PassQueen
a.k.a dumpsqueen.com

Securing Networks with Cisco Firepower (300-710 SNCF)

Cisco 300-710

Version Demo

Total Demo Questions: 54

Total Premium Questions: 545

Buy Premium PDF

https://passqueen.com

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, Deployment	164
Topic 2, Configuration	158
Topic 3, Policies	126
Topic 4, Services	96
Topic 5, Mix Questions	1
Total	545

QUESTION NO: 1

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.)

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:

`manage_procs.pl` and `sudo stats_unified.pl` are the appropriate commands when troubleshooting an FMC-to-FTD communication problem involving missing heartbeats and events. The management connection depends on Secure Firewall services that maintain the encrypted management tunnel and process status/event communications. `manage_procs.pl` is used from the expert shell to manage Secure Firewall processes; it enables the engineer to restart or otherwise recover the relevant communication processes so the FMC and FTD can establish their secure management channel again. This is the operational action needed when a service is stalled or has lost its connection state.

`sudo stats_unified.pl` provides the status and statistics needed to validate the Unified/Secure Firewall service processing after recovery. It allows the engineer to confirm that the relevant services are functioning and that management and event-related communications are again being handled normally. Used together, these commands support service recovery and post-recovery verification for the FMC-managed device relationship, which is essential before expecting health-monitor heartbeats and event delivery to resume. Cisco documents Secure Firewall diagnostic and process-management procedures in its Secure Firewall Command Reference and FMC communication troubleshooting guidance in the Secure Firewall Management Center Troubleshooting Guide.

QUESTION NO: 2

A network engineer is configuring URL Filtering on Firepower Threat Defense. Which two port requirements on the Firepower Management Center must be validated to allow communication with the cloud service? (Choose two.)

A. outbound port TCP/443

B. inbound port TCP/80

C. outbound port TCP/8080

D. inbound port TCP/443

E. outbound port TCP/80

ANSWER: A E

Explanation:

URL Filtering requires the Firepower Management Center to initiate connections to Cisco's cloud-based URL categorization and reputation service. Therefore, the required firewall validation is for outbound connectivity from the Firepower Management Center, rather than unsolicited inbound access. The service communication requirements include **outbound port TCP/443**, which provides encrypted HTTPS connectivity for cloud-service queries and related secure exchanges. They also include **outbound port TCP/80**, which is required for HTTP-based communication used by the cloud-service workflow and associated access requirements documented for Firepower Management Center internet connectivity. These ports must be permitted from the Firepower Management Center management interface or from the applicable routed path through any

intervening firewall, proxy, or egress-control device. If an organization uses restrictive outbound policy rules, allowing these TCP destinations is necessary so URL lookups can reach the Cisco cloud service and URL Filtering can categorize requested sites as intended. Cisco documents the required internet-access and communication ports for Firepower Management Center at Cisco Firepower Management Center Configuration Guide: Internet Access and Communication Ports. Additional URL Filtering configuration context is available in the Cisco Secure Firewall Management Center URL Filtering documentation.

QUESTION NO: 3

A network engineer is planning on replacing an Active/Standby pair of physical Cisco Secure Firewall ASAs with a pair of Cisco Secure Firewall Threat Defense Virtual appliances. Which two virtual environments support the current High Availability configuration? (Choose two.)

A. KVM

B. Azure

C. ESXi

D. AWS

E. Openstack

ANSWER: C D

Explanation:

ESXi and **AWS** support the Cisco Secure Firewall Threat Defense Virtual active/standby High Availability configuration. On VMware ESXi, two FTDv devices can be paired so that one device actively processes traffic while the peer is ready to take over. The HA pair exchanges state and health information through its configured failover and state-link interfaces, allowing the standby unit to assume the active role when a failure is detected. VMware deployments must also meet the documented virtual-switch, port-group, and interface requirements for FTDv HA.

AWS also supports an FTDv HA deployment. The implementation uses separate FTDv instances and AWS networking constructs, with the required interfaces and routing designed so that traffic can be redirected to the active firewall after a failover. This provides firewall redundancy in an AWS virtual private cloud while preserving the active/standby operating model required by the scenario. Cisco documents platform-specific HA prerequisites and deployment considerations, so the selected environment's release-specific FTDv guide should always be used during implementation. See Cisco's FTDv High Availability documentation and the FTDv virtual deployment overview.

QUESTION NO: 4

A network engineer wants to disable the HTTP response page and interactive blocking of the entire access control policy in Cisco Secure Firewall Management Center. What must be

selected in Block Response Page and Interactive Block Response Page?

A. Custom

B. View

C. System

D. None

ANSWER: D

Explanation:

None must be selected for both *Block Response Page* and *Interactive Block Response Page* in the access control policy's advanced settings. These settings control whether Secure Firewall inserts an HTTP block-response page when it blocks web

traffic and whether it presents an interactive response mechanism for applicable connections. Selecting **None** disables the associated response-page behavior at the policy level, so blocked HTTP requests are denied without the configured block page or interactive blocking presentation being supplied by the firewall. This is appropriate when an organization wants blocking to occur silently, wants to avoid presenting information to end users, or uses another mechanism to communicate acceptable-use or access-denial information. The configuration is policy-wide, so the setting applies to rules in that access control policy unless a more specific supported configuration changes the applicable behavior. Cisco's Secure Firewall Management Center documentation describes response-page configuration as part of access control policy advanced settings and identifies the available response-page choices, including disabling them. See the Cisco Secure Firewall Management Center access-control advanced settings documentation and the Cisco Secure Firewall access control configuration guide.

QUESTION NO: 5

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

A. FMC CLI

B. FTD CLI

C. FXOS CLI

D. FMC GUI

ANSWER: C

Explanation:

FXOS CLI is correct because EtherChannel configuration on a Firepower 9300 is a chassis-level function. The Firepower 9300 runs Cisco Firepower eXtensible Operating System (FXOS), which owns and configures the physical Ethernet interfaces, their port-channel membership, speed, and link-aggregation characteristics. An administrator creates the port channel in FXOS, adds the relevant physical interfaces to it, and then presents or assigns that aggregated interface to the applicable logical device. This architecture applies before the FTD logical device uses the interface for data-plane connectivity and before FMC centrally deploys FTD policy and device configuration. In a high-availability design, the corresponding chassis-side connectivity must be consistently built on each appliance so that the FTD HA pair can use equivalent interfaces. Cisco documents Firepower 9300 chassis and interface administration under FXOS, including the configuration of port channels and interface resources. See Cisco's FXOS Interfaces Configuration Guide and the Firepower 9300 support documentation for platform-specific configuration guidance.

QUESTION NO: 6

A network administrator is reviewing a weekly scheduled attacks risk report and notices a host that is flagged for an impact 2 attack. Where should the administrator look within Cisco FMC to find out more relevant information about this host and attack?

