Cisco

(300-710)

Securing Networks with Cisco Firepower (300-710 SNCF)

Total: **307 Questions**

Link:

Question: 1

What is a result of enabling Cisco FTD clustering?

A.For the dynamic routing feature, if the master unit fails, the newly elected master unit maintains all existing connections.

B.Integrated Routing and Bridging is supported on the master unit.

C.Site-to-site VPN functionality is limited to the master unit, and all VPN connections are dropped if the master unit fails.

D.All Firepower appliances support Cisco FTD clustering.

Answer: C

Explanation:

C. Site-to-site VPN functionality is limited to the master unit, and all VPN connections are dropped if the master unit fails.

When Cisco FTD (Firepower Threat Defense) devices are configured in a clustering setup, certain features have limitations, particularly when it comes to stateful services like VPN.

Site-to-Site VPN and Clustering:
Only the master unit in the cluster handles site-to-site VPN connections.

If the master unit fails, the VPN connections do not fail over gracefully to other units.

As a result, all VPN tunnels are dropped, and they must be re-established on the newly elected master. This makes site-to-site VPN a master-dependent feature in FTD clustering.

Why the other options are incorrect:

A. "For the dynamic routing feature, if the master unit fails, the newly elected master unit maintains all existing connections."
→ Incorrect. While dynamic routing is supported in clustering, connections are not maintained automatically on a master failover — they are rebuilt.

B. "Integrated Routing and Bridging is supported on the master unit."→
Incorrect. IRB is not supported in clustered mode on Cisco FTD.

D. "All Firepower appliances support Cisco FTD clustering."
→ Incorrect. Only specific models support clustering (e.g., 4100 and 9300 series, some 2100 series with limitations). Not all appliances support it.

Reference:
https://www.cisco.com/c/en/us/td/docs/security/firepower/640/configuration/guide/fpmc-config-guide-v64/clustering_for_the_firepower_threat_defense.html

Question: 2

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: AE

Explanation:

A. The units must be the same version.

E. The units must be the same model.

A. The units must be the same version:
For high availability to work properly, both Cisco FTD (Firepower Threat Defense) devices need to run the same software version. This ensures compatibility and seamless failover between the devices.

E. The units must be the same model:
High availability requires that both devices be identical in terms of hardware model and capabilities. Differences in models can lead to mismatched configurations and failure of high availability.

Why Other Options Are Incorrect:

B: Devices must be in the same group and domain, but the option suggests they can belong to different groups, which is incorrect.

C: The units must be the same model, not different ones, even if they're part of the same series.

D: High availability supports both routed mode and transparent mode, so restricting it to routed mode is inaccurate.

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

Question: 3

On the advanced tab under inline set properties, which allows interfaces to emulate a passive interface?

A.transparent inline mode
B.TAP mode
C.strict TCP enforcement
D.propagate link state

Answer: B

Explanation:

B. **TAP mode.**

TAP mode is a configuration that allows interfaces to emulate passive interfaces. In this mode, the device monitors and analyzes traffic without actively interfering with the packets. This is often used for network traffic analysis or IDS (Intrusion Detection System) setups, where no active blocking or manipulation occurs. It enables passive observation of network traffic while maintaining transparency.

Why Other Options Are Incorrect:

A. Transparent inline mode: This mode enables the device to operate as a bridge, inspecting and allowing traffic to pass through, but it doesn't emulate a passive interface.

C. Strict TCP enforcement: This feature enforces strict compliance with TCP standards, ensuring proper session handling, but it doesn't relate to passive interface emulation.

D. Propagate link state: This is used for managing link states across connected devices but doesn't involve passive monitoring of traffic.

Question: 4

What are the minimum requirements to deploy a managed device inline?

A.inline interfaces, security zones, MTU, and mode
B.passive interface, MTU, and mode
C.inline interfaces, MTU, and mode
D.passive interface, security zone, MTU, and mode

Answer: C

Explanation:

C. inline interfaces, MTU, and mode.

Inline Interfaces:
Interfaces must be properly configured to operate in inline mode for packet inspection and enforcement.

MTU (Maximum Transmission Unit):
The MTU settings must be configured to ensure proper packet handling and throughput.

Mode:
The device must be set to the correct operational mode (inline mode) for traffic interception and inspection.

Why Other Options Are Incorrect:

A: While security zones are often part of a broader configuration, they are not a minimum requirement for deploying a managed device in inline mode.

B: Passive interfaces are unrelated to inline deployment; they are used for monitoring traffic without active intervention.

D: Passive interfaces and security zones are not directly relevant to inline mode deployment.

Reference:
https://www.cisco.com/c/en/us/td/docs/security/firepower/650/configuration/guide/fpmc-config-guide-v65/ips_device_deployments_and_configuration.html

Question: 5

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: D

Explanation:

D. Inline mode can drop malicious traffic.

In inline mode, the device is placed directly in the path of network traffic and can actively block or drop malicious traffic. In contrast, inline tap mode sends a copy of the traffic to another device for analysis without affecting the actual traffic flow.

Question: 6

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: D

Explanation:

Passive will only receive a copy of the traffic through SPAN so it does not go through the appliance, inline tap is pretty much just IDS (only inspects the traffic) but it does go through the appliance D is the answer.

Question: 7

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: AB

Explanation:

A. Transparent.

Acts like a Layer 2 bridge.

Supports high availability using failover pairs.

B. Routed.

Acts like a Layer 3 router.

Also supports high availability using failover configurations.

Reference:
https://www.cisco.com/c/en/us/td/docs/security/firepower/610/configuration/guide/fpmc-config-guide-v61/firepower_threat_defense_high_availability.html

Question: 8 Which protocol establishes network redundancy in a switched Firepower device deployment?

A.STP
B.HSRP
C.GLBP
D.VRRP

Answer: A

Explanation:

A. STP .

In a switched Firepower device deployment, network redundancy is typically achieved using Spanning Tree Protocol (STP). STP prevents loops in a Layer 2 (switched) network by blocking redundant paths and only allowing one active path at a time. If the active path fails, STP automatically reactivates one of the blocked paths, providing redundancy and failover.

Reference:
https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-config-guide-v62/firepower_threat_defense_high_availability.html

Question: 9 Which interface type allows packets to be dropped?

A.passive
B.inline
C.ERSPAN
D.TAP

Answer: B

Explanation:

B. inline.

In an inline interface configuration, packets can be actively inspected and then either forwarded or dropped based on the security policies applied. This mode allows for intrusion prevention, as it operates directly in the traffic flow, enabling the device to take action (like dropping malicious packets) in real time.

Reference:

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

Question: 10

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: CE

Explanation:

C. Speed

E. Duplex.

When configuring a routed interface in Cisco Firepower Threat Defense (FTD), the speed and duplex settings must be specified to ensure proper interface functionality and compatibility with the connected devices. These settings determine the data transfer rate (speed) and how communication happens over the interface (duplex: full or half).

Reference:

https://www.cisco.com/c/en/us/td/docs/security/firepower/610/fdm/fptd-fdm-config-guide-610/fptd-fdm-interfaces.html

Question: 11

Which two dynamic routing protocols are supported in Cisco FTD without using FlexConfig? (Choose two.)

A.EIGRP

B.OSPF

C.static routing

D.IS-IS

E.BGP

Answer: BE

Explanation:

B. OSPF

E. BGP.

Cisco Firepower Threat Defense (FTD) natively supports OSPF (Open Shortest Path First) and BGP (Border Gateway Protocol) as dynamic routing protocols without requiring FlexConfig. These protocols are commonly used for scalable and efficient routing in modern networks:
OSPF is an interior gateway protocol (IGP) that uses link-state information to calculate the best paths within an autonomous system.

BGP is an exterior gateway protocol (EGP) that facilitates routing between different autonomous systems, making it essential for internet-facing deployments.

