control rule does not match. Multiple access control rules can be created when different intrusion policies or protection levels are needed at different times. Secure Firewall Management Center does not require an external scheduled task to enable and disable individual intrusion rules. Cisco documents time-range objects as the mechanism for making supported policies apply only during defined periods. Therefore, time-based access control rules are the correct implementation. Cisco time-range objects

NEW QUESTION: 110

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

A. configure coredump packet-engine enable

B. capture-traffic

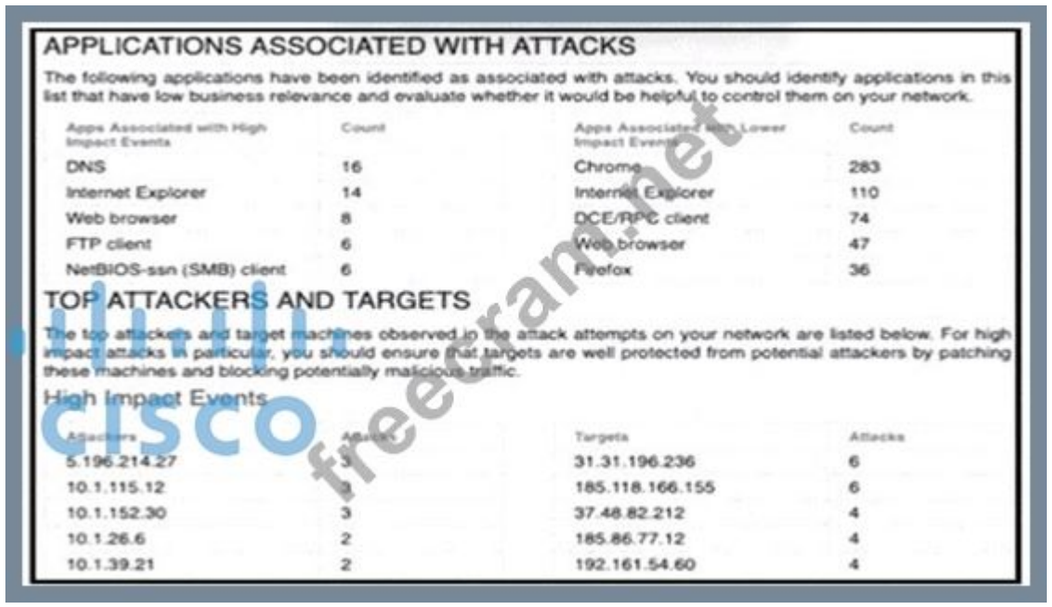
C. capture

D. capture WORD

Answer: (SHOW ANSWER)

Reason: the command " capture-traffic " is used for SNORT Engine Captures. To capture a LINA Engine Capture, you use the " capture " command. Since the Lina Engine represents the actual physical interface of the device, " capture " is the only reasonable choice Reference:https://www.cisco.com/c/en/us/support/docs /security/firepower-ngfw/212474-working-with-firepower-threat-defense-f.html#anc10 The command is firepower# capture DMZ interface dmz trace detail match ip host 192.168.76.14 host 192.168.76.100 firepower# capture INSIDE interface inside trace detail match ip host 192.168.76.14 host 192.168.75.14

NEW QUESTION: 111


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: 112
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. passive
B. Inline tap
C. routed
D. transparent
Answer: B (LEAVE A REPLY)

NEW QUESTION: 113
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: A (LEAVE A REPLY)
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: 114
An organization has noticed that malware was downloaded from a website that does not currently have a known bad reputation. How will this issue be addresses globally in the quickest way possible and with the least amount of impact?
A. by creating a URL object in the policy to block the website
B. by Isolating the endpoint
C. by denying outbound web access
D. Cisco Talos will automatically update the policies.

Answer: (SHOW ANSWER)

NEW QUESTION: 115
Which two packet captures does the FTD LINA engine support? (Choose two.)
A. Layer 7 network ID
B. source IP
C. application ID
D. dynamic firewall importing
E. protocol
Answer: (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: 116
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. Disable TCP inspection.
D. Enable lhe FXOS for multi-instance.
Answer: (SHOW ANSWER)

NEW QUESTION: 117
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. There is a host limit set.
B. Cisco AMP for Networks is unable to contact Cisco Threat Grid Cloud.
C. The user agent status is set to monitor.
D. Cisco AMP for Networks is unable to contact Cisco Threat Grid on premise.
Answer: (SHOW ANSWER)