A. Analysis > Lookup > Whols

B. Analysis > Correlation > Correlation Events

C. Analysis > Hosts > Vulnerabilities

D. Analysis > Hosts > Host Attributes

ANSWER: C

Explanation:

Analysis > Hosts > Vulnerabilities is the appropriate FMC location because the host vulnerability view correlates host-specific discovery data, including operating-system and application details, with vulnerabilities identified as relevant to that host. When an attacks risk report identifies an impact-level attack, the administrator needs to investigate the affected asset in

the context of its exposure and the vulnerabilities that could make the attack significant. The Vulnerabilities page provides the host-focused information needed to assess that relationship, such as applicable vulnerability records and associated host details. This supports prioritizing remediation and determining whether the observed attack targets a known weakness on the flagged system. Cisco FMC host discovery and vulnerability information is designed to provide this asset and vulnerability context for intrusion-related investigation, rather than merely presenting a high-level report result. Review Cisco's Secure Firewall Management Center documentation and the Firepower Management Center user guide library for the applicable FMC release and detailed host-vulnerability workflow.

QUESTION NO: 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: A B

Explanation:

High availability for a Cisco Secure Firewall Threat Defense device is supported when the device is deployed in either transparent or routed mode. In both cases, two compatible devices can be configured as an active/standby failover pair. The peers synchronize essential configuration and operational state information, allowing the standby unit to take over traffic forwarding if the active unit fails. This design reduces service disruption while retaining the deployment model appropriate for the network: transparent mode provides Layer 2-style, inline inspection without requiring the firewall to act as an IP hop, while routed mode forwards traffic at Layer 3 and commonly serves as a security routing boundary between networks.

Cisco documents that Threat Defense high availability uses active/standby pairs and supports both routed and transparent firewall modes. Proper HA implementation also requires compatible hardware and software, correctly connected failover and state links, and matching interface and licensing considerations. For configuration details and platform-specific requirements, see Cisco's High Availability for Firewall Devices documentation and the Secure Firewall Threat Defense Command Reference.

QUESTION NO: 8

A security engineer must add a new policy to block UDP traffic to one server. The engineer adds a new object. Which action must the engineer take next to identify all the UDP ports?

A. Define the transport protocol and the mandatory port range.

B. Add the transport number and specify the type and code.

C. Add the corresponding IP protocol number for UDP and TCP.

D. Specify the transport protocol and leave the port number empty.

ANSWER: D

Explanation:

Specify the transport protocol and leave the port number empty. is correct because a Cisco Secure Firewall port object can be defined by protocol without restricting it to one or more individual port values. Selecting UDP identifies the Layer 4 transport protocol to which the object applies, and leaving the port field empty represents all UDP destination ports. The resulting object can then be used in an access-control rule whose destination is the specified server, causing the rule to match UDP traffic regardless of its destination port. This is the appropriate configuration when the requirement is to block

every UDP-based service on that server, rather than only selected services such as DNS or NTP. Cisco Secure Firewall object management separates the protocol selection from optional port constraints; the absence of a port constraint is what allows the object to encompass the full UDP port space. The access-control policy can therefore make the intended decision using the server network object together with this UDP-wide port object. See Cisco's Secure Firewall port object documentation and access control rule documentation.

QUESTION NO: 9

An engineer is investigating connectivity problems on Cisco Firepower that is using service group tags. Specific devices are not being tagged correctly, which is preventing clients from using the proper policies when going through the firewall How is this issue resolved?

A. Use traceroute with advanced options.

B. Use Wireshark with an IP subnet filter.

C. Use a packet capture with match criteria.

D. Use a packet sniffer with correct filtering

ANSWER: C

Explanation:

Use a packet capture with match criteria. A targeted capture is the appropriate Firepower troubleshooting method because it isolates the affected client flows without collecting unrelated traffic. Match criteria can focus collection on the relevant source or destination address, protocol, and port, allowing the engineer to correlate the exact connection with the security-group-tag information and policy processing observed for that traffic. This makes it practical to verify whether packets from the affected endpoints reach the firewall as expected and to gather evidence needed to correct the tag-to-identity or policy mapping that is causing the improper handling.

In Secure Firewall management workflows, traffic captures are intended for focused diagnosis of connection and inspection behavior. Limiting the capture to the impacted flow reduces noise, avoids an unnecessarily large capture file, and provides a repeatable test after the tagging configuration is corrected. Cisco documents traffic-capture configuration and analysis in the Secure Firewall Management Center traffic capture documentation. Cisco also describes Security Group Tag policy use and identity-based access control in its identity policy documentation.

QUESTION NO: 10

An organization recently implemented a transparent Cisco FTD in their network. They must ensure that the device does not respond to insecure SSL/TLS protocols. Which action accomplishes this task?

A. Modify the device's settings using the device management feature within Cisco FMC to force only secure protocols.

B. Use the Cisco FTD platform policy to change the minimum SSL version on the device to TLS 1.2.

C. Enable the UCAPL/CC compliance on the device to support only the most secure protocols available.

D. Configure a FlexConfig object to disable any insecure TLS protocols on the Cisco FTD device.

ANSWER: B

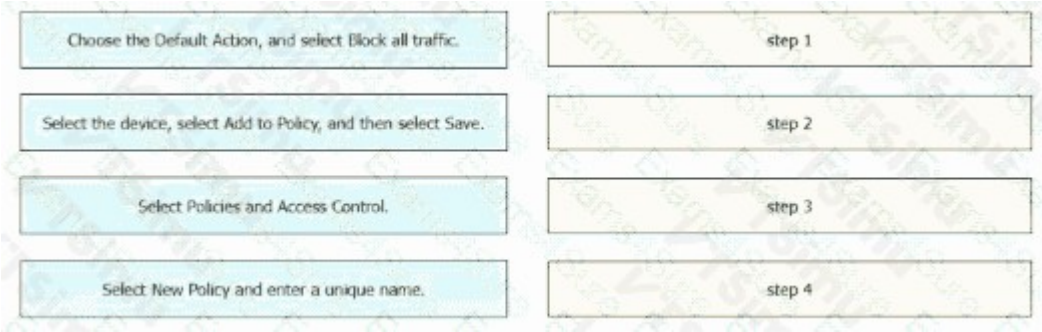
Explanation:

Use the Cisco FTD platform policy to change the minimum SSL version on the device to TLS 1.2. A platform settings policy centrally defines device-level behavior for managed Secure Firewall Threat Defense devices, including the SSL/TLS settings used by the device's management-facing services. Setting the minimum permitted SSL/TLS version to TLS 1.2 prevents the device from negotiating older protocol versions, such as SSLv3, TLS 1.0, and TLS 1.1, when clients connect to applicable FTD services. This directly meets the requirement that the transparent FTD not respond using insecure SSL/TLS protocols. Transparent versus routed deployment does not change where this control is configured; it remains a device platform setting

assigned through Secure Firewall Management Center. TLS 1.2 is an appropriate minimum where interoperability requirements permit it because it removes legacy protocol versions with known cryptographic weaknesses and aligns with common enterprise security baselines. Cisco documents platform settings policies as the mechanism for configuring device-wide settings and describes the SSL/TLS controls available for managed FTD devices. See the Cisco Secure Firewall Management Center Device Configuration Guide and Cisco's Secure Firewall Threat Defense configuration guides.