Question: 12

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?

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: C

Explanation:

C. no policy rule is included.

During the initial deployment of a Cisco NGFW (Next-Generation Firewall) via the Cisco FMC (Firewall Management Center) GUI, no policy rule is included by default in the deployment of a local DMZ. The administrator must manually create and define the necessary policies to regulate traffic and secure the DMZ as per the organization's requirements.

Question: 13

What are two application layer preprocessors? (Choose two.)

A.CIFS

B.IMAP

C.SSL

D.DNP3

E.ICMP

Answer: BC

Explanation:

IMAP : This preprocessor is used for inspecting email traffic and ensuring that the traffic conforms to protocol standards.

SSL: The SSL preprocessor helps in inspecting encrypted traffic by either terminating or analyzing the SSL/TLS handshake.

Reference:

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

Question: 14

An engineer is implementing Cisco FTD in the network and is determining which Firepower mode to use. The organization needs to have multiple virtual
Firepower devices working separately inside of the FTD appliance to provide traffic segmentation. Which deployment mode should be configured in the Cisco
Firepower Management Console to support these requirements?

A.multi-instance

B.multiple deployment

C.single deployment

D.single-context

Answer: A

Explanation:

A. multi-instance.

In multi-instance mode, a single Cisco Firepower Threat Defense (FTD) appliance can host multiple independent virtual instances of Firepower devices. Each instance operates as an isolated virtual firewall with its own policies, configurations, and interfaces, providing the traffic segmentation required by the organization. This deployment is ideal for environments that need logical separation of traffic within a single physical device.

Question: 15

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 assigning an inline set interface

B.by using a BVI and creating a BVI IP address in the same subnet as the user segment

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

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

Answer: B

Explanation:

B. by using a BVI and creating a BVI IP address in the same subnet as the user segment.

A BVI (Bridge Virtual Interface) is used to extend a user segment through a Cisco Firepower Threat Defense (FTD) device in routed mode while keeping the traffic within the same IP subnet. The BVI acts as a logical interface that bridges multiple physical interfaces, allowing seamless traffic inspection without requiring a new subnet.

Question: 16 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.passive
B.routed
C.transparent
D.inline set

Answer: D

Explanation:

D. inline set.

In IPS-only mode, the Cisco Firepower Threat Defense (FTD) appliance is configured to detect and prevent intrusions without performing full firewalling functions. To use fail-to-wire interfaces in this mode, inline set is required. Inline set mode allows the appliance to inspect and act on traffic while ensuring traffic continuity even if the device fails, hence providing the fail-to-wire capability.

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

Question: 17 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: BE

Explanation:

B. Bridge groups are supported in both transparent and routed firewall modes.

In Cisco FTD, bridge groups operate in both transparent and routed modes. Transparent mode allows Layer 2 traffic to pass through without IP address changes, while routed mode enables Layer 3 traffic routing between different subnets. This flexibility is key for various deployment scenarios.

E. Each directly connected network must be on the same subnet.

Bridge Virtual Interfaces (BVIs) require that all connected devices within the bridge group remain on the same

IP subnet. This ensures smooth Layer 2 switching and connectivity within the bridged network.

Question: 18

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

A.drop packet
B.generate events
C.drop connection
D.drop and generate

Answer: A

Explanation:

A. drop packet.

By configuring the action as drop packet, the Cisco FMC can discard the low-priority events without generating logs or alerts for them. This reduces the noise in the event dashboard, allowing high-priority events to become more visible and easier to monitor. Unlike "generate events" or "drop and generate," this approach minimizes unnecessary logging and focuses only on critical traffic analysis.

Question: 19

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

A.subinterface
B.switch virtual
C.bridge virtual
D.bridge group member

Answer: C

Explanation:

C. bridge virtual.

In Cisco FTD's integrated routing and bridging, the Bridge Virtual Interface (BVI) is used for communication between a bridge group and a routed interface. The BVI acts as a logical Layer 3 interface that bridges traffic between the Layer 2 bridge group and the routed Layer 3 interfaces, enabling seamless communication across different segments.

Reference:

https://www.cisco.com/c/en/us/td/docs/security/firepower/640/configuration/guide/fpmc-config-guide-v64/transparent_or_routed_firewall_mode_for_firepower_threat_defense.html

Question: 20

An engineer is setting up a new Firepower deployment and is looking at the default FMC policies to start the implementation. During the initial trial phase, the organization wants to test some common Snort rules while still allowing the majority of network traffic to pass. Which default policy should be used?

A.Balanced Security and Connectivity
B.Security Over Connectivity
C.Maximum Detection
D.Connectivity Over Security

Answer: D

Explanation:

D. Connectivity Over Security.

When an organization is in a trial phase and wants to test Snort rules while ensuring that most network traffic is still allowed to pass, the Connectivity Over Security policy is the most suitable choice. This default policy prioritizes network connectivity, allowing traffic to flow freely with minimal inspection and restriction. It enables easier testing of Snort rules because it focuses less on strict security enforcement and more on maintaining operational functionality during this initial phase.

Question: 21

An engineer is configuring a second Cisco FMC as a standby device but is unable to register with the active unit. What is causing this issue?

A.The code versions running on the Cisco FMC devices are different.
B.The licensing purchased does not include high availability.
C.The primary FMC currently has devices connected to it. D.There is only 10 Mbps of bandwidth between the two devices.

Answer: A

Explanation:

A. The code versions running on the Cisco FMC devices are different.

For Cisco FMC high availability to work, both the active and standby units must be running the same software version. If the code versions differ, the standby device will be unable to register with the active unit, as synchronization between the devices requires identical configurations.

Question: 22

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

A.inline set
B.passive
C.transparent
D.inline tap

Answer: A

Explanation:

A. inline set.

An inline set allows Cisco Firepower Threat Defense (FTD) to inspect and process traffic passing through the appliance without requiring routing or VLAN rewriting. Inline sets are commonly used in scenarios where traffic needs to flow seamlessly while still being inspected for threats or vulnerabilities. This mode places the FTD appliance transparently between two network segments, ensuring traffic is inspected inline without making changes to IP addresses or VLAN tags.

Question: 23

A mid-sized company is experiencing higher network bandwidth utilization due to a recent acquisition. The network operations team is asked to scale up their one
Cisco FTD appliance deployment to higher capacities due to the increased network bandwidth. Which design option should be used to accomplish this goal?

A.Deploy multiple Cisco FTD HA pairs in clustering mode to increase performance.

B.Deploy multiple Cisco FTD appliances in firewall clustering mode to increase performance.

C.Deploy multiple Cisco FTD appliances using VPN load-balancing to scale performance.

D.Deploy multiple Cisco FTD HA pairs to increase performance.

Answer: B

Explanation:

B. Deploy multiple Cisco FTD appliances in firewall clustering mode to increase performance.

Firewall clustering allows multiple Cisco FTD appliances to work together as a single logical unit, effectively distributing the traffic load across the devices. This setup is ideal for scaling performance in environments experiencing increased network bandwidth utilization, as it enhances throughput and redundancy without requiring separate configurations for each appliance.

Reference:

https://www.cisco.com/c/en/us/td/docs/security/firepower/fxos/clustering/ftd-cluster-solution.html#concept_C8502505F840451C9E600F1EED9BC18E

Question: 24

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

A.minor upgrade

B.local import of intrusion rules

C.Cisco Geolocation Database

D.local import of major upgrade

Answer: B

Explanation:

B. Local import of intrusion rules .

In a multi-tenant deployment, the Global Domain applies to all tenants, while each tenant has its own domain with its own policies, objects, and configurations. If a minor upgrade or a major upgrade is applied, it should be done globally and affects all tenants. Similarly, the Cisco Geolocation Database should be updated globally as it applies to all tenants.