NEW QUESTION: 118
What is the advantage of having Cisco Firepower devices send events to Cisco Threat Response via the security services exchange portal directly as opposed to using syslog?
A. Cisco Firepower devices do not need to be connected to the Internet.
B. An on-premises proxy server does not need to be set up and maintained.
C. All types of Cisco Firepower devices are supported.
D. Supports all devices that are running supported versions of Cisco Firepower.
Answer: (SHOW ANSWER)

NEW QUESTION: 119

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: 120

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

A. apex

B. mobility

C. base

D. plus

Answer: (SHOW ANSWER)

NEW QUESTION: 121

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

A. VPN connections can be re-established only if the failed master unit recovers.

B. Smart License is required to maintain VPN connections simultaneously across all cluster units.

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

D. Only established VPN connections are maintained when a new master unit is elected.

Answer: C (LEAVE A REPLY)

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

Valid 300-710 Dumps shared by ExamDiscuss.com for Helping Passing 300-710 Exam! ExamDiscuss.com now offer the **newest 300-710 exam dumps**, the ExamDiscuss.com 300-710 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com 300-710 dumps with Test Engine here: https://www.examdiscuss.com/Cisco/exam/300-710/premium/ (**446** Q&As Dumps, **35%OFF Special Discount Code: freecram**)

NEW QUESTION: 122

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

A. application detector

B. access control

C. intrusion

D. correlation

Answer: (SHOW ANSWER)

A correlation policy is a feature that allows you to respond in real time to threats or specific conditions on your network, using correlation rules. A correlation rule can trigger when the system generates a specific type of event, or when your network traffic deviates from its normal profile1. When a correlation rule triggers, the system generates a correlation event and can also launch a response, such as sending an alert, blocking an IP address, or scanning a host1.
In this case, the security engineer can configure a correlation rule that triggers when the system detects five or more connections from external sources within 2 minutes. The engineer can also configure a response that sends an alert to the FMC or an email recipient when this condition is triggered. The engineer can then create a correlation policy that includes this rule and activate it on the FTD device1.
The other options are incorrect because:
* An application detector is a feature that allows you to detect web applications, clients, and application protocols based on patterns in network traffic. An application detector does not generate alerts based on the number of connections from external sources2.
* An access control policy is a feature that allows you to control traffic flow through your network and inspect traffic for intrusions, malware, and files. An access control policy does not generate alerts based on the number of connections from external sources3.
* An intrusion policy is a feature that allows you to detect and prevent malicious network activity using Snort rules. An intrusion policy does not generate alerts based on the number of connections from external sources4.

NEW QUESTION: 123
Which firewall mode is Cisco Secure Firewall Threat Defense in when two physical interfaces are assigned to a named BVI?
A. routed
B. transparent
C. in-line
D. IPS only
Answer: B (LEAVE A REPLY)

NEW QUESTION: 124
IT management is asking the network engineer to provide high-level summary statistics of the Cisco FTD appliance in the network. The business is approaching a peak season so the need to maintain business uptime is high. Which report type should be used to gather this information?
A. Malware Report
B. SNMP Report
C. Risk Report
D. Standard Report
Answer: (SHOW ANSWER)

NEW QUESTION: 125
What is the advantage of having Cisco Firepower devices send events to Cisco Threat response via the security services exchange portal directly as opposed to using syslog?
A. Firepower devices do not need to be connected to the internet.
B. All types of Firepower devices are supported.
C. Supports all devices that are running supported versions of Firepower
D. An on-premises proxy server does not need to set up and maintained
Answer: (SHOW ANSWER)
Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/integrations/CTR/ Firepower_and_Cisco_Threat_Response_Integration_Guide.pdf

NEW QUESTION: 126

In which two places can thresholding settings be configured? (Choose two.)
A. on each IPS rule
B. globally, within the network analysis policy
C. globally, per intrusion policy
D. on each access control rule
E. per preprocessor, within the network analysis policy
Answer: (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.pdf

NEW QUESTION: 127
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: 128
A network administrator must send a daily email report to management detailing changes made during the previous 24 hours in Cisco Secure Firewall Management Center. Which system setting must be enabled to meet this requirement?
A. Change Reconciliation
B. Send Audit Log to HTTP Server
C. Send Audit Log to Syslog
D. STIG Compliance
Answer: (SHOW ANSWER)
Change Reconciliation records snapshots whenever users save system-configuration changes and combines those snapshots into a detailed report covering the previous 24 hours. Under System > Configuration > Change Reconciliation, the administrator enables the feature, selects the daily execution time, and specifies management's recipient email addresses. The administrator can also include policy-configuration changes and enable the full change history instead of receiving only a consolidated view. An email relay host must be configured so that Management Center can deliver the report. Sending audit logs to an HTTP or syslog server streams audit events to an external collector; it does not generate the required daily email summary. STIG Compliance applies security-hardening settings and is unrelated to scheduled change reporting. Cisco Change Reconciliation documentation