QUESTION NO: 11 - (DRAG DROP)

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



ANSWER:



Explanation:

A Cisco Secure Firewall Management Center access control policy is created from the policy-navigation workflow. The engineer first opens **Policies** and then **Access Control**, which displays the area used to create and manage access control policies. From there, selecting **New Policy** begins the policy-creation process and requires a unique policy name so the new policy can be identified and managed within the deployment.

The policy's default action is then set to **Block all traffic**. This establishes a deny-by-default posture: traffic does not match an allow decision unless the administrator later adds an access control rule that explicitly permits the intended traffic. This is the appropriate baseline for a basic restrictive policy because the default action handles packets that reach the end of policy evaluation without matching a preceding rule.

After the policy settings are defined, the managed firewall device is selected and added to the policy. Saving completes the creation and device association so that the policy is available for deployment to that device. Cisco documents access control policy configuration, including default actions and policy assignment, in the Cisco Secure Firewall Management Center access control documentation. Cisco's procedure for creating an access control policy also describes creating the policy, configuring its behavior, and associating it with target devices.

QUESTION NO: 12

An organization has a Cisco IPS running in inline mode and is inspecting traffic for malicious activity. When traffic is received by the Cisco IPS, if it is not dropped, how does the traffic get to its destination?

A. It is retransmitted from the Cisco IPS inline set

B. The packets are duplicated and a copy is sent to the destination

C. It is transmitted out of the Cisco IPS outside interface

D. It is routed back to the Cisco ASA interfaces for transmission

ANSWER: A

Explanation:

In an inline deployment, the Cisco IPS is physically and logically in the forwarding path. Traffic enters one member of an inline interface pair, is inspected by the sensor's detection and prevention engines, and is then forwarded through the paired inline interface when no configured action blocks it. Thus, *It is retransmitted from the Cisco IPS inline set* accurately describes normal forwarding behavior: the IPS itself receives the packet, makes the enforcement decision, and sends permitted traffic onward toward its destination. An inline set is designed to bridge traffic between its paired sensing interfaces while allowing the IPS to drop malicious packets before they continue through the network. This differs from a passive monitoring design, where the IPS receives a copied packet rather than forwarding the production packet. Cisco's IPS documentation describes inline interface pairs as the mechanism used to place a sensor directly in the traffic flow and permit or prevent traffic based on inspection results. See Cisco's Intrusion Prevention System configuration guides and the Cisco Intrusion Prevention System product documentation for inline deployment concepts.

QUESTION NO: 13

An engineer wants an FTD static default route to be removed automatically when an ISP next hop becomes unreachable. Which two configuration tasks are required? (Choose two.)

A. Configure an SLA monitor.

B. Associate the SLA monitor with the static route.

C. Configure a BGP route reflector.

D. Enable transparent firewall mode.

E. Create a Security Intelligence network feed.

ANSWER: A B

Explanation:

An **SLA monitor** must be configured to test reachability of a reliable destination through the ISP path. The monitor sends probes and determines whether the specified target remains reachable by using the configured interface and next hop.

The SLA monitor must then be **associated with the static route**. When the monitored destination becomes unreachable, FTD can remove the tracked route from the routing table and allow a backup route to be selected. When reachability is restored, the tracked route can be installed again. Cisco documents SLA monitoring and static-route tracking in the Secure Firewall routing documentation.

QUESTION NO: 14

An engineer configures a network discovery policy on Cisco FMC. Upon configuration, it is noticed that excessive and misleading events filing 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 configurationchange must be made to alleviate this issue?

A. Leave default networks.

B. Change the method to TCP/SYN.

C. Increase the number of entries on the NAT device.

D. Exclude load balancers and NAT devices.

ANSWER: D

Explanation:

Exclude load balancers and NAT devices. Cisco FMC network discovery is designed to build host profiles from observed network activity. NAT devices can obscure the identity of the real endpoints because many hosts and connections may be represented through translated addresses. When a monitored NAT device generates frequent operating-system update traffic, discovery can interpret the rapidly changing connections and application observations as numerous host changes. This can create a large volume of misleading discovery events and unnecessary database records, which in turn increases FMC processing and storage load.

Excluding NAT devices from the network discovery policy prevents their translated, aggregated traffic from being used to create or update discovery host data. Cisco also recommends excluding load balancers for the same general reason: they can represent or distribute traffic for many backend hosts, making discovery results inaccurate or excessively noisy. The exclusion keeps discovery focused on networks where observed addresses and attributes more reliably represent individual hosts, reducing event volume while preserving useful host profiling for the intended monitored environment. See Cisco's Network Discovery Policies documentation and the Secure Firewall Management Center network discovery guide.

QUESTION NO: 15

An engineer must configure a Cisco FMC dashboard in a multidomain deployment Which action must the engineer take to edit a report template from an ancestor domain?

A. Add it as a separate widget.

B. Copy it to the current domain

C. Assign themselves ownership of it

D. Change the document attributes.

ANSWER: B

Explanation:

Copy it to the current domain is correct. In a Cisco Secure Firewall Management Center multidomain deployment, descendant domains can use objects and report templates that are inherited from ancestor domains, which supports centralized administration and consistent reporting. However, an inherited template remains owned and controlled by the domain in which it was originally created. A user working in a descendant domain cannot directly modify that ancestor-owned template because changes to it could affect how the shared item is used elsewhere in the domain hierarchy.

To customize the report for the current domain, the engineer must create a local copy of the inherited report template. The copied template belongs to the current domain and can then be edited to alter report content, sections, scheduling, or other template settings without modifying the ancestor-domain template. This preserves inheritance boundaries while allowing domain-specific reporting requirements. Cisco documents that shared configurations in multidomain environments are inherited downward and that domain administrators can copy inherited report templates for local modification. See Cisco's Secure Firewall Management Center report documentation and its multidomain management documentation.

QUESTION NO: 16

Which two routing options are valid with Cisco Firepower Threat Defense? (Choose two.)

A. BGPv6

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

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

D. BGPv4 in transparent firewall mode

E. BGPv4 with nonstop forwarding

ANSWER: A B

Explanation:

Cisco Firepower Threat Defense supports IPv6 dynamic routing with BGPv6 when BGP is configured as a virtual router routing protocol. This enables the device to establish IPv6 BGP peerings and exchange IPv6 network-layer reachability information, subject to the platform, software release, and licensing requirements applicable to the deployment. Cisco documents BGP support as part of the FTD virtual-router routing configuration.

FTD also supports equal-cost multipath routing for static routes. A maximum of three equal-cost static routes can be configured for a destination network, and the equal-cost routes use different egress interfaces. This provides path sharing and redundancy when multiple next hops have the same administrative distance and metric. Therefore, *BGPv6* and *ECMP with up to three equal cost paths across multiple interfaces* are valid routing capabilities. See Cisco's Secure Firewall Management Center routing documentation and the FTD command reference for BGP and routing-command support.

