Free Questions for 300-710 by certscare

Shared by Lucas on 22-07-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

What is the role of realms in the Cisco ISE and Cisco FMC integration?

Options:

A- AD definition

B- TACACS+ database

C- Cisco ISE context

D- Cisco Secure Firewall VDC

Answer:

A

Explanation:

In the integration between Cisco Identity Services Engine (ISE) and Cisco Firewall Management Center (FMC), realms are used to define the Active Directory (AD) configuration. Realms in FMC specify the AD servers, domain, and other authentication settings

necessary to authenticate and authorize users.

Steps to configure realms:

In FMC, navigate to System > Integration > Realms and Directory.

Add a new realm and configure the AD settings.

Ensure the realm settings match the AD environment for seamless integration.

Realms are essential for integrating AD with FMC, allowing the firewall to use AD for user authentication and policy enforcement.

Question 2

Question Type: MultipleChoice

An administrator must fix a network problem whereby traffic from the inside network to a webserver is not getting through an instance of Cisco Secure Firewall Threat Defense. Which command must the administrator use to capture packets to the webserver that are dropped by Secure Firewall Throat Defense and resold the issue?

Options:

A- capture CAP int OUTSIDE match ip any host WEBSERVERIP

B- capture CAP type asp-drop all headers-only

C- capture CAP int INSIDE match ip any host WEBSERVERIP

D- capture CAP int INSIDE match tcp any 80 host WEBSERVERlP 80

Answer:

B

Explanation:

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.

Question 3

Question Type: MultipleChoice

Which action must be taken to configure an isolated bridge group for IRB mode on a Cisco Secure Firewall device?

Options:

A- Add the restricted segment to the ACL.

B- Leave BVI interface name empty.

C- Define the NAT pool for the blocked traffic.

D- Remove the route from the routing table.

Answer:

B

Explanation:

To configure an isolated bridge group for Integrated Routing and Bridging (IRB) mode on a Cisco Secure Firewall device, the action to take is to leave the BVI (Bridge Virtual Interface) interface name empty. This ensures that the bridge group operates in an isolated manner, where Layer 3 routing is not applied to the bridged interfaces, effectively isolating the traffic within the bridge group.

Steps:

Access the firewall's configuration interface.

Configure the bridge group interfaces.

Ensure that the BVI interface name is left empty to isolate the bridge group.

This configuration prevents Layer 3 routing for the isolated bridge group, ensuring that traffic remains contained within the bridge group.

Question 4

Question Type: MultipleChoice

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 .... by performance issues after deploying the access control policy Which access control Action rule must be configured to handle the VoIP traffic?

Options:

A- monitor

B- trust

C- block

D- allow

Answer:

B

Explanation:

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.

Question 5

Question Type: **MultipleChoice**

An engineer is troubleshooting an intermittent connectivity issue on a Cisco Secure Firewall Threat Defense appliance and must collect 24 hours' worth of dat

a. The engineer started a packet capture. Whenever it stops prematurely during this time period. The engineer notices that the packet capture butter size is set to the default of 32 MB Which butter S170 is the maximum that the engineer must sot to able the packet capture to run successfully?

Options:

A- 64 MB

B- 1 GB

C- 10 GB

D- 100 GB

Answer:

B

Explanation:

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

Steps:

Access the packet capture configuration on the FTD device.