However, intrusion rules can be specific to a tenant's needs and should be imported locally in the tenant's domain to ensure that only the desired rules are applied to that tenant's traffic.

Question: 25

An organization has a compliancy requirement to protect servers from clients, however, the clients and servers all reside on the same Layer 3 network. Without readdressing IP subnets for clients or servers, how is segmentation achieved?

A.Change the IP addresses of the servers, while remaining on the same subnet.

B.Deploy a firewall in routed mode between the clients and servers.

C.Change the IP addresses of the clients, while remaining on the same subnet.

D.Deploy a firewall in transparent mode between the clients and servers.

Answer: D

Explanation:

D. Deploy a firewall in transparent mode between the clients and servers.

In transparent mode, the firewall operates as a Layer 2 device, allowing it to inspect traffic between clients and servers on the same subnet without requiring readdressing or routing changes. This mode is ideal for scenarios where segmentation is needed without altering the existing Layer 3 network architecture.

Question: 26

Network traffic coming 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.Change the intrusion policy from security to balance.

B.Configure a trust policy for the CEO.

C.Configure firewall bypass.

D.Create a NAT policy just for the CEO.

Answer: B

Explanation:

B. Configure a trust policy for the CEO.

A trust policy allows specified traffic to bypass inspection, ensuring that critical traffic—like that from the organization's CEO—is always allowed. By configuring such a policy, the deployment engineer ensures that the CEO's traffic is neither inspected nor denied, without the need to create a broader rule that permits all traffic.

Question: 27 What is a characteristic of bridge groups on a Cisco FTD?

A.In routed firewall mode, routing between bridge groups is supported.

B.Routing between bridge groups is achieved only with a router-on-a-stick configuration on a connected router. C.In routed firewall mode, routing between bridge groups must pass through a routed interface.

D.In transparent firewall mode, routing between bridge groups is supported.

Answer: A

Explanation:

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.

Reference:

https://www.cisco.com/c/en/us/td/docs/security/asa/asa97/configuration/general/asa-97-general-config/intro-fw.pdf

Question: 28 A Cisco FTD device is running in transparent firewall mode with a VTEP bridge group member ingress interface. What must be considered by an engineer tasked with specifying a destination MAC address for a packet trace? A.The output format option for the packet logs is unavailable.

B.Only the UDP packet type is supported.

C.The destination MAC address is optional if a VLAN ID value is entered.

D.The VLAN ID and destination MAC address are optional.

Answer: C

Explanation:

C. The destination MAC address is optional if a VLAN ID value is entered.

When running a packet trace on a Cisco FTD device in transparent firewall mode with a VTEP (Virtual Tunnel Endpoint) bridge group member ingress interface, the destination MAC address becomes optional if a VLAN ID is specified. This allows for greater flexibility during the packet trace configuration while analyzing traffic.

Reference:

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

Question: 29 With Cisco FTD software, which interface mode must be configured to passively receive traffic that passes through the appliance?

A.ERSPAN
B.firewall
C.tap
D.IPS-only

Answer: C

Explanation:

C. tap.

In tap mode, the Cisco Firepower Threat Defense (FTD) appliance passively receives traffic for inspection without altering it. This mode is commonly used for monitoring and analyzing network traffic while ensuring the original flow of data remains unaffected.

Question: 30

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 passive IDS ports for both departments.

B.Use a dedicated IPS inline set for each department to maintain traffic separation. C.Use 802.1Q inline set Trunk interfaces with VLANs to maintain logical traffic separation. D.Use one pair of inline set in TAP mode for both departments.

Answer: A

Explanation:

Using Passive Mode for these two department which just only consume two interfaces. While all the other options would consume four interfaces. Besides, Passive Mode is configured on interface level, it can highly prevent policy misconfiguration on applying Access Control Policy with drop action, traffic redirection, SSL Encryption, etc., which can provide confidence to users.

Question: 31

A hospital network needs to upgrade their Cisco FMC managed devices and needs to ensure that a disaster recovery process is in place. What must be done in order to minimize downtime on the network?

A.Configure a second circuit to an ISP for added redundancy.
B.Keep a copy of the current configuration to use as backup.
C.Configure the Cisco FMCs for failover.

D.Configure the Cisco FMC managed devices for clustering.

Answer: D

Explanation:

D. Configure the Cisco FMC managed devices for clustering.To minimize downtime on the network during an upgrade, the hospital network should configure the Cisco FMC managed devices for clustering. Clustering allows multiple FMC devices to be managed as a single entity, providing redundancy and load sharing. If one device in the cluster fails or needs to be taken offline for maintenance, the other devices can continue to operate, minimizing downtime.

Question: 32

An organization has implemented Cisco Firepower without IPS capabilities and now wants to enable inspection for their traffic. They need to be able to detect protocol anomalies and utilize the Snort rule sets to detect malicious behavior. How is this accomplished?

A.Modify the network discovery policy to detect new hosts to inspect.

B.Modify the access control policy to redirect interesting traffic to the engine.

C.Modify the intrusion policy to determine the minimum severity of an event to inspect.

D.Modify the network analysis policy to process the packets for inspection.

Answer: B

Explanation:

B. Modify the access control policy to redirect interesting traffic to the engine.

In Cisco Firepower, to enable intrusion inspection (using Snort rules and detecting anomalies), you must apply an Intrusion Policy to your traffic.

This is done through the Access Control Policy — by editing the policy and selecting an intrusion policy (such as "Security Over Connectivity" or a custom one) for the matching traffic.

Network analysis policies (option D) are about pre-processing traffic (e.g., normalizing, decoding), not about deciding what gets inspected.

Network discovery policies (option A) are for passive asset identification, not inspection.

Intrusion policy severity (option C) controls alerting and actions, but you first have to apply the intrusion inspection to traffic before any of that matters.

Question: 33

An engineer is tasked with deploying an internal perimeter firewall that will support multiple DMZs. Each DMZ has a unique private IP subnet range. How is this requirement satisfied?

A.Deploy the firewall in transparent mode with access control policies

B.Deploy the firewall in routed mode with access control policies

C.Deploy the firewall in routed mode with NAT configured

D.Deploy the firewall in transparent mode with NAT configured

Answer: B

Explanation:

B. By deploying the firewall in routed mode with access control policies, the engineer can configure the firewall to route traffic between the DMZs and the internal network based on their unique private IP subnet ranges. The access control policies can be used to enforce security policies to control which traffic is allowed between the DMZs and the internal network. This provides a secure and efficient way to manage traffic between the DMZs and the internal network.

Question: 34

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 a cluster span EtherChannel

C.in active/passive mode

D.in cluster interface mode

Answer: C

Explanation:

In active/passive mode, only one device actively processes traffic at a time, while the other remains on standby. If the active device fails, the standby device seamlessly takes over, ensuring network continuity without requiring concurrent traffic handling.

This mode is suitable for scenarios where the infrastructure does not support load balancing or simultaneous data forwarding by multiple devices.

Question: 35

When deploying a Cisco ASA Firepower module, an organization wants to evaluate the contents of the traffic without affecting the network. It is currently configured to have more than one instance of the same device on the physical appliance. Which deployment mode meets the needs of the organization?

A.inline tap monitor-only mode

B.passive monitor-only mode

C.passive tap monitor-only mode

D.inline mode

Answer: A

Explanation:

Passive monitor only (B) could be the answer if there was only 1 instance but the question says there are more tan one.Thus the second option which does not affect traffic is inline tap monitor only (A)

Inline tap monitor-only mode (ASA inline)—In an inline tap monitor-only deployment, a copy of the traffic is sent to the ASA FirePOWER module, but it is not returned to the ASA. Inline tap mode lets you see what the ASA FirePOWER module would have done to traffic, and lets you evaluate the content of the traffic, without impacting the network. However, in this mode, the ASA does apply its policies to the traffic, so traffic can be dropped due to access rules, TCP normalization, and so forth.

