Cisco.300-710.v2026-11-21.q241

Exam Code:	300-710
Exam Name:	Securing Networks with Cisco Firepower
Certification Provider:	Cisco
Free Question Number:	241
Version:	v2026-11-21
# of views:	106
# of Questions views:	2782
https://www.freecram.net/torrent/Cisco.300-710.v2026-11-21.q241.html	

NEW QUESTION: 1
A security engineer is configuring an Access Control Policy for multiple branch locations.
These locations share a common rule set and utilize a network object called INSIDE_NET which contains the locally significant internal network subnets at each location.
What technique will retain the policy consistency at each location but allow only the locally significant network subnet within the applicable rules?
A. utilizing a dynamic ACP that updates from Cisco Talos
B. utilizing policy inheritance
C. creating a unique ACP per device
D. creating an ACP with an INSIDE_NET network object and object overrides
Answer: (SHOW ANSWER)

NEW QUESTION: 2
Refer to the exhibit. An engineer is configuring access control rules on a Cisco Secure Firewall Threat Defense device. The access control rules must include a file policy with rules that will trigger when MSEXE files are accessed. Which two actions must be configured in the access rule? (Choose two.)



A. block files with reset
B. interactive block
C. monitor
D. allow
E. trust
Answer: (SHOW ANSWER)
The first row in the exhibit shows an action for MSEXE files set to "Block Files with Reset". This action will block the MSEXE files and send a TCP reset to terminate the connection, effectively preventing the files from being accessed or downloaded.
The second row shows an action for MSEXE files set to "Detect Files". This is essentially a monitoring action that allows the system to log and detect MSEXE file access events without blocking them.

In this configuration, combining "Block Files with Reset" and "Detect Files" enables both blocking specific actions and monitoring file access, providing comprehensive control and visibility for MSEXE files.

NEW QUESTION: 3
An engineer is configuring Cisco Security Devices by using Cisco Secure Firewall Management Center. Which configuration command must be run to compare the CA certificate bundle on the local system to the latest CA bundle from the Cisco server?
A. configure cert-update run-now
B. configure cert-update test
C. configure cert-update compare
D. configure cert-update auto-update enable
Answer: (SHOW ANSWER)
The **configure cert-update compare** command is used in Cisco Secure Firewall Management Center to compare the local CA certificate bundle with the latest bundle available from Cisco's update server. This helps verify whether the local system has the most up-to-date CA certificates before performing a manual or automatic update.

NEW QUESTION: 4
A network administrator wants to configure a default policy to block malicious sites based on the requested URL lookup. Which feature meets the requirement?
A. file policies
B. malware policies
C. DNS policies
D. URL filtering policies
Answer: (SHOW ANSWER)
URL filtering allows control over website access based on the URL's category and reputation, which includes blocking malicious or risky sites by inspecting the requested URL.
This feature can use category and reputation-based filtering to automatically block URLs classified as malicious or high risk, fulfilling the requirement for a default blocking policy.
URL filtering works by inspecting HTTP/HTTPS traffic and matching URLs against Cisco's URL database or manually configured URL lists.
https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/management-center/device- config/720/management-center-device-config-72/access-url-filtering.html

NEW QUESTION: 5
An analyst is reviewing the Cisco FMC reports for the week. They notice that some peer-to-peer applications are being used on the network and they must identify which poses the greatest risk to the environment. Which report gives the analyst this information?
A. Advanced Malware Risk Report
B. Attacks Risk Report
C. User Risk Report
D. Network Risk Report
Answer: (SHOW ANSWER)

NEW QUESTION: 6
An engineer is configuring a new dashboard within Cisco Secure Firewall Management Center and is having trouble implementing a custom widget. When a custom analysis widget is configured, which option is mandatory for the system to display the information?
A. table
B. title
C. filter

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

NEW QUESTION: 7
An engineer must implement static route tracking on Cisco Secure Firewall Threat Defense and reroute traffic by using a backup path if the primary path fails. The engineer already defined the primary static route, and the primary path is already monitored. Which action must the engineer take to meet the requirement?
A. Establish an IP SLA ICMP echo request.
B. Configure a tracking object for the static route
C. Assign a unique tracking ID to the static route
D. Configure a secondary static route that has higher precedence
Answer: (SHOW ANSWER)
Create the backup static route that will be used if the primary route fails. This route must have a larger metric than the primary route. For example, if the primary route is 1, the backup route could be 10. You would also normally select a different interface for the backup route.
https://www.cisco.com/c/en/us/td/docs/security/firepower/70/fdm/fptd-fdm-config-guide-700/fptd- fdm- routing.html#:~:text=Create%20the%20backup%20static%20route%20that%20will%20be%20use
d%20if%20the%20primary%20route%20fails.%20This%20route%20must%20have%20a%20larg er%20metric%20than%20the%20primary%20route.%20For%20example%2C%20if%20the%20pr
imary%20route%20is%201%2C%20the%20backup%20route%20could%20be%2010

NEW QUESTION: 8
How does Cisco Secure Cloud Analytics handle information about network traffic?
A. It stores the information in a database without any analysis.
B. It performs a heuristic analysis on events and network flow data.
C. It forwards the information to other devices without storing it.
D. It performs a behavioral analysis on events and network flow data.
Answer: (SHOW ANSWER)
Cisco Secure Cloud Analytics (formerly Stealthwatch Cloud) uses behavioral analysis to monitor events and network flow data. It builds a baseline of normal network behavior and then detects anomalies, such as data exfiltration or lateral movement, indicating potential threats.

NEW QUESTION: 9
An engineer must build redundancy into the network and traffic must continuously flow if a redundant switch in front of the firewall goes down.
What must be configured to accomplish this task?
A. redundant interfaces on the firewall cluster mode and switches
B. redundant interfaces on the firewall noncluster mode and switches
C. vPC on the switches to the interface mode on the firewall duster
D. vPC on the switches to the span EtherChannel on the firewall cluster
Answer: (SHOW ANSWER)

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

NEW QUESTION: 10

Which two features of Cisco AMP for Endpoints allow for an uploaded file to be blocked? (Choose two.)

A. application blocking
B. simple custom detection
C. file repository
D. exclusions
E. application whitelisting
Answer: (SHOW ANSWER)

Configure custom malware detection policies and profiles for your entire organization, as well as perform flash and full scans on all your users' files perform malware analysis, including view heat maps, detailed file information, network file trajectory, and threat root causes configure multiple aspects of outbreak control, including automatic quarantines, application blocking to stop non- quarantined executables from running, and exclusion lists.
https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config- guide-v60/Reference_a_wrapper_Chapter_topic_here.html#id_96014

NEW QUESTION: 11

While configuring FTD, a network engineer wants to ensure that traffic passing through the appliance does not require routing or Vlan rewriting.
Which interface mode should the engineer implement to accomplish this task?

A. passive
B. transparent
C. Inline tap
D. Inline set
Answer: (SHOW ANSWER)

Passive: traffic does not flow through the IPS.
Inline Tap: it gets a copy of the packets, traffic does not flow through the IPS.
Transparent: it is Transparent inline mode, then this can be an answer as well.
Inline set: it is called bump-on-wire mode. Traffic passes through the appliance, but it does not require routing and Vlan rewriting.
https://www.cisco.com/c/en/us/td/docs/security/firepower/630/configuration/guide/fpmc-config- guide-v63/inline_sets_and_passive_interfaces_for_firepower_threat_defense.html

NEW QUESTION: 12

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)

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

NEW QUESTION: 13

administrator is configuring SNORT inspection policies and is seeing failed deployment messages in Cisco FMC.
What information should the administrator generate for Cisco TAC to help troubleshoot?
A. A Troubleshoot" file for the device in question.
B. A "show tech" file for the device in question
C. A "show tech" for the Cisco FMC.
D. A "troubleshoot" file for the Cisco FMC
Answer: (SHOW ANSWER)
https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-config- guide-v62/troubleshooting_the_system.html

NEW QUESTION: 14
Which limitation applies to Cisco Firepower Management Center dashboards in a multidomain environment?
A. Child domains can view but not edit dashboards that originate from an ancestor domain.
B. Child domains have access to only a limited set of widgets from ancestor domains.
C. Only the administrator of the top ancestor domain can view dashboards.
D. Child domains cannot view dashboards that originate from an ancestor domain.
Answer: D (LEAVE A REPLY)
https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config- guide-v60/Using_Dashboards.html

NEW QUESTION: 15
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)
You can set a global threshold across all traffic to limit how often events from a specific source or destination are logged and displayed per specified time period. For more information, see Understanding Thresholding, page 22-1 and Configuring Global Thresholds, page 22-3.
* You can set thresholds per shared object rule, standard text rule, or preprocessor rule in your intrusion policy configuration, as described in Configuring Event Thresholding, page 20-21.
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: 16
A security engineer is reviewing a Cisco Secure Endpoint public cloud instance. The engineer discovers a malicious verdict for a SHA-256 hash of 689efc1ecdc23ec0b0885a80663e30ea013d493f8e88224b570a1234567890.
Which configuration action must be done in Secure Endpoint console to mitigate the threat?
A. Add the hash to the custom detection list.
B. Set access control policy and deny files with the hash.
C. Configure correlation policy to block the hash.
D. Apply regular expression to block the malicious file.
Answer: (SHOW ANSWER)

To mitigate a known malicious file in Cisco Secure Endpoint, the security engineer can add the hash (SHA-256) to the custom detection list. This action ensures that Cisco Secure Endpoint will automatically block or quarantine any file matching this hash in the environment, preventing it from executing or spreading further.

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
What is the result of specifying of QoS rule that has a rate limit that is greater than the maximum throughput of an interface?
A. The rate-limiting rule is disabled.
B. Matching traffic is not rate limited.
C. The system rate-limits all traffic.
D. The system repeatedly generates warnings.
Answer: (SHOW ANSWER)
If you specify a limit greater than the maximum throughput of an interface, the system does not rate limit matching traffic. Maximum throughput may be affected by an interface's hardware configuration, which you specify in each device's properties (Devices > Device Management).
https://www.cisco.com/c/en/us/td/docs/security/firepower/640/configuration/guide/fpmc-config- guide-v64/quality_of_service__qos__for_firepower_threat_defense.html

NEW QUESTION: 18
Refer to the exhibit. An engineer is analyzing a Network Risk Report generated in Cisco Secure Firewall Management Center. Against which application must immediate action be taken to prevent unauthorized and uninspected network use?

ENCRYPTED APPLICATIONS

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

Application	Times Accessed	Application Risk	Productivity Rating	Data Transferred (MB)
SSL	11,926,818	Medium	Medium	1449773.319273
Kerberos	6,694,337	Very Low	High	16476.005748
SSH	727,527	High	Medium	72265.972372
Microsoft Azure	467,381	Medium	Very Low	149794.0941926
SFTP	361,783	Medium	Medium	3858.8765371

EVASIVE APPLICATIONS

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

Application	Times Accessed	Application Risk	Productivity Rating	Data Transferred (MB)
BitTorrent	18	Very High	Very Low	0.65208434901
Xunlei	3	Very High	Very Low	0.022660255
Hotspot Shield	75	High	Low	0.068893432
NordVPN	8	High	Low	0.048398018
Proton VPN	1	High	Low	0.048279762

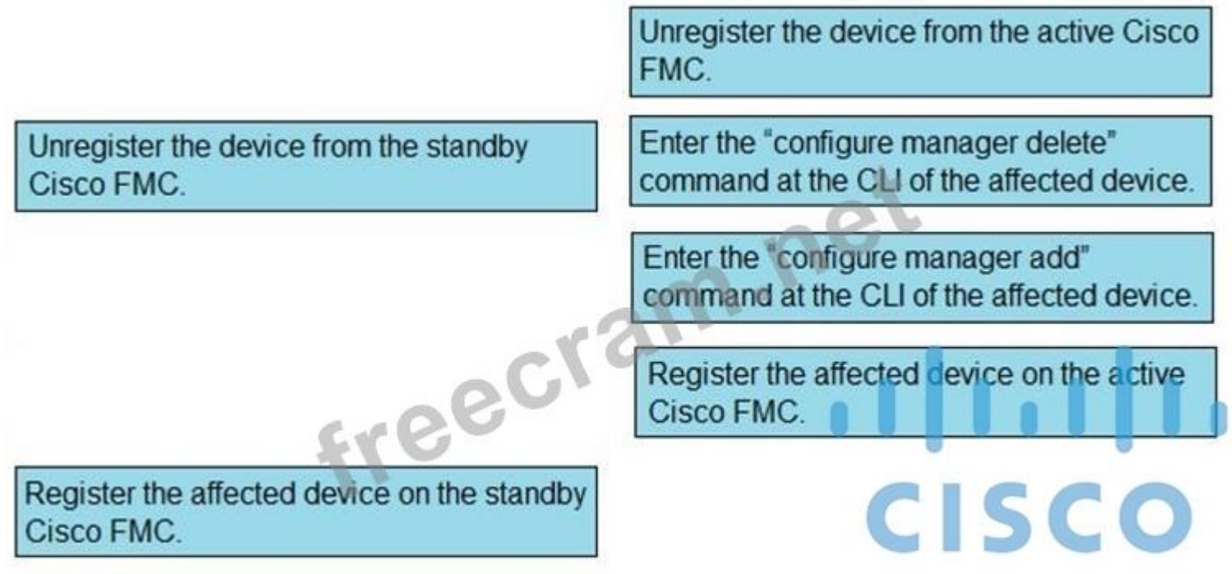
cisco
freecram.net

A. Xunlei
B. BitTorrent
C. SSH
D. Hotspot Shield
Answer: B (LEAVE A REPLY)
BitTorrent poses the highest application risk ("Very High") and shows measurable data transfer, indicating actual usage. As a peer-to-peer file sharing application, it can lead to data exfiltration or malware introduction and is typically unauthorized in enterprise networks.
Immediate action should be taken to block it.

NEW QUESTION: 19
Drag and Drop Question
Drag and drop the steps to restore an automatic device registration failure on the standby Cisco FMC from the left into the correct order on the right. Not all options are used.



Answer:



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

NEW QUESTION: 20
Refer to the exhibit. An engineer is analyzing a Network Risk Report from Cisco FMC. Which application must the engineer take immediate action against to prevent unauthorized network use?

IIGH BANDWIDTH APPLICATIONS

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

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

ENCRYPTED APPLICATIONS

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

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

EVASIVE APPLICATIONS

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

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

A. YouTube

B. Chrome

C. Kerberos

D. TOR

Answer: (SHOW ANSWER)

NEW QUESTION: 21
An engineer is analyzing a risk report generated by using Cisco Secure Firewall Management Center. The report contains these fields:
- Total Attacks
- Events Requiring Attention
- Hosts Targeted
- Hosts Connected to CnC Servers
Which type of risk report is the engineer analyzing-
A. attacks
B. network
C. events
D. hosts
Answer: (SHOW ANSWER)
The presence of fields like "Hosts Targeted" and "Hosts Connected to CnC Servers" indicates that this is a hosts risk report. This report focuses on host-level security posture, showing which internal systems are being attacked, are compromised, or are behaving suspiciously based on threat intelligence and traffic analysis.

NEW QUESTION: 22
What is the result when two users modify a VPN policy at the same time on a Cisco Secure Firewall Management Center managed device?
A. Both users can edit the policy and the last saved configuration persists.
B. The changes from both users will be merged together into the policy.
C. The first user locks the configuration when selecting edit on the policy.
D. The system prevents modifications to the policy by multiple users.
Answer: (SHOW ANSWER)
Two users must not edit a remote access VPN policy at the same time; however, the web interface does not prevent simultaneous editing. If this occurs, the last saved configuration persists.
https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/management-center/device-config/710/management-center-device-config-71/vpn-remote-access.html

NEW QUESTION: 23
Which description of a passive interface on a Cisco Firepower NGFW is true?
A. Receives traffic that is specified on an NGIPS
B. Inaccessible when disable
C. Effected by firewall mode
D. Retransmits received traffic
Answer: (SHOW ANSWER)

- Pure IDS deployment–If you do not want to use the system as a firewall or IPS (intrusion prevention system), you can deploy it passively as an IDS (intrusion detection system). In this deployment method, you would use an access control rule to apply an intrusion policy to all traffic. You would also have the system monitor multiple source ports on the switch. Then, you would be able to use the dashboards to monitor the threats seen on the network. However, in this mode, the system can do nothing to prevent these threats.

NEW QUESTION: 24
An engineer is configuring a Cisco Secure Firewall Threat Defense device and wants to create a new intrusion rule based on the detection of a specific pattern in the data payload for a new zero- day exploit. Which keyword type must be used to add a line that identifies the author of the rule and the date it was created?

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

NEW QUESTION: 25
An engineer is working on a LAN switch and has noticed that its network connection to the mime Cisco IPS has gone down.
Upon troubleshooting it is determined that the switch is working as expected. What must have been implemented for this failure to occur?
A. The upstream router has a misconfigured routing protocol
B. Link-state propagation is enabled
C. The Cisco IPS has been configured to be in fail-open mode
D. The Cisco IPS is configured in detection mode
Answer: (SHOW ANSWER)
If link-state propagation is enabled on a switch, it can cause the switch to incorrectly detect a link failure, which can lead to network connectivity issues. In the case of the inline Cisco IPS, the switch may detect a link failure due to the IPS not responding to certain types of traffic, even though the IPS is functioning properly.

NEW QUESTION: 26
An organization is configuring a new Cisco Firepower High Availability deployment. Which action must be taken to ensure that failover is as seamless as possible to end users?
A. Set up a virtual failover MAC address between chassis.
B. Use a dedicated stateful link between chassis.
C. Load the same software version on both chassis.
D. Set the same FQDN for both chassis.
Answer: (SHOW ANSWER)
Configuring virtual MAC addresses on an FTD HA pair is beneficial to the availability of a network. Virtual MAC addresses allow the primary and secondary FTD to maintain consistent MAC addresses which prevents certain traffic disruptions.
https://www.cisco.com/c/en/us/support/docs/security/secure-firewall-threat-defense- virtual/222235-configure-virtual-mac-addresses-for-ftd.html

NEW QUESTION: 27
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 HTTPS and SNMP under the Access List section.
C. Enable SCP under the Access List section.
D. Enable HTTP and define an access list.
Answer: (SHOW ANSWER)

NEW QUESTION: 28
An engineer must change the mode of a Cisco Secure Firewall Threat Defense (FTD) firewall in the Cisco Secure Firewall Management Center (FMC) inventory. The engineer must take these actions:
- Register Secure FTD with Secure FMC.
- Change the firewall mode.
- Deregister the Secure FTD device from Secure FMC.
How must the engineer take FTD take the actions?
A. Reload the Secure FTD device.
B. Configure the management IP address.
C. Access the Secure FTD CLI from the console port.
D. Erase the Secure FTD configuration
Answer: (SHOW ANSWER)
To change the mode of a Cisco Secure Firewall Threat Defense (FTD) device in the Cisco Secure Firewall Management Center (FMC) inventory, the engineer must follow these steps:
Register the Secure FTD with Secure FMC.
Change the firewall mode.
Deregister the Secure FTD device from Secure FMC.
To perform these actions, accessing the Secure FTD CLI from the console port is necessary. This allows the engineer to execute the required commands to change the firewall mode and manage the registration status of the FTD device.
Steps:
Connect to the Secure FTD device via the console port. Access the CLI and execute the command to change the firewall mode (configure firewall-mode).
Deregister the device from FMC if needed.
Register or re-register the device with FMC as required.

NEW QUESTION: 29
An engineer must deploy a high-availability that includes two Cisco Secure Firewall Threat Defense devices. The deployment must have a mechanism that protects synchronization between cluster members. Which action must the engineer take to meet the requirements?
A. Configure an SSL VPN tunnel between units.
B. Clear the commit queue at the time of a sync.
C. Select the Key Generation method for IPsec.
D. Encrypt the synchronization traffic with SSL.
Answer: (SHOW ANSWER)
Secure Firewall Threat Defense high-availability pairs can use IPsec encryption to protect synchronization traffic carried over the failover links. During HA configuration, the engineer enables IPsec encryption and selects the Key Generation method used to secure communications between the two units.

NEW QUESTION: 30

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

Freecram.net

A. Set the allow action in the access policy to trust.
B. Enable IPsec inspection on the access policy.
C. Modify the NAT policy to use the interface PAT.
D. Change the access policy to allow all ports.
Answer: (SHOW ANSWER)
In a site-to-site IPsec VPN configuration where one router is behind a Cisco FTD (Firepower Threat Defense) firewall, proper NAT traversal is critical.
Even if you've allowed UDP 500 (ISAKMP), UDP 4500 (NAT-T), and ESP (IP protocol 50) in the access policy, NAT can still break the VPN unless handled properly.