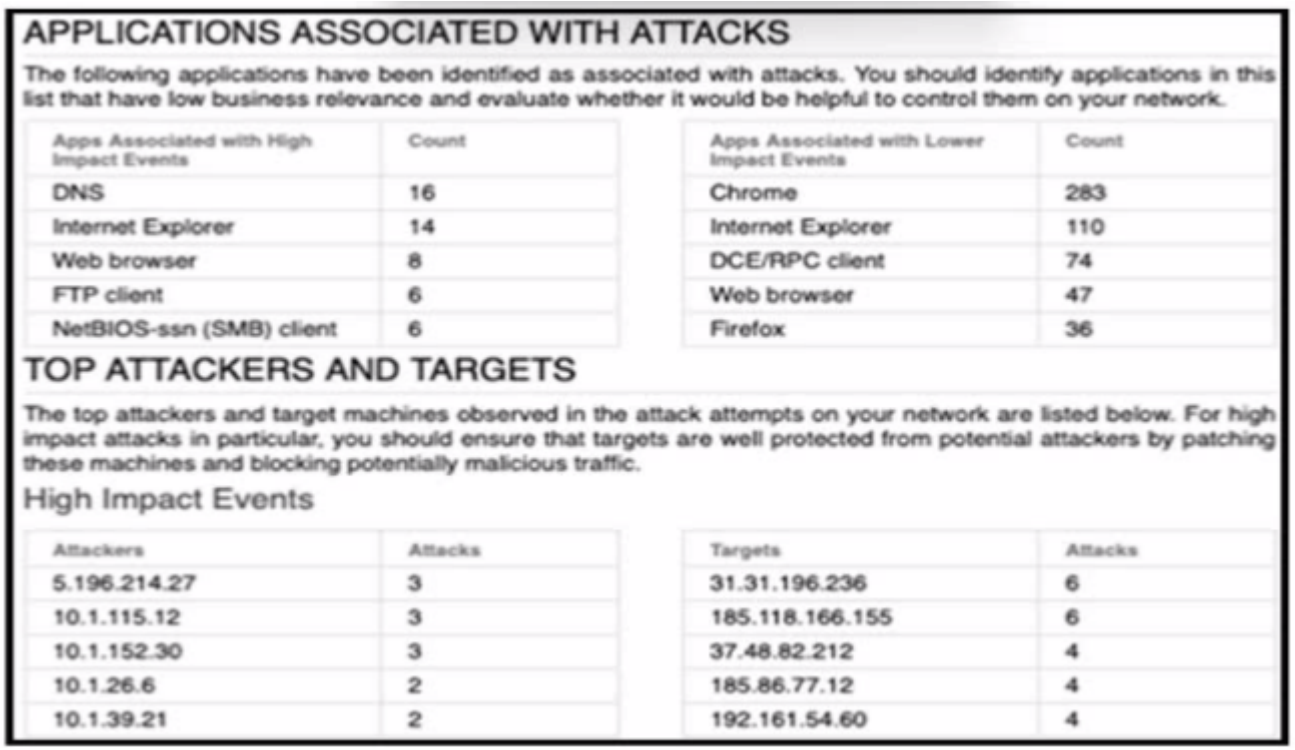
Increase the buffer size to 1 GB, which provides a significantly larger capacity for capturing packets over a 24-hour period.

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

Question 6

Question Type: MultipleChoice

Refer to the Exhibit.



APPLICATIONS ASSOCIATED WITH ATTACKS

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

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

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

TOP ATTACKERS AND TARGETS

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

High Impact Events

Attackers	Attacks
5.196.214.27	3
10.1.115.12	3
10.1.152.30	3
10.1.26.6	2
10.1.39.21	2

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

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

Options:

A- Inspect DNS traffic

B- Block NetBIOS.

C- Block Internal Explorer

D- Inspect TCP port 80 traffic

Answer:

A

Explanation:

Based on the Attacks Risk Report, DNS is associated with a high number of impact events (16). DNS traffic is critical for network operations but can also be exploited for malicious activities such as DNS tunneling, DDoS attacks, and data exfiltration. To improve security, the security engineer should focus on inspecting DNS traffic. This involves deploying DNS security solutions and monitoring DNS traffic for anomalies to detect and mitigate potential threats.

Steps:

Implement DNS security tools such as DNS filtering, DNSSEC, and DNS anomaly detection.

Configure the firewall to inspect DNS traffic for malicious activities.

Regularly analyze DNS logs to identify and respond to threats.

This action addresses a significant risk identified in the report and helps to mitigate potential attacks exploiting DNS.

Question 7

Question Type: MultipleChoice

An engineer is configuring a Cisco Secure Firewall Threat Defense device and warns 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?

Options:

A- metadata

B- content

C- reference

D- gtp_info

Answer:

A

Explanation:

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.