Question: 36

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 neighboring 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: A

Explanation:

A. Create a firewall rule to allow CDP traffic

In bridge group deployments on Cisco FTD, the firewall blocks certain Layer 2 control protocols like CDP (Cisco Discovery Protocol) and multicast by default for security reasons.

To allow CDP or multicast traffic through a bridge group, you must explicitly create rules (using Access Control Policies) that permit those protocols.

B is incorrect — the bridge group already exists.

C is incorrect — the firewall is already in transparent mode (required for bridge groups).

D is incorrect — routed mode would not fix this and would fundamentally change how the firewall processes traffic.

Question: 37

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: D

Explanation:

D. Configure a bridge group in transparent mode.

By configuring the Cisco Firepower device in transparent mode and using a bridge group, the appliance can act as a "bump in the wire," analyzing traffic without requiring changes to the network's topology. This mode allows the device to inspect and alert on malicious activity while operating at Layer 2, ensuring seamless traffic flow without routing or IP address configuration.

Question: 38

Which two conditions must be met to enable high availability between two Cisco FTD devices? (Choose two.)

A.same flash memory size
B.same NTP configuration
C.same DHCP/PPoE configuration

D.same host name
E.same number of interfaces

Answer: BE

Explanation:

B. same NTP configuration.

E. same number of interfaces.

Same NTP configuration: For high availability to function properly, both Cisco FTD devices must be synchronized to the same Network Time Protocol (NTP) settings. Time synchronization is crucial for the accurate operation of failover mechanisms.

Same number of interfaces: Both devices must have the same number of physical and logical interfaces configured. This ensures that failover can occur seamlessly, maintaining consistent traffic flow across the network.

Question: 39

An engineer is building a new access control policy using Cisco FMC. The policy must inspect a unique IPS policy as well as log rule matching. Which action must be taken to meet these requirements?

A.Configure an IPS policy and enable per-rule logging
B.Disable the default IPS policy and enable global logging
C.Configure an IPS policy and enable global logging
D.Disable the default IPS policy and enable per-rule logging

Answer: A

Explanation:

A. Configure an IPS policy and enable per-rule logging.

To meet the requirements, the engineer needs to specify a unique IPS policy for intrusion detection and prevention, tailored to the specific needs of the traffic being inspected. Additionally, per-rule logging ensures that rule matching events are logged individually, providing detailed visibility into traffic behavior and policy enforcement.

Question: 40

Which two OSPF routing features are configured in Cisco FMC and propagated to Cisco FTD? (Choose two.)

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: BE

Explanation:

B. virtual links .

E. MD5 authentication to OSPF packets.

Virtual links: These are supported and can be configured in Cisco FMC to ensure OSPF connectivity across areas that do not have direct physical links to the backbone area.

MD5 authentication to OSPF packets: Cisco FMC allows the configuration of MD5 authentication for OSPF, which secures OSPF packet exchanges between routers by ensuring their integrity and authenticity.

Reference:

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

Question: 41

When creating a report template, how are the results limited to show only the activity of a specific subnet?

A.Create a custom search in Cisco FMC and select it in each section of the report.

B.Add an Input Parameter in the Advanced Settings of the report, and set the type to Network/IP.

C.Add a Table View section to the report with the Search field defined as the network in CIDR format. D.Select IP Address as the X-Axis in each section of the report.

Answer: B

Explanation:

B. Add an Input Parameter in the Advanced Settings of the report, and set the type to Network/IP.

By using the Input Parameter in the Advanced Settings of a report template, you can restrict the data displayed in the report to a specific subnet. Setting the parameter type to Network/IP allows the report to focus only on traffic related to the specified subnet, ensuring precise results.

Reference:

https://www.cisco.com/c/en/us/td/docs/security/firesight/541/user-guide/FireSIGHT-System-UserGuide-v5401/Reports.html#87267

Question: 42

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

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

B.Smart License is required to maintain VPN connections simultaneously across all cluster units. C.VPN connections must be re-established when a new master unit is elected.

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

Answer: C

Explanation:

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

In a clustered-units environment, when the master unit fails and a new master unit is elected, any existing VPN connections are dropped and must be re-established. This results in temporary disruption of VPN connectivity, which is a notable disadvantage in such setups.

Reference:

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

Question: 43 What are two features of bridge-group interfaces in Cisco FTD? (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: BE

Explanation:

B. Bridge groups are supported in both transparent and routed firewall modes.

E. Each directly connected network must be on the same subnet.

Bridge groups in both transparent and routed modes: Cisco FTD supports bridge groups in both transparent and routed firewall modes, providing flexibility for traffic segmentation and inspection across different deployment scenarios.

Same subnet for directly connected networks: For bridge-group interfaces, each directly connected network within a bridge group must reside on the same subnet. This ensures seamless Layer 2 communication and traffic flow.

Question: 44 Which command is run on an FTD unit to associate the unit to an FMC manager that is at IP address 10.0.0.10, and that has the registration key Cisco123?

A.configure manager local 10.0.0.10 Cisco123

B.configure manager add Cisco123 10.0.0.10

C.configure manager local Cisco123 10.0.0.10

D.configure manager add 10.0.0.10 Cisco123

Answer: D

Explanation:

D. configure manager add 10.0.0.10 Cisco123.

This command is used to associate a Cisco FTD (Firepower Threat Defense) unit to an FMC (Firepower Management Center) manager. The "add" directive establishes the connection to the specified IP address (10.0.0.10) of the FMC, using the given registration key (Cisco123) for secure communication.

Reference:

https://www.cisco.com/c/en/us/td/docs/security/firepower/misc/fmc-ftd-mgmt-nw/fmc-ftd-mgmt-nw.html#id_106101

Question: 45 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: AB

Explanation:

A. Block with Reset .

B. Monitor.

Block with Reset: This action blocks the connection and sends a TCP reset to terminate the session, providing immediate feedback to the sender that the connection was refused.

Monitor: This action allows traffic to pass while logging its details for analysis, which is often used for troubleshooting or observing network behavior without enforcing a strict policy.

Reference:

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

Question: 46 Which two routing options are valid with Cisco FTD? (Choose two.)

A.BGPv6

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

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

D.BGPv4 in transparent firewall mode

E.BGPv4 with nonstop forwarding

Answer: AC

Explanation:

A. BGPv6: Cisco Firepower Threat Defense (FTD) supports BGPv6 (Border Gateway Protocol for IPv6), enabling dynamic routing in IPv6 environments. This is a valid option for routing configuration on Cisco FTD.

C. ECMP with up to three equal cost paths across a single interface: Cisco FTD supports Equal-Cost Multi-Path (ECMP) routing, allowing traffic to be distributed across multiple equal-cost paths. In this case, it can be configured across a single interface, making it another valid option.

Reference:

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

Question: 47 Which object type supports object overrides?

A.time range
B.security group tag
C.network object
D.DNS server group

Answer: C

Explanation:

C. network object.

Object overrides are supported for network objects in Cisco FMC. This allows administrators to customize the behavior of network objects within specific access control policies without affecting the global definition of the object. Overrides provide flexibility in tailoring security policies to meet unique requirements.

Reference:

https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Reusable_Objects.html#concept_8BFE8B9A83D742D9B647A74F7AD50053

Question: 48 Which Cisco Firepower rule action displays an HTTP warning page?

A.Monitor
B.Block
C.Interactive Block
D.Allow with Warning

Answer: C

Explanation:

C. Interactive Block.

The Interactive Block rule action in Cisco Firepower displays an HTTP warning page to the user when a web request violates policy rules. This feature is often used to notify users of prohibited activities while giving them an opportunity to acknowledge the warning or take corrective action.