NEW QUESTION: 31
What is a feature of Cisco AMP private cloud?
A. It supports anonymized retrieval of threat intelligence
B. It supports security intelligence filtering.
C. It disables direct connections to the public cloud.
D. It performs dynamic analysis
Answer: (SHOW ANSWER)
Connecting a Firepower Management Center to an AMP private cloud disables existing direct connections to the public AMP cloud.
https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-config- guide-v62/file_policies_and_amp_for_firepower.html

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
An engineer is attempting to add a new FTD device to their FMC behind a NAT device with a NAT ID of ACME001 and a password of Cisco388267669.
Which command set must be used in order to accomplish this?
A. configure manager add ACME001 <registration key> <FMC IP>
B. configure manager add <FMC IP> ACME0O1 <registration key>
C. configure manager add DONTRESOLVE <FMC IP> AMCE001 <registration key>
D. configure manager add <FMC IP> registration key> ACME001
Answer: (SHOW ANSWER)
https://www.cisco.com/c/en/us/support/docs/security/firesight-management-center/118596-configure-firesight-00.html

NEW QUESTION: 33
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. manage_procs.pl

B. show disk-manager
C. show history
D. sudo perfstats -Cq < /var/sf/rna/correlator-stats/now
E. sudo stats_unified.pl
Answer: (SHOW ANSWER)
When connectivity issues are detected between Cisco Secure Firewall Management Center (FMC) and Cisco Secure Firewall Threat Defense (FTD) devices, and initial troubleshooting indicates that heartbeats and events are not being received, the engineer can run the following commands to resolve the issue by re-establishing secure channels and checking process statuses:
manage_procs.pl: This script is used to manage and restart processes on the FTD device.
Running this script can help restart any malfunctioning processes and re-establish connectivity between the FMC and FTD.
sudo stats_unified.pl: This command provides detailed statistics and status of the unified system processes. It helps in diagnosing and resolving issues related to the secure channel and event reporting.
Steps:
Access the FTD CLI.
Run the command manage_procs.pl to restart processes.
Run the command sudo stats_unified.pl to gather detailed process statistics and verify the status.
These commands help resolve connectivity issues by ensuring that all necessary processes are running correctly and secure channels are re-established.

NEW QUESTION: 34
Which function is the primary function of Cisco AMP threat Grid?
A. applying a real-time URI blacklist
B. automated malware analysis
C. monitoring network traffic
D. automated email encryption
Answer: (SHOW ANSWER)

NEW QUESTION: 35
Which type of certificate must be exported from Cisco ISE to integrate with Cisco Secure Firewall Management Center pxGrid?
A. self-signed certificate authority signed from a third-party
B. self-signed SAML of the domain controller
C. ublic key certificate of the domain
D. certificate authority of the pxGrid node server
Answer: D (LEAVE A REPLY)
The certificate authority associated with the pxGrid node server must be exported from Cisco ISE and trusted by Secure Firewall Management Center. This establishes certificate trust so FMC can securely authenticate and communicate with the ISE pxGrid service.

NEW QUESTION: 36
An administrator needs to configure Cisco Secure Firewall Threat Defense to decrypt outbound SSL traffic to inspect for malware. Which two components must be configured to accomplish this? (Choose two.)
A. SSL Policy
B. Identity Policy
C. Known key certificate

D. Re-sign certificate
E. File Policy
Answer: (SHOW ANSWER)
To decrypt outbound SSL traffic, the administrator configures an SSL Policy and applies a re-sign certificate (also called a resign or "decrypt-resign" action), which allows the firewall to act as a man-in-the-middle by generating a new certificate signed by an internal CA trusted by clients.

NEW QUESTION: 37
Which firewall mode must be deployed on a Cisco Secure Firewall Threat Defense interface when implementing an IPS using a SPAN port for traffic monitoring?
A. Routed
B. Passive
C. Transparent
D. Inline
Answer: (SHOW ANSWER)
Passive mode is used when the Secure Firewall Threat Defense interface receives a copy of traffic from a SPAN or mirror port. The interface monitors and analyzes the traffic without being placed inline and therefore does not forward the monitored packets.

NEW QUESTION: 38
Which Cisco Advanced Malware Protection for Endpoints policy is used only for monitoring endpoint actively?
A. Windows domain controller
B. audit
C. triage
D. protection
Answer: B (LEAVE A REPLY)
Log the detection: In this mode, the identified malicious process is not blocked by MAP, but the detection is logged in the AMP for Endpoints console. (This is Audit mode, where no blocking or quarantine action happens, but the detection is logged.)
https://www.cisco.com/c/en/us/products/collateral/security/amp-for-endpoints/white-paper-c11-740980.html

NEW QUESTION: 39
An administrator is setting up Cisco Firepower to send data to the Cisco Stealthwatch appliances.
The NetFlow_Set_Parameters object is already created, but NetFlow is not being sent to the flow collector. What must be done to prevent this from occurring?
A. Add the NetFlow_Add_Destination object to the configuration
B. Create a service identifier to enable the NetFlow service
C. Create a Security Intelligence object to send the data to Cisco Stealthwatch
D. Add the NetFlow_Send_Destination object to the configuration
Answer: (SHOW ANSWER)

NEW QUESTION: 40
Which two OSPF routing features are configured in Cisco FMC and propagated to Cisco FTD? (Choose two.)
FreeCramm.net
A. OSPFv2 with IPv6 capabilities
B. virtual links

C. SHA authentication to OSPF packets
D. area boundary router type 1 LSA filtering
E. MD5 authentication to OSPF packets
Answer: (SHOW ANSWER)
The Firepower Threat Defense device supports the following OSPF features:
Intra-area, inter-area, and external (Type I and Type II) routes.
Virtual links.
LSA flooding.
Authentication to OSPF packets (both password and MD5 authentication).
Configuring the Firepower Threat Defense device as a designated router or a designated backup router. The Firepower Threat Defense device also can be set up as an ABR.
Stub areas and not-so-stubby areas.
Area boundary router Type 3 LSA filtering.
https://www.cisco.com/c/en/us/td/docs/security/firepower/610/configuration/guide/fpmc-config- guide-v61/ospf_for_firepower_threat_defense.html

NEW QUESTION: 41
An engineer must configure a new identity policy in Cisco Firepower Management Center. Active authentication must be configured by using a Kerberos connection. Which two realms must be configured? (Choose two.)
A. directory username
B. active directory join username
C. directory password
D. active directory primary domain
E. active directory join password
Answer: (SHOW ANSWER)
To enable Kerberos-based Active Authentication in Cisco FMC, the system must join the Active Directory domain. This requires credentials with permissions to join:
- The Active Directory join username and
- The Active Directory join password.
These allow FMC to authenticate users via Kerberos by establishing trust with the AD domain.

NEW QUESTION: 42
An administrator must fix a network problem whereby traffic from the inside network to a webserver is not getting through an instance of Cisco Secure Firewall Threat Defense. Which command must the administrator use to capture packets to the webserver that are dropped by Secure Firewall Threat Defense and resolve the issue?
A. capture CAP int INSIDE match ip any host WEBSERVERIP
B. capture CAP int OUTSIDE match ip any host WEBSERVERIP
C. capture CAP int INSIDE match tcp any 80 host WEBSERVERIP 80
D. capture CAP type asp-drop all headers-only
Answer: (SHOW ANSWER)
To capture packets that are dropped by Cisco Secure Firewall Threat Defense (FTD) and troubleshoot the issue of traffic from the inside network to a webserver not getting through, the administrator should use the command to capture packets dropped by the accelerated security path (ASP) engine.
The correct command is:
capture CAP type asp-drop all headers-only
This command captures all packets dropped by the ASP engine, which includes packets that are being blocked by access control policies, NAT issues, or other security checks.

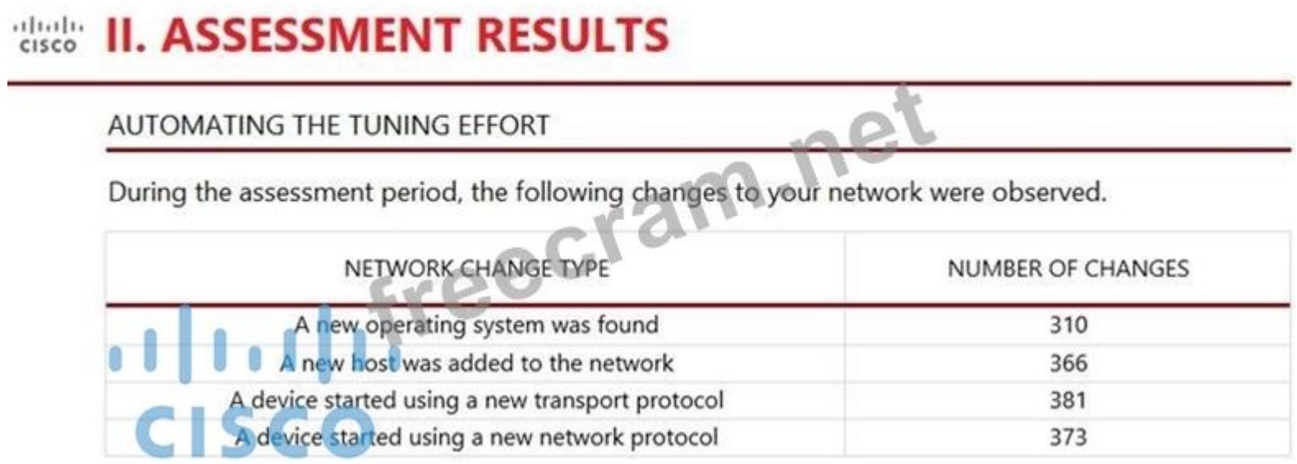
Steps:
Access the FTD CLI.
Run the command capture CAP type asp-drop all headers-only to capture dropped packets.
Analyze the captured data to identify the cause of the drops. This command provides detailed information on why packets are being dropped, helping the administrator resolve the issue.

NEW QUESTION: 43
Which action must be taken to permit communication between a bridge group and routed interface on Cisco Secure Firewall?
A. Create an access rule to allow the traffic.
B. Define a source NAT address.
C. Enable split tunneling.
D. Create an ACL for the bridge group.
Answer: (SHOW ANSWER)

NEW QUESTION: 44
A network administrator is configuring a Cisco AMP public cloud instance and wants to capture infections and polymorphic variants of a threat to help detect families of malware. Which detection engine meets this requirement?
A. RBAC
B. Tetra
C. Spero
D. Ethos
Answer: D (LEAVE A REPLY)

NEW QUESTION: 45
An organization is using a Cisco FTD and Cisco ISE to perform identity-based access controls. A network administrator is analyzing the Cisco FTD events and notices that unknown user traffic is being allowed through the firewall. How should this be addressed to block the traffic while allowing legitimate user traffic?
A. Modify lhe Cisco ISE authorization policy to deny this access to the user.
B. Modify Cisco ISE to send only legitimate usernames to the Cisco FTD.
C. Add the unknown user in the Access Control Policy in Cisco FTD.
D. Add the unknown user in the Malware & File Policy in Cisco FTD.
Answer: C (LEAVE A REPLY)
Unkown is a special identity that can be used in a rule if you use identity policies.

NEW QUESTION: 46
Refer to the exhibit. And engineer is analyzing the Attacks Risk Report and finds that there are over 300 instances of new operating systems being seen on the network.
How is the Firepower configuration updated to protect these new operating systems?



A. Cisco Firepower automatically updates the policies.
B. The administrator requests a Remediation Recommendation Report from Cisco Firepower
C. Cisco Firepower gives recommendations to update the policies.
D. The administrator manually updates the policies.
Answer: (SHOW ANSWER)
Firepower Recommendations for IPS policies is a tool that work with network discovery to apply recommendations to IPS policies, but you have to apply that unless you configure your custom IPS policy to automatically take recommendations (not suggested for low end FW like 1010 because of the memory limit).
https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Tailoring_Intrusion_Protection_to_Your_Network_Assets.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: 47
An engineer is attempting to create a new dashboard within the Cisco FMC to have a single view with widgets from many of the other dashboards. The goal is to have a mixture of threat and security related widgets along with Cisco Firepower device health information.
Which two widgets must be configured to provide this information? (Choose two.)
A. Intrusion Events
B. Correlation Information
C. Appliance Status
D. Current Sessions
E. Network Compliance
Answer: A,C (LEAVE A REPLY)
https://www.cisco.com/c/en/us/td/docs/security/firepower/640/configuration/guide/fpmc-config- guide-v64/dashboards.html#ID-2206-00000283

NEW QUESTION: 48

A network engineer is configuring URL Filtering on Firepower Threat Defense. Which two port requirements on the Firepower Management Center must be validated to allow communication with the cloud service? (Choose two.)
A. outbound port TCP/443
B. inbound port TCP/80
C. outbound port TCP/8080
D. inbound port TCP/443
E. outbound port TCP/80
Answer: (SHOW ANSWER)
https://www.cisco.com/c/en/us/support/docs/security/firesight-management-center/118852- technote-firesight-00.html
https://community.cisco.com/t5/security-documents/ftd-url-filtering-how-it-works/ta-p/3347292

NEW QUESTION: 49
Which two statements about bridge-group interfaces in Cisco FTD are true? (Choose two.)
A. The BVI IP address must be in a separate subnet from the connected network.
B. Bridge groups are supported in both transparent and routed firewall modes.
C. Bridge groups are supported only in transparent firewall mode.
D. Bidirectional Forwarding Detection echo packets are allowed through the FTD when using bridge- group members.
E. Each directly connected network must be on the same subnet.
Answer: B,E (LEAVE A REPLY)
https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-config- guide-v62/transparent_or_routed_firewall_mode_for_firepower_threat_defense.html

NEW QUESTION: 50
Within Cisco Firepower Management Center, where does a user add or modify widgets?
A. dashboard
B. reporting
C. context explorer
D. summary tool
Answer: A (LEAVE A REPLY)
https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config- guide-v60/Using_Dashboards.html

NEW QUESTION: 51
Which Cisco Secure Firewall Threat Defense interface mode must be deployed when implementing an IPS that must receive and retransmit all traffic unless the traffic is explicitly dropped?
A. Routed
B. Inline
C. Passive
D. Transparent
Answer: (SHOW ANSWER)
An inline set consists of paired Secure Firewall Threat Defense interfaces placed directly in the network traffic path. The interfaces operate like a bump in the wire: one interface receives the traffic, the inspection engine evaluates it, and the paired interface retransmits it unless an access- control, intrusion, file, or other security policy explicitly drops it. This arrangement enables the IPS to prevent attacks because the device can stop malicious packets before forwarding them. A passive interface also receives traffic unconditionally, but it receives copied traffic from a SPAN or mirror port and

retransmits none of it. Routed and transparent modes describe broader firewall packet-forwarding behavior rather than this IPS-only interface characteristic. Therefore, an inline deployment satisfies the requirement to inspect, retransmit, and selectively drop traffic.

NEW QUESTION: 52
A network administrator is configuring a transparent Cisco Secure Firewall Threat Defense registered to a Cisco Secure Firewall Management Center. The administrator wants to configure the Secure Firewall Threat Defense to allow ARP traffic to pass between two interfaces of a bridge group. What must be configured?
A. Use the default configuration on the devices.
B. An access policy must allow MAC address 0100.0CCC.CCCD.
C. ARP inspection must be disabled.
D. An access policy must allow MAC address FFFF.FFFF.FFFF.
Answer: (SHOW ANSWER)
By default, all ARP packets are passed within the bridge group.
https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/management-center/device- config/760/management-center-device-config-76/device-ops-tfw.html

NEW QUESTION: 53
An engineer configures an access control rule that deploys file policy configurations to security zone or tunnel zones, and it causes the device to restart. What is the reason for the restart?
A. Source or destination security zones in the access control rule matches the security zones that are associated with interfaces on the target devices.
B. The source tunnel zone in the rule does not match a tunnel zone that is assigned to a tunnel rule in the destination policy.
C. Source or destination security zones in the source tunnel zone do not match the security zones that are associated with interfaces on the target devices.
D. The source tunnel zone in the rule does not match a tunnel zone that is assigned to a tunnel rule in the source policy.
Answer: (SHOW ANSWER)
Note that access control rules that deploy these file policy configurations to security zones or tunnel zones cause a restart only when your configuration meets the following conditions:
Source or destination security zones in your access control rule must match the security zones associated with interfaces on the target devices.
Unless the destination zone in you access control rule is any, a source tunnel zone in the rule must match a tunnel zone assigned to a tunnel rule in the prefilter policy.
https://www.cisco.com/c/en/us/td/docs/security/firepower/623/configuration/guide/fpmc-config- guide-v623/policy_management.html

NEW QUESTION: 54
An engineer must configure a Cisco FMC dashboard in a child domain.
Which action must be taken so that the dashboard is visible to the parent domain?
A. Create a copy of the dashboard.
B. Add a separate tab.
C. Add a separate widget.
D. Adjust policy inheritance settings.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 55
An engineer must deploy a Cisco FTD appliance via Cisco FMC to span a network segment to detect malware and threats. When setting the Cisco FTD interface mode, which sequence of actions meets this requirement?
A. Set to passive, and configure an access control policy with an intrusion policy and a file policy defined
B. Set to none, and configure an access control policy with an intrusion policy and a file policy defined
C. Set to none, and configure an access control policy with a prefilter policy defined

D. Set to passive, and configure an access control policy with a prefilter policy defined
Answer: (SHOW ANSWER)

NEW QUESTION: 56
What is the maximum bit size that Cisco FMC supports for HTTPS certificates?
A. 1024
B. 8192
C. 4096
D. 2048
Answer: C (LEAVE A REPLY)
Since version 6.2 (incl) all FMC versions supports 4096 HTTPS Certificates.
https://www.cisco.com/c/en/us/td/docs/security/firepower/610/configuration/guide/fpmc-config- guide-v61/system_configuration.html

NEW QUESTION: 57
An engineer is configuring a custom intrusion rule on Cisco FMC. The engineer needs the rule to search the payload or stream for the string "|44 78 97 13 2 0A|". Which keyword must the engineer use with this string to create an argument for packet inspection?
A. content
B. data
C. protected_content
D. metadata
Answer: (SHOW ANSWER)

NEW QUESTION: 58
What is a limitation to consider when running a dynamic routing protocol on a Cisco FTD device in IRB mode?
A. Only distance vector routing protocols are supported.
B. Only EtherChannel interfaces are supposed.
C. Only nonbridge interfaces are supported.
D. Only link-stale routing protocols are supported.
Answer: (SHOW ANSWER)

NEW QUESTION: 59
A network administrator sees an attempted attack from a specific IP address in the Cisco Secure Firewall Management Center. Which Cisco security tool must be used directly from the Secure Firewall Management Center web page to find out more information about the IP address?
A. Cisco Threat Response browser plugin
B. Cisco Secure Network Analytics
C. Cisco Identity Services Engine
D. Cisco Secure Endpoint
Answer: (SHOW ANSWER)
The Cisco Threat Response browser plugin can be used directly from a web page to investigate observables such as IP addresses. It allows an administrator to select or pivot on an IP address and quickly retrieve threat intelligence and related investigation context from Cisco Threat Response.

NEW QUESTION: 60

An engineer is configuring two new Cisco Secure Firewall Threat Defense devices to replace the existing firewalls. The devices must provide system visibility within the network without being in the flow of network traffic. What must the engineer implement next to accomplish the goal?

Freecram.net

A. Inline Pair mode

B. ERSPAN Passive mode

C. routed mode

D. Passive mode

Answer: (SHOW ANSWER)

Passive mode allows a Cisco Secure Firewall Threat Defense device to monitor a copy of network traffic without being placed directly in the traffic path. This provides visibility and inspection capabilities while avoiding any impact on packet forwarding.

NEW QUESTION: 61

Which two conditions are necessary for high availability to function between two Cisco FTD devices? (Choose two.)

A. The units must be the same version

B. Both devices can be part of a different group that must be in the same domain when configured within the FMC.

C. The units must be different models if they are part of the same series.

D. The units must be configured only for firewall routed mode.

E. The units must be the same model.

Answer: (SHOW ANSWER)

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

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

A company is in the process of deploying intrusion protection with Cisco FTDs managed by a Cisco FMC. Which action must be selected to enable fewer rules detect only critical conditions and avoid false positives?

A. Balanced Security and Connectivity

B. No Rules Active

C. Connectivity Over Security

D. Maximum Detection

Answer: C (LEAVE A REPLY)

NEW QUESTION: 63

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

A. Analysis > Status with a sliding time window of one day

B. Events by priority and classification and set a sliding time window of one day
C. Reports with a daily recurring task that generates based on the network risk report template
D. Security Intelligence Statistics dashboard set to Show the Last option to one day
Answer: (SHOW ANSWER)
Scheduled reports using the network risk report template provide executives with a concise, high- level summary of emerging threats and overall network risk. Automating it on a daily cadence ensures upper management receives consistent updates without manual intervention.