NEW QUESTION: 129
An administrator must fix a network problem whereby traffic from the inside network to a webserver is not getting through an instance of Cisco Secure Firewall Threat Defense. Which command must the administrator use to capture packets to the webserver that are dropped by Secure Firewall Throat Defense and resold the issue?
A. capture CAP int OUTSIDE match ip any host WEBSERVERIP
B. capture CAP type asp-drop all headers-only
C. capture CAP int INSIDE match ip any host WEBSERVERIP
D. capture CAP int INSIDE match tcp any 80 host WEBSERVERIP 80

Answer: B (LEAVE A REPLY)
To capture packets that are dropped by Cisco Secure Firewall Threat Defense (FTD) and troubleshoot the issue of traffic from the inside network to a webserver not getting through, the administrator should use the command to capture packets dropped by the accelerated security path (ASP) engine. The correct command is:
capture CAP type asp-drop all headers-only
This command captures all packets dropped by the ASP engine, which includes packets that are being blocked by access control policies, NAT issues, or other security checks.
Steps:
* Access the FTD CLI.
* Run the command capture CAP type asp-drop all headers-only to capture dropped packets.
* Analyze the captured data to identify the cause of the drops.
This command provides detailed information on why packets are being dropped, helping the administrator resolve the issue.
References: Cisco Secure Firewall Threat Defense Configuration Guide, Chapter on Packet Capture and ASP Drop Captures.

NEW QUESTION: 130
How should a high-availability pair of Cisco Secure Firewall Threat Defense Virtual appliances be deployed to Cisco Secure Firewall Management Center?
Freecram.net
A. Configure high availability first, then add the primary and secondary appliances to Cisco Secure Firewall Management Center.
B. Configure high availability first, then add only the primary Cisco Secure Firewall Threat Defense Virtual appliance to Cisco Secure Firewall Management Center.
C. Add the primary and secondary Cisco Secure Firewall Threat Defense Virtual appliances to Cisco Secure Firewall Management Center first, then configure high availability.
D. Add the primary appliance to Cisco Secure Firewall Management Center first, then configure high availability.
Answer: (SHOW ANSWER)

NEW QUESTION: 131
A network security engineer must export packet captures from the Cisco FMC web browser while troubleshooting an issue. When navigating to the address https:// < FMC IP > /capture/CAPI/pcap/test.pcap.
an error 403: Forbidden is given instead of the PCAP file. Which action must the engineer take to resolve this issue?
A. Enable the HTTPS server for the device platform policy.
B. Disable the HTTPS server and use HTTP instead.
C. Use the Cisco FTD IP address as the proxy server setting on the browser.
D. Disable the proxy setting on the browser.
Answer: (SHOW ANSWER)

NEW QUESTION: 132
An engineer is deploying a Cisco Secure Firewall Management Center appliance. The company must send data to Cisco Secure Network Analytics appliances. Which two actions must the engineer take? (Choose two.)
A. Configure Security Intelligence object to send data to Cisco Secure Network Analytics.
B. Create a service identifier to enable the NetFlow service.
C. Add the Netflow_Set_Parameters object to the configuration.
D. Add the Netflow_Send_Destination object to the configuration.
E. Add the Netflow_Add_Destination object to the configuration.
Answer: (SHOW ANSWER)

NEW QUESTION: 133
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: 134
Which connector is used to integrate Cisco ISE with Cisco FMC for Rapid Threat Containment?
A. FMC RTC
B. FTD RTC
C. ISEGrid
D. pxGrid
Answer: (SHOW ANSWER)

NEW QUESTION: 135
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. Change the HTTP response in the access control policy to custom.
B. Write CSS code with the information for the policies and procedures.
C. Modify the system-provided block page result using Python.
D. Create HTML code with the information for the policies and procedures.
E. Edit the HTTP request handling in the access control policy to customized block.
Answer: (SHOW ANSWER)

NEW QUESTION: 136

An engineer is troubleshooting the upgrade of a Cisco Secure Firewall Threat Defense device on the Secure Firewall Management Center 7.0 GUI. The engineer wants to collect the upgrade data and logs. Which two actions must the engineer take? (Choose two.)