QUESTION NO: 17

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

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

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

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

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

E. reputation-based objects, such as URL categories

ANSWER: B C

Explanation:

Cisco FMC supports reusable objects so that commonly used match criteria can be defined once and consistently referenced across policies and configurations. The supported network-based object category includes objects used to identify network traffic and endpoints, including IP addresses and networks, port and protocol criteria, VLAN tags, security zones, and geographic locations used for source or destination country matching. These objects can be selected in access-control, NAT, and other policy contexts, reducing duplication and simplifying policy maintenance.

Cisco FMC also supports reputation-based objects for policy matching that depends on threat intelligence, application reputation or classification, and file characteristics. This category includes Security Intelligence feeds and lists, application filters that can be built from application category and risk/reputation attributes, and file lists used in file-policy processing. Reusing these objects allows changes to an intelligence source, application grouping, or file definition to propagate wherever that object is referenced. Cisco documents reusable objects as a core FMC configuration feature and describes the network, Security Intelligence, application-filter, and file-list object types in its object-management guidance. See the Cisco Firepower Management Center reusable objects documentation and the Cisco Secure Firewall Management Center object documentation.

QUESTION NO: 18

An engineer is working on a LAN switch and has noticed that its network connection to the inline Cisco IPS has gone down. Upon troubleshooting, it is determined that the switch is working as expected. What must have been implemented for this failure to occur?

A. The upstream router has a misconfigured routing protocol.

B. Link-state propagation is enabled.

C. The Cisco IPS has been configured to be in fail-open mode.

D. The Cisco IPS is configured in detection mode.

ANSWER: B

Explanation:

Link-state propagation is enabled. In an inline Cisco IPS deployment, traffic normally passes through a paired set of sensing interfaces positioned between network devices. Link-state propagation is an availability and fault-signaling feature that couples the operational state of the two interfaces in an inline pair. If the IPS detects that the link on one side of the pair has failed, it deliberately brings down the link state on the paired interface as well. This action makes the device connected to the still-physical side, such as the LAN switch in this scenario, detect a link failure rather than continue forwarding toward an unavailable path.

Accordingly, a switch reporting that its connection to an otherwise functioning inline IPS is down is the expected visible effect when link-state propagation has been configured and the IPS has detected a failure on the opposite interface or path. Propagating the state allows adjacent network equipment and routing or switching designs to react quickly to the loss of end-to-end inline connectivity, including selecting an alternate path where one exists. Cisco documents link-state propagation as a setting for inline interface pairs that propagates a link-down condition from one interface to its paired interface. See the Cisco IPS Interface Configuration Guide and Cisco Intrusion Prevention System documentation.

QUESTION NO: 19

Refer to the exhibit.

A systems administrator conducts a connectivity test to their SCCM server from a host machine and gets no response from the server. Which action ensures that the ping packets reach the destination and that the host receives replies?

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

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

C. Modify the Snort rules to allow ICMP traffic.

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

ANSWER: A

Explanation:

Create an access control policy rule that allows ICMP traffic. is the appropriate action because access control policy rules are the primary mechanism Cisco Secure Firewall Threat Defense uses to permit or block traffic flows. The rule should match the relevant source host or network, the SCCM server as the destination, and ICMP as the protocol or application criteria, then use an Allow action. It must also be positioned above any broader blocking rule so that the ICMP echo request is evaluated against the permit rule before an implicit or explicit deny can apply.

When the firewall permits the ICMP echo request, it tracks the exchange so the corresponding ICMP echo reply can return to the initiating host. This provides the complete ping test: the request reaches the SCCM server and the reply is delivered back through the firewall. Access control rules are evaluated for traffic entering the device, and rule order is therefore essential when a policy includes more general restrictions. Cisco documents access control policy behavior and rule matching in the Secure Firewall Management Center Device Configuration Guide. Cisco also describes configuration and ordering of access control rules.

QUESTION NO: 20

An engineer must configure the firewall to monitor traffic within a single subnet without increasing the hop count of that traffic. How would the engineer achieve this?

A. Configure Cisco Firepower as a transparent firewall

B. Set up Cisco Firepower as managed by Cisco FDM

C. Configure Cisco Firepower in FXOS monitor only mode.

D. Set up Cisco Firepower in intrusion prevention mode

ANSWER: A

Explanation:

Configure Cisco Firepower as a transparent firewall is correct because transparent mode deploys the firewall as a Layer 2 bridge rather than as a routed Layer 3 hop. Hosts on either side of the appliance can remain in the same IP subnet and retain their existing default gateway configuration. The firewall forwards frames between its bridge-member interfaces while applying access-control, intrusion, and other configured inspection policies inline. As a result, traffic can be inspected and controlled without introducing a routed network boundary or requiring an additional IP hop in the traffic path.

This deployment is particularly appropriate when an engineer must insert Firepower into an existing segment with minimal addressing and routing changes, including a segment in which endpoints use the same subnet. The transparent firewall still needs a management address for administration, but its data interfaces operate as a bridge group for the protected traffic. Cisco describes transparent mode as a Layer 2 deployment model that allows the firewall to be placed between two Layer 3 devices without requiring changes to their IP addressing. See Cisco's Transparent or Routed Firewall Mode documentation and the Cisco Secure Firewall transparent mode reference.

QUESTION NO: 21

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: B E

Explanation:

Cisco FTD supports equal-cost multipath routing by installing as many as three equal-cost routes for the same destination when those routes use separate egress interfaces. Therefore, *ECMP with up to three equal cost paths across multiple interfaces* is a supported routing option. ECMP provides path redundancy and can distribute traffic over the available equal-cost next hops, subject to normal flow-based forwarding behavior. Cisco documents the three-path limit and the requirement that the paths use different interfaces in its FTD routing configuration guidance.

BGPv4 with nonstop forwarding is also valid. FTD supports BGP version 4 for IPv4 routing, including Nonstop Forwarding support. NSF is intended to preserve forwarding continuity during a routing-process restart or control-plane recovery: forwarding can continue using the previously programmed forwarding information while BGP adjacency and route information are recovered. This capability is particularly useful where routing resiliency is required and is part of the supported BGPv4 functionality described for the platform.

See Cisco's Firepower Management Center Configuration Guide: Routing for the FTD routing feature set, ECMP behavior, and BGP support details.

QUESTION NO: 22

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:

The option indicates whether the packet was dropped or successful. Enabling trace on a Cisco Secure Firewall packet capture adds packet-processing trace information to the capture. This information records the way the firewall handled a matching packet as it moved through relevant processing stages and provides the resulting disposition. As a result, an administrator can use the capture not only to inspect traffic on an interface, but also to determine whether the traffic was permitted to continue or was dropped during processing. This is especially useful when troubleshooting a connection that is present in a capture but does not reach its intended destination: the trace output supplies the firewall's processing outcome and helps correlate the observed packet with the device decision. Cisco's packet-capture documentation describes packet capture as a troubleshooting tool and includes trace as an advanced capture capability for examining how packets are processed. See the Cisco Secure Firewall Management Center packet capture documentation and the Cisco Secure Firewall capture command reference.