NEW QUESTION: 64
The network engineer at an organization must provide a high-level statistics summary about the 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)
A risk report provides a portable, high-level summary of security risks and trends in the organization. It is designed to present concise, easy-to-interpret information without requiring detailed investigation of individual events, making it appropriate for obtaining an overall security posture summary while operational continuity is important.

NEW QUESTION: 65
A network engineer wants to disable the HTTP response page and interactive blocking of the entire access control policy in Cisco Secure Firewall Management Center. What must be selected in Block Response Page and Interactive Block Response Page?
A. View
B. Custom
C. System
D. None
Answer: (SHOW ANSWER)
In Cisco Secure Firewall Management Center, to disable the HTTP response page and interactive blocking of the entire access control policy, the engineer must select None for both the Block Response Page and Interactive Block Response Page settings. This configuration prevents the firewall from displaying any HTTP response page or offering interactive blocking features when a policy action is triggered, such as blocking traffic based on access control rules.

NEW QUESTION: 66
An engineer is configuring URL filtering for a Cisco FTD device in Cisco FMC. Users must receive a warning when they access http://www.badadultsite.com with the option of continuing to the website if they choose to. No other websites should be blocked. Which two actions must the engineer take to meet these requirements? (Choose two.)
A. On the HTTP Responses tab of the access control policy editor, set the Interactive Block Response Page to System-provided.
B. Configure the default action for the access control policy to Interactive Block.
C. Configure an access control rule that matches an URL object for http://www.badadultsite.com/ and set the action to Interactive Block.
D. Configure an access control rule that matches the Adult URL category and set the action to Interactive Block.
E. On the HTTP Responses tab of the access control policy editor, set the Block Response Page to Custom.
Answer: (SHOW ANSWER)
To configure URL filtering such that users receive a warning when they access a specific website (e.g., http://www.badadultsite.com) and have the option to continue to the site, the engineer needs to perform the following actions:

Configure an access control rule:
Create a URL object for http://www.badadultsite.com.
Set the action for this URL object to "Interactive Block," which prompts the user with a warning and allows them to proceed if they choose to.
Set the Interactive Block Response Page:
Navigate to the HTTP Responses tab in the access control policy editor. Set the Interactive Block Response Page to "System-provided" to ensure that users see the default warning page provided by Cisco Secure Firewall Management Center. These actions ensure that only the specified website triggers an interactive block, while other websites are not blocked.

NEW QUESTION: 67
A software development company hosts the website https://dev.company.com for contractors to share code for projects they are working on with internal developers. The web server is on premises and is protected by a Cisco Secure Firewall Threat Defense appliance. The network administrator is worried about someone trying to transmit infected files to internal users via this site. Which type of policy must be associated with an access control policy to enable Cisco Secure Firewall Malware Defense to detect and block malware?
A. SSL policy
B. file policy
C. network discovery policy
D. prefilter policy
Answer: (SHOW ANSWER)
To enable Cisco Secure Firewall Malware Defense to detect and block malware transmitted through a web server, you must associate a file policy with an access control policy.
A file policy is a set of configurations that the Secure Firewall uses to inspect files in network traffic for malware. By associating file policies with access control rules, the firewall inspects files before allowing them through, enabling detection and blocking of malware in transmitted files.
This is essential for controlling file-based threats coming from sources like web servers, email, or other vectors.
https://secure.cisco.com/secure-firewall/docs/malware-and-file-policy

NEW QUESTION: 68
Which communication is blocked from the bridge groups when multiple are configured in transparent mode on a Cisco Secure Firewall Threat Defense appliance?
A. with other routers
B. with client devices
C. with each other
D. with the internet
Answer: (SHOW ANSWER)
On a Cisco Secure Firewall Threat Defense appliance operating in transparent mode, multiple bridge groups are isolated from each other. Traffic is blocked between bridge groups by default, and communication is only allowed within the same bridge group unless explicitly routed or permitted through additional configuration.

NEW QUESTION: 69
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 AMP for Endpoints service.
C. The Cisco FMC needs to connect to the Cisco ThreatGrid service directly for sandboxing.
D. The Cisco FMC needs to connect with the FireAMP Cloud.
E. The Cisco FMC needs to include a file inspection policy for malware lookup.
Answer: (SHOW ANSWER)

1. The Cisco FMC needs to include a file inspection policy for malware lookup.
File policies in FMC define how files are inspected for malware and control actions such as blocking or allowing files based on their analysis. These file policies are associated with access control rules to inspect matching traffic for malware.
2. The Cisco FMC needs to connect with the FireAMP Cloud.
Cisco FMC integrates with the Cisco Advanced Malware Protection (AMP) cloud service (formerly FireAMP Cloud) to perform malware lookups and analysis. This connection allows FMC to submit files for cloud-based malware analysis and receive threat intelligence to detect and block malicious files.

NEW QUESTION: 70

A network administrator notices that inspection has been interrupted on all non-managed interfaces of a device. What is the cause of this?

FreeCram.net

A. The value of the highest MTU assigned to any non-management interface was changed.
B. The value of the highest MSS assigned to any non-management interface was changed.
C. A passive interface was associated with a security zone.
D. Multiple inline interface pairs were added to the same inline interface.
Answer: (SHOW ANSWER)
Changing the highest MTU value among all non-management interfaces on the device restarts the Snort process when you deploy configuration changes, temporarily interrupting traffic inspection. Inspection is interrupted on all non-management interfaces, not just the interface you modified. Whether this interruption drops traffic or passes it without further inspection depends on the model of the managed device and the interface type. See Snort Restart Traffic Behavior for more information.
https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config- guide-v60/fpmc-config-guide-v60_chapter_01101010.html

NEW QUESTION: 71
What is the disadvantage of setting up a site-to-site VPN in a clustered-units environment?
A. VPN connections can be re-established only if the failed master unit recovers.
B. Smart License is required to maintain VPN connections simultaneously across all cluster units.
C. VPN connections must be re-established when a new master unit is elected.
D. Only established VPN connections are maintained when a new master unit is elected.
Answer: (SHOW ANSWER)
https://www.cisco.com/c/en/us/td/docs/security/firepower/fxos/clustering/ftd-cluster- solution.html#concept_g32_yml_y2b

NEW QUESTION: 72
Refer to the exhibit. A network engineer is analyzing a Network Risk Report generated in Cisco Secure Firewall Management Center that focuses on network security and efficient bandwidth utilization. Which application should be restricted?

HIGH BANDWIDTH APPLICATIONS

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

Application	Times Accessed	Application Risk	Productivity Rating	Data Transferred (MB)
BitTorrent	230,431	High	Low	141212.0074025
Ubuntu Update Manager	30,620	Medium	Low	9937.3018802...
Tivoli	3,872,608	Very Low	Very High	5972.237919
SIP	130,389	Low	Medium	4073.94787107
upLynk	11	Medium	Medium	84.0107183

ENCRYPTED APPLICATIONS

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

Application	Times Accessed	Application Risk	Productivity Rating	Data Transferred (MB)
SSL	11,926,818	Medium	Medium	1449773.319273
Kerberos	6,694,337	Very Low	High	16476.005748
SSH	727,527	High	Medium	72265.972372
Microsoft Azure	467,381	Medium	Very Low	149794.0941926
SFTP	361,783	Medium	Medium	3858.8765371

A. SFTP
B. BitTorrent
C. Tivoli
D. SSH
Answer: (SHOW ANSWER)
From the exhibit, BitTorrent is categorized as a high-risk application with high bandwidth usage and a low productivity rating. This indicates that it is primarily used for activities unrelated to legitimate business purposes, such as peer-to-peer file sharing, which often includes illegal or unauthorized downloads. Restricting or blocking BitTorrent would enhance network security and improve bandwidth efficiency.

NEW QUESTION: 73

freecram.net

Drag and Drop Question

Refer to the exhibit. An engineer configures a NAT rule allowing clients to use the internet only if clients are located on the directly connected internal network. Dynamic auto PAT must be configured.

Drag and drop the NAT rules from the left onto the corresponding targets on the right.

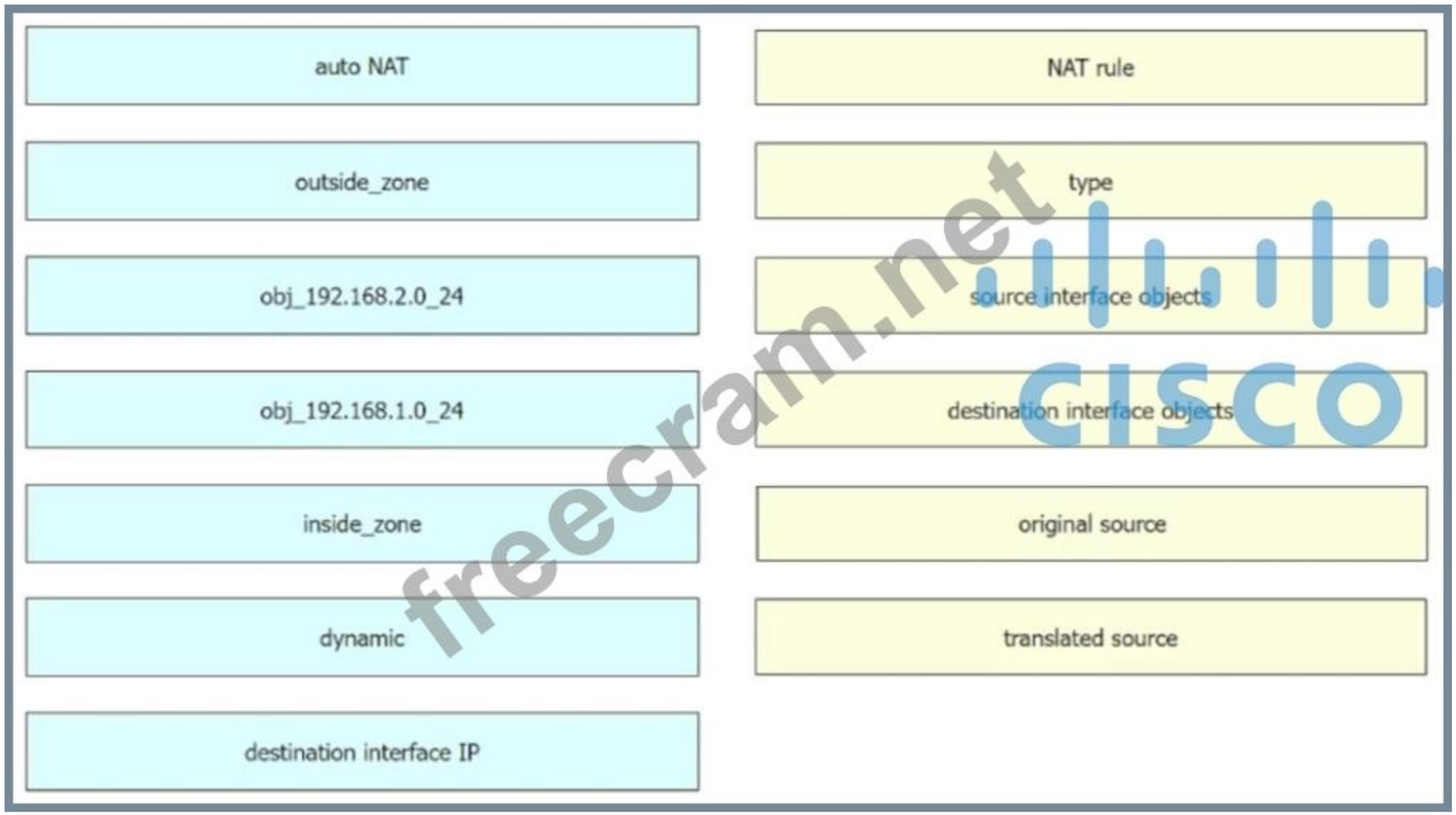
Not all options are used.

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

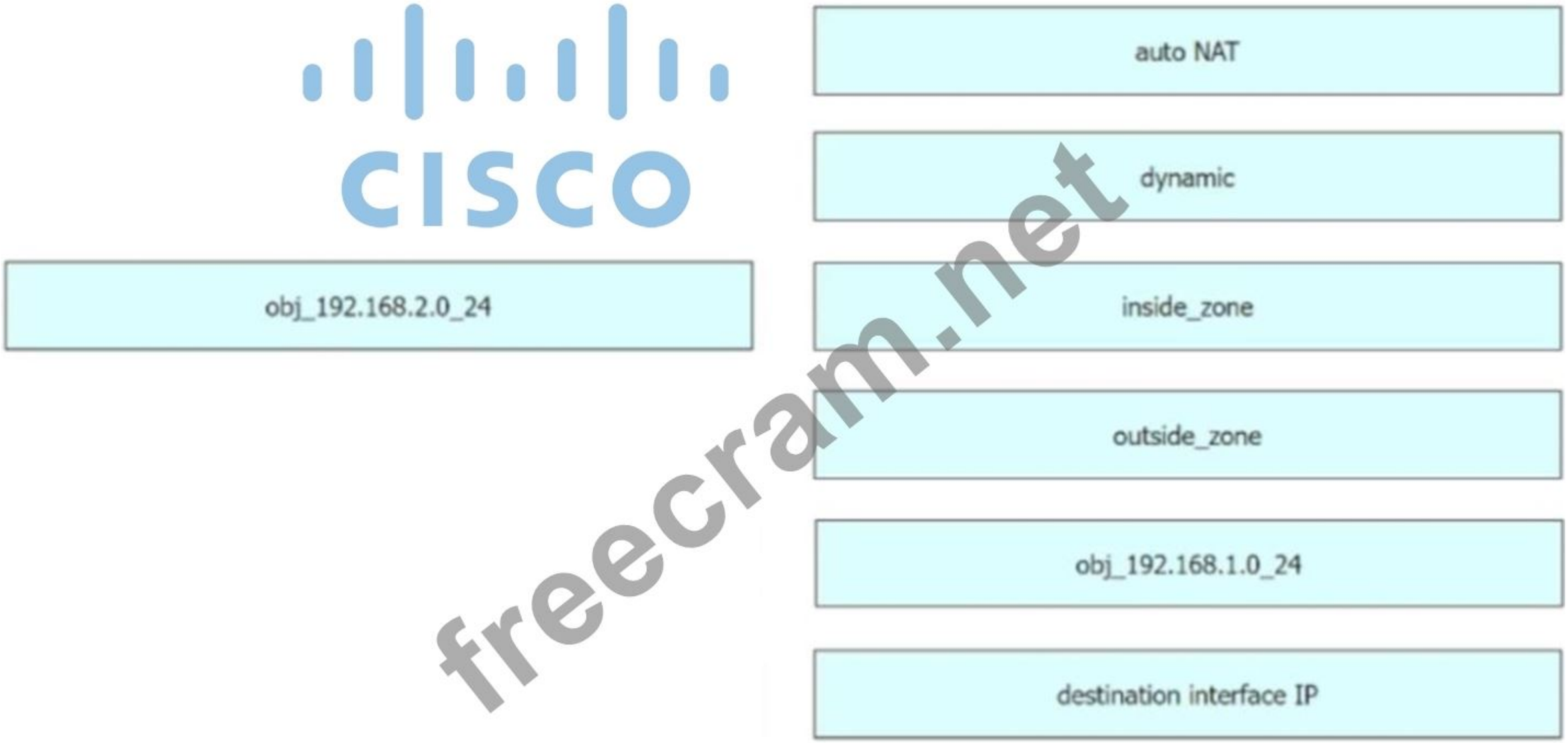
Name	Value	Type
obj_192.168.1.0_24	192.168.1.0/24	Network
obj_192.168.1.1_32	192.168.1.1	Host
obj_192.168.1.254_32	192.168.1.254	Host
obj_192.168.2.0_24	192.168.2.0/24	Network
obj_209.165.201.1_32	209.165.201.1	Host
obj_any	0.0.0.0/0	Network

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

freecram.net


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

Answer:



freecram.net

NEW QUESTION: 74
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?

```
Phase: 16
Type: SNORT
Subtype:
Result: DROP
Config:
Additional Information:
Snort Trace:
Packet: ICMP
Session: new snort session
Firewall: starting rule matching, zone 4 -> 1, geo 0 -> 0, vlan 0, sgt 0, src sgt type 0, dest_sgt_tag 0, dest sgt type 0, username 'No Authentication Required', , icmpType 8, icmpCode 0
Firewall: block rule,  'Ping' , drop
Snort: processed decoder alerts or actions queue, drop
Snort id 0, NAP id 2, IPS id 0, Verdict BLACKLIST, Blocked by Firewall
Snort Verdict: (black-list) black list this flow

Result:
input-interface: ACCESS41_Inside1
input-status: up
input-line-status: up
Action: drop
Drop-reason: (firewall) Blocked or blacklisted by the firewall preprocessor, Drop-location: frame 0x000055d2b0f8b7e0 flow (NA)/NA
```

freecram.net

A. Create an access control policy rule that allows ICMP traffic.

B. Configure a custom Snort signature to allow ICMP traffic after Inspection.

C. Modify the Snort rules to allow ICMP traffic.

D. Create an ICMP allow list and add the ICMP destination to remove it from the implicit deny list.

Answer: (SHOW ANSWER)

https://community.cisco.com/t5/network-security/ftd-firewall-blocked-or-blacklisted/td-p/4494363

NEW QUESTION: 75

An engineer is configuring a Cisco Secure Firewall Management Center appliance. The company requires the use of a TAXII server in Threat Intelligence Director. The company requires that in Threat Intelligence Director, Action must be set to Block. On which two items must the engineer configure a block? (Choose two.)

A. Observable

B. Element

C. Indicator

D. Complex indicator

E. Source

Answer: (SHOW ANSWER)

For threat intelligence received from a TAXII source, blocking can be configured on individual observables and simple indicators after the data is ingested. TAXII sources themselves cannot use Block as their action because STIX data may contain complex indicators that Secure Firewall devices cannot directly block.

NEW QUESTION: 76

Network traffic coining from an organization's CEO must never be denied.

Which access control policy configuration option should be used if the deployment engineer is not permitted to create a rule to allow all traffic?

A. Configure a trust policy for the CEO.

B. Create a NAT policy just for the CEO.

C. Configure firewall bypass.

D. Change the intrusion policy from security to balance.

Answer: A (LEAVE A REPLY)

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
What is the purpose of the Cisco Secure Firewall Threat Defense "Balanced Security and Connectivity" network analysis policy?
A. It maximizes throughput by disabling all preprocessors.
B. It provides a default set of preprocessor and detection settings that balance security effectiveness with performance impact.
C. It enables only file and malware inspection.
D. It disables intrusion rule evaluation entirely.
Answer: (SHOW ANSWER)
The Balanced Security and Connectivity network analysis policy is a Cisco-provided default policy that offers a reasonable trade-off between thorough traffic normalization/inspection and system performance, making it suitable for most deployments as a starting point.

NEW QUESTION: 78
With Cisco FTD software, which interface mode must be configured to passively receive traffic that passes through the appliance?
A. ERSPAN
B. IPS-only
C. firewall
D. tap
Answer: (SHOW ANSWER)
With tap mode, the FTD is deployed inline, but the network traffic flow is undisturbed. Instead, the FTD makes a copy of each packet so that it can analyze the packets. Note that rules of these types do generate intrusion events when they are triggered, and the table view of intrusion events indicates that the triggering packets would have dropped in an inline deployment. There are benefits to using tap mode with FTDs that are deployed inline.

NEW QUESTION: 79
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. Cisco ISE Security Group Tag
B. Inspect Local Traffic Bypass
C. Automatic Application Bypass
D. Fast-Path Rules Bypass
Answer: (SHOW ANSWER)

NEW QUESTION: 80
Which feature is supported by IRB on Cisco FTD devices?