Reference:

https://www.cisco.com/c/en/us/td/docs/security/firesight/541/user-guide/FireSIGHT-System-UserGuide-v5401/AC-Rules-Tuning-Overview.html#76698

Question: 49

What is the result a 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: B

Explanation:

B. Matching traffic is not rate limited.

If a QoS (Quality of Service) rule specifies a rate limit greater than the maximum throughput of an interface, the rule essentially becomes ineffective because the traffic cannot exceed the interface's maximum capacity. As a result, the matching traffic flows without being rate-limited.

Reference:

https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-config-guide-v62/quality_of_service_qos.pdf

Question: 50

Which Firepower feature allows users to configure bridges in routed mode and enables devices to perform Layer 2 switching between interfaces?

A.FlexConfig

B.BDI

C.SGT

D.IRB

Answer: D

Explanation:

D. IRB .

IRB is a feature in Cisco Firepower that enables devices to combine Layer 2 switching and Layer 3 routing on the same interface, allowing bridges to be configured in routed mode. This is particularly useful for environments that require seamless traffic handling across multiple network layers.

Reference:
https://www.cisco.com/c/en/us/td/docs/security/firepower/620/relnotes/Firepower_System_Release_Notes_Versio
new_features_and_functionality.html

Question: 51 In which two places are thresholding settings 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: AC

Explanation:

A. on each IPS rule.

C. globally, per intrusion policy.

A: You can configure thresholding directly on individual IPS (Snort) rules, to control when alerts are generated (e.g., after X number of events).

C: You can configure global thresholding per intrusion policy, applying to all matching events in that policy.

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

Question: 52 In which two ways do access control policies operate on a Cisco Firepower system? (Choose two.)

A.Traffic inspection is interrupted temporarily when configuration changes are deployed.

B.The system performs intrusion inspection followed by file inspection.

C.They block traffic based on Security Intelligence data.

D.File policies use an associated variable set to perform intrusion prevention.

E.The system performs a preliminary inspection on trusted traffic to validate that it matches the trusted parameters.

Answer: CE

Explanation:

C. They block traffic based on Security Intelligence data: Access control policies integrate with Cisco's Security Intelligence feeds to block traffic based on malicious IP addresses, domains, and URLs. This mechanism enables proactive threat prevention, leveraging global threat intelligence to protect the network.

E. The system performs a preliminary inspection on trusted traffic to validate that it matches the trusted parameters: In Cisco Firepower, trusted traffic is inspected initially to confirm it meets predefined trusted parameters. If validated, it is allowed to pass without undergoing deeper inspection, thereby enhancing performance and efficiency.

Question: 53

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

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

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

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

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

E.reputation-based objects, such as URL categories

Answer: BC

Explanation:

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

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

Reputation-based objects: These are reusable and include Security Intelligence feeds and lists, as well as filters based on reputation (e.g., file reputation and application category), enabling streamlined security operations.

Network-based objects: These objects represent foundational components such as IP addresses, networks, port/protocol combinations, VLAN tags, security zones, and even geographical origin/destination.

Reference:

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

Question: 54

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 application rules?

A.utilizing a dynamic ACP that updates from Cisco Talos

B.creating a unique ACP per device

C.utilizing policy inheritance

D.creating an ACP with an INSIDE_NET network object and object overrides

Answer: D

Explanation:

D. creating an ACP with an INSIDE_NET network object and object overrides.

By creating an Access Control Policy (ACP) that uses the INSIDE_NET network object along with object overrides, the security engineer can maintain consistency across all branch locations. Object overrides allow the engineer to customize the INSIDE_NET object for each branch location while retaining a uniform rule set in the policy. This ensures that only the locally significant internal network subnets are applied at each branch without altering the main policy.

Question: 55

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 NAT policy so that the Cisco Firepower device does not have to translate as many addresses.

B.Create a flexconfig policy to use WCCP for application aware bandwidth limiting.

C.Create a QoS policy rate-limiting high bandwidth applications.

D.Create a VPN policy so that direct tunnels are established to the business applications.

Answer: C

Explanation:

C. Create a QoS policy rate-limiting high bandwidth applications.

By implementing a QoS (Quality of Service) policy on the Cisco Firepower device, the organization can prioritize traffic and rate-limit high-bandwidth applications. This ensures that legitimate business-critical traffic receives higher priority and bandwidth, alleviating congestion and improving overall network performance.

Question: 56

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: A

Explanation:

A. Source or destination security zones in the access control rule matches the security zones that are associated with interfaces on the target devices.

When an access control rule specifies security zones, and these zones align with the security zones associated with the interfaces of the target devices, the Cisco Firepower system may trigger a device restart.

This occurs because changes in policies that directly affect active zones and their traffic flow require the system to reload configurations to apply the updates effectively.

Reference:

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

Question: 57

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: AC

Explanation:

A. Intrusion Events - This provides insights into threat and security-related events, showing detailed intrusion activity.

C. Appliance Status - This offers health information about the Cisco Firepower devices, such as device status and performance.

Reference:

https://www.cisco.com/c/en/us/td/docs/security/firepower/640/configuration/guide/fpmc-config-guide-v64/dashboards.html#ID-2206-00000283

Question: 58

There is an increased amount of traffic on the network and for compliance reasons, management needs visibility into the encrypted traffic. What is a result of enabling TLS/SSL decryption to allow this visibility?

A.It prompts the need for a corporate managed certificate.

B.It will fail if certificate pinning is not enforced.

C.It has minimal performance impact.

D.It is not subject to any Privacy regulations.

Answer: A

Explanation:

A. It prompts the need for a corporate managed certificate.

Enabling TLS/SSL decryption requires a corporate-managed certificate to decrypt and inspect encrypted traffic securely. This certificate is essential to ensure the organization's ability to intercept and analyze encrypted data while maintaining trust with clients and devices on the network. Without it, the decryption process would fail or compromise security.

Question: 59

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

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

B.Confirm that both devices are configured with the same types of interfaces.

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

D.Confirm that both devices have the same port-channel numbering.

Answer: A

Explanation:

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

For synchronization between two Cisco FTD devices (often configured as an HA pair) to succeed, both devices must be running the same software version and patch level. Any mismatch in software versions will cause the synchronization process to fail. This ensures compatibility and consistency in configurations and operations between the two devices.

Question: 60

An organization wants to secure traffic from their branch office to the headquarters building using Cisco Firepower devices. They want to ensure that their Cisco
Firepower devices are not wasting resources on inspecting the VPN traffic. What must be done to meet these requirements?

A.Configure the Cisco Firepower devices to bypass the access control policies for VPN traffic.

B.Tune the intrusion policies in order to allow the VPN traffic through without inspection.

C.Configure the Cisco Firepower devices to ignore the VPN traffic using prefilter policies.

D.Enable a flexconfig policy to re-classify VPN traffic so that it no longer appears as interesting traffic.

Answer: A

Explanation:

A. Configure the Cisco Firepower devices to bypass the access control policies for VPN traffic.By configuring the Cisco Firepower devices to bypass the access control policies for VPN traffic, the devices will not perform security inspection on the VPN traffic, which will help to conserve resources. This can be done by creating an access control rule that matches the VPN traffic and then setting the action to "Trust". This will allow the traffic to bypass the access control policies and not consume resources.

Reference:

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

Question: 61

An administrator is working on a migration from Cisco ASA to the Cisco FTD appliance and needs to test the rules without disrupting the traffic. Which policy type should be used to configure the ASA rules during this phase of the migration?

A.Prefilter
B.Intrusion
C.Access Control
D.Identity

Answer: C

Explanation:

C. Access Control.

During a migration from Cisco ASA to Cisco Firepower Threat Defense (FTD), the Access Control Policy is used to configure rules that dictate how traffic is allowed, denied, or monitored. These policies allow administrators to test and validate the behavior of rules without impacting live traffic. Access Control Policies are highly flexible and can be used to implement granular control, ensuring smooth traffic flow while testing the configurations.

