Free Questions for 300-710 by braindumpscollection

Shared by Jacobson on 12-12-2023

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

A network administrator reviews me attack risk report and notices several Low-Impact attacks. What does this type of attack indicate?

Options:

A- All attacks are listed as low until manually categorized.

B- The host is not vulnerable to those attacks.

C- The attacks are not dangerous to the network.

D- The host is not within the administrator's environment.

Answer:

B

Explanation:

A low-impact attack indicates that the host is not vulnerable to those attacks.A low-impact attack is an attack that does not exploit any known vulnerability on the target host or does not match any signature or anomaly rule on the FTD device5. A low-impact attack does

not mean that the attack is not dangerous to the network or that the host is not within the administrator's environment. It simply means that the attack did not succeed in compromising or affecting the host.

The other options are incorrect because:

All attacks are not listed as low until manually categorized.The FTD device automatically assigns an impact level to each attack based on various factors, such as vulnerability information, threat score, and confidence rating5. The impact level can be high, medium, or low, depending on how likely and how severe the attack is.

The attacks are not necessarily harmless to the network.A low-impact attack may still cause some damage or disruption to the network, such as consuming bandwidth, generating noise, or distracting attention from other attacks6.A low-impact attack may also indicate that the attacker is probing or scanning the network for potential vulnerabilities or weaknesses7.

The host is not necessarily outside the administrator's environment. A low-impact attack can target any host on the network, regardless of its location or ownership. A low-impact attack does not imply that the host is external or irrelevant to the administrator's environment.

Question 2

Question Type: **MultipleChoice**

An engineer plans to reconfigure an existing Cisco FTD from transparent mode to routed mode. Which additional action must be taken to maintain communication Between me two network segments?

Options:

A- Configure a NAT rule so mat traffic between the segments is exempt from NAT.

B- Update the IP addressing so that each segment is a unique IP subnet.

C- Deploy inbound ACLs on each interface to allow traffic between the segments.

D- Assign a unique VLAN ID for the interface in each segment.

Answer:

B

Explanation:

When reconfiguring an existing Cisco FTD from transparent mode to routed mode, an additional action that must be taken to maintain communication between the two network segments is to update the IP addressing so that each segment is a unique IP subnet. This is because in routed mode, the FTD device acts as a router hop in the network and requires each interface to be on a different subnet.In transparent mode, the FTD device acts as a layer 2 firewall and does not require different subnets for each interface1.

The other options are incorrect because:

Configuring a NAT rule so that traffic between the segments is exempt from NAT is not necessary to maintain communication between the two network segments. NAT is used to translate IP addresses between different networks, but it does not affect the routing of packets.Moreover, NAT is optional in routed mode and can be disabled if not needed2.

Deploying inbound ACLs on each interface to allow traffic between the segments is not required to maintain communication between the two network segments. ACLs are used to control access to network resources based on source and destination addresses, protocols, and ports. They do not affect the routing of packets.Furthermore, ACLs are optional in routed mode and can be configured as needed3.

Assigning a unique VLAN ID for the interface in each segment is not relevant to maintain communication between the two network segments. VLANs are used to create logical groups of hosts that share the same broadcast domain, regardless of their physical location or connection. They do not affect the routing of packets.Besides, VLANs are not supported in routed mode and can only be used in transparent mode4.

Question 3

Question Type: MultipleChoice

A consultant Is working on a project where the customer is upgrading from a single Cisco Firepower 2130 managed by FDM to a pair of Cisco Firepower 2130s managed oy FMC tor nigh availability. The customer wants the configures of the existing device being managed by FDM to be carried over to FMC and then replicated to the additional: device being added to create the high availability pair. Which action must the consultant take to meet this requirement?

Options:

A- The current FDM configuration must be configured by hand into FMC before the devices are registered.

B- The current FDM configuration will be converted automatically into FMC when the device registers.

C- The current FDM configuration must be migrated to FMC using the Secure Firewall Migration Tool.

D- The FTD configuration must be converted to ASA command format, which can then be migrated to FMC.

Answer:

B

Explanation:

When an FTD device that is managed by FDM is registered to FMC, the existing configuration is automatically converted and imported into FMC. The FMC then pushes the configuration back to the device. This process preserves most of the FDM configuration, except for some features that are not supported by FMC, such as VPN wizards and certificates.

Question 4

Question Type: MultipleChoice

An engineer Is configuring a Cisco FTD device to place on the Finance VLAN to provide additional protection tor company financial dat

a. The device must be deployed without requiring any changes on the end user workstations, which currently use DHCP lo obtain an IP address. How must the engineer deploy the device to meet this requirement?

Options:

A- Deploy the device in routed mode and allow DHCP traffic in the access control policies.

B- Deploy the device in routed made aid 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 transparent mode and enable the DHCP Server feature.