A. redundant interface
B. dynamic routing protocol
C. EtherChannel interface
D. high-availability cluster
Answer: A (LEAVE A REPLY)
https://www.cisco.com/c/en/us/td/docs/security/firepower/70/configuration/guide/fpmc-config- guide-v70/transparent_or_routed_firewall_mode_for_firepower_threat_defense.html#id_40010

NEW QUESTION: 81
An organization has a Cisco FTD that uses bridge groups to pass traffic from the inside interfaces to the outside interfaces. They are unable to gather information about neighbouring Cisco devices or use multicast in their environment. What must be done to resolve this issue?
A. Create a firewall rule to allow CDP traffic.
B. Create a bridge group with the firewall interfaces.
C. Change the firewall mode to transparent.
D. Change the firewall mode to routed.
Answer: (SHOW ANSWER)
"In routed firewall mode, broadcast and multicast traffic is blocked even if you allow it in an access rule..."
"The bridge group does not pass CDP packets packets..."
https://www.cisco.com/c/en/us/td/docs/security/asa/asa913/configuration/general/asa-913- general-config/intro-fw.html

NEW QUESTION: 82
Which interface type allows packets to be dropped?
A. passive
B. inline
C. ERSPAN
D. TAP
Answer: (SHOW ANSWER)
https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/200908-configuring- firepower-threat-defense-int.html

NEW QUESTION: 83
A network administrator is configuring a BVI interface on a routed FTD. The administrator wants to isolate traffic on the interfaces connected to the bridge group and not have the FTD route this traffic using the routing table. What must be configured?
A. A new VRF must be created for the BVI interface
B. An IP address must be configured on the BVI
C. IP routing must be removed from the physical interfaces connected to the BVI
D. The BVI interface must be configured for transparent mode
Answer: A (LEAVE A REPLY)
https://www.cisco.com/c/en/us/td/docs/security/firepower/660/configuration/guide/fpmc-config-guide-v66/virtual-routing-for-firepower-threat-defense.html

NEW QUESTION: 84
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.

NEW QUESTION: 85
Which feature sets up multiple interfaces on a Cisco Secure Firewall Threat Defense to be on the same subnet?
A. EtherChannel
B. SVI
C. BVI
D. security levels
Answer: (SHOW ANSWER)
A Bridge-Group Virtual Interface (BVI) lets you bridge multiple physical interfaces into a single logical interface so they share the same IP subnet on Cisco Secure Firewall Threat Defense.

NEW QUESTION: 86
An engineer must permit SSH on the inside interface of a Cisco Secure Firewall Threat Defense device. SSH is currently permitted only on the management interface. Which type of policy must the engineer configure?
A. platform policy
B. access control policy
C. NAT policy
D. intrusion policy
Answer: A (LEAVE A REPLY)
Enabling SSH on a data-plane interface is controlled by the platform policy, which governs management protocols per interface rather than traffic filtering or inspection.

NEW QUESTION: 87
Which default action setting in a Cisco FTD Access Control Policy allows all traffic from an undefined application to pass without Snort inspection?
A. Network Discovery Only
B. Inherit from Base Policy
C. Trust All Traffic
D. Intrusion Prevention
Answer: C (LEAVE A REPLY)

NEW QUESTION: 88

A network administrator cannot select the link to be used for failover when configuring an active/passive HA Cisco FTD pair. Which configuration must be changed before setting up the high availability pair?

A. An IP address in the same subnet must be added to each Cisco FTD on the interface.

B. The interface name must be removed from the interface on each Cisco FTD.

C. The name Failover must be configured manually on the interface on each Cisco FTD.

D. The interface must be configured as part of a LACP Active/Active EtherChannel.

Answer: (SHOW ANSWER)

To resolve the issue where a network administrator cannot select the failover link for a Cisco FTD active/passive HA pair, the interface name must be removed from both devices. This is required because interfaces configured with names cannot be used for failover links. The failover interface must be dedicated solely to HA communication and cannot function as a normal named networking interface.

https://www.cisco.com/c/en/us/td/docs/security/firepower/660/fdm/fptd-fdm-config-guide-660/fptd- fdm- ha.html#concept_8C628FB71F0444A6BAC6D33FD72FB2EE#:~:text=you%20cannot%20specify%20an%20interface%20that%20is%20currently%20configured%20with%20a%20name

NEW QUESTION: 89

An engineer is configuring a Cisco Secure Firewall Management Center appliance. Secure Firewall Management Center must respond in real time to threats on the network and use a host profile qualification to trigger a response. Which type of policy must be configured in Secure Firewall Management Center?

A. application detector

B. network discovery

C. correlation

D. intrusion

Answer: (SHOW ANSWER)

A correlation policy enables Secure Firewall Management Center to respond in real time to detected network threats. Correlation rules can use host profile qualifications and other observed network conditions to identify specified activity and trigger configured responses when those conditions are met.

NEW QUESTION: 90

Drag and Drop Question

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



Answer Area



CISCO
freecram.net

Answer:

Answer Area



CISCO freecram.net

NEW QUESTION: 91

Which two TCP ports can allow the Cisco Firepower Management Center to communication with FireAMP cloud for file disposition information? (Choose two.)
A. 8080
B. 22
C. 32137
D. 8305
E. 443
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: 92
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 > Host Attributes
B. Analysis > Hosts > Indications of Compromise
C. Analysis > Files > Malware Events
D. Analysis > Files > Network File Trajectory
Answer: (SHOW ANSWER)

NEW QUESTION: 93
An engineer must implement Cisco Secure Firewall transparent mode due to a new server recently being added that must communicate with an existing server that is currently separated by the firewall. Which implementation action must be taken next by the engineer to accomplish the goal?
A. Configure the same default gateway for both servers.
B. Ensure that both servers are in the same bridge domain.
C. Enable both servers to share the same VXLAN segment.
D. Assign the same subnet to both servers.
Answer: B (LEAVE A REPLY)
In transparent mode, Cisco Secure Firewall Threat Defense (FTD) operates as a Layer 2 firewall, acting as a "bump in the wire" without performing routing functions. This mode allows devices on either side of the firewall to communicate as if they were on the same network. To achieve this, the firewall typically uses bridge domains or similar configurations to group devices.
A bridge domain groups interfaces in transparent mode so that devices on each side of the firewall can communicate directly. Ensuring that both servers are in the same bridge domain allows traffic to pass through the firewall transparently, enabling communication between the two servers as if the firewall were not there.

NEW QUESTION: 94
Refer to the exhibit. An engineer is configuring an instance of Cisco Secure Firewall Threat Defense with a Secure Firewall Threat Defense interface in IPS Inline Pair mode. What must the engineer configure on interface e1/6?



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

NEW QUESTION: 95
Users report that Cisco Duo 2FA fails when they attempt to connect to the VPN on a Cisco Secure Firewall Threat Defense (FTD) device. IT staff have VPN profiles that do not require multifactor authentication and they can connect to the VPN without any issues. When viewing the VPN troubleshooting log in Cisco Secure Firewall Management Center (FMC), the network administrator sees an error that the Cisco Duo AAA server has been marked as failed. What is the root cause of the issue?
A. AD Trust certificates are missing from the Secure FTD device.
B. Multifactor authentication is not supported on Secure FMC managed devices.
C. The internal AD server is unreachable from the Secure FTD device.
D. Duo trust certificates are missing from the Secure FTD device.
Answer: (SHOW ANSWER)
If users report that Cisco Duo 2FA fails when attempting to connect to the VPN on a Cisco Secure Firewall Threat Defense (FTD) device, and the VPN troubleshooting log in FMC shows an error indicating that the Cisco Duo AAA server has been marked as failed, the root cause is likely missing Duo trust certificates on the FTD device. Trust certificates are essential for establishing a secure and trusted connection between the FTD and the Duo authentication service.
Steps:
Obtain the necessary Duo trust certificates.
Install the certificates on the FTD device.
Verify the configuration to ensure that the FTD device can properly communicate with the Duo AAA server.
This resolves the authentication failure by ensuring that the FTD device can trust the Duo server.

NEW QUESTION: 96
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. Enable the FXOS for multi-instance.
B. Configure a prefilter policy.
C. Configure modular policy framework.

D. Disable TCP inspection.
Answer: (SHOW ANSWER)
https://www.cisco.com/c/en/us/td/docs/security/firepower/610/configuration/guide/fpmc-config- guide-v61/prefiltering_and_prefilter_policies.html

NEW QUESTION: 97
Which Cisco Secure Firewall Management Center feature allows an administrator to compare the running configuration of two managed devices side by side?
A. Health Monitor
B. Audit Log
C. Configuration Comparison Report
D. System Policy
Answer: (SHOW ANSWER)
The Configuration Comparison Report in Cisco Secure Firewall Management Center allows administrators to compare configurations between two devices, or between two versions of the same device's configuration, to identify differences and troubleshoot inconsistencies.

NEW QUESTION: 98
An engineer must configure and generate a report in Cisco Secure Firewall Management Center.
The report must allow for the addition of headers and footers, and it will contain many pages.
Which format must the engineer configure the report to use?
A. pdf
B. xls
C. xml
D. doc
Answer: A (LEAVE A REPLY)
A report is a document file formatted in PDF, HTML, or CSV.
https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/management- center/admin/740/management-center-admin-74/report-reports.html

NEW QUESTION: 99
Which two field can be used to create a new email alert within the Cisco Firepower Management center under Policies > Actions > Alerts tab? (Choose two.)
A. Device
B. Destination
C. From
D. Source
E. Relay Host
Answer: C,E (LEAVE A REPLY)

NEW QUESTION: 100
Which policy rule is included in the deployment of a local DMZ during the initial deployment of a Cisco NGFW through the Cisco FMC GUI?
Freecram.net
A. a default DMZ policy for which only a user can change the IP addresses.
B. deny ip any
C. no policy rule is included

D. permit ip any
Answer: (SHOW ANSWER)
No policy rule is included in the deployment of a local DMZ during the initial deployment of a Cisco NGFW through the Cisco FMC GUI. The administrator must create the necessary policy rules to allow traffic to and from the DMZ.

NEW QUESTION: 101
When do you need the file-size command option during troubleshooting with packet capture?
A. when capture packets are less than 16 MB
B. when capture packets are restricted from the secondary memory
C. when capture packets exceed 10 GB
D. when capture packets exceed 32 MB
Answer: (SHOW ANSWER)
https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-config- guide-v62/troubleshooting_the_system.html

NEW QUESTION: 102
Refer to the exhibit. A Cisco Secure Firewall Management Center, 7.0 device fails to receive intelligence feed updates.
The Cisco Secure Firewall Management Center is configured to use a proxy server that performs SSL inspection.
Which action allows the Cisco Secure Firewall Management Center device to download the intelligence feed updates?