Question: 62

A network administrator is seeing an unknown verdict for a file detected by Cisco FTD. Which malware policy configuration option must be selected in order to further analyze the file in the Talos cloud?

A.malware analysis
B.dynamic analysis
C.sandbox analysis
D.Spero analysis

Answer: B

Explanation:

B. dynamic analysis

Dynamic analysis allows Cisco FTD to send files to the Talos cloud for deeper examination. This ensures more comprehensive file evaluation to determine potential threats.

Reference:

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

Question: 63

An engineer has been tasked with providing disaster recovery for an organization's primary Cisco FMC. What must be done on the primary and secondary Cisco
FMCs to ensure that a copy of the original corporate policy is available if the primary Cisco FMC fails?

A.Restore the primary Cisco FMC backup configuration to the secondary Cisco FMC device when the primary device fails.

B.Connect the primary and secondary Cisco FMC devices with Category 6 cables of not more than 10 meters in length.

C.Configure high-availability in both the primary and secondary Cisco FMCs.

D.Place the active Cisco FMC device on the same trusted management network as the standby device.

Answer: C

Explanation:

C. Configure high-availability in both the primary and secondary Cisco FMCs.

To ensure disaster recovery and availability of the corporate policy, configuring high-availability between the primary and secondary Cisco FMCs is essential. High-availability ensures that the secondary Cisco FMC automatically takes over and maintains access to policies and settings if the primary FMC fails. This setup provides seamless redundancy and avoids manual restoration steps.

Reference:

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

Question: 64

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 Cisco0391521107. Which command set must be used in order to accomplish this?

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

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

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

D.configure manager add DONTRESOLVE <FMC IP> AMCE001<registration key>

Answer: A

Explanation:

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

When an engineer is adding a Firepower Threat Defense (FTD) device to Firepower Management Center (FMC), the command syntax configure manager add <FMC IP> <registration key> ACME001 is used for registration. This format specifies the FMC's IP address first, followed by the registration key, and concludes with the NAT ID (ACME001).

<FMC IP>: This indicates the address of the Firepower Management Center, which the FTD device needs to register with.

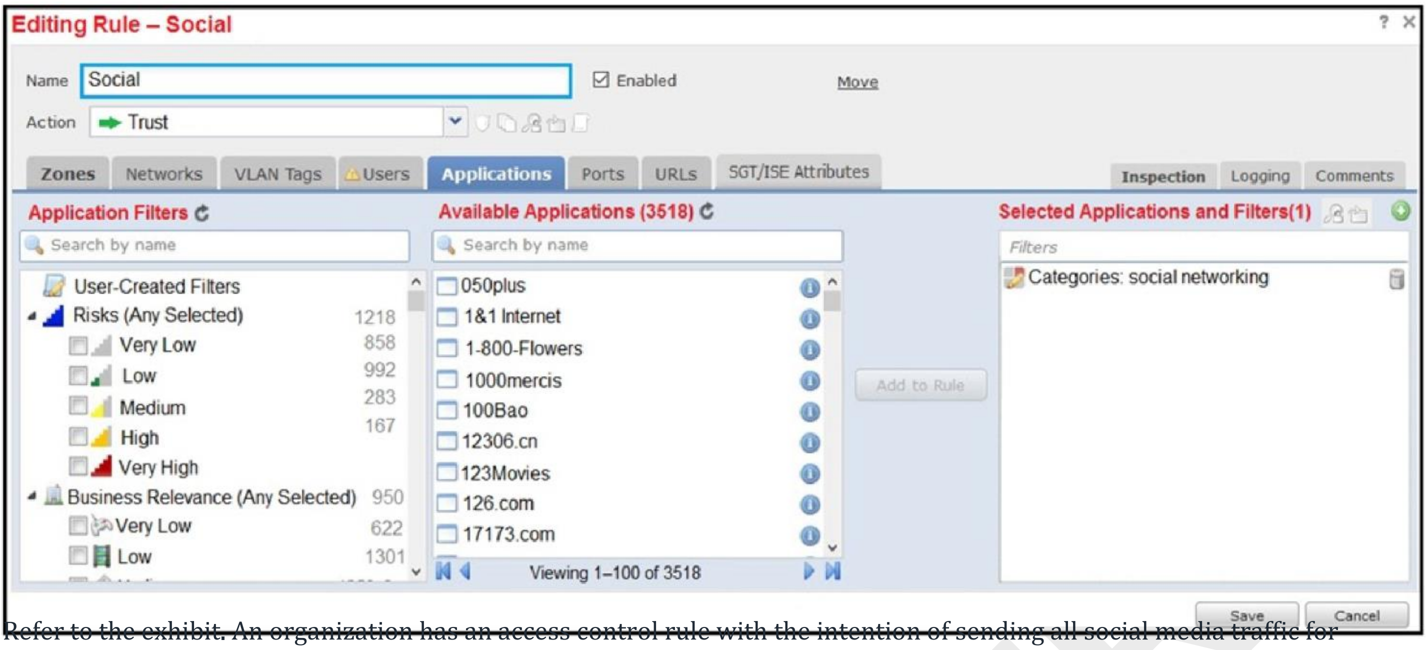
<registration key>: This is the secure password (Cisco0391521107) used to authenticate the FTD device during the registration process.

ACME001: The NAT ID is appended at the end to ensure the device can identify itself properly when communicating behind a NAT configuration.

Reference:

https://www.cisco.com/c/en/us/support/docs/security/firesight-management-center/118596-configure-firesight-00.html

Question: 65



Name: Social

☑ Enabled

Action: Trust

Categories: social networking

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.Add the social network URLs to the block list.

B.Change the intrusion policy to connectivity over security.

C.Modify the selected application within the rule.

D.Modify the rule action from trust to allow.

Answer: D

Explanation:

D: Modify the rule action from trust to allow.

When the access control rule action is set to "trust," it essentially bypasses all inspection processes, allowing traffic to flow freely without any inspection or enforcement applied. This means the traffic matching the rule is neither blocked nor subjected to inspection, defeating the original intention of inspecting all social media traffic.

To address this issue, the rule action must be changed from "trust" to "allow." The "allow" action permits the traffic but ensures that it goes through the inspection processes defined in the rule, such as intrusion prevention, malware scanning, and other security checks. By selecting "allow," you enforce inspection mechanisms while still permitting the traffic.

Question: 66 A user within an organization opened a malicious file on a workstation which in turn caused a ransomware attack on the network. What should be configured within the Cisco FMC to ensure the file is tested for viruses on a sandbox system?

A.Spero analysis
B.capacity handling
C.local malware analysis
D.dynamic analysis

Answer: D

Explanation:

D. dynamic analysis.

Dynamic analysis ensures that files are sent to a sandbox system for detailed inspection in a controlled environment. This allows for the detection of ransomware or other malware by analyzing file behavior before it impacts the network. By configuring dynamic analysis in Cisco FMC, malicious files can be identified and blocked before they cause harm.

Reference:
https://www.cisco.com/c/en/us/td/docs/security/firepower/623/configuration/guide/fpmc-config-guide-v623/file_policies_and_advanced_malware_protection.html#ID-2199-000005d8

Question: 67 An engineer configures a network discovery policy on Cisco FMC. Upon configuration, it is noticed that excessive and misleading events are filling the database and overloading the Cisco FMC. A monitored NAT device is executing multiple updates of its operating system in a short period of time. What configuration change must be made to alleviate this issue?

A.Exclude load balancers and NAT devices.
B.Leave default networks.
C.Increase the number of entries on the NAT device.
D.Change the method to TCP/SYN.