A. Access the Health Monitor page.

B. View the system and troubleshooting details.

C. Select the Secure Firewall Management Center device.

D. Select the Secure Firewall Threat Defense device properties.

E. Access the Health Events page.

Answer: (SHOW ANSWER)

Valid 300-710 Dumps shared by ExamDiscuss.com for Helping Passing 300-710 Exam! ExamDiscuss.com now offer the **newest 300-710 exam dumps**, the ExamDiscuss.com 300-710 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com 300-710 dumps with Test Engine here: https://www.examdiscuss.com/Cisco/exam/300-710/premium/ (**446** Q&As Dumps, **35%OFF Special Discount Code: freecram**)

NEW QUESTION: 137

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: 138

A network administrator configured a NAT policy that translates a public IP address to an internal web server IP address. An access policy has also been created that allows any source to reach the public IP address on port 80. The web server is still not reachable from the Internet on port 80. Which configuration change is needed?

A. The intrusion policy must be disabled for port 80.

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

C. The access policy must allow traffic to the internal web server IP address.

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

Answer: C (LEAVE A REPLY)

NEW QUESTION: 139

A network engineer is receiving reports of users randomly getting disconnected from their corporate applications which traverses the data center FTD appliance Network monitoring tools show that the FTD appliance utilization is peaking above 90% of total capacity. What must be done in order to further analyze this issue?

A. Use the Packet Export feature to save data onto external drives

B. Use the Packet Capture feature to collect real-time network traffic

C. Use the Packet Tracer feature for traffic policy analysis

D. Use the Packet Analysis feature for capturing network data

Answer: (SHOW ANSWER)

NEW QUESTION: 140

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?

Freecram.net

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: 141

An engineer wants to change an existing transparent Cisco FTD to routed mode.
The device controls traffic between two network segments. Which action is mandatory to allow hosts to reestablish communication between these two segments after the change?
A. implement non-overlapping IP subnets on each segment.
B. assign unique VLAN IDs to each firewall interface.
C. remove the existing dynamic routing protocol settings.
D. configure multiple BVIs to route between segments.
Answer: (SHOW ANSWER)

NEW QUESTION: 142

An engineer is troubleshooting connectivity to the DNS servers from hosts behind a new Cisco FTD device.
The hosts cannot send DNS queries to servers in the DMZ. Which action should the engineer take to troubleshoot this issue using the real DNS packets?
A. Use the show blocks command in the Threat Defense CLI tool and create a policy to allow the blocked traffic.
B. Use the packet tracer tool to determine at which hop the packet is being dropped.
C. Use the packet capture tool to check where the traffic is being blocked and adjust the access control or intrusion policy as needed.
D. Use the Connection Events dashboard to check the block reason and adjust the inspection policy as needed.
Answer: (SHOW ANSWER)

NEW QUESTION: 143

What is the difference between inline and inline tap on Cisco Firepower?
A. Inline mode can drop malicious traffic.
B. Inline mode cannot do SSL decryption.
C. Inline tap mode can send a copy of the traffic to another device.
D. Inline tap mode does full packet capture.
Answer: (SHOW ANSWER)

NEW QUESTION: 144

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. sudo perfstats -Cq < /var/sf/rna/correlator-stats/now

C. manage_procs.pl

D. show disk-manager

E. show history

Answer: (SHOW ANSWER)

NEW QUESTION: 145

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. link state propagation

B. strict TCP enforcement

C. tap mode

D. bypass

Answer: (SHOW ANSWER)

NEW QUESTION: 146

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 SSH and define an access list.

B. Enable SCP under the Access List section.

C. Enable HTTPS and SNMP under the Access List section.

D. Enable HTTP and define an access list.

Answer: (SHOW ANSWER)

NEW QUESTION: 147

Which Cisco FMC report gives the analyst information about the ports and protocols that are related to the configured sensitive network for analysis?