QUESTION NO: 23

An engineer must configure the Encrypted Visibility Engine in Cisco Secure Firewall Management Center. The engineer has already created an access control policy. Which two actions must be taken to complete the configuration? (Choose two.)

A. Configure an SSL/TLS policy.

B. Enable the Cisco Success Network.

C. Configure automatic updates for the Cisco Vulnerability Database.

D. Configure an identity policy for user identification.

E. Enable application detectors in the network discovery policy.

ANSWER: A E

Explanation:

Encrypted Visibility Engine uses metadata from TLS ClientHello messages, including TLS fingerprints, to identify applications traversing encrypted sessions without decrypting their payloads. To apply this capability in Secure Firewall Management Center, the access control policy must have an SSL/TLS policy associated with it. The SSL/TLS policy provides the encrypted-traffic policy context in which the system evaluates TLS flows and makes the handshake information available for encrypted-traffic analysis. The policy can be configured to inspect traffic without decrypting it, which preserves privacy while allowing fingerprint-based application identification.

Application detectors must also be enabled in the network discovery policy. These detectors supply the application-discovery functionality used to recognize and classify the application information derived from observed network traffic, including encrypted-flow visibility data. After the relevant SSL/TLS policy and network discovery policy are configured, they must be associated with the access control policy and deployed to the managed devices. This combination enables Secure Firewall to collect TLS handshake attributes and use Cisco-provided fingerprint intelligence to identify supported encrypted applications. Cisco documents the Encrypted Visibility Engine workflow and its policy requirements in the Secure Firewall Management Center SSL/TLS configuration guide and the Network Discovery configuration guide.

QUESTION NO: 24

An engineer is attempting to create a new dashboard within the Cisco FMC to have a single view with widgets from many of the other dashboards. The goal is to have a mixture of threat and security related widgets along with Cisco Firepower device health information. Which two widgets must be configured to provide this information? (Choose two).

A. Intrusion Events

B. Correlation Information

C. Appliance Status

D. Current Sessions

E. Network Compliance

ANSWER: A C

Explanation:

Intrusion Events provides the threat and security-focused portion of the consolidated FMC dashboard. This widget presents detected intrusion activity generated by the intrusion policy, enabling an administrator to quickly view and investigate security events from managed Firepower devices. It is therefore appropriate for a dashboard intended to bring together threat visibility with operational data.

Appliance Status provides Firepower device health information. It displays the operational status of managed appliances, allowing the engineer to monitor whether devices are healthy and available from the same custom dashboard used for security-event monitoring. Combining these widgets meets the requirement for both intrusion-related security insight and device-health visibility in a single FMC view.

Cisco FMC dashboards support adding widgets that summarize event and device information, while health monitoring supplies status data for managed devices. For further details, see Cisco's Dashboard documentation and Health Monitoring documentation.

QUESTION NO: 25

An organization must use geolocation criteria in a Cisco FMC access control rule to restrict traffic involving selected countries. Which two traffic characteristics can be matched by geolocation criteria? (Choose two.)

A. source country

B. destination country

C. source autonomous system number

D. destination MPLS label

E. client browser language

ANSWER: A B

Explanation:

Geolocation criteria can match the **source country** of traffic. FMC uses the source IP address to determine the associated country and can use that result as a condition in an access control rule. This is useful when connections originating from selected geographic regions must be blocked, monitored, or handled by a separate inspection policy.

Geolocation criteria can also match the **destination country**. The destination IP address is compared against the geolocation database, allowing an organization to control outbound connections to systems hosted in specified countries. Cisco documents country-based source and destination matching as part of access control rule configuration in the Secure Firewall access control rule components documentation.

QUESTION NO: 26

An engineer is configuring two new Cisco Secure Firewall Threat Defense appliances as a high-availability pair. The high-availability pair must detect a failure on the failover link and trigger failover more quickly. Which two settings must the engineer decrease? (Choose two.)

A. Interface poll time

B. Peer hold time

C. Interface failure limit

D. Peer poll time

E. Interface hold time

ANSWER: B D

Explanation:

Peer hold time and **Peer poll time** control the health monitoring performed directly between the two members of a Cisco Secure Firewall Threat Defense high-availability pair. Peer poll time is the interval at which an appliance sends health-check or polling traffic to its peer across the failover link. Reducing this interval makes the appliances check peer reachability more frequently. Peer hold time is the maximum period that an appliance can go without receiving the expected peer communication before it considers its peer failed. Reducing this value shortens the time required to declare the peer unavailable and initiate failover processing.

These two peer-specific timers therefore directly reduce the detection interval for a failure of the failover link or loss of peer responsiveness. Cisco documents peer monitoring as part of high-availability health monitoring and provides configurable peer polling and hold timers to tune failover sensitivity. The values should be lowered carefully: timers that are too aggressive can increase the chance of an unnecessary failover when the devices experience temporary congestion, packet loss, or high resource utilization. See Cisco's Secure Firewall Management Center high-availability documentation and the device high-availability monitoring documentation.

QUESTION NO: 27

An administrator is configuring their transparent Cisco FTD device to receive ERSPAN traffic from multiple switches on a passive port, but the Cisco FTD is not processing the traffic. What is the problem?

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

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

C. The Cisco FTD must be in routed mode to process ERSPAN traffic.

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

ANSWER: C

Explanation:

The Cisco FTD must be in routed mode to process ERSPAN traffic. ERSPAN encapsulates mirrored packets in GRE and sends them across an IP network from an ERSPAN source, such as a switch, to an ERSPAN destination. For FTD to decapsulate that GRE traffic and inspect the original mirrored packets, it must support the ERSPAN destination function on an interface operating in routed mode. Routed mode provides the Layer 3 interface behavior required for addressing and receiving the GRE-encapsulated ERSPAN stream.

A transparent-mode FTD is designed primarily to bridge traffic at Layer 2 between interface pairs or interface groups. Although transparent deployments can have management and diagnostic IP addressing, their data interfaces do not provide the routed ERSPAN-termination capability needed to receive and process an ERSPAN session. Therefore, sending ERSPAN traffic to a passive interface on a transparent FTD does not make the encapsulated traffic available for inspection. The deployment must instead use a routed-mode FTD and configure the appropriate ERSPAN destination interface and related policy configuration. Cisco documents ERSPAN configuration and its interface requirements in the Secure Firewall Management Center Device Configuration Guide; Cisco's interface-mode documentation is available in the interface modes guide.

QUESTION NO: 28

Which two statements about deleting and re-adding a device to Cisco FMC are true? (Choose two.)

A. An option to re-apply NAT and VPN policies during registration is available, so users do not need to re- apply the policies after registration is completed.

B. Before re-adding the device in Cisco FMC, you must add the manager back in the device.

C. No option to delete and re-add a device is available in the Cisco FMC web interface.

D. The Cisco FMC web interface prompts users to re-apply access control policies.

E. No option to re-apply NAT and VPN policies during registration is available, so users need to re-apply the policies after registration is completed.