Answer: A

Explanation:

A. Exclude load balancers and NAT devices.

Excluding load balancers and NAT devices from the network discovery policy prevents the FMC from generating excessive and misleading events caused by frequent updates or repetitive traffic patterns. This approach minimizes database overload and ensures more relevant and actionable events are logged.

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

Question: 68

A network administrator notices that remote access VPN users are not reachable from inside the network. It is determined that routing is configured correctly; however, return traffic is entering the firewall but not leaving it. What is the reason for this issue?

A.A manual NAT exemption rule does not exist at the top of the NAT table B.An external NAT IP address is not configured
C.An external NAT IP address is configured to match the wrong interface D.An object NAT exemption rule does not exist at the top of the NAT table

Answer: A

Explanation:

A. A manual NAT exemption rule does not exist at the top of the NAT table.

The issue arises because the firewall is likely performing NAT on the return traffic from the remote access VPN users, causing it to fail to route back to its destination properly. Adding a manual NAT exemption rule at the top of the NAT table ensures that the VPN traffic bypasses NAT processing, allowing proper bidirectional communication between remote users and the internal network.

Question: 69

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

A.The interfaces are being used for NAT for multiple networks B.The administrator is adding interfaces of multiple types
C.The administrator is adding an interface that is in multiple zones
D.The interfaces belong to multiple interface groups

Answer: B

Explanation:

B is correct. All interfaces in an interface object must be of the same type: all inline, passive, switched, routed, or ASA FirePOWER. After you create an interface object, you cannot change the type of interfaces it contains.

Question: 70

An organization is using a Cisco FTD and Cisco ISE to perform identity-based access controls. A network administrator is analyzing the Cisco FTD events and notices that unknown user traffic is being allowed through the firewall. How should this be addressed to block the traffic while allowing legitimate user traffic?

A.Modify the Cisco ISE authorization policy to deny this access to the user
B.Modify Cisco ISE to send only legitimate usernames to the Cisco FTD C.Add the unknown user in the Access Control Policy in Cisco FTD
D.Add the unknown user in the Malware & File Policy in Cisco FTD

Answer: C

Explanation:

C: Add the unknown user in the Access Control Policy in Cisco FTD.

When unknown user traffic is being allowed through the firewall, it typically means there is no explicit rule handling such traffic in the Access Control Policy (ACP) of the Cisco Firepower Threat Defense (FTD). This results in the traffic being matched against the default action of the firewall, which might be to allow the traffic.

To block this traffic while still allowing legitimate user traffic, you need to update the Access Control Policy in Cisco FTD by explicitly adding a rule to handle unknown users.

Reference:

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

Question: 71 What is the benefit of selecting the trace option for packet capture?

A.The option indicates whether the packet was dropped or successful.

B.The option indicates whether the destination host responds through a different path. C.The option limits the number of packets that are captured.

D.The option captures details of each packet.

Answer: A

Explanation:

A. The option indicates whether the packet was dropped or successful.

When the trace option is enabled for packet capture in Cisco Firepower, it provides visibility into whether each packet was successfully forwarded or dropped by the device. This is useful for troubleshooting network issues and analyzing traffic behavior.

Question: 72 After deploying a network-monitoring tool to manage and monitor networking devices in your organization, you realize that you need to manually upload an MIB for the Cisco FMC. In which folder should you upload the MIB file?

A./etc/sf/DCMIB.ALERT
B./sf/etc/DCEALERT.MIB
C./etc/sf/DCEALERT.MIB
D.system/etc/DCEALERT.MIB

Answer: C

Explanation:

C. /etc/sf/DCEALERT.MIB.

When manually uploading an MIB (Management Information Base) for Cisco FMC, the correct directory is

/etc/sf/DCEALERT.MIB. This ensures the MIB file is placed in the appropriate location for the system to recognize and use it effectively.

Reference:

https://www.cisco.com/c/en/us/td/docs/security/firesight/541/firepower-module-user-guide/asa-firepower-module-user-guide-v541/Intrusion-External-Responses.pdf

Question: 73 Which command should be used on the Cisco FTD CLI to capture all the packets that hit an interface?

A.configure coredump packet-engine enable
B.capture-traffic
C.capture
D.capture WORD

Answer: D

Explanation:

D: capture WORD.

The capture WORD command is used on the Cisco FTD CLI to initiate a packet capture for all the packets matching the defined criteria on an interface. In this case:

- WORD represents the name you assign to the capture session, which allows you to distinguish multiple captures or reference the specific one you configure.

- This command is versatile and allows you to further define details like filters (e.g., source, destination, protocol) and interfaces to narrow down the capture scope.

Why other options are incorrect:

- A: configure coredump packet-engine enable: This is unrelated to packet capture. It enables core dumps for troubleshooting specific packet engine issues.

- B: capture-traffic: This is not a valid Cisco FTD CLI command.

- C: capture: This is incomplete and would require additional parameters (like WORD) to function correctly.

Question: 74 Which report template field format is available in Cisco FMC?

A.box lever chart
B.arrow chart
C.bar chart
D.benchmark chart

Answer: C

Explanation:

C. bar chart.

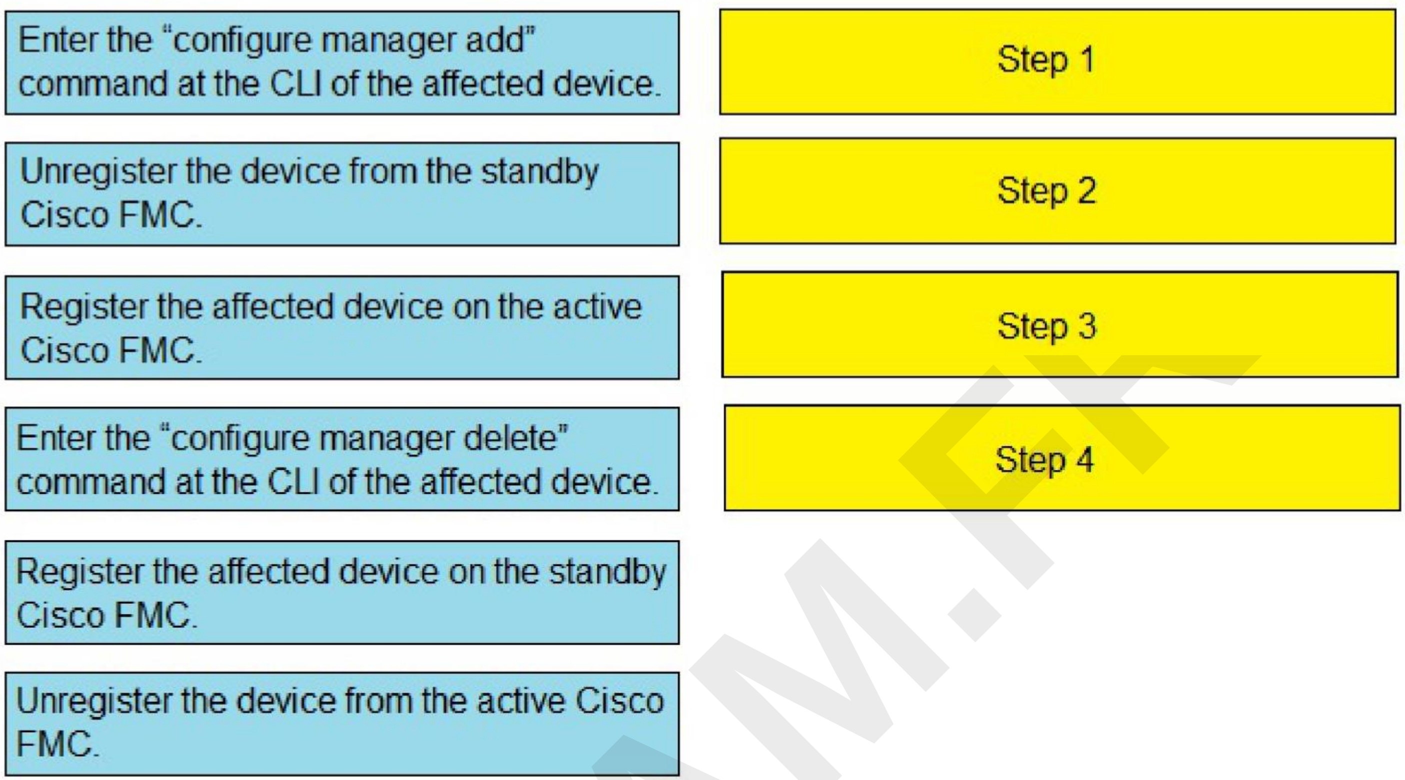
In Cisco FMC, the bar chart format is one of the available field formats in report templates. It allows data to be visualized in a clear and concise manner, making it easier to interpret trends and compare metrics.