Question 8

Question Type: MultipleChoice

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

Options:

A- Both users can edit the policy arid the last saved configuration persists.

B- The first user locks the configuration when selecting edit on the policy.

C- The changes from both users will be merged together into the policy.

D- The system prevents modifications to the policy by multiple users.

Answer:

B

Explanation:

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

Steps:

When the first user selects edit on the VPN policy, FMC locks the policy for editing.

The lock ensures that only the first user can make changes.

Once the first user saves or cancels their changes, the lock is released.

Other users can then edit the policy.

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

Question 9

Question Type: MultipleChoice

An organization created a custom application that is being flagged by Cisco Secure Endpoint. The application must be exempt from being flagged. What is the process to meet the requirement?

Options:

A- Modify the custom detection list to exclude me custom application.

B- Preculculate the hash value of the custom application and add it to the allowed applications.

C- Configure the custom application to use the information-store paths.

D- Add the custom application to the DFC 1st and update the policy.

Answer:

B

Explanation:

To exempt a custom application from being flagged by Cisco Secure Endpoint, the organization must precalculate the hash value of the custom application and add it to the allowed applications list. This process involves creating a hash of the executable file, which uniquely identifies it, and then configuring Cisco Secure Endpoint to recognize this hash as trusted.

Steps:

Calculate the hash value (e.g., SHA-256) of the custom application executable.

In the Cisco Secure Endpoint management console, navigate to the policy configuration.

Add the calculated hash value to the list of allowed applications or exclusions.

Save and deploy the updated policy.

By adding the hash value to the allowed applications, Cisco Secure Endpoint will recognize the custom application as trusted and will no longer flag it.

Question 10

Question Type: MultipleChoice

A network administrator is deploying a new Cisco Secure Firewall Threat Defense (FTD) firewall After Cisco Secure FTD is deployed, inside clients nave intermittent connectivity to each other. When ... the packet capture on the Secure FTD firewall, the administrator sees that Secure FID is responding to all the AW requests on the inside network. Which action must the network administrator e to resolve the issue"

Options:

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

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

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

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

Answer:

A

Explanation:

If inside clients have intermittent connectivity issues and the Cisco Secure FTD is responding to all ARP requests on the inside network, it indicates that there may be an incorrect proxy ARP configuration in the NAT policy. Proxy ARP can cause the FTD to respond to ARP requests on behalf of other devices, leading to connectivity issues.

Steps to resolve:

Review the NAT policy on the FTD to identify any incorrect proxy ARP configurations.

Disable the proxy ARP setting for the relevant NAT rules that are causing the issue.

This ensures that the FTD only responds to ARP requests as needed, preventing it from interfering with normal ARP traffic on the inside network.

Question 11

Question Type: **MultipleChoice**

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

Options:

A- manage_procs.pl

B- sudo stats_unified.pl

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

D- show history

E- show disk-manager

Answer:

A, B

Explanation:

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.

Question 12

Question Type: **MultipleChoice**

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

Options:

A- EtherChannel interfaces

B- Route Tracking

C- SLA Monitor

D- Redundant interfaces

E- BGP

Answer:

B, C

Explanation:

To ensure high availability of internet access when deploying a pair of Cisco Secure Firewall Threat Defense (FTD) devices managed by Cisco Secure Firewall Management Center (FMC), the following features must be deployed:

Route Tracking: This feature monitors the reachability of a specified target (such as an external IP address) through the configured routes. If the route to the target is lost, the FTD can dynamically adjust the routing to use an alternate path, ensuring continuous internet access.

SLA Monitor: Service Level Agreement (SLA) monitoring works alongside route tracking to continuously verify the status and performance of the internet links. If the SLA for one of the ISP links fails (indicating the link is down or underperforming), the FTD can switch traffic to the secondary ISP link.

Steps to configure:

In FMC, navigate to Devices > Device Management.

Select the FTD device and configure route tracking to monitor the ISP links.

Configure SLA monitors to continuously check the health and performance of the internet circuits.

These configurations ensure that internet access remains available to users even if one of the ISPs goes down.