Answer:

C

Explanation:

Transparent mode allows the FTD device to act as a "bump in the wire" that does not affect the IP addressing of the network. The end user workstations will not need any changes to their configuration, as they will still receive an IP address from the same DHCP server.However, the FTD device must allow DHCP traffic in the access control policies, otherwise it will block the DHCP requests and replies1

Question 5

Question Type: MultipleChoice

A network administrator must create an EtherChannel Interface on a new Cisco Firepower 9300 appliance registered with an FMC tor high availability. Where must the administrator create the EtherChannel interface?

Options:

A- FMC CLI

B- FTD CLI

C- FXOS CLI

D- FMC GUI

Answer:

C

Explanation:

An EtherChannel interface is a logical interface that consists of a bundle of individual Ethernet links that act as a single network link.An EtherChannel interface can increase the bandwidth and reliability of a network connection5.

On a Cisco Firepower 9300 appliance registered with an FMC for high availability, the network administrator must create the EtherChannel interface on the FXOS CLI.The FXOS is the operating system that runs on the Firepower 9300 chassis and provides hardware management functions such as interface configuration, power supply status, fan speed control, and so on6.

To create an EtherChannel interface on the FXOS CLI, the network administrator can follow these steps5:

Connect to the FXOS CLI using SSH or console.

Enter scope eth-uplink command to enter Ethernet uplink mode.

Enter create port-channel command to create an EtherChannel interface.

Enter a port-channel ID (1-48) and a mode (on or active) for the EtherChannel interface.

Enter add interface command to add physical interfaces to the EtherChannel interface.

Enter one or more interface IDs (for example, 1/1) for the physical interfaces.

Enter commit-buffer command to save the changes.

The other options are incorrect because:

The FMC CLI does not provide any commands to create an EtherChannel interface on a Firepower 9300 appliance.The FMC CLI is mainly used for managing FMC settings such as backup, restore, upgrade, troubleshoot, and so on7.

The FTD CLI does not provide any commands to create an EtherChannel interface on a Firepower 9300 appliance.The FTD CLI is mainly used for managing FTD settings such as routing, NAT, VPN, access control, and so on8.

The FMC GUI does not provide any options to create an EtherChannel interface on a Firepower 9300 appliance.The FMC GUI is mainly used for managing FTD policies such as access control, intrusion, file, malware, and so on9.

Question 6

Question Type: MultipleChoice

Which default action setting in a Cisco FTD Access Control Policy allows all traffic from an undefined application to pass without Snort Inspection?

Options:

A- Trust All Traffic

B- Inherit from Base Policy

C- Network Discovery Only

D- Intrusion Prevention

Answer:

A

Explanation:

The default action setting in a Cisco FTD Access Control Policy determines how the system handles and logs traffic that is not handled by any other access control configuration.The default action can block or trust all traffic without further inspection, or inspect traffic for intrusions and discovery data3.

The Trust All Traffic option allows all traffic from an undefined application to pass without Snort inspection. This option also disables Security Intelligence filtering, file and malware inspection, and URL filtering for all traffic handled by the default action.This option is useful when you want to minimize the performance impact of access control on your network3.

The other options are incorrect because:

The Inherit from Base Policy option inherits the default action setting from the base policy. The base policy is the predefined access control policy that you use as a starting point for creating your own policies.Depending on which base policy you choose, the inherited default action setting can be different3.

The Network Discovery Only option inspects all traffic for discovery data only. This option enables Security Intelligence filtering for all traffic handled by the default action, but disables file and malware inspection, URL filtering, and intrusion inspection.This option is useful when you want to collect information about your network before you configure access control rules3.

The Intrusion Prevention option inspects all traffic for intrusions and discovery data. This option enables Security Intelligence filtering, file and malware inspection, URL filtering, and intrusion inspection for all traffic handled by the default action.This option provides the most comprehensive protection for your network, but also has the most performance impact3.

Question 7

Question Type: MultipleChoice

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

Options:

A- application detector

B- access control

C- intrusion

D- correlation

Answer:

D

Explanation:

A correlation policy is a feature that allows you to respond in real time to threats or specific conditions on your network, using correlation rules.A correlation rule can trigger when the system generates a specific type of event, or when your network traffic deviates from its normal profile1.When a correlation rule triggers, the system generates a correlation event and can also launch a response, such as sending an alert, blocking an IP address, or scanning a host1.

In this case, the security engineer can configure a correlation rule that triggers when the system detects five or more connections from external sources within 2 minutes. The engineer can also configure a response that sends an alert to the FMC or an email recipient when this condition is triggered.The engineer can then create a correlation policy that includes this rule and activate it on the FTD device1.

The other options are incorrect because:

An application detector is a feature that allows you to detect web applications, clients, and application protocols based on patterns in network traffic.An application detector does not generate alerts based on the number of connections from external sources2.

An access control policy is a feature that allows you to control traffic flow through your network and inspect traffic for intrusions, malware, and files.An access control policy does not generate alerts based on the number of connections from external sources3.

An intrusion policy is a feature that allows you to detect and prevent malicious network activity using Snort rules.An intrusion policy does not generate alerts based on the number of connections from external sources4.