A. Host Report

B. Network Report

C. Malware Report

D. Firepower Report

Answer: B (LEAVE A REPLY)

NEW QUESTION: 148

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

A. Confirm that both devices have the same flash memory sizes

B. Confirm that both devices are running the same software version

C. Confirm that both devices have the same port-channel numbering
D. Confirm that both devices are configured with the same types of interfaces
Answer: (SHOW ANSWER)

NEW QUESTION: 149
What is an attribute of the risk reporting capability in Cisco Secure Firewall Management Center?
A. Uses the same templates available to standard reports
B. Includes all domains in a multidomain system
C. Includes the current domain in a multidomain system
D. Uses the XML format to export all reporting
Answer: (SHOW ANSWER)

NEW QUESTION: 150
A network administrator discovers that a user connected to a file server and downloaded a malware file.
The Cisc FMC generated an alert for the malware event, however the user still remained connected.
Which Cisco APM file rule action within the Cisco FMC must be set to resolve this issue?
Freecram.net
A. Detect Files
B. Malware Cloud Lookup
C. Local Malware Analysis
D. Reset Connection
Answer: (SHOW ANSWER)

NEW QUESTION: 151
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.

Valid 300-710 Dumps shared by ExamDiscuss.com for Helping Passing 300-710 Exam! ExamDiscuss.com now offer the **newest 300-710 exam dumps**, the ExamDiscuss.com 300-710 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com 300-710 dumps with Test Engine here: https://www.examdiscuss.com/Cisco/exam/300-710/premium/ (**446** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 152
An engineer is setting up a remote access VPN on a Cisco FTD device and wants to define which traffic gets sent over the VPN tunnel. Which named object type in Cisco FMC must be used to accomplish this task?
A. split tunnel
B. access list
C. route map
D. crypto map
Answer: (SHOW ANSWER)

NEW QUESTION: 153
An engineer is investigating connectivity problems on Cisco Firepower that is using service group tags.
Specific devices are not being tagged correctly, which is preventing clients from using the proper policies when going through the firewall How is this issue resolved?
A. Use traceroute with advanced options.
B. Use a packet sniffer with correct filtering
C. Use Wireshark with an IP subnet filter.
D. Use a packet capture with match criteria.
Answer: (SHOW ANSWER)

NEW QUESTION: 154
An engineer must block all the web traffic that targets an IP address instead of the associated hostname by using Secure Firewall Management Center. Access control, intrusion, and file policies have been configured; however, specific web traffic that has been identified is still coming through Which configuration must be done next for protection?
A. NMAPscan
B. SNMP alert
C. application detector
D. correlation policy
Answer: (SHOW ANSWER)

NEW QUESTION: 155

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

A. Specify the buffer size.

B. Specify the packet size.

C. Enable the Trace option.

D. Enable the Continuous Capture option.

Answer: (SHOW ANSWER)

NEW QUESTION: 156

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

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

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

C. Change the base policy to Security over Connectivity.

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

Answer: (SHOW ANSWER)

NEW QUESTION: 157

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: 158

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: B (LEAVE A REPLY)

Reference:https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/212474-working-with- firepower-threat-defense-f.html

NEW QUESTION: 159
A network administrator notices that SI events are not being updated The Cisco FTD device is unable to load all of the SI event entries and traffic is not being blocked as expected. What must be done to correct this issue?
A. Restart the affected devices in order to reset the configurations
B. Redeploy configurations to affected devices so that additional memory is allocated to the SI module
C. Replace the affected devices with devices that provide more memory
D. Manually update the SI event entries to that the appropriate traffic is blocked
Answer: (SHOW ANSWER)

NEW QUESTION: 160
Which type of certificate must be exported from Cisco ISE to integrate Cisco Secure Firewall Management Center with pxGrid?
Freecram.net
A. A self-signed SAML certificate from the domain controller
B. The certificate authority certificate of the pxGrid server node
C. A self-signed certificate authority certificate signed by a third party
D. The public-key certificate of the domain
Answer: (SHOW ANSWER)
Secure Firewall Management Center must trust the certificate presented by the Cisco ISE pxGrid server.
Therefore, the certificate authority certificate that signed the pxGrid node's server certificate must be exported from ISE and imported into Management Center as a trusted CA object. If primary and secondary pxGrid nodes are deployed, Cisco requires their certificates to be signed by the same trusted certificate authority.
Depending on the integration design, the engineer might also need the monitoring-node CA certificate and a pxGrid client certificate with its private key for Management Center. However, the question specifically asks which certificate establishes trust with the pxGrid server node. SAML and domain-controller certificates are unrelated, and a certificate cannot simultaneously be self-signed and signed by a third-party CA. Cisco ISE and Secure Firewall certificate integration