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

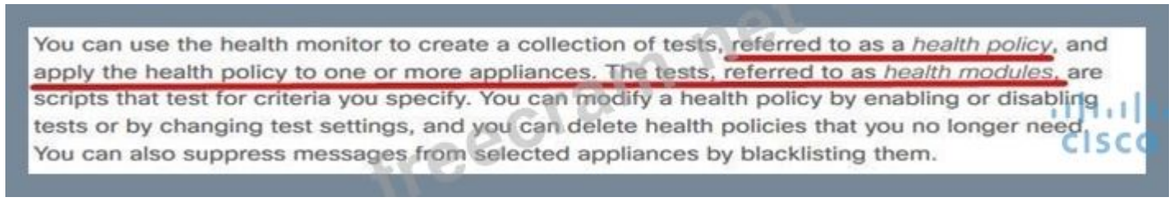
Sourcefire3D SF-IMS[24085]: [24090] CloudAgent:IPReputation [WARN] Download
 unsucessful: Failure when receiving data from the peer
```

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

NEW QUESTION: 103
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 cryptomining networks.
Which system settings must the administrator configure in Secure Firewall Management Center to meet the requirement?
A. Intrusion Policy, Security Intelligence
B. Access Policy, Security Intelligence
C. Malware Policy, Rules
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.

NEW QUESTION: 104
On Cisco Firepower Management Center, which policy is used to collect health modules alerts from managed devices?
A. health policy
B. system policy
C. correlation policy
D. access control policy
E. health awareness policy
Answer: (SHOW ANSWER)



NEW QUESTION: 105
A Cisco FTD has two physical interfaces assigned to a BVI. Each interface is connected to a different VLAN on the same switch.
Which firewall mode is the Cisco FTD set up to support?
A. active/active failover
B. transparent
C. high availability clustering
D. routed
Answer: (SHOW ANSWER)

NEW QUESTION: 106
An engineer is implementing a new Cisco Secure Firewall. The firewall must filler traffic between the three subnets:
- LAN 192.168.101.0/24
- 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.

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
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)
https://www.cisco.com/c/en/us/td/docs/security/firepower/integrations/CTR/Firepower_and_Cisco_Threat_Response_Integration_Guide/about_integrating_firepower_and_cisco_threat_response.html

NEW QUESTION: 108
Which connector is used to integrate Cisco ISE with Cisco FMC for Rapid Threat Containment?
A. pxGrid
B. FTD RTC
C. FMC RTC
D. ISEGrid
Answer: (SHOW ANSWER)
The FireSIGHT Management Center (FMC) is configured for using self-signed certificates for ISE pxGrid node operation.

NEW QUESTION: 109
Drag and Drop Question

Refer to the exhibit. An engineer must configure a connection on a Cisco ASA 5500-X Series with a Cisco Secure Firewall Services Module to ensure that the secondary interface takes over all the functions of the primary interface if the primary interface fails. Drag and drop the code snippets from the bottom onto the boxes in the CLI commands to configure the failover. Not all options are used.

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

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

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

cisco
freecram.net

member-interface GigabitEthernet1/5	member-interface GigabitEthernet1/4
GigabitEthernet1/5	backup interface GigabitEthernet1/4
Redundant1	reactivation mode timed
failover link Redundant1 GigabitEthernet1/4	

Answer:

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

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

cisco
freecram.net

GigabitEthernet1/5

backup interface GigabitEthernet1/4

reactivation mode timed

failover link Redundant1 GigabitEthernet1/4

Explanation:

ASA(config)# interface Redundant1

ASA(config-if)# member-interface GigabitEthernet1/5

ASA(config-if)# member-interface GigabitEthernet1/4

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

NEW QUESTION: 110

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

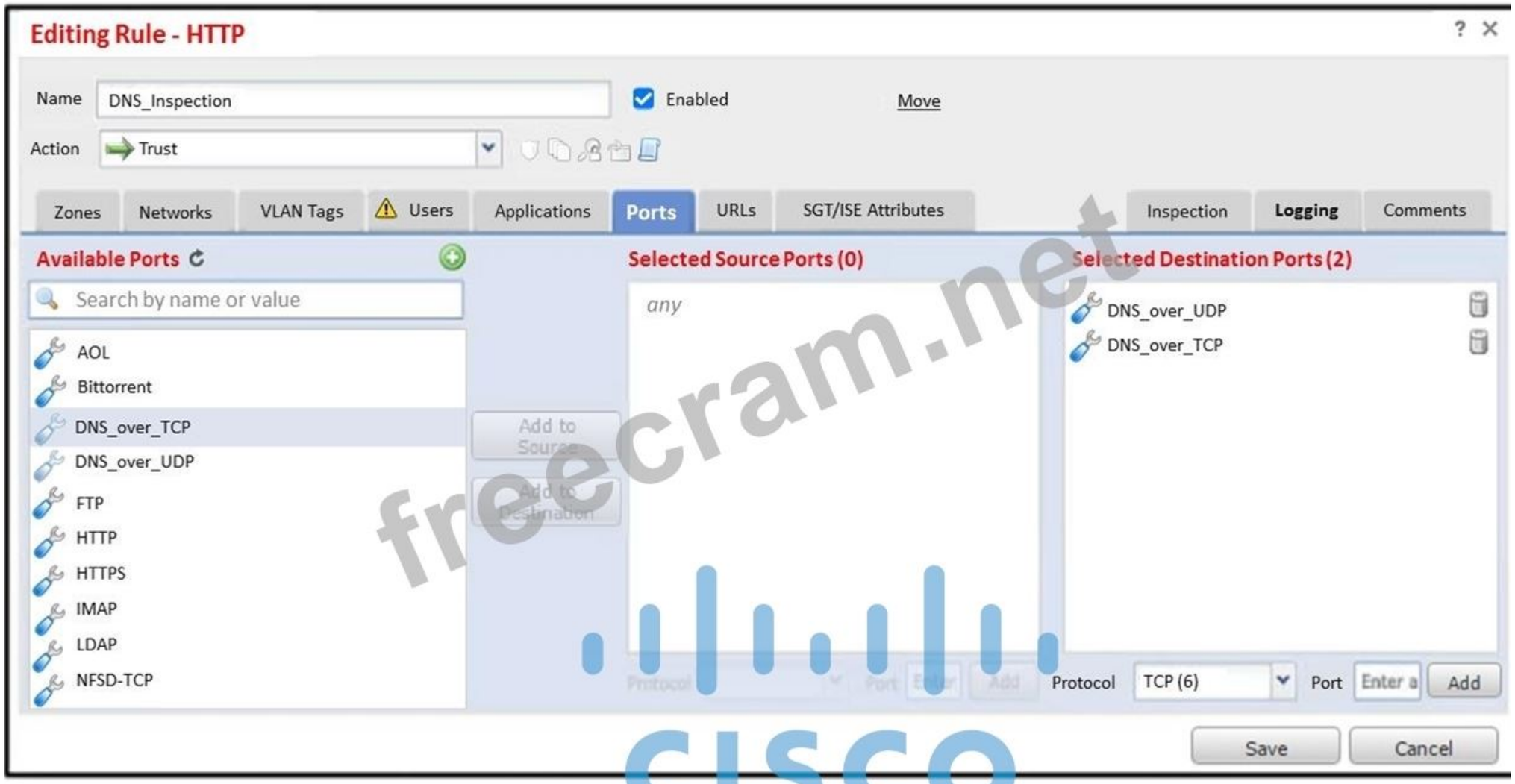
Freecram.net

A. investigate

B. reporting
C. enforcement
D. REST
Answer: C (LEAVE A REPLY)
The Umbrella Enforcement API is a feature that allows for automated addition of new domains to a security enforcement list.

NEW QUESTION: 111
A network administrator is configuring an FTD in transparent mode. A bridge group is set up and an access policy has been set up to allow all IP traffic. Traffic is not passing through the FTD.
What additional configuration is needed?
A. A default route must be added to the FTD.
B. An IP address must be assigned to the BVI.
C. A mac-access control list must be added to allow all MAC addresses.
D. The security levels of the interfaces must be set.
Answer: (SHOW ANSWER)

NEW QUESTION: 112
Refer to the exhibit. An engineer is modifying an access control pokey to add a rule to inspect all DNS traffic that passes through the firewall.
After making the change and deploying the pokey they see that DNS traffic is not bang inspected by the Snort engine. What is the problem?



freecram.net

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

NEW QUESTION: 113
Refer to the exhibit. What is the effect of the existing Cisco FMC configuration?



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

NEW QUESTION: 114
Which Cisco Firepower Threat Defense, which two interface settings are required when configuring a routed interface? (Choose two.)
A. Redundant Interface
B. EtherChannel
C. Speed
D. Media Type
E. Duplex
Answer: (SHOW ANSWER)
https://www.cisco.com/c/en/us/td/docs/security/firepower/610/fdm/fptd-fdm-config-guide-610/fptd-fdm- interfaces.html

NEW QUESTION: 115
An engineer is troubleshooting a file that is being blocked by a Cisco FTD device on the network.
The user is reporting that the file is not malicious. Which action does the engineer take to identify the file and validate whether or not it is malicious?
A. Right click the connection event and send the file to AMP for Endpoints to see if the hash is malicious.
B. Identify the file in the intrusion events and submit it to Threat Grid for analysis.
C. Use the context explorer to find the file and download it to the local machine for investigation.
D. Use FMC file analysis to look for the file and select Analyze to determine its disposition.
Answer: (SHOW ANSWER)

NEW QUESTION: 116
An engineer must investigate a connectivity issue by using Cisco Secure Firewall Management Center to access the Packet Capture feature on a Cisco Secure Firewall Threat Defense device.
The engineer must see a real packet going through the Secure Firewall Threat Defense device and the Snort detection actions. While reviewing the packet capture, the engineer discovers that the Snort detection actions are missing. Which action must the engineer take to resolve the issue?

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

NEW QUESTION: 117
An organization must be able to ingest NetFlow traffic from their Cisco FTD device to Cisco Stealthwatch for behavioral analysis.
What must be configured on the Cisco FTD to meet this requirement?
A. flexconfig object for NetFlow
B. interface object to export NetFlow
C. security intelligence object for NetFlow
D. variable set object for NetFlow
Answer: (SHOW ANSWER)
Step 4. Configure the Netflow Destination
In order to configure the Netflow Destination, navigate to Objects > FlexConfig > FlexConfig Objects
https://www.cisco.com/c/en/us/support/docs/quality-of-service-qos/netflow/216126-configure- netflow-secure-event-logging-o.html#anc14

NEW QUESTION: 118
Which command is run at the CLI when logged in to an FTD unit, to determine whether the unit is managed locally or by a remote FMC server?
A. system generate-troubleshoot
B. show configuration session
C. show managers
D. show running-config | include manager
Answer: (SHOW ANSWER)
https://www.cisco.com/c/en/us/td/docs/security/firepower/command_ref/b_Command_Reference_ for_Firepower_Threat_Defense/c_3.html

NEW QUESTION: 119
An organization has a Cisco IPS running in inline mode and is inspecting traffic for malicious activity. When traffic is received by the Cisco IRS, if it is not dropped, how does the traffic get to its destination?
A. It is retransmitted from the Cisco IPS inline set.
B. The packets are duplicated and a copy is sent to the destination.
C. It is transmitted out of the Cisco IPS outside interface.
D. It is routed back to the Cisco ASA interfaces for transmission.
Answer: (SHOW ANSWER)
Inline interfaces receive all traffic unconditionally, but all traffic received on these interfaces is retransmitted out of an inline set unless explicitly dropped.
https://www.cisco.com/c/en/us/td/docs/security/firepower/601/configuration/guide/fpmc-config- guide-v601/fpmc-config-guide-v60_chapter_01011010.pdf

NEW QUESTION: 120

Which two statements are valid regarding the licensing model used on Cisco Secure Firewall Threat Defense Virtual appliances? (Choose two.)

Freecram.net

A. All licenses support a maximum of 250 VPN peers
B. All licenses support up to 16 vCPUs
C. Licenses can be used on any supported cloud platform
D. Licenses can be used on both physical and virtual appliances
E. All licenses require 500G of available storage for the VM
Answer: (SHOW ANSWER)

NEW QUESTION: 121
A network engineer implements a new Cisco Firepower device on the network to take advantage of its intrusion detection functionality. There is a requirement to analyze the traffic going across the device, alert on any malicious traffic, and appear as a bump in the wire How should this be implemented?
A. Specify the BVI IP address as the default gateway for connected devices.
B. Enable routing on the Cisco Firepower
C. Add an IP address to the physical Cisco Firepower interfaces.
D. Configure a bridge group in transparent mode.
Answer: (SHOW ANSWER)
Traditionally, a firewall is a routed hop and acts as a default gateway for hosts that connect to one of its screened subnets. A transparent firewall, on the other hand, is a Layer 2 firewall that acts like a "bump in the wire," or a "stealth firewall," and is not seen as a router hop to connected devices. However, like any other firewall, access control between interfaces is controlled, and all of the usual firewall checks are in place.
Layer 2 connectivity is achieved by using a "bridge group" where you group together the inside and outside interfaces for a network, and the ASA uses bridging techniques to pass traffic between the interfaces. Each bridge group includes a Bridge Virtual Interface (BVI) to which you assign an IP address on the network. You can have multiple bridge groups for multiple networks.
In transparent mode, these bridge groups cannot communicate with each other.
https://www.cisco.com/c/en/us/td/docs/security/asa/asa97/configuration/general/asa-97-general- config/intro-fw.html

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

NEW QUESTION: 123
A network administrator is trying to configure an access rule to allow access to a specific banking site over HTTPS. Which method must the administrator use to meet the requirement?
A. Enable SSL decryption and specify the URL.
B. Define the URL to be blocked and set the application to HTTP.
C. Define the URL to be blocked and disable SSL inspection.
D. Block the category of banking and define the application of WWW.
Answer: (SHOW ANSWER)
To allow access to a specific banking site over HTTPS, the network administrator must use SSL decryption (also known as SSL/TLS inspection) and specify the URL. This is because HTTPS traffic is encrypted, and the firewall needs to decrypt the traffic to inspect the URL and enforce the access rule.
Steps:
Enable SSL Decryption: Configure SSL policies to decrypt the HTTPS traffic.
Specify the URL: Define the URL of the banking site in the access control policy, ensuring that the decrypted traffic is inspected and allowed based on the specified URL.
This method ensures that only the desired banking site is accessed over HTTPS, while other HTTPS traffic can be filtered or blocked according to the organization's security policies.

NEW QUESTION: 124
Which Cisco Firepower rule action displays an HTTP warning page?
A. Monitor
B. Block
C. Interactive Block
D. Allow with Warning
Answer: (SHOW ANSWER)
https://www.cisco.com/c/en/us/td/docs/security/firesight/541/user-guide/FireSIGHT-System- UserGuide-v5401/AC-Rules-Tuning-Overview.html#76698

NEW QUESTION: 125
An engineer is deploying a Cisco ASA Secure Firewall module. The engineer must be able to examine traffic without impacting the network, and the ASA has been deployed with a single context.
Which ASA Secure Firewall module deployment mode must be implemented to meet the requirements?
A. routed mode with inline tap monitor-only mode
B. transparent mode with passive monitor-only mode
C. transparent mode with inline tap monitor-only mode
D. routed mode with passive monitor-only mode
Answer: (SHOW ANSWER)
In this scenario, the engineer's requirement is to inspect traffic without impacting the network. To meet this, the passive monitor-only mode is an appropriate choice:
- Transparent Mode: In this mode, the Cisco ASA acts as a "bump in the wire," making it effectively invisible to the network. This mode does not require IP addresses on the interfaces, allowing it to inspect traffic without altering or routing it, making it ideal for passive monitoring scenarios.
- Passive Monitor-Only Mode: This mode is specifically designed to allow traffic inspection without interference. Traffic flows through the device, allowing it to inspect packets but without enforcing policies or disrupting packet flow, which is crucial to meet the requirement of "no network impact."
- Single Context Requirement: The setup specifies a single context, which simplifies the deployment by using one consistent inspection policy across the traffic.

NEW QUESTION: 126
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)
https://www.cisco.com/c/en/us/td/docs/security/firepower/630/configuration/guide/fpmc-config- guide-v63/inline_sets_and_passive_interfaces_for_firepower_threat_defense.html

NEW QUESTION: 127
A network administrator manages a network with multiple firewalls in a data center. The administrator must change a next-generation firewall from routed to transparent mode. Which action must the administrator take to meet the requirement?
A. Deregister the firewall in Cisco Secure Firewall Management Center.
B. Enter the configure firewall transparent command from the CLI.
C. Manually delete the interface configuration from the CLI.
D. Create one or more bridge groups from the CLI.
Answer: (SHOW ANSWER)
Step 1. Deregister the Firepower Threat Defense device from the FMC.
Step 2. Access the Firepower Threat Defense device CLI, preferably from the console port.
Step 3. > configure firewall [routed | transparent]
Step 4. Re-register with the FMC
https://www.cisco.com/c/en/us/td/docs/security/firepower/70/configuration/guide/fpmc-config- guide-v70/transparent_or_routed_firewall_mode_for_firepower_threat_defense.html

NEW QUESTION: 128
Which action should you take when Cisco Threat Response notifies you that AMP has identified a file as malware?
A. Wait for Cisco Threat Response to automatically block the malware.
B. Forward the result of the investigation to an external threat-analysis engine.
C. Add the malicious file to the block list.
D. Send a snapshot to Cisco for technical support.
Answer: (SHOW ANSWER)

NEW QUESTION: 129
An engineer is troubleshooting application failures through a FTD deployment.
While using the FMC CLI. it has been determined that the traffic in question is not matching the desired policy. What should be done to correct this?
A. Use the system support firewall-engine-debug command to determine which rules the traffic matching and modify the rule accordingly
B. Use the system support application-identification-debug command to determine which rules the traffic matching and modify the rule accordingly
C. Use the system support firewall-engine-dump-user-f density-data command to change the policy and allow the application through the firewall.
D. Use the system support network-options command to fine tune the policy.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 130

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?

Freecram.net

A. by creating a URL object in the policy to block the website
B. by Isolating the endpoint
C. Cisco Talos will automatically update the policies.
D. by denying outbound web access
Answer: (SHOW ANSWER)

NEW QUESTION: 131
A security analyst is investigating a potential network compromise. The analyst must produce a report of the suspicious activity from Cisco Secure Firewall Management Center. Which two details must be included in the report to assist the investigation? (Choose two.)
A. Client applications by user
B. Intrusion events
C. Host connections
D. Number of attacked machines
E. User connections
Answer: B,C (LEAVE A REPLY)
Intrusion events provide the detection evidence needed to understand which signatures fired, the affected source and destination addresses, event severity, protocol information, and other indicators associated with the suspected compromise. Host connections provide the corresponding network context, allowing the analyst to determine which systems communicated, when the sessions occurred, and which ports, applications, or protocols were involved. Together, these details connect security detections with the traffic flows that produced them and support reconstruction of the incident. Client applications by user and user connections are useful when the investigation is primarily identity-focused, but they do not provide the same direct combination of exploit evidence and host-level network activity. The number of attacked machines is an aggregate measurement and lacks the granular information necessary to investigate the suspicious communications and determine their cause.

NEW QUESTION: 132
A security engineer must configure policies for a recently deployed Cisco FTD. The security policy for the company dictates that when five or more connections from external sources are initiated within 2 minutes, there is cause for concern. Which type of policy must be configured in Cisco FMC to generate an alert when this condition is triggered?
A. correlation
B. application detector
C. access control
D. intrusion
Answer: (SHOW ANSWER)

NEW QUESTION: 133
What are 2 types or forms of suppression on a FirePower policy (or FTD)?
A. source
B. application
C. port
D. protocol
E. rule

Answer: (SHOW ANSWER)

NEW QUESTION: 134
Which Cisco Secure Firewall Threat Defense CLI command is used to display the current status of a High Availability pair?
A. show failover
B. show ha-status
C. show cluster status
D. show high-availability
Answer: (SHOW ANSWER)
The command "show failover" on Cisco Secure Firewall Threat Defense displays the current state of the High Availability (failover) pair, including which unit is active/standby and synchronization status.

NEW QUESTION: 135
An engineer is reviewing a ticket that requests to allow traffic for some devices that must connect to a server over 8699/udp. The request mentions only one IP address, 172.16.18.15, but the requestor asked for the engineer to open the port for all machines that have been trying to connect to it over the last week. Which action must the engineer take to troubleshoot this issue?
A. Use the context explorer to see the destination port blocks
B. Filter the connection events by the destination port 8699/udp.
C. Filter the connection events by the source port 8699/udp.
D. Use the context explorer to see the application blocks by protocol.
Answer: (SHOW ANSWER)

NEW QUESTION: 136
An administrator is adding a QoS policy to a Cisco FTD deployment. When a new rule is added to the policy and QoS is applied on 'Interfaces in Destination Interface Objects", no interface objects are available What is the problem?
A. The FTD is out of available resources lor use. so QoS cannot be added
B. The network segments that the interfaces are on do not have contiguous IP space
C. QoS is available only on routed interfaces, and this device is in transparent mode.
D. A conflict exists between the destination interface types that is preventing QoS from being added
Answer: (SHOW ANSWER)
https://www.cisco.com/c/en/us/td/docs/security/firepower/640/configuration/guide/fpmc-config- guide-v64/quality_of_service__qos__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: 137
An engineer is deploying AMP for the first time and cannot afford any interrupted to network traffic.
Which policy types does NOT disrupted the network?
A. Audit
B. Protect

C. tnage
D. Server
Answer: (SHOW ANSWER)