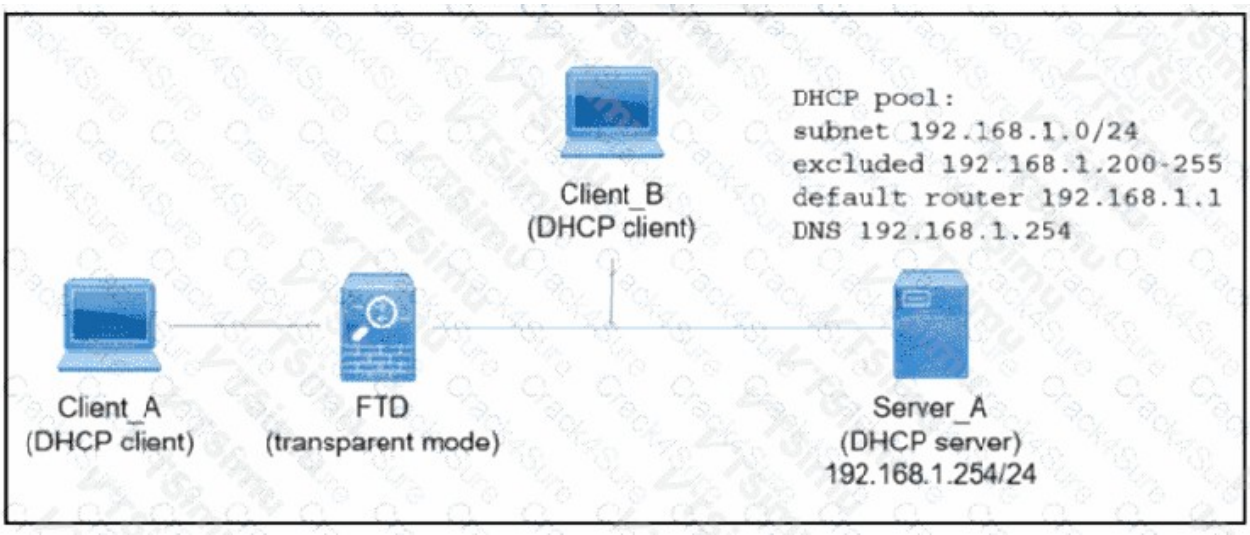
ANSWER: D E

Explanation:

When a managed device is deleted from Cisco Firepower Management Center and then registered again, FMC retains enough device-related policy association information to recognize that access control policy assignment needs attention. During the re-registration workflow, the FMC web interface prompts the administrator to re-apply the access control policy. This prompt is important because access control policy is the primary policy governing traffic inspection and handling on the managed device, and it must be deployed after reassociation for the device to enforce the intended configuration.

NAT and VPN policy handling differs during this delete-and-re-add process. FMC does not provide a registration-time option that automatically re-applies NAT and VPN policies. After registration is complete, the administrator must explicitly re-apply the relevant NAT and VPN policies and deploy the changes to the device. This ensures that policy deployment is intentional and that the administrator can verify the device's current interfaces, routing, objects, and policy requirements before restoring those configurations. Cisco documents this re-add workflow and the required policy reassociation behavior in its Firepower Management Center device-management guidance: Cisco Firepower Management Center Configuration Guide—Device Management Basics.

QUESTION NO: 29



Refer to the exhibit. An engineer is deploying a new instance of Cisco Secure Firewall Threat Defense. Which action must the engineer take next so that Client_A and Client_B receive an IP address via DHCP from Server_A?

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

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

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

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

ANSWER: B

Explanation:

Add access rules that allow DHCP traffic by using Cisco Secure Firewall Management Center. DHCP clients initially send broadcast requests, but when Secure Firewall Threat Defense is configured as a DHCP relay, it forwards the client request to the DHCP server as relay traffic and returns the server response to the client-facing network. The access-control policy must therefore permit the DHCP/BOOTP exchanges between the relevant client-side interface, relay, and Server_A network. In FMC, the engineer should use an access-control rule with the appropriate source and destination zones or networks and a DHCP service definition that permits UDP ports 67 and 68 as required for the relay workflow. The policy must be deployed to the managed Threat Defense device after the rule is added. This enables the DHCP relay configuration already present on the firewall to pass the client requests to Server_A and deliver the offered address and lease information back to Client_A and Client_B. Cisco's Secure Firewall documentation covers DHCP relay configuration and the associated policy requirements in the DHCP Relay documentation; rule creation and deployment are described in the Access Control documentation.

QUESTION NO: 30

A network engineer must provide redundancy between two Cisco FTD devices. The redundancy configuration must include automatic configuration, translation, and connection updates. After the initial configuration of the two appliances, which two steps must be taken to proceed with the redundancy configuration? (Choose two.)

A. Configure the virtual MAC address on the failover link.

B. Disable hellos on the inside interface.

C. Configure the standby IP addresses.

D. Ensure the high availability license is enabled.

E. Configure the failover link with stateful properties.

ANSWER: C E

Explanation:

Stateful high availability on Cisco FTD requires a dedicated failover link configured to carry stateful replication. The failover link supports the communication necessary for the active and standby peers to maintain high-availability status and to synchronize dynamic state. Enabling its stateful properties provides the connection and translation replication required by the scenario, allowing eligible active flows and NAT/xlate information to be maintained during a failover. Cisco refers to this as stateful failover, which supplements configuration synchronization with operational-state synchronization.

Each routed data interface participating in the high-availability pair must also have addressing for both members. Configuring standby IP addresses supplies the address used by the standby unit on each applicable interface, while the active unit uses the primary interface address. This interface-pair addressing is required for the two FTD devices to operate as an active/standby pair and transition roles correctly. Together, standby interface addressing and a stateful failover link establish the appliance redundancy configuration needed for configuration, translation, and connection updates. Cisco documents the high-availability design and configuration workflow in the Secure Firewall Management Center High Availability documentation and the high-availability configuration guide.

QUESTION NO: 31

Which two considerations must be made when deleting and re-adding devices while managing them via Cisco FMC (Choose two).

A. Before re-adding the device In Cisco FMC, the manager must be added back.

B. The Cisco FMC web interface prompts users to re-apply access control policies.

C. Once a device has been deleted, It must be reconfigured before it is re-added to the Cisco FMC.

D. An option to re-apply NAT and VPN policies during registration is available, so users do not need to re-apply the polices after registration is completed.

E. There is no option to re-apply NAT and VPN policies during registration is available, so users need to re-apply the policies after registration is completed.

ANSWER: B E

Explanation:

When a managed device is deleted and later registered again with Cisco FMC, its prior association with policies must be restored deliberately. Cisco FMC retains the access control policy association information for a deleted device and, when that device is re-added, the web interface prompts the administrator to reapply the relevant access control policy. This helps ensure that traffic inspection and enforcement return to the intended policy posture after the device is registered again. Administrators should treat this prompt as part of the re-registration workflow and deploy the policy after it is reapplied.