NEW QUESTION: 161
Which Cisco Secure Firewall Threat Defense interface mode must be deployed when implementing an IPS that uses a SPAN port for traffic monitoring?
A. Routed
B. Passive
C. Transparent
D. Inline
Answer: (SHOW ANSWER)
A passive interface is specifically designed to monitor copied network traffic received from a switch SPAN or mirror port. Because the Secure Firewall Threat Defense device is not physically placed in the traffic path, it receives a copy of the packets for inspection but does not retransmit them. This provides network and intrusion visibility without affecting production traffic. The trade-off is that a passive deployment cannot directly block, shape, or modify the monitored traffic because the original packets continue through the switch independently. An inline deployment, by comparison, places paired interfaces directly in the forwarding path and can drop malicious traffic. Routed and transparent describe firewall forwarding modes and are not the appropriate SPAN-based IPS interface type. Therefore, a SPAN-port monitoring deployment requires a passive interface. Cisco passive-interface documentation

NEW QUESTION: 162

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.

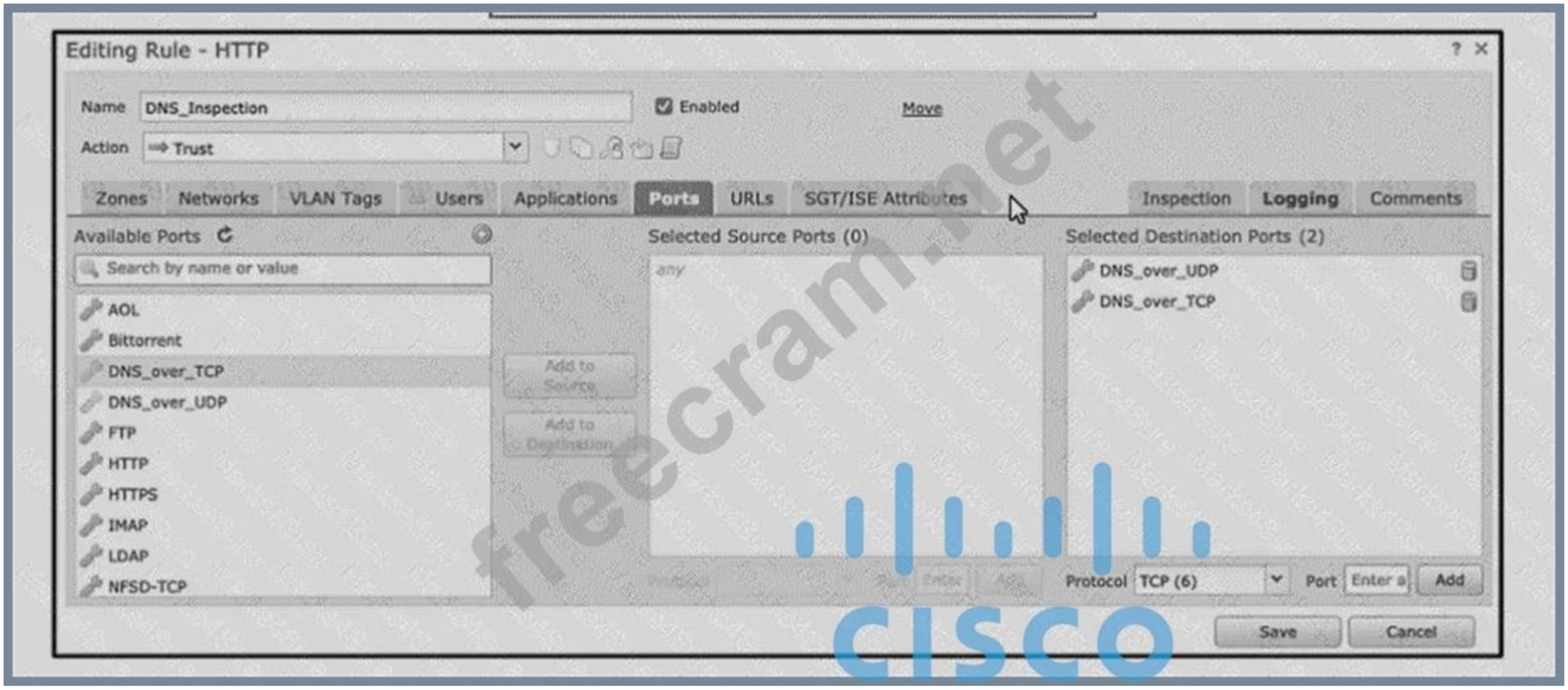
The other options are incorrect because:

* 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: 163



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

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

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

Answer: (SHOW ANSWER)

NEW QUESTION: 164

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. application detector

B. intrusion policy

C. file and malware policy

D. correlation policy

Answer: (SHOW ANSWER)