NEW QUESTION: 138
Which Cisco Rapid Threat Containment mitigation action is enabled by integrating pxGrid Adaptive Network Control with Cisco ISE and Cisco Secure Firewall Management Center?
A. reject
B. suspend
C. terminate
D. block
Answer: (SHOW ANSWER)
When Cisco pxGrid Adaptive Network Control is integrated with Cisco ISE and Cisco Secure Firewall Management Center (FMC), the "block" action is used to enforce Rapid Threat Containment. This action enables the firewall to dynamically block malicious traffic or quarantine compromised hosts based on threat intelligence shared across pxGrid.

NEW QUESTION: 139
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 ISE
D. Network Protection Services
Answer: (SHOW ANSWER)
Adaptive Network Control provides the remediation mechanism used with Cisco ISE for Rapid Threat Containment. Through pxGrid integration, it allows Secure Firewall Management Center to trigger actions such as quarantining or unquarantining endpoints and changing their network access state in response to detected threats.

NEW QUESTION: 140
An engineer wants to control which URLs users are allowed to access based on category and reputation. Which Cisco Secure Firewall feature should be configured?
Freecram.net
A. URL Filtering in Access Control Policy
B. Security Intelligence Feed
C. File Policy
D. Network Discovery Policy
Answer: (SHOW ANSWER)
URL Filtering, configured within the Access Control Policy, allows administrators to control web access based on URL category (such as gambling, social media) and reputation score, using Cisco's cloud-based URL intelligence.

NEW QUESTION: 141
A network engineer must provide redundancy between two Cisco FTD devices. The redundancy configuration must include automatic configuration, translation, and connection updates. After the initial configuration of the two appliances, which two steps must be taken to proceed with the redundancy configuration? (Choose two.)
A. Configure the virtual MAC address on the failover link.
B. Disable hellos on the inside interface.
C. Configure the standby IP addresses.

D. Ensure the high availability license is enabled.
E. Configure the failover link with stateful properties.
Answer: (SHOW ANSWER)
Configure the standby IP addresses
Standby IP addresses must be configured on the failover interfaces to enable communication and synchronization between the primary and secondary FTD devices. These IP addresses are used for the failover and stateful failover links that carry the synchronization and state information between the two units.
Configure the failover link with stateful properties
The failover link is a dedicated connection between the two FTD devices that carries failover communication, including unit state, hello messages, MAC address exchange, and configuration synchronization. Configuring the failover link with stateful properties ensures that connection state information is passed to the standby device, allowing active connections to be preserved during failover.
Note: You cannot configure a virtual MAC address for the failover or Stateful Failover links. The MAC and IP addresses for those links do not change during failover.
https://www.cisco.com/c/en/us/td/docs/security/asa/asa72/configuration/guide/conf_gd/failover.ht ml

NEW QUESTION: 142
After using Firepower for some time and learning about how it interacts with the network, an administrator is trying to correlate malicious activity with a user.
Which widget should be configured to provide this visibility on the Cisco Firepower dashboards?
A. Custom Analysis
B. Current Status
C. Current Sessions
D. Correlation Events
Answer: (SHOW ANSWER)
The Correlation Events widget should be configured to provide visibility of malicious activity correlated with a user on the Cisco Firepower dashboards.
https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/management- center/admin/710/management-center-admin-71/events-correlation-compliance.html

NEW QUESTION: 143
An engineer must deploy URL filtering in Cisco Secure Firewall Management Center Version 7.0.
The engineer is configuring the condition for an access control rule to filter URLs that display bad behavior or are malicious or undesirable. Which reputation level URL must be configured?
A. Questionable
B. Untrusted
C. Favorable
D. Neutral
Answer: (SHOW ANSWER)
The Untrusted reputation level identifies URLs exhibiting exceptionally bad, malicious, or undesirable behavior. It represents the lowest URL reputation level and is appropriate when an access control rule must target sites considered highly risky or malicious.

NEW QUESTION: 144
A network engineer is tasked with minimising traffic interruption during peak traffic limes.
When the SNORT inspection engine is overwhelmed, what must be configured to alleviate this issue?
A. Enable IPS inline link state propagation
B. Enable Pre-filter policies before the SNORT engine failure.
C. Set a Trust ALL access control policy.

D. Enable Automatic Application Bypass.
Answer: (SHOW ANSWER)
Automatic Application Bypass (AAB) allows packets to bypass detection if Snort is down or if a packet takes too long to process. AAB causes Snort to restart within ten minutes of the failure, and generates troubleshooting data that can be analyzed to investigate the cause of the Snort failure.
https://www.cisco.com/c/en/us/td/docs/security/firepower/623/configuration/guide/fpmc-config- guide-v623/device_management_basics.html

NEW QUESTION: 145
Which Cisco Secure Firewall feature allows administrators to define traffic that should bypass deep packet inspection to reduce load on the Snort engine?
A. Access Control Policy
B. Prefilter Policy
C. Intrusion Policy
D. Identity Policy
Answer: (SHOW ANSWER)
The Prefilter Policy operates before the Access Control Policy and uses outer packet header data (such as IP and port) to fastpath, block, or send traffic to the Access Control Policy for further inspection. This allows administrators to exclude high-volume, trusted, or encapsulated traffic (like tunneled traffic) from deep inspection, reducing Snort engine load.

NEW QUESTION: 146
An engineer must configure high availability for the Cisco Firepower devices. The current network topology does not allow for two devices to pass traffic concurrently.
How must the devices be implemented in this environment?
A. in active/active mode
B. in cluster interface mode
C. in a cluster span EtherChannel
D. in active/passive mode
Answer: (SHOW ANSWER)

NEW QUESTION: 147
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: A (LEAVE A REPLY)
When configuring a new report template based on a saved search in Cisco Secure Firewall Management Center (FMC), it is important to note that saved searches are specific to the report template they were created with. Saved searches cannot be freely used across different report templates.
To use a different type of saved search, you must ensure that it aligns with the specific report template being used.
This restriction ensures that the saved search parameters match the report's data requirements.

NEW QUESTION: 148
A network engineer is planning on deploying a Cisco Secure Firewall Threat Defense Virtual appliance in transparent mode. Which two virtual environments support this configuration?
(Choose two.)

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

NEW QUESTION: 149
A security engineer is deploying a pair of primary and secondary Cisco FMC devices. The secondary must also receive updates from Cisco Talos. Which action achieves this goal?
A. Force failover for the secondary Cisco FMC to synchronize the rule updates from the primary.
B. Configure the secondary Cisco FMC so that it receives updates from Cisco Talos.
C. Manually import rule updates onto the secondary Cisco FMC device.
D. Configure the primary Cisco FMC so that the rules are updated.
Answer: D (LEAVE A REPLY)
If your deployment includes a high availability pair of Firepower Management Centers, import the update on the primary only. The secondary Firepower Management Center receives the rule update as part of the regular synchronization process.
https://www.cisco.com/c/en/us/td/docs/security/firepower/670/configuration/guide/fpmc-config- guide-v67/system_software_updates.html

NEW QUESTION: 150
A Cisco Secure Firewall Threat Defense device is configured in inline IPS mode to inspect all traffic that passes through the interfaces in the inline set. Which setting in the inline set configuration must be selected to allow traffic to pass through uninterrupted when VDB updates are being applied?
Freecram.net
A. Tap Mode
B. Strict TCP Enforcement
C. Propagate Link State
D. Snort Fail Open
Answer: (SHOW ANSWER)
In inline IPS mode, to ensure that traffic passes through uninterrupted when VDB (Vulnerability Database) updates are being applied, the "Short Fall Open" setting must be configured. This setting allows traffic to continue to flow through the firewall even if there are issues with the inspection process, such as during updates or if the inspection engine fails.
Steps:
In FMC, navigate to the inline set configuration.
Enable the "Short Fall Open" option.
Deploy the configuration to the FTD device.
This ensures that network traffic is not disrupted during updates or other issues with the inspection process.

NEW QUESTION: 151
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. Manually update the SI event entries to that the appropriate traffic is blocked
C. Replace the affected devices with devices that provide more memory

D. Redeploy configurations to affected devices so that additional memory is allocated to the SI module
Answer: (SHOW ANSWER)
Workaround: If you think this is happening, redeploy configurations to the affected devices.
https://www.cisco.com/c/en/us/td/docs/security/firepower/670/configuration/guide/fpmc-config- guide-v67/security_intelligence_blacklisting.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: 152
Which two dynamic routing protocols are supported in FirePower Threat Defense v6.0? (Choose Two)
A. EIGRP
B. OSPF
C. static routing
D. IS-IS
E. BGP
Answer: (SHOW ANSWER)

NEW QUESTION: 153
An engineer is implementing Cisco FTD in the network and is determining which Firepower mode to use. The organization needs to have multiple virtual Firepower devices working separately inside of the FTD appliance to provide traffic segmentation.
Which deployment mode should be configured in the Cisco Firepower Management Console to support these requirements?
A. multiple deployment
B. single-context
C. single deployment
D. multi-instance
Answer: (SHOW ANSWER)
https://www.cisco.com/c/en/us/td/docs/security/firepower/fxos/multi-instance/multi- instance_solution.html#concept_vc4_2lh_3hb

NEW QUESTION: 154
Which group within Cisco does the Threat Response team use for threat analysis and research?
A. Cisco Deep Analytics
B. OpenDNS Group
C. Cisco Network Response
D. Cisco Talos
Answer: D (LEAVE A REPLY)
https://www.cisco.com/c/en/us/products/security/threat-response.html#~benefits

NEW QUESTION: 155

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

NEW QUESTION: 156
A network administrator reviews the attack risk report and notices several low-impact attacks.
What does this type of attack indicate?
A. All attacks are listed as low until manually recategorized.
B. The attacks are not dangerous to the network.
C. The host is not within the administrator's environment.
D. The host is not vulnerable to those attacks.
Answer: (SHOW ANSWER)

NEW QUESTION: 157
Which file format can standard reports from Cisco Secure Firewall Management Center be downloaded in?
A. doc
B. ppt
C. csv
D. xls
Answer: (SHOW ANSWER)
Standard reports from Cisco Secure Firewall Management Center can be downloaded in CSV (Comma-Separated Values) format. This format is widely used for data exchange and can be opened in various applications such as Microsoft Excel.
Steps to download reports:
Navigate to Reports > Report Designer in the FMC.
Select or create the report you wish to download.
Choose the CSV format option when exporting the report. This allows the network engineer to analyze and manipulate the report data easily.

NEW QUESTION: 158
When packet capture is used on a Cisco Secure Firewall Threat Defense device and the packet flow is waiting on the malware query, which Snort verdict appears?
A. block
B. retry
C. replace
D. blockflow
Answer: B (LEAVE A REPLY)

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

NEW QUESTION: 159
An engineer has been tasked with performing an audit of network objects to determine which objects are duplicated across the various firewall models (Cisco Secure Firewall Threat Defense, Cisco Secure Firewall ASA, and Meraki MX Series) deployed throughout the company. Which tool will assist the engineer in performing that audit?
A. Cisco Firepower Device Manager
B. Cisco Defense Orchestrator
C. Cisco Secure Firewall Management Center
D. Cisco SecureX
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.

NEW QUESTION: 160
An engineer must integrate Cisco Secure Endpoint with Cisco Secure Firewall Management Center. The company deploys Secure Endpoint to the public cloud and plans to use the same public cloud provider for Cisco Secure Firewall Malware Defense. What must the engineer configure to meet these requirements?
Freecram.net
A. file and malware policy
B. Secure Endpoint for Secure Firewall
C. proxy for Secure Firewall connection
D. SSL encryption certificate
Answer: (SHOW ANSWER)
To integrate Cisco Secure Endpoint with Cisco Secure Firewall Management Center and leverage public cloud-based Secure Firewall Malware Defense, the engineer must configure "Secure Endpoint for Secure Firewall". This establishes the connection between FMC and Secure Endpoint for sharing malware event data.

NEW QUESTION: 161
Refer to the exhibit. An engineer must import three network objects into the Cisco Secure Firewall Management Center by using a CSV file. Which header must be configured in the CSV file to accomplish the task?

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

A. NAME;DESCRIPTION;TYPE;VALUE;LOOKUP;
B. Name;Description;Type;Value;Lookup;

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

NEW QUESTION: 162
A security engineer is adding three Cisco FTD devices to a Cisco FMC. Two of the devices have successfully registered to the Cisco FMC. The device that is unable to register is located behind a router that translates all outbound traffic to the router's WAN IP address. Which two steps are required for this device to register to the Cisco FMC? (Choose two.)
A. Add the port number being used for PAT on the router to the device's IP address in the Cisco FMC.
B. Configure a NAT ID on both the Cisco FMC and the device.
C. Reconfigure the Cisco FMC to use the device's hostname instead of IP address.
D. Remove the IP address defined for the device in the Cisco FMC.
E. Reconfigure the Cisco FMC lo use the device's private IP address instead of the WAN address.
Answer: (SHOW ANSWER)

NEW QUESTION: 163
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?

EVASIVE APPLICATIONS

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

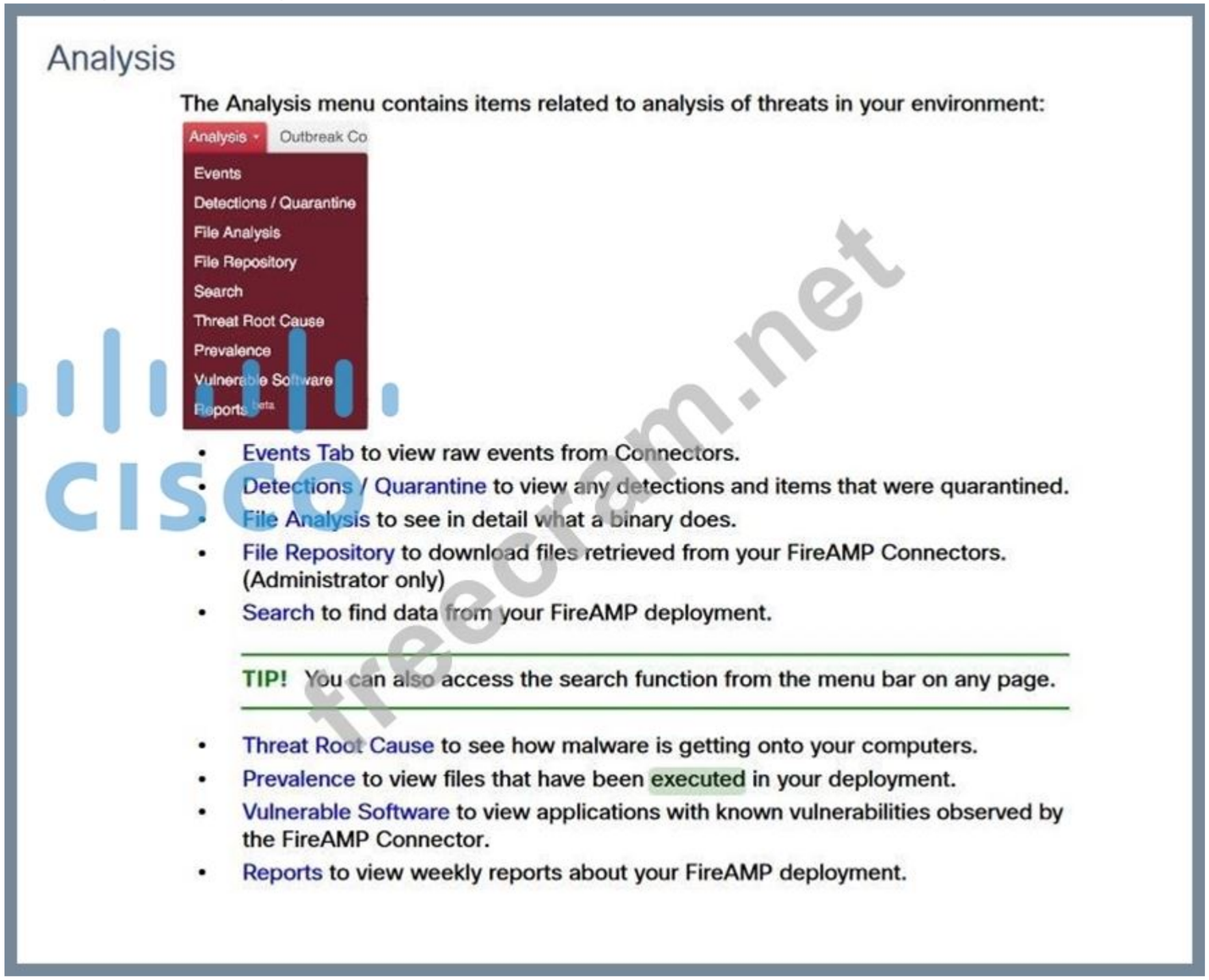
APPLICATION	TIMES ACCESSED	APPLICATION RISK	PRODUCTIVITY RATING	DATA TRANSFERRED (MB)
SSL client	60,712	Medium	Medium	8,510.48

freeCram.net

A. Use SSL decryption to analyze the packets.
B. Use encrypted traffic analytics to detect attacks
C. Use Cisco AMP for Endpoints to block all SSL connection

D. Use Cisco Tetration to track SSL connections to servers.
Answer: (SHOW ANSWER)
https://www.cisco.com/c/en/us/td/docs/security/firepower/623/fdm/fptd-fdm-config-guide-623/fptd-fdm-ssl-decryption.html

NEW QUESTION: 164
With Cisco AMP for Endpoints, which option shows a list of all files that have been executed in your environment?
A. vulnerable software
B. file analysis
C. detections
D. prevalence
E. threat root cause
Answer: (SHOW ANSWER)



NEW QUESTION: 165
Which description of a correlation, policy configuration in the Cisco Firepower Management Center, is true?
A. Deleting a response group deletes the responses of that group.
B. The system displays correlation policies that are created on all of the domains in a multidomain deployment.
C. Correlation policy priorities override whitelist priorities.
D. You cannot add a host profile qualification to a correlation rule that is triggered by a malware event.
Answer: (SHOW ANSWER)

NEW QUESTION: 166
Which object type supports object overrides?
A. time range
B. security group tag
C. network object
D. DNS server group
Answer: C (LEAVE A REPLY)
Object Overrides supported are:
Network
Port
VLAN tag
URL
https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config- guide-v60/Reusable_Objects.html#concept_8BFE8B9A83D742D9B647A74F7AD50053

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 license type is required on Cisco ISE to integrate with Cisco FMC pxGrid?
A. mobility
B. plus
C. base
D. apex
Answer: (SHOW ANSWER)
The Cisco Identity Services Engine (ISE) uses the Platform Exchange Grid (pxGrid) to integrate with other security products, such as the Cisco Firepower Management Center (FMC). To use pxGrid, a Plus license is required on Cisco ISE. The Plus license provides advanced network access control and security features, including integration with third-party products via pxGrid.
https://www.cisco.com/c/en/us/products/collateral/security/identity-services-engine/ise-licensing-guide-og.html#3CiscoISELicenses

NEW QUESTION: 168

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

NEW QUESTION: 169
An organization is implementing Cisco FTD using transparent mode in the network. Which rule in the default Access Control Policy ensures that this deployment does not create a loop in the network?
A. ARP inspection is enabled by default.
B. Multicast and broadcast packets are denied by default.
C. STP BPDU packets are allowed by default.
D. ARP packets are allowed by default.
Answer: (SHOW ANSWER)
https://www.cisco.com/c/en/us/td/docs/security/firepower/630/configuration/guide/fpmc-config- guide-v63/transparent_or_routed_firewall_mode_for_firepower_threat_defense.html

NEW QUESTION: 170
An analyst is investigating a potentially compromised endpoint within the network and pulls a host report for the endpoint in question to collect metrics and documentation. What information should be taken from this report for the investigation?
Freecram.net
A. client applications by user, web applications, and user connections
B. number of attacked machines, sources of the attack, and traffic patterns
C. threat detections over time and application protocols transferring malware
D. intrusion events, host connections, and user sessions
Answer: (SHOW ANSWER)
The Firepower System correlates various types of data (intrusion events, Security Intelligence, connection events, and file or malware events) to determine whether a host on your monitored network is likely to be compromised by malicious means. Certain combinations and frequencies of event data trigger indications of compromise (IOC) tags on affected hosts.
https://www.cisco.com/c/en/us/td/docs/security/firepower/640/configuration/guide/fpmc-config-guide-v64/using_host_profiles.html#ID-2218-000003be

NEW QUESTION: 171
An engineer must deny ICMP traffic to the networks of separate departments that use Cisco Secure Firewall Management Center. The engineer must use the same object on the relevant device for each network. What must be configured in Secure Firewall Management Center?
A. Allow Overrides check box
B. IP address
C. Deny ICMP check box
D. IP range
Answer: (SHOW ANSWER)
In Cisco Secure Firewall Management Center (FMC), if an engineer needs to apply the same object across multiple devices or networks but may want to configure specific settings for each device or network, they can use the "Allow Overrides" option. When the Allow Overrides checkbox is selected, it enables flexibility by allowing the object to have different configurations or values on different devices while still being centrally managed. This is useful when a single object is applied across multiple networks, as it lets the engineer tailor the settings for each department while maintaining consistency in object management.