NAT and VPN policy assignments require separate attention. Cisco FMC does not provide a registration-time option that automatically reapplies NAT and VPN policies for a device that was deleted and then added back. After registration is complete, the administrator must explicitly reapply the appropriate NAT policy and any applicable VPN configuration, then deploy the resulting changes to the device. This distinction is important because access control policy restoration is handled through the re-add workflow, whereas NAT and VPN settings must be restored through their respective policy and configuration workflows. Cisco documents these device deletion and re-add considerations in its Secure Firewall Management Center device-management documentation and administration guide.

QUESTION NO: 32

When a Cisco FTD device is configured in transparent firewall mode, on which two interface types can an IP address be configured? (Choose two.)

A. Diagnostic

B. EtherChannel

C. BVI

D. Physical

E. Subinterface

ANSWER: A C

Explanation:

In transparent firewall mode, Cisco FTD forwards traffic at Layer 2 between interfaces assigned to the same bridge group, so the member data interfaces themselves do not require or use Layer 3 addressing for normal traffic forwarding. A BVI is the logical routed interface associated with a bridge group and is the appropriate location for an IP address. This address provides an in-band management or control-plane address for the transparent firewall and can be used for services such as device management and routing traffic generated by the firewall itself, subject to the deployment configuration. The Diagnostic interface is a separate physical interface intended for out-of-band diagnostic and management connectivity. It is not part of the transparent data path and can be assigned an IP address independently, allowing administrators to reach the device for troubleshooting or management even when normal bridge-group connectivity is unavailable. Cisco's Secure Firewall documentation identifies the Bridge Virtual Interface and the Diagnostic interface as the interfaces that can be addressed when transparent mode is used. See Cisco Secure Firewall interface modes documentation and Cisco Secure Firewall interface configuration documentation.

QUESTION NO: 33

A security engineer is adding three Cisco FTD devices to a Cisco FMC. Two of the devices have successfully registered to the Cisco FMC. The device that is unable to register is located behind a router that translates all outbound traffic to the router's WAN IP address. Which two steps are required for this device to register to the Cisco FMC? (Choose two.)

A. Reconfigure the Cisco FMC lo use the device's private IP address instead of the WAN address.

B. Configure a NAT ID on both the Cisco FMC and the device.

C. Add the port number being used for PAT on the router to the device's IP address in the Cisco FMC.

D. Reconfigure the Cisco FMC to use the device's hostname instead of IP address.

E. Remove the IP address defined for the device in the Cisco FMC.

ANSWER: B E

Explanation:

For an FTD device whose management traffic is translated by NAT, configure a NAT ID on both the FMC and the FTD device. The NAT ID is a shared, case-sensitive value used during the registration process to authenticate and associate the device when its source address is changed in transit. It allows FMC to recognize that the registering connection belongs to the intended managed device despite the router replacing the device’s private source IP address with its WAN address.

Remove the IP address defined for the device in the Cisco FMC. In this NAT deployment, FMC cannot reliably use the FTD’s original private address as the device-management address, because that address is not reachable across the translated path. Cisco’s NAT registration workflow requires the FMC-side device record to use the NAT ID without an IP address; the FTD then initiates the registration connection toward FMC. This is particularly important when the FTD is behind dynamic PAT, where the translated public address and source port are not suitable as a stable device address. Cisco documents NAT ID registration and the requirement to omit the device IP address in the FMC add-device workflow at Cisco Secure Firewall Management Center Device Management and Cisco Secure Firewall Threat Defense Management Commands.

QUESTION NO: 34

Which component simplifies incident investigation with Cisco Threat Response?

A. Cisco AMP client

B. local CVE database

C. Cisco Secure Firewall appliance

D. browser plug-in

ANSWER: D

Explanation:

The **browser plug-in** simplifies incident investigation by making Cisco Threat Response capabilities available while an analyst is viewing content in a web browser. It enables the analyst to submit an observable, such as an IP address, domain, URL, file hash, or email-related value, to Threat Response and immediately retrieve correlated context from integrated security telemetry and threat-intelligence sources. This reduces the manual effort of copying indicators between separate consoles and helps investigators pivot quickly among related observables, sightings, and enrichment data.

In practical incident-response workflows, browser-based investigation is valuable because many alerts, case records, webmail messages, and security portals already present potentially suspicious indicators as text or links. The extension supports an investigation workflow at that point of discovery, rather than requiring a separate local database or a particular endpoint or firewall component. Threat Response is designed to correlate information across Cisco security products and connected third-party tools, giving analysts a unified investigation view and helping them make informed triage decisions more efficiently. Cisco describes Threat Response integrations and investigation capabilities in its Cisco Threat Response developer documentation and provides product resources through the Cisco Threat Response support page.

QUESTION NO: 35

Which Cisco Secure Firewall Threat Defense interface mode must be deployed when implementing an IPS that must receive and retransmit all traffic unless the traffic is explicitly dropped?

A. Routed

B. Inline

C. Passive

D. Transparent

ANSWER: B

Explanation:

Inline is correct because an inline interface set places the Secure Firewall Threat Defense device directly in the traffic path. It uses two linked data interfaces: traffic enters one member of the set, is inspected by the device, and is sent out through the paired member. This makes the deployment appropriate for intrusion *prevention*, rather than monitoring alone, because the device has control over whether inspected traffic continues onward.

In this mode, traffic is normally retransmitted after inspection, preserving the intended network flow. However, if access control, intrusion prevention, file inspection, malware, or other configured security policy identifies traffic that must not be allowed, Secure Firewall Threat Defense can drop it before it leaves the paired interface. Cisco describes inline sets as operating similarly to a bump in the wire and identifies them as the interface arrangement used for inline IPS deployments. This directly fulfills the requirement that all traffic be received and retransmitted unless a policy explicitly drops it.

For Cisco's configuration and deployment details, see the Cisco Secure Firewall interface modes documentation and the Cisco inline sets documentation.

QUESTION NO: 36

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:

The `sudo sf_troubleshoot.pl` command is correct because it runs the Firepower Management Center troubleshooting collection script. When executed from the FMC command-line interface, the script gathers relevant diagnostic information from the appliance, including configuration details, system status, logs, and other support data needed to investigate operational issues. The resulting troubleshooting archive can be retrieved and supplied to Cisco Technical Assistance Center for analysis, or used by an administrator during structured fault isolation.

The command requires `sudo` because the collection process must access protected system files, service information, and logs that are not available to an unprivileged shell user. This is a purpose-built FMC support command rather than a command intended merely to display configuration or enter a different diagnostic environment. Cisco documents the troubleshooting-file collection procedure for Firepower Management Center in its support guidance: Cisco: Generate a Troubleshooting File from Firepower Management Center. Additional FMC administration and support documentation is available through the Cisco Firepower Management Center Maintenance Guides.