NEW QUESTION: 165

Refer to the exhibit.
A systems administrator conducts a connectivity test to their SCCM server from a host machine and gets no response from the server. Which action ensures that the ping packets reach the destination and that the host receives replies?
A. Configure a custom Snort signature to allow ICMP traffic after Inspection.
B. Create an access control policy rule that allows ICMP traffic.
C. Modify the Snort rules to allow ICMP traffic.
D. Create an ICMP allow list and add the ICMP destination to remove it from the implicit deny list.
Answer: (SHOW ANSWER)

NEW QUESTION: 166
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 application-identification-debug command to determine which rules the traffic matching and modify the rule accordingly
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 firewall-engine-dump-user-f density-data command to change the policy and allow the application through the firewall.
Answer: (SHOW ANSWER)

Valid 300-710 Dumps shared by ExamDiscuss.com for Helping Passing 300-710 Exam! ExamDiscuss.com now offer the **newest 300-710 exam dumps**, the ExamDiscuss.com 300-710 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com 300-710 dumps with Test Engine here: https://www.examdiscuss.com/Cisco/exam/300-710/premium/ (**446** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 167
Which command is typed at the CLI on the primary Cisco FTD unit to temporarily stop running high- availability?
A. configure high-availability resume
B. configure high-availability disable
C. system support network-options
D. configure high-availability suspend
Answer: (SHOW ANSWER)
Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/610/configuration/guide/fpmc-config- guide-v61/firepower_threat_defense_high_availability.html

NEW QUESTION: 168
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: 169
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: 170
Refer to the exhibit.

```
firepower# packet-tracer input dmz tcp 10.10.5.20 60001 172.20.1.100 502 detailed

Phase 1: ROUTE-LOOKUP
  Destination 172.20.1.100  Next-hop 172.20.0.1 via ot-segment
  Action: ALLOW

Phase 2: ACCESS-LIST
  Rule: dmz_to_ot_permit  Action: ALLOW

Phase 3: IP-OPTIONS  Action: ALLOW

Phase 4: INSPECT  Action: ALLOW

Phase 5: SNORT
  Snort id: 3  Action: BLOCK
  GID:1 SID:24910 triggered
  Drop-reason: (snort) Snort is blocking the session

Result: DROP
```

freecram.net

At a manufacturing facility, a historian server 10.10.5.20 in the OT DMZ is intermittently unable to reach a remote PLC at 172.20.1.100 on TCP 502 Modbus. A security engineer runs packet-tracer on Cisco Secure Firewall Threat Defence and captures the output. The access policy is verified as correct. Which action must be performed to resolve the issue?

A. Increase the MTU on the of-segment interface to prevent Modbus payload fragmentation during deep packet inspection.

B. Disable logging for the rule matching traffic from 10.10.5.20 to 172.20.1.100 on port TCP 502 Modbus.

C. Associate the ACP rule " dmz_to_of_permit " with a separate intrusion policy that excludes Modbus protocol signatures.

D. Create intrusion policy exception for SID 24910 scoped to the historian-to-PLC Modbus flow with rule action to Alert/Generate Events.

Answer: (SHOW ANSWER)

NEW QUESTION: 171

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: 172

An engineer has been asked to show application usages automatically on a monthly basis and send the information to management What mechanism should be used to accomplish this task?

A. event viewer

B. reports

C. dashboards

D. context explorer

Answer: (SHOW ANSWER)

NEW QUESTION: 173

With a recent summer time change, system logs are showing activity that occurred to be an hour behind real time Which action should be taken to resolve this issue?

A. Manually adjust the time to the correct hour on all managed devices

B. Configure the system clock settings to use NTP

C. Manually adjust the time to the correct hour on the Cisco FMC.

D. Configure the system clock settings to use NTP with Daylight Savings checked

Answer: (SHOW ANSWER)

NEW QUESTION: 174

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

NEW QUESTION: 175

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

Total Attacks

Events Requiring Attention

Hosts Targeted

Hosts Connected to CnC Servers

Which type of risk report is the engineer analyzing?