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

Question: 75 DRAG DROP -

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.

Select and Place:



Enter the "configure manager add" command at the CLI of the affected device.

Unregister the device from the standby Cisco FMC.

Register the affected device on the active Cisco FMC.

Enter the "configure manager delete" command at the CLI of the affected device.

Register the affected device on the standby Cisco FMC.

Unregister the device from the active Cisco FMC.

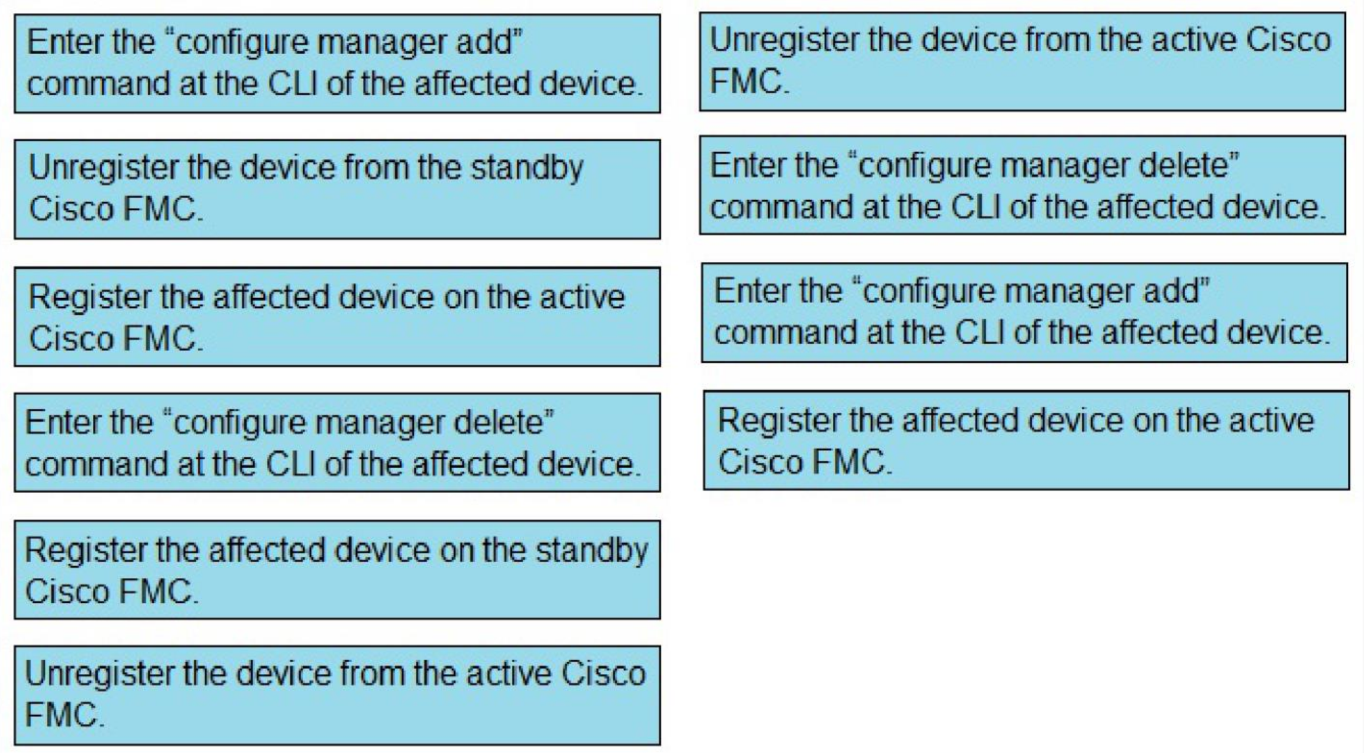
Step 1

Step 2

Step 3

Step 4

Answer:



Enter the “configure manager add” command at the CLI of the affected device.

Unregister the device from the standby Cisco FMC.

Register the affected device on the active Cisco FMC.

Enter the “configure manager delete” command at the CLI of the affected device.

Register the affected device on the standby Cisco FMC.

Unregister the device from the active Cisco FMC.

Unregister the device from the active Cisco FMC.

Enter the “configure manager delete” command at the CLI of the affected device.

Enter the “configure manager add” command at the CLI of the affected device.

Register the affected device on the active Cisco FMC.

Explanation:

Unregister the device from the active Cisco FMC.

First, remove the device registration from the active FMC.

Enter the configure manager delete command at the CLI of the affected device.

On the device (e.g., FTD), remove the FMC manager settings completely.

It deletes the trusted relationship.

Enter the configure manager add command at the CLI of the affected device.

Now, add back the FMC manager settings.

Typically you'll point the device to the active FMC's IP address.

Register the affected device on the active Cisco FMC.

From the FMC console, you now re-register the device.

The FMC will send configuration and policy.

Reference:
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

Question: 76

Which CLI command is used to generate firewall debug messages on a Cisco Firepower?

A.system support firewall-engine-debug
B.system support ssl-debug
C.system support platform

D.system support dump-table

Answer: A

Explanation:

A. system support firewall-engine-debug.

The command system support firewall-engine-debug is specifically used to generate and display detailed firewall debug messages on a Cisco Firepower device. This command helps in troubleshooting and analyzing firewall operations effectively.

Reference:

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

Question: 77

Which command-line mode is supported from the Cisco FMC CLI?

A.privileged
B.user
C.configuration
D.admin

Answer: C

Explanation:

Reference:

https://www.cisco.com/c/en/us/td/docs/security/firepower/660/configuration/guide/fpmc-config-guide-v66/command_line_reference.pdf

Question: 78

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: D

Explanation:

D. sudo sf_troubleshoot.pl.

The sudo sf_troubleshoot.pl command is used in the Cisco FMC CLI to generate a troubleshooting file. This file collects diagnostic information about the system, which is useful for analyzing and resolving issues within the Cisco FMC environment.

Reference:
https://www.cisco.com/c/en/us/support/docs/security/sourcefire-defense-center/117663-technote-SourceFire-00.html

Question: 79

Which CLI command is used to control special handling of ClientHello messages?

A.system support ssl-client-hello-tuning
B.system support ssl-client-hello-display
C.system support ssl-client-hello-force-reset
D.system support ssl-client-hello-reset

Answer: A

Explanation:

A. system support ssl-client-hello-tuning.

This command allows administrators to control and fine-tune the special handling of ClientHello messages in SSL/TLS communications on Cisco Firepower. It's particularly useful for troubleshooting and optimizing SSL/TLS-related traffic flows.

Reference:
https://www.cisco.com/c/en/us/td/docs/security/firepower/610/configuration/guide/fpmc-config-guide-v61/firepower_command_line_reference.html

Question: 80

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: D

Explanation:

D. configure high-availability suspend.

This command is used on the primary Cisco FTD unit to temporarily suspend high-availability operations. It allows the administrator to pause HA functionality without fully disabling it, which can be useful for maintenance or troubleshooting purposes.