QUESTION NO: 37

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: A E

Explanation:

Bridge-group interfaces enable Cisco FTD to bridge traffic at Layer 2 while the appliance itself remains deployed in routed firewall mode. A Bridge Virtual Interface (BVI) provides the bridge group with a Layer 3 presence for management and services. The BVI address must use a subnet separate from the subnet used by hosts on the network being bridged. This separation prevents the BVI from becoming an ordinary endpoint in the bridged user subnet while still allowing the FTD to be addressed and managed through an appropriate routed path.

Because the member interfaces form one bridged Layer 2 segment, the networks directly attached on either side must belong to the same IP subnet. In practice, bridge-group members are commonly used when an FTD is inserted transparently between portions of an existing LAN without requiring hosts to change their default gateways or addressing. The bridge forwards frames between member interfaces, and the BVI remains logically distinct from that bridged host network. Cisco documents these bridge-group requirements, including the separate BVI subnet and same-subnet requirement for directly connected networks, in its Firepower Threat Defense configuration guidance: Cisco Firepower Management Center Configuration Guide.

QUESTION NO: 38

An organization is implementing Cisco FTD using transparent mode in the network. Which rule in the default Access Control Policy ensures that this deployment does not create a loop in the network?

A. ARP inspection is enabled by default.

B. Multicast and broadcast packets are denied by default.

C. STP BPDU packets are allowed by default.

D. ARP packets are allowed by default.

ANSWER: C

Explanation:

STP BPDU packets are allowed by default. is correct because a transparent Cisco FTD operates as a Layer 2 bridge between its interfaces. In a switched network, Spanning Tree Protocol prevents redundant Layer 2 paths from forming forwarding loops by exchanging Bridge Protocol Data Units. Allowing these control frames to traverse the transparent firewall lets the adjacent switches maintain a consistent spanning-tree topology and place redundant paths into the appropriate forwarding or blocking state. This is essential when a transparent firewall is inserted inline between switches or within a redundant switched design, because the firewall must not prevent the switches from detecting the topology through it. Cisco documents that transparent-mode deployments support the forwarding of STP BPDUs so that the firewall can participate safely in an environment protected by spanning tree. The access-control behavior for these packets therefore preserves the loop-prevention mechanism that the surrounding switching infrastructure relies on. See Cisco's Secure Firewall Management Center Device Configuration Guide and the Cisco transparent firewall mode configuration guidance for transparent-mode and bridging behavior.

QUESTION NO: 39

Which command is run at the CLI when logged in to an FTD unit, to determine whether the unit is managed locally or by a remote FMC server?

A. system generate-troubleshoot

B. show configuration session

C. show managers

D. show running-config | include manager

ANSWER: C

Explanation:

`show managers` is the appropriate FTD CLI command because it displays the device's management configuration and registration state. Its output identifies the configured manager, allowing an administrator to establish whether the firewall is under centralized management by a Firepower Management Center (FMC) or is operating with local management through Firepower Device Manager (FDM). When FMC management is configured, the command reports manager information such as the FMC address, registration status, and related connection details. This is particularly useful during onboarding and troubleshooting because the management plane can be verified directly from the FTD device, without relying on the FMC interface or making assumptions based on deployed policies.

Management mode is fundamental to FTD administration: an FMC-managed device receives most policy and configuration changes centrally, whereas a locally managed device is administered through its local FDM workflow. Cisco documents `show managers` in the FTD command reference as the command for viewing manager configuration and status. See the Cisco Secure Firewall Threat Defense Command Reference and Cisco's device management overview.

QUESTION NO: 40

An engineer is configuring URL filtering for a Cisco FTD device in Cisco FMC. Users must receive a warning when they access http:/ ' www.Dac ' additstte.corn with the option of continuing to the website if they choose to. No other websites should be blacked. Which two actions must the engineer lake to meet these requirements? (Choose two.)

A. On the HTTP Responses tab of the access control policy editor, set the Block Response Page to Custom.

B. On the HTTP Responses tab of the access control policy editor, set the Interactive Block Response Page to system-provided.

C. Configure the default action for the access control policy to Interactive Block.

D. Configure an access control rule that matches the Adult URL category and set the action to Interactive Block.

E. Configure an access control rule that matches a URL object for http://www.badadultsite.com and set the action to Interactive Block.

ANSWER: B E

Explanation:

Interactive blocking is designed for situations in which users should be warned before access is allowed. In an access control policy, an Interactive Block rule redirects an HTTP request to an interactive response page. That page presents the user with a warning and a choice to continue to the requested destination, which meets the requirement to allow an informed user override. Configuring the Interactive Block Response Page as system-provided on the HTTP Responses tab supplies the response page that FMC displays for this workflow. The system-provided page is sufficient when no organization-specific wording, branding, or custom instructions are required.

The access control rule must be scoped to a URL object containing `http://www.badadultsite.com` and use the Interactive Block action. A URL object provides the necessary specificity: only traffic matching that explicitly identified destination is handled by the interactive-block workflow. Combined with the policy's normal permissive handling for traffic

that does not match this rule, this ensures that the warning-and-continue experience is limited to the named website rather than being applied broadly. Cisco documents Interactive Block as an access-control action and describes HTTP response-page configuration in the FMC access control policy workflow. See the Cisco Secure Firewall Management Center URL Filtering documentation and the Cisco access control policy documentation.

QUESTION NO: 41

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

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: B E

Explanation:

Cisco FMC supports configuring OSPF virtual links and deploying that dynamic-routing configuration to managed Cisco FTD devices. A virtual link provides a logical connection through a non-backbone transit area so that an area border router can maintain the required connectivity to the OSPF backbone, Area 0. In FMC, the virtual-link definition includes the appropriate transit area and remote router ID, and it is included when the device configuration is deployed to FTD.

Cisco FMC also supports MD5 authentication for OSPF packets. MD5 authentication is configured as part of OSPF interface authentication settings and uses a key ID and shared key so participating OSPF neighbors can authenticate routing protocol traffic. This allows the deployed FTD configuration to validate OSPF packets received on the interface before accepting routing information, helping protect the routing domain from unauthorized adjacency formation and route updates. Cisco documents OSPF configuration and supported routing settings for FTD managed by FMC in the Secure Firewall Management Center Device Configuration Guide. Additional OSPF protocol behavior and authentication concepts are described in RFC 2328.

QUESTION NO: 42

Which two solutions are used to access and view aggregated log data from the firewalls using Cisco Security Analytics and Logging? (Choose two.)

A. Cisco Secure Network Analytics

B. Cisco Defense Orchestrator

C. Cisco Catalyst Center

D. Secure Cloud Analytics

E. Cisco Prime Infrastructure

ANSWER: A D

Explanation:

Cisco Security Analytics and Logging (SAL) centralizes and retains firewall event data in Cisco's cloud logging infrastructure, then makes the aggregated data available for investigation through Cisco security analytics products. **Cisco Secure Network Analytics** is one supported consumer of SAL data. It provides network-focused visibility and analytics, allowing security teams to investigate traffic behavior and events using the centrally collected log information. Cisco documents