A. Network Risk Report

B. Attacks Risk Report

C. Events Risk Report

D. Hosts Risk Report

Answer: (SHOW ANSWER)

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

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

"Events Risk Report" and "Hosts Risk Report" are not the applicable standard risk-report templates. List B incorrectly marks Network Risk Report; Cisco's report documentation explicitly assigns all four fields to the Attacks Risk Report, so the verified answer is B. Cisco risk-report templates

NEW QUESTION: 176
A company is deploying Cisco Secure Endpoint private cloud. The Secure Endpoint private cloud instance has already been deployed by the server administrator. The server administrator provided the hostname of the private cloud instance to the network engineer via email. What additional information does the network engineer require from the server administrator to be able to make the connection to Secure Endpoint private cloud in Cisco Secure Firewall Management Centre?
A. SSL certificate for the Secure Endpoint ornate cloud instance
B. Internet access for the Secure End point private cloud to reach the Secure Endpoint public cloud
C. Username and password to the Secure Endpoint private cloud instance
D. IP address and port number for the connection proxy
Answer: (SHOW ANSWER)
To connect to a Secure Endpoint private cloud instance from Cisco Secure Firewall Management Center (FMC), the network engineer requires the SSL certificate for the Secure Endpoint private cloud instance. This SSL certificate is necessary to establish a secure, trusted connection between the FMC and the private cloud instance.
Steps:
* Obtain the SSL certificate from the server administrator.
* Import the SSL certificate into the FMC.
* Configure the connection to the Secure Endpoint private cloud instance using the provided hostname and SSL certificate.
This ensures a secure and authenticated connection to the private cloud instance.
References: Cisco Secure Firewall Management Center Integration Guide, Chapter on Secure Endpoint Integration.

NEW QUESTION: 177
A security analyst is investigating a potential network compromise. The analyst must produce a report of the suspicious activity from Cisco Secure Firewall Management Center. Which two details must be included in the report to assist the investigation? (Choose two.)
A. Client applications by user
B. Intrusion events
C. Host connections
D. Number of attacked machines
E. User connections
Answer: (SHOW ANSWER)
Intrusion events provide the detection evidence needed to understand which signatures fired, the affected source and destination addresses, event severity, protocol information, and other indicators associated with the suspected compromise. Host connections provide the corresponding network context, allowing the analyst to determine which systems communicated, when the sessions occurred, and which ports, applications, or protocols were involved. Together, these details connect security detections with the traffic flows that produced them and support reconstruction of the incident. Client applications by user and user connections are useful when the investigation is primarily identity-focused, but they do not provide the same direct combination of exploit evidence and host-level network activity. The number of attacked machines is an aggregate measurement and lacks the granular information necessary to investigate the suspicious communications and determine their cause.

NEW QUESTION: 178
An organization has a compliancy requirement to protect servers from clients, however, the clients and servers all reside on the same Layer 3 network Without readdressing IP subnets for clients or servers, how is segmentation achieved?
A. Deploy a firewall in routed mode between the clients and servers

B. Change the IP addresses of the clients, while remaining on the same subnet.
C. Deploy a firewall in transparent mode between the clients and servers.
D. Change the IP addresses of the servers, while remaining on the same subnet
Answer: (SHOW ANSWER)

NEW QUESTION: 179
An administrator is working on a migration from Cisco ASA to the Cisco FTD appliance and needs to test the rules without disrupting the traffic. Which policy type should be used to configure the ASA rules during this phase of the migration?
A. identity
B. Intrusion
C. Access Control
D. Prefilter
Answer: (SHOW ANSWER)
Reference:
https://www.cisco.com/c/en/us/td/docs/security/firepower/migration-tool/migration-guide/ASA2FTD-with-FP-Migration-Tool/b_Migration_Guide_ASA2FTD_chapter_01011.html

NEW QUESTION: 180
What is the RTC workflow when the infected endpoint is identified?
A. Cisco ISE instructs Cisco AMP to contain the infected endpoint.
B. Cisco ISE instructs Cisco FMC to contain the infected endpoint.
C. Cisco FMC instructs Cisco ISE to contain the infected endpoint.
D. Cisco AMP instructs Cisco FMC to contain the infected endpoint.
Answer: (SHOW ANSWER)

NEW QUESTION: 181
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.

Valid 300-710 Dumps shared by ExamDiscuss.com for Helping Passing 300-710 Exam! ExamDiscuss.com now offer the **newest 300-710 exam dumps**, the ExamDiscuss.com 300-710 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com 300-710 dumps with Test Engine here: https://www.examdiscuss.com/Cisco/exam/300-710/premium/ (**446** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

Valid 300-710 Dumps shared by ExamDiscuss.com for Helping Passing 300-710 Exam! ExamDiscuss.com now offer the **newest 300-710 exam dumps**, the ExamDiscuss.com 300-710 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com 300-710 dumps with Test Engine here: https://www.examdiscuss.com/Cisco/exam/300-710/premium/ (**446** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)