NEW QUESTION: 172
An engineer is configuring a Cisco Secure Firewall Threat Defense device to operate in transparent mode between two switch stacks. VLAN 10 is used for in-band management on both switch stacks.
Which two actions are required on the device to inspect traffic between the two switch stacks without causing any interruption to network traffic? (Choose two.)
A. Set the MTU to 9198 on all interfaces to support jumbo frames.
B. Add separate routes for data and management traffic.
C. Exempt BPDUs from advanced inspection
D. Configure a BVI interface for VLAN 10.
E. Configure at least one bridge group.
Answer: (SHOW ANSWER)
In transparent mode, a Cisco Secure Firewall Threat Defense (FTD) device must be configured with:
- A Bridge Virtual Interface (BVI) for management access (e.g., VLAN 10) since it does not participate in IP routing.
- At least one bridge group to enable traffic forwarding between interfaces (i.e., the switch stacks), as transparent mode uses bridging at Layer 2 to inspect traffic.
These two actions allow the device to inspect traffic without disrupting the Layer 2 forwarding behavior of the existing network.

NEW QUESTION: 173
An engineer is creating an URL object on Cisco FMC How must it be configured so that the object will match for HTTPS traffic in an access control policy?
A. Specify the protocol to match (HTTP or HTTPS).
B. Use the FQDN including the subdomain for the website
C. Define the path to the individual webpage that uses HTTPS.
D. Use the subject common name from the website certificate
Answer: (SHOW ANSWER)
The subject common name from the website certificate is used to match HTTPS traffic without performing SSL inspection. This allows the system to identify and match the URLs without decrypting the traffic, hence avoiding SSL inspection.

NEW QUESTION: 174
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: C (LEAVE A REPLY)
https://www.ciscolive.com/c/dam/r/ciscolive/emea/docs/2019/pdf/BRKSEC-3455.pdf

NEW QUESTION: 175
An engineer is configuring a Cisco FTD device to place on the Finance VLAN to provide additional protection for company financial data. The device must be deployed without requiring any changes on the end user workstations, which currently use DHCP to obtain an IP address.
How must the engineer deploy the device to meet this requirement?
A. Deploy the device in transparent mode and enable the DHCP Server feature.
B. Deploy the device in routed mode and enable the DHCP Relay feature.

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

NEW QUESTION: 176
A network engineer must monitor threat events from the console of Cisco Secure Firewall Management Center. The engineer integrates the Cisco Secure Firewall Malware Defense in Secure Firewall Management Center. Which action must the engineer take next?
A. Add a Secure Firewall Malware Defense cloud connection in Secure FMC, select the Secure Firewall Malware Defense cloud for Secure Endpoint, log in to Secure Endpoint, and click Allow to authorize the Secure Firewall Malware Defense to Secure FMC connection
B. Add a Secure Firewall Malware Defense cloud connection in Secure FMC, log in to Secure Endpoint, and click Allow to authorize the Secure Firewall Malware Defense to Secure FMC connection
C. Log in to Cisco Secure Endpoint, click Allow to authorize the Secure Firewall Malware Defense to Secure FMC connection, and add a Secure Firewall Malware Defense cloud connection to Secure FMC
D. Log in to Secure Endpoint, click Allow to authorize the Secure Firewall Malware Defense to Secure FMC connection, add a Secure Firewall Malware Defense cloud connection to Secure FMC, and select the Secure Firewall Malware Defense cloud for Secure Endpoint.
Answer: (SHOW ANSWER)
After integrating Cisco Secure Firewall Malware Defense with Secure Firewall Management Center (FMC), the next required step is to add the Malware Defense cloud connection in FMC.
Then, from Secure Endpoint, the engineer must authorize the connection by clicking Allow.
This two-step process ensures proper synchronization and visibility of threat events in FMC.

NEW QUESTION: 177
An organization is migrating their Cisco ASA devices running in multicontext mode to Cisco FTD devices.
Which action must be taken to ensure that each context on the Cisco ASA is logically separated in the Cisco FTD devices?
A. Add a native instance to distribute traffic to each Cisco FTD context.
B. Add the Cisco FTD device to the Cisco ASA port channels.
C. Configure a container instance in the Cisco FTD for each context in the Cisco ASA.
D. Configure the Cisco FTD to use port channels spanning multiple networks.
Answer: C (LEAVE A REPLY)
On Cisco ASA, multi-context mode allows a single physical device to run multiple virtual firewalls, called "contexts," each with separate configurations and policies. The equivalent solution in Cisco FTD is the multi-instance (container instance) feature. This allows you to carve up the physical appliance into multiple FTD instances (or containers), each operating as an independent firewall with its own dedicated interfaces, resource allocation, and policy sets.
Each migrated ASA context maps to a separate FTD container instance to maintain isolation and separation of security policies and network segmentation. This setup ensures each virtual firewall from ASA becomes its own logically isolated FTD instance after migration.
https://community.cisco.com/t5/security-blogs/migrating-asa-multi-context-to-ftd-multi- instance/ba-p/3893465

NEW QUESTION: 178
An engineer must configure an ERSPAN passive interface on a Cisco Secure IPS by using the Cisco Secure Firewall Management Center. These configurations have been performed already:
- Configure the passive interface.
- Configure the ERSPAN IP address.

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

A. Destination MAC

B. TCP Intercept

C. Bypass Mode

D. Flow Id

E. Source IP

Answer: (SHOW ANSWER)

To complete the configuration of an ERSPAN passive interface on a Cisco Secure IPS using Cisco Secure Firewall Management Center, the following additional settings are required:

- Destination MAC: Needed to identify the intended recipient of the ERSPAN traffic.
- Flow ID: Uniquely identifies the ERSPAN session, which is essential for processing mirrored traffic correctly.

NEW QUESTION: 179

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. routed

B. Inline tap

C. transparent

D. passive

Answer: (SHOW ANSWER)

NEW QUESTION: 180

Network users are experiencing intermittent issues with internet access. An engineer identified that the issue is being caused by NAT exhaustion. How must the engineer change the dynamic NAT configuration to provide internet access for more users without running out of resources?

Freecram.net

A. Convert the dynamic auto NAT rule to dynamic manual NAT.

B. Add an identity NAT rule to handle the overflow of users.

C. Define an additional static NAT for the network object in use.

D. Configure fallthrough to interface PAT on the Advanced tab.

Answer: D (LEAVE A REPLY)

NEW QUESTION: 181

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

A. Triage

B. Quarantine

C. Protect

D. Audit

Answer: (SHOW ANSWER)

An Audit policy only monitors and logs endpoint behavior without any enforcement actions, no file isolation and no network-connection blocking, making it ideal for testing.

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: 182
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. Configure multiple BVIs to route between segments.
B. Assign unique VLAN IDs to each firewall interface.
C. Remove the existing dynamic routing protocol settings.
D. Implement non-overlapping IP subnets on each segment.
Answer: (SHOW ANSWER)

NEW QUESTION: 183
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. Standard Report
C. SNMP Report
D. Risk Report
Answer: (SHOW ANSWER)
The Risk Report does provide valuable insights into potential vulnerabilities and threats, which are important for maintaining security. However, for high-level summary statistics specifically related to the performance and uptime of the Cisco FTD appliance, the Standard Report is generally recommended.

NEW QUESTION: 184
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.

NEW QUESTION: 185
A network administrator is concerned about the high number of malware files affecting users' machines. What must be done within the access control policy in Cisco FMC to address this concern?
A. Create an intrusion policy and set the access control policy to block.
B. Create an intrusion policy and set the access control policy to allow.
C. Create a file policy and set the access control policy to allow.
D. Create a file policy and set the access control policy to block.
Answer: (SHOW ANSWER)
Access control rules:
Rule 3: Block evaluates traffic third. Matching traffic is blocked without further inspection. Traffic that does not match continues to the final rule.
Rule 4: Allow is the final rule. For this rule, matching traffic is allowed; however, prohibited files, malware, intrusions, and exploits within that traffic are detected and blocked. Remaining non- prohibited, non-malicious traffic is allowed to its destination, though it is still subject to identity requirements and rate limiting. You can configure Allow rules that perform only file inspection, or only intrusion inspection, or neither.

NEW QUESTION: 186
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)
If you choose disable, you will PERMANENTLY break the high availability connection.
The keyword here is "TEMPORARILY".
https://www.cisco.com/c/en/us/support/docs/security/firepower-management-center/212699-configure-ftd-high-availability-on-firep.html

NEW QUESTION: 187
A security engineer must add a new policy to block UDP traffic to one server. The engineer adds a new object. Which action must the engineer take next to identify all the UDP ports?
A. Specify the transport protocol and leave the port number empty.
B. Define the transport protocol and the mandatory port range.
C. Add the transport number and specify the type and code.
D. Add the corresponding IP protocol number for UDP and TCP.
Answer: (SHOW ANSWER)
When creating an access rule or object to block all UDP traffic to a server, specifying the transport protocol as UDP without defining any specific port number effectively matches all UDP ports. This means the rule will apply to all UDP traffic regardless of port number.

NEW QUESTION: 188
Upon detecting a flagrant threat on an endpoint, which two technologies instruct Cisco Identity Services Engine to contain the infected endpoint either manually or automatically? (Choose two.)
A. Cisco ASA 5500 Series
B. Cisco FMC
C. Cisco AMP
D. Cisco Stealthwatch

E. Cisco ASR 7200 Series

Answer: C,D (LEAVE A REPLY)

Cisco AMP provides endpoint threat detection and can send threat intelligence to Cisco ISE to trigger containment actions such as quarantine or restricted access based on detected malware or compromise.

Cisco Stealthwatch offers network traffic analysis and behavioral detection of threats, which can also integrate with ISE to initiate containment by identifying suspicious or malicious endpoint activity.

https://community.cisco.com/t5/network-access-control/cisco-ise-amp-for-endpoints- integration/td-p/4273949

NEW QUESTION: 189

A network engineer is extending a user segment through an FTD device for traffic inspection without creating another IP subnet.

How is this accomplished on an FTD device in routed mode?

A. by leveraging the ARP to direct traffic through the firewall

B. by assigning an inline set interface

C. by using a BVI and create a BVI IP address in the same subnet as the user segment

D. by bypassing protocol inspection by leveraging pre-filter rules

Answer: (SHOW ANSWER)

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

NEW QUESTION: 190

Which two actions can be used in an access control policy rule? (Choose two.)

A. Block with Reset

B. Monitor

C. Analyze

D. Discover

E. Block ALL

Answer: (SHOW ANSWER)

https://www.cisco.com/c/en/us/td/docs/security/firesight/541/firepower-module-user-guide/asa- firepower-module-user-guide-v541/AC-Rules-Tuning-Overview.html#71854

NEW QUESTION: 191

Which two elements are required to configure Remote Access VPN on Cisco Secure Firewall Threat Defense using FMC? (Choose two.)

A. Connection Profile

B. Group Policy

C. NAT Exemption only

D. Security Intelligence feed

E. Correlation rule

Answer: (SHOW ANSWER)

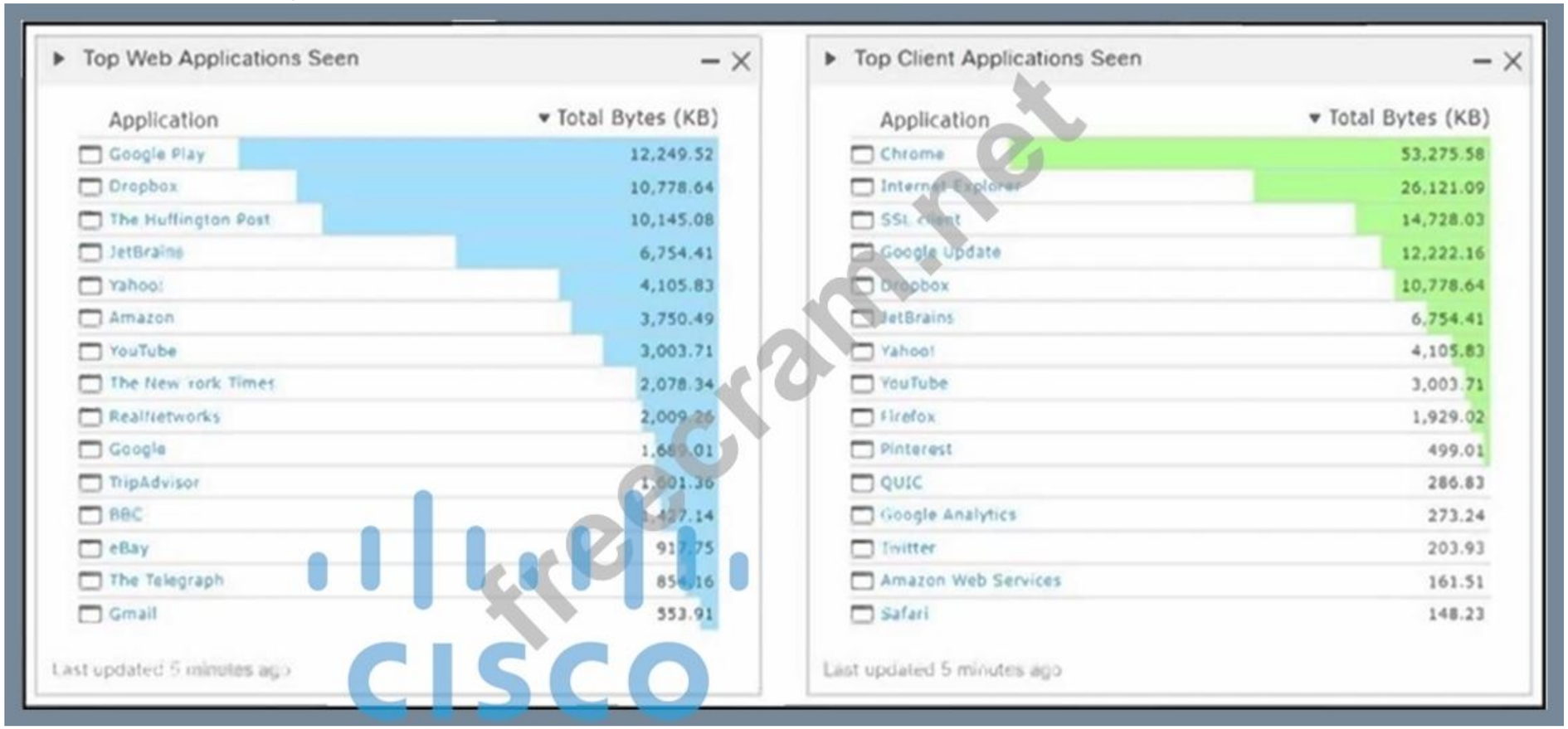
Configuring Remote Access VPN on FTD via FMC requires defining a Connection Profile (which specifies authentication method and address assignment) and a Group Policy (which defines settings such as split tunneling, DNS, and session timers) applied to connecting users.

NEW QUESTION: 192

What is a characteristic of bridge groups on a Cisco FTD?

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

NEW QUESTION: 193
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?





freecram.net

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

NEW QUESTION: 194
A security engineer must configure a Cisco FTD appliance to inspect traffic coming from the internet. The Internet traffic will be mirrored from the Cisco Catalyst 9300 Switch.
Which configuration accomplishes the task?
A. Set the firewall mode to routed.
B. Set interface configuration mode to none.
C. Set interface configuration mode to passive.
D. Set the firewall mode to transparent.
Answer: (SHOW ANSWER)

NEW QUESTION: 195
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. context explorer
B. event viewer
C. dashboards
D. reports
Answer: (SHOW ANSWER)

NEW QUESTION: 196
Cisco Security Analytics and Logging SaaS licenses come with how many days of data retention by default?
A. 60
B. 90
C. 120
D. 365
Answer: (SHOW ANSWER)
Cisco Security Analytics and Logging (SaaS) licenses come with a default data retention period of
90 days. This retention period allows organizations to store and analyze their security event data for up to 90 days, providing sufficient time for security monitoring and forensic investigations.

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: 197
A company is deploying a Cisco Secure IPS device configured in inline mode with a single Interface set that contains four interface pairs. Which two configurations must be implemented to allow the IPS device to uniquely identify packet flows and prevent the reporting of duplicate traffic and false positives? (Choose two.)
A. Set the source SPAN ports to tx only on the switches connected to the IPS interfaces
B. Modify the security zones used by the Cisco Secure IPS device
C. Change the MTU for the inline set to at least 1518
D. Reconfigure access rules to drop all but the first occurrence of the packet
E. Reassign the interface pairs to separate inline sets
Answer: (SHOW ANSWER)
https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-config-guide-v62/ips_device_deployments_and_configuration.pdf

NEW QUESTION: 198
Which two remediation options are available when Cisco FMC is integrated with Cisco ISE?
(Choose two.)
A. dynamic null route configured
B. DHCP pool disablement

C. quarantine
D. port shutdown
E. host shutdown
Answer: (SHOW ANSWER)
Firepower 6.1 Remediation module allows Firepower system to use ISE EPS capabilities (quarantine, unquarantine, port shutdown) as a remediation when correlation rule is matched.
https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/210524-configure-firepower-6-1-pxgrid-remediati.html

NEW QUESTION: 199
Encrypted Visibility Engine (EVE) is enabled under which tab on an access control policy in Cisco Secure Firewall Management Center?
A. Network Analysis Policy
B. SSL
C. Advanced
D. Security Intelligence
Answer: (SHOW ANSWER)
Available under the Advanced tab of the access control policy, to enable or disable EVE.
https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/management- center/snort/720/snort3-configuration-guide-v72/m_encrypted-visibility-engine.pdf

NEW QUESTION: 200
A security engineer needs to configure a network discovery policy on a Cisco FMC appliance and prevent excessive network discovery events from overloading the FMC database? Which action must be taken to accomplish this task?
Freecram.net
A. Exclude load balancers and NAT devices in the policy.
B. Change the network discovery method to TCP/SYN.
C. Configure NetFlow exporters for monitored networks.
D. Monitor only the default IPv4 and IPv6 network ranges.
Answer: (SHOW ANSWER)

NEW QUESTION: 201
An engineer currently has a Cisco FTD device registered to the Cisco FMC and is assigned the address of 10 10.50.12. The organization is upgrading the addressing schemes and there is a requirement to convert the addresses to a format that provides an adequate amount of addresses on the network.
What should the engineer do to ensure that the new addressing takes effect and can be used for the Cisco FTD to Cisco FMC connection?
A. Delete and reregister the device to Cisco FMC
B. Update the IP addresses from IFV4 to IPv6 without deleting the device from Cisco FMC
C. Format and reregister the device to Cisco FMC.
D. Cisco FMC does not support devices that use IPv4 IP addresses.
Answer: (SHOW ANSWER)
If you registered a FMC and a device using IPv4 and want to convert them to IPv6, you must delete and reregister the device.
https://www.cisco.com/c/en/us/td/docs/security/firepower/70/configuration/guide/fpmc-config- guide-v70/device_management_basics.html

NEW QUESTION: 202

An engineer must create an access control policy on a Cisco Secure Firewall Threat Defense device. The company has a contact center that utilizes VoIP heavily, and it is critical that this traffic is not impacted by performance issues after deploying the access control policy. Which access control action rule must be configured to handle the VoIP traffic?

A. block

B. trust

C. monitor

D. allow

Answer: (SHOW ANSWER)

To ensure that VoIP traffic in a contact center is not impacted by performance issues after deploying an access control policy on a Cisco Secure Firewall Threat Defense (FTD) device, the engineer should configure the access control rule with the "trust" action. The "trust" action allows traffic to bypass inspection and policy enforcement, ensuring that critical VoIP traffic is not delayed or degraded.

Steps:

In FMC, navigate to Policies > Access Control > Access Control Policy.

Create a new rule or edit an existing rule.

Set the source and destination for the VoIP traffic.

Set the action to "trust" to ensure the VoIP traffic is not inspected. By configuring the rule with the

"trust" action, the VoIP traffic will be prioritized, maintaining the quality and performance required for the contact center operations.

NEW QUESTION: 203

An engineer must configure a remote access VPN on Cisco Secure Firewall Management Center.

The engineer created a new remote access VPN policy and updated the access control policy deployed on the device. Which additional action must the engineer take to ensure a successful VPN connection?

A. Define NAT for split tunneling

B. Add a mandatory NAT exemption

C. Preconfigure a RADIUS/LDAP server

D. Configure an IP address pool for VPN clients

Answer: D (LEAVE A REPLY)

After creating a remote access VPN policy and updating the access control policy, the engineer must configure an IP address pool that will be assigned to VPN clients. This is essential for clients to receive valid internal IP addresses during connection establishment.

NEW QUESTION: 204

Refer to the exhibit. An engineer is troubleshooting connectivity issues over a VPN tunnel. Users from the 192.168.68.0/24 network report that they cannot connect to a remote web server that has an IP address of 192.168.67.100. The engineer confirms that NAT and access control rules on the local Cisco Secure Firewall Threat Defense Virtual will allow the connection. Which two configuration changes must the engineer make to resolve the connectivity issues? (Choose two.)

```
FMC: System > Monitor > [FTDv] > Advanced Troubleshooting > Threat Defense CLI

Command: show, Parameter: crypto ipsec sa (reduced output)

interface: public
    Crypto map tag: CSM_public_map, seq num: 1, local addr: 209.165.201.5
      access-list CSM_IPSEC_ACL_1 extended permit ip 192.168.68.0 255.255.255.0
      192.168.67.0 255.255.255.0
      local ident (addr/mask/prot/port): (192.168.68.0/255.255.255.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.67.0/255.255.255.0/0/0)
      current_peer: 209.165.201.1
      #pkts encaps: 7719, #pkts encrypt: 7719, #pkts digest: 7719
      #pkts decaps: 4326, #pkts decrypt: 4326, #pkts verify: 4326
      #send errors: 0, #recv errors: 0
      local crypto endpt.: 209.165.201.5/500, remote crypto endpt.:
      209.165.201.1/500
      path mtu 1500, ipsec overhead 58(36), media mtu 1500
      PMTU time remaining (sec): 0, DF policy: copy-df
      ICMP error validation: disabled, TFC packets: disabled
      current outbound spi: EEAB3BDB
      current inbound spi : 4DB7C4CD
    inbound esp sas:
      spi: 0x4DB7C4CD (1303889101)
         SA State: active
         transform: esp-des esp-sha-hmac no compression
         in use settings ={L2L, Tunnel, IKEv2, }
         slot: 0, conn_id: 1, crypto-map: CSM_public_map
         sa timing: remaining key lifetime (kB/sec): (4193072/24908)
    outbound esp sas:
      spi: 0xEEAB3BDB (4004199387)
         SA State: active
         transform: esp-des esp-sha-hmac no compression
         in use settings ={L2L, Tunnel, IKEv2, }
         slot: 0, conn_id: 1, crypto-map: CSM_public_map
         sa timing: remaining key lifetime (kB/sec): (4228990/24908)
```

freecram.net

A. Unblock the remote firewall connection.
B. Set the VPN to support two-way traffic.
C. Bring the VPN tunnel up.
D. Match the crypto access control list.
E. Reconfigure the web server.
Answer: A,D (LEAVE A REPLY)
The tunnel SAs are active, and local NAT/ACLs already allow the traffic. Connectivity failures in this state are typically due to (1) mismatched proxy IDs/crypto ACLs between peers, and/or (2) the remote firewall blocking the return traffic.
Adjust the crypto ACLs so both sides' encryption domains match (192.168.68.0/24 ↔ 192.168.67.0/24) and ensure the remote firewall policy permits the web traffic.

NEW QUESTION: 205
An organization has seen a lot of traffic congestion on their links going out to the internet There is a Cisco Firepower device that processes all of the traffic going to the internet prior to leaving the enterprise. How is the congestion alleviated so that legitimate business traffic reaches the destination?
A. Create a VPN policy so that direct tunnels are established to the business applications
B. Create a NAT policy so that the Cisco Firepower device does not have to translate as many addresses
C. Create a flexconfig policy to use WCCP for application aware bandwidth limiting
D. Create a QoS policy rate-limiting high bandwidth applications
Answer: (SHOW ANSWER)

NEW QUESTION: 206
How should a high-availability pair of Cisco Secure Firewall Threat Defense Virtual appliances be deployed to Cisco Secure Firewall Management Center?
A. Add the primary appliance to Cisco Secure Firewall Management Center first, then configure high availability.
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. Configure high availability first, then add the primary and secondary appliances to Cisco Secure Firewall Management Center.
Answer: (SHOW ANSWER)
For Cisco Secure Firewall Threat Defense Virtual (FTDv) appliances in a high-availability pair, you must first configure high availability directly on the FTD appliances, then register only the primary unit to Cisco Secure Firewall Management Center (FMC). FMC automatically detects and manages the secondary unit as part of the HA pair after the primary is added.

NEW QUESTION: 207
What is the maximum SHA level of filtering that Threat Intelligence Director supports?
A. SHA-1024
B. SHA-4096
C. SHA-512
D. SHA-256
Answer: (SHOW ANSWER)
https://www.cisco.com/c/en/us/td/docs/security/firepower/623/configuration/guide/fpmc-config- guide-v623/cisco_threat_intelligence_directortid_.html

NEW QUESTION: 208
An engineer installs a Cisco FTD device and wants to inspect traffic within the same subnet passing through a firewall and inspect traffic destined to the Internet. Which configuration will meet this requirement?

A. transparent firewall mode with IRB only
B. routed firewall mode with BVI and routed interfaces
C. transparent firewall mode with multiple BVIs
D. routed firewall mode with routed interfaces only
Answer: (SHOW ANSWER)
https://www.cisco.com/c/en/us/td/docs/security/firepower/640/configuration/guide/fpmc-config- guide-v64/transparent_or_routed_firewall_mode_for_firepower_threat_defense.html

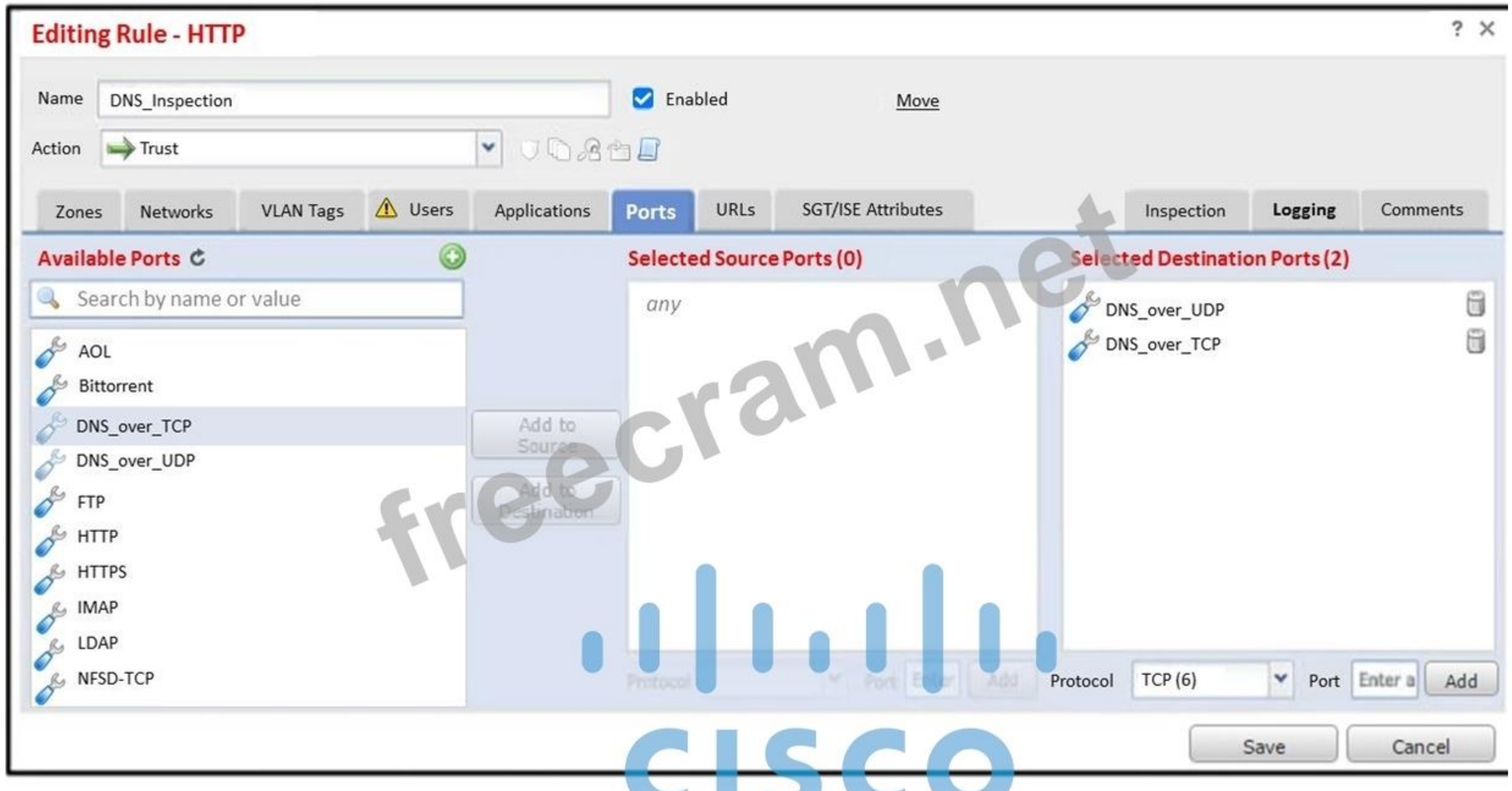
NEW QUESTION: 209
Which command is entered in the Cisco FMC CLI to generate a troubleshooting file?
A. show running-config
B. show tech-support chassis
C. system support diagnostic-cli
D. sudo sf_troubleshoot.pl
Answer: (SHOW ANSWER)
Enter this command on the Firepower Management Center in order to generate a troubleshoot file:
admin@FMC:~$ sudo sf_troubleshoot.pl
https://www.cisco.com/c/en/us/support/docs/security/sourcefire-defense-center/117663-technote- SourceFire-00.html

NEW QUESTION: 210
Which firewall mode must be deployed when implementing IPS to receive and retransmit all traffic unless explicitly dropped that is flowing through a Cisco Secure Firewall Threat Defense interface?
freecram.net
A. passive
B. transparent
C. routed
D. inline
Answer: (SHOW ANSWER)
Inline mode places the Secure Firewall Threat Defense device directly in the traffic path. The device receives packets on one interface and retransmits them through the paired interface unless the configured security policy explicitly drops the traffic.

NEW QUESTION: 211
What is an attribute of the risk reporting capability in Cisco Secure Firewall Management Center?
A. Includes all domains in a multidomain system
B. Uses the same templates available to standard reports
C. Includes the current domain in a multidomain system
D. Uses the XML format to export all reporting
Answer: C (LEAVE A REPLY)
Risk reports in FMC are generated per domain context and only cover the objects and events within the active (current) domain, not the entire multidomain hierarchy.

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: 212
Refer to the exhibit. An engineer is modifying an access control policy to add a rule to inspect all DNS traffic that passes through the firewall. After making the change and deploying the policy, they see that DNS traffic is not being inspected by the Snort engine. What is the problem?



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

Answer: (SHOW ANSWER)

NEW QUESTION: 213
A network engineer must configure an existing firewall to have a NAT configuration. The new configuration must support more than two interfaces per context. The firewall has previously been operating in transparent mode. The Cisco Secure Firewall Threat 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 firewall routed command from the Secure FTD device CLI, and reregister with Secure FMC.
B. Run the configure manager add routed command from the Secure FMC CLI. and reregister with Secure FMC.
C. Run the configure manager add routed command from the Secure FTD device 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 command configure firewall routed to switch the firewall from transparent mode to routed mode.
Reregister the FTD device with the FMC by running the configure 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.

NEW QUESTION: 214
Refer to the exhibit. An organization has an access control rule with the intention of sending all social media traffic for inspection. After using the rule for some time, the administrator notices that the traffic is not being inspected, but is being automatically allowed.
What must be done to address this issue?

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

NEW QUESTION: 215
Which two characteristics represent a Cisco device operating in tap mode? (Choose two.)
A. It analyzes copies of packets from the packet flow
B. The device is deployed in a passive configuration
C. If a rule is triggered the device generates an intrusion event.
D. The packet flow traverses the device
E. If a rule is triggered the device drops the packet
Answer: (SHOW ANSWER)
The two characteristics that represent a Cisco device operating in tap mode are:
A: It analyzes copies of packets from the packet flow.

cisco freecram.net

D: The packet flow traverses the device.
In tap mode, a Cisco device creates a copy of the traffic flowing through it, which can then be analyzed by a monitoring device. The original traffic is not affected, and continues to flow through the network as normal.

NEW QUESTION: 216
Which option is the main function of Cisco Firepower impact flags?
A. They highlight known and suspected malicious IP addresses in reports.
B. They alert administrators when critical events occur.
C. They correlate data about intrusions and vulnerability.
D. They identify data that the ASA sends to the Firepower module.
Answer: (SHOW ANSWER)

NEW QUESTION: 217
Which two deployment types support high availability? (Choose two.)
A. transparent
B. routed
C. clustered
D. intra-chassis multi-instance
E. virtual appliance in public cloud
Answer: (SHOW ANSWER)
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: 218
A network administrator is trying to configure Active Directory authentication for VPN authentication to a Cisco Secure Firewall Threat Defence instance that is registered with Cisco Secure Firewall Management Center. Which system settings must be configured first in Secure Firewall Management Center to accomplish the goal?
A. Device, Remote Access VPN
B. System, Realms
C. Policies, Authentication
D. Authentication, Device
Answer: (SHOW ANSWER)
To configure Active Directory authentication for VPN authentication on a Cisco Secure Firewall Threat Defense (FTD) instance registered with Cisco Secure Firewall Management Center (FMC), the administrator needs to configure Realms in the System settings of the FMC. Realms in FMC are used to define the directory servers (e.g., Active Directory) and how they are used for user authentication.
Steps to configure this in FMC:
Navigate to System > Integration > Realms and Directory.
Add a new realm and configure the necessary details such as the directory server type (e.g., Active Directory), server address, and bind credentials.
Test the connection to ensure it works correctly.
This setup allows the FMC to authenticate VPN users against the Active Directory, thereby enabling secure access control for VPN connections.

NEW QUESTION: 219

An engineer must investigate a connectivity issue from an endpoint behind a Cisco FTD device and a public DNS server. The endpoint cannot perform name resolution queries. Which action must the engineer perform to troubleshoot the issue by simulating real DNS traffic on the Cisco FTD while verifying the Snort verdict?

A. Use the Capture w/Trace wizard in Cisco FMC.

B. Run the system support firewall-engine-debug command from the FTD CLI.

C. Create a Custom Workflow in Cisco FMC.

D. Perform a Snort engine capture using tcpdump from the FTD CLI.

Answer: (SHOW ANSWER)

To trace a real packet is very useful to troubleshoot connectivity issues. It allows you to see all the internal checks that a packet goes through. Add the trace detail keywords and specify the number of packets that you want to be traced. By default, the FTD traces the first 50 ingress packets.

In this case, enable capture with trace detail for the first 100 packets that FTD receives on the INSIDE interface:

> capture CAPI2 interface INSIDE trace detail trace-count 100 match icmp host 192.168.103.1 host 192.168.101.1

NEW QUESTION: 220

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?

prepcram.net

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

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

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

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

Answer: (SHOW ANSWER)

NEW QUESTION: 221

An engineer wants to connect a single IP subnet through a Cisco FTD firewall and enforce policy.

There is a requirement to present the internal IP subnet to the outside as a different IP address.

What must be configured to meet these requirements?

A. Configure the upstream router to perform NAT.

B. Configure the downstream router to perform NAT.

C. Configure the Cisco FTD firewall in transparent mode with NAT enabled.

D. Configure the Cisco FTD firewall in routed mode with NAT enabled.

Answer: (SHOW ANSWER)

NEW QUESTION: 222

When using Cisco AMP for Networks, which feature copies a file to the Cisco AMP cloud for analysis?

A. sandbox analysis

B. malware analysis

C. dynamic analysis

D. Spero analysis

Answer: (SHOW ANSWER)

NEW QUESTION: 223

Which access control policy action must be selected to inspect traffic for malware using cisco AMP for Networks?

A. monitor
B. allow
C. trust
D. inspect
Answer: (SHOW ANSWER)

NEW QUESTION: 224
Which command-line mode is supported from the Cisco Firepower Management Center CLI?
A. privileged
B. user
C. configuration
D. admin
Answer: (SHOW ANSWER)
The CLI encompasses four modes. The default mode, CLI Management, includes commands for navigating within the CLI itself. The remaining modes contain commands addressing three different areas of Firepower Management Center functionality; the commands within these modes begin with the mode name: system, show, or configure.
https://www.cisco.com/c/en/us/td/docs/security/firepower/660/configuration/guide/fpmc-config- guide-v66/command_line_reference.pdf

NEW QUESTION: 225
A network engineer must deploy a Cisco ASA to an existing network without changing any IP addresses or networking settings. The external devices connected to the firewall will be on the same subnet as the internal devices. Which command must the engineer use to meet the requirements?
A. firewall transparent
B. firewall routed
C. mode multiple
D. no firewall transparent
Answer: (SHOW ANSWER)
To deploy a Cisco ASA without changing existing IP addresses or network topology, the firewall must operate in transparent mode. The firewall transparent command enables this mode, allowing the ASA to act as a Layer 2 bridge, where internal and external devices remain on the same subnet while still enforcing security policies.

NEW QUESTION: 226
What is the role of the casebook feature in Cisco Threat Response?
A. sharing threat analysts
B. pulling data via the browser extension
C. triage automaton with alerting
D. alert prioritization
Answer: A (LEAVE A REPLY)
The casebook and pivot menu are widgets available in Cisco Threat Response. Casebook - It is used to record, organize, and share sets of observables of interest primarily during an investigation and threat analysis. You can use a casebook to get the current verdicts or dispositions on the observables.

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: 227
Which Cisco Secure Firewall Management Center dashboard widget provides a summary of the health status of managed devices?
A. Network Discovery Widget
B. Health Monitor Widget
C. Correlation Widget
D. Custom Analysis Widget
Answer: B (LEAVE A REPLY)
The Health Monitor Widget on the FMC dashboard provides administrators with a summary of the operational health status of managed devices, including CPU, memory, disk usage, and interface status, helping to quickly identify issues.

NEW QUESTION: 228
An engineer needs to identify which user is generating a specific type of traffic on the network.
Which Cisco Secure Firewall Management Center feature provides this visibility?
A. Network Discovery Policy
B. Identity Policy with realm integration
C. File Policy
D. Malware and File Policy
Answer: (SHOW ANSWER)
The Identity Policy, when integrated with a realm (such as Active Directory) and identity sources like Cisco ISE or user agent, allows Cisco Secure Firewall Management Center to map network traffic to specific usernames, providing user-based visibility and policy enforcement.

NEW QUESTION: 229
What is a purpose of the network analysis policy on a Cisco Firepower NGIPS?
A. it governs how traffic is preprocessed before inspection
B. it specifies the outer-header criteria used to process traffic without using advanced inspection
C. it examines packets for attacks by using intrusion rules
D. it defines the rules for encrypting traffic
Answer: (SHOW ANSWER)

NEW QUESTION: 230
Which two descriptions of a Cisco Firepower NGIPS deployment that uses an Inline Pair interface in tap mode are true? (Choose two)
Freecram.net
A. The deployment is available in transparent mode only.
B. Wore than two interfaces can be bridged.
C. Transit traffic can be dropped
D. Two physical interfaces are bridged internally.

E. All the Cisco ASA engine features are available
Answer: (SHOW ANSWER)

NEW QUESTION: 231
An engineer must configure a Cisco FMC dashboard in a child domain.
Which action must be taken so that the dashboard is visible to the parent domain?
A. Create a copy of the dashboard.
B. Add a separate widget.
C. Add a separate tab.
D. Adjust policy inheritance settings.
Answer: (SHOW ANSWER)

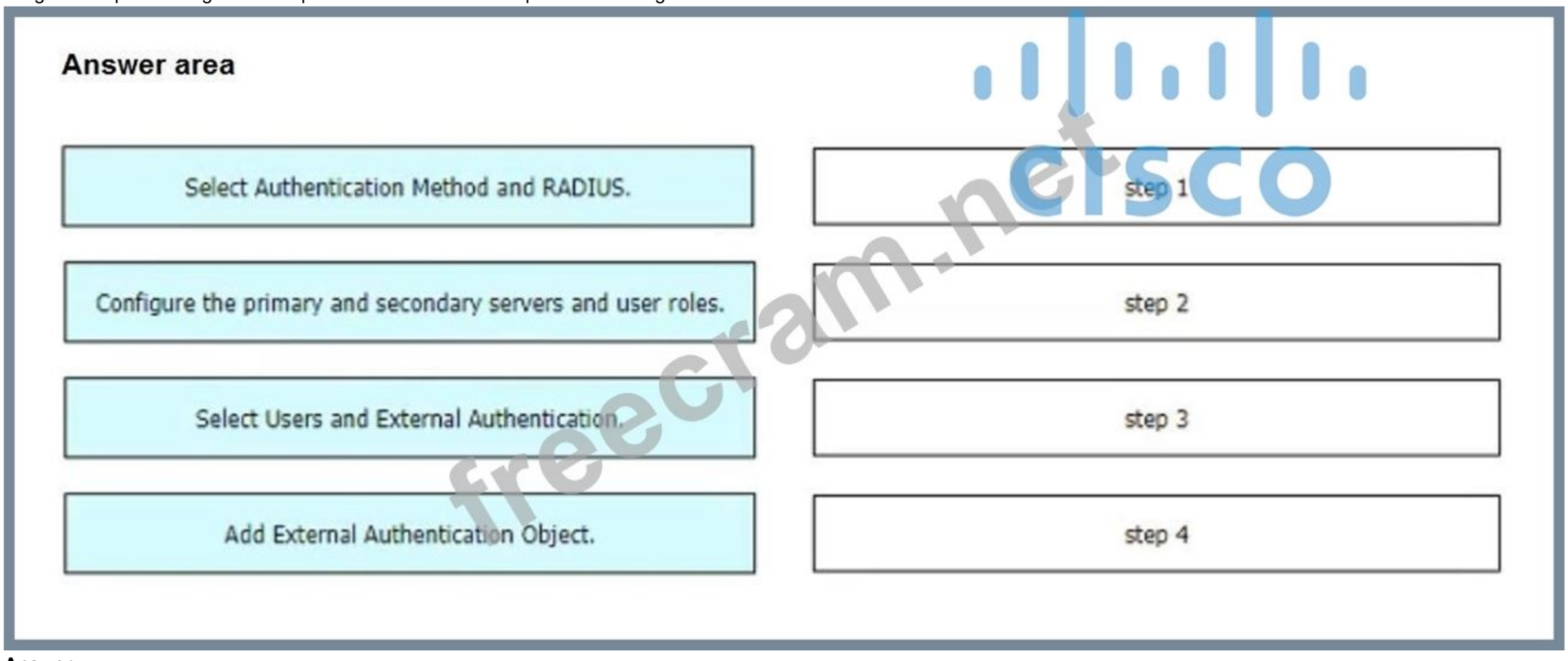
NEW QUESTION: 232
An engineer is monitoring network traffic from their sales and product development departments, which are on two separate networks.
What must be configured in order to maintain data privacy for both departments?
A. Use a dedicated IPS inline set for each department to maintain traffic separation
B. Use 802.1Q mime set Trunk interfaces with VLANs to maintain logical traffic separation
C. Use passive IDS ports for both departments
D. Use one pair of inline set in TAP mode for both departments
Answer: (SHOW ANSWER)
To maintain data privacy between the sales and product development departments, which are on two separate networks, the key requirement is to ensure logical traffic separation so that data from one department cannot be accessed or intercepted by the other.
The best approach is to use VLANs with 802.1Q trunking to maintain logical traffic separation.
VLANs (Virtual Local Area Networks) allow network administrators to segment the network logically by department or function, isolating traffic within each VLAN and preventing unauthorized access between them. This segmentation improves security by containing any potential breaches within a VLAN and ensuring sensitive data remains accessible only to authorized users within that VLAN.
The 802.1Q standard enables VLAN tagging, which inserts a VLAN identifier into Ethernet frames, allowing multiple VLANs to share the same physical network infrastructure (trunk links) without mixing traffic. This tagging ensures that traffic from sales and product development departments remains separate even though it may traverse the same physical switches.

NEW QUESTION: 233
An engineer wants to ensure that if a policy deployment causes issues, the device configuration can be reverted quickly. Which FMC feature should be used?
A. Configuration Import
B. Deployment Rollback
C. High Availability Failover
D. Backup and Restore
Answer: (SHOW ANSWER)
Cisco Secure Firewall Management Center supports Deployment Rollback, which allows an administrator to revert a managed device to its previous deployed configuration if a recent deployment causes unexpected issues.

NEW QUESTION: 234
With Cisco Firepower Threat Defense software, which interface mode must be configured to passively receive traffic that passes through the appliance?
A. inline set

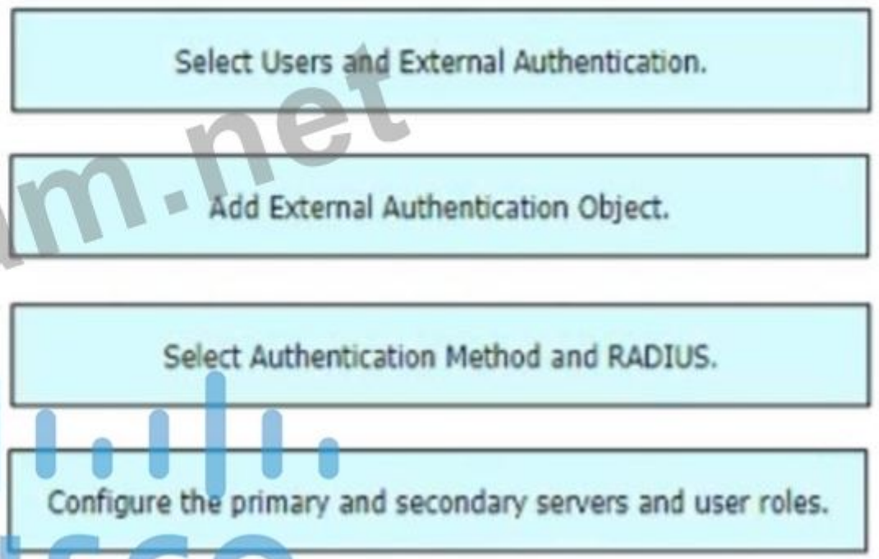
B. passive
C. routed
D. inline tap
Answer: (SHOW ANSWER)
With tap mode, the FTD is deployed inline, but the network traffic flow is undisturbed. Instead, the FTD makes a copy of each packet so that it can analyze the packets. Note that rules of these types do generate intrusion events when they are triggered, and the table view of intrusion events indicates that the triggering packets would have dropped in an inline deployment. There are benefits to using tap mode with FTDs that are deployed inline.

NEW QUESTION: 235
Drag and Drop Question
Drag and drop the configuration steps from the left into the sequence on the right to enable external authentication on Cisco FMC to a RADIUS server.



Answer:

Answer area



freecram.net

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

NEW QUESTION: 236
An engineer must define a URL object on Cisco FMC.
What is the correct method to specify the URL without performing SSL inspection?
A. Use Subject Common Name value.
B. Specify all subdomains in the object group.
C. Specify the protocol in the object.
D. Include all URLs from CRL Distribution Points.
Answer: (SHOW ANSWER)
HTTPS filtering, unlike HTTP filtering, disregards subdomains within the subject common name.
Do not include subdomain information when manually filtering HTTPS URLs.
https://www.cisco.com/c/en/us/td/docs/security/firepower/670/fdm/fptd-fdm-config-guide-670/fptd-fdm-access.html

NEW QUESTION: 237
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 Threat Defense certificate must be added to the LDAPS server
B. LDAPS server certificate must be added to Secure Firewall Management Center realms
C. Secure Firewall Management Center certificate must be added to the LDAPS server

D. LDAPS server certificate must be added to Secure Firewall Threat Defense
Answer: (SHOW ANSWER)
Import the Root CA Certificate that has signed the LDAPS service Certificate on the Windows Server under Objects > PKI > Trusted CAs > Add Trusted CA, as this is referenced under theDirectory Server Configuration of the Realm
https://www.cisco.com/c/en/us/support/docs/security/anyconnect-secure-mobility-client- v4x/220880-configure-password-management-using-ldap.html#toc-hId--2065014694

NEW QUESTION: 238
Which component is needed to perform rapid threat containment with Cisco FMC?
A. ISE
B. RESTful API
C. SIEM
D. DDI
Answer: (SHOW ANSWER)
To perform rapid threat containment with Cisco FMC, the necessary component is Cisco Identity Services Engine (ISE). ISE integrates with FMC to provide dynamic network access control and enforcement, allowing for quick isolation of compromised endpoints based on security events detected by FMC.
Steps:
Integrate FMC with ISE by configuring the necessary settings in both platforms.
Define security policies in FMC that trigger rapid threat containment actions via ISE.
When a threat is detected, FMC can instruct ISE to isolate the affected endpoint, limiting its access to the network.
This integration enables automated and efficient threat containment, reducing the response time and mitigating the impact of security incidents.

NEW QUESTION: 239
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. An high availability license must be added to the Cisco FMC before adding the high availability pair.
B. Both Cisco FTD devices are not at the same software version.
C. The failover link must be defined on each Cisco FTD before adding the high availability pair.
D. The second Cisco FTD is not the same model as the primary Cisco FTD.
Answer: (SHOW ANSWER)

NEW QUESTION: 240
What is the difference between inline and inline tap on Cisco Firepower?
A. Inline tap mode can send a copy of the traffic to another device.
B. Inline tap mode does full packet capture.
C. Inline mode cannot do SSL decryption.
D. Inline mode can drop malicious traffic.
Answer: (SHOW ANSWER)
A threat defense in inline interface mode can block unintended traffic while it remains invisible to the network hosts. Inline mode allows a threat defense to block traffic based on the access control and intrusion rules you enable.

NEW QUESTION: 241

An engineer must deploy a Cisco FTD device. Management wants to examine traffic without requiring network changes that will disrupt end users. Corporate security policy requires the separation of management traffic from data traffic and the use of SSH over Telnet for remote administration. How must the device be deployed to meet these requirements?

A. in routed mode with a diagnostic interface

B. in routed mode with a bridge virtual interface

C. in transparent made with a data interface

D. in transparent mode with a management Interface

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**)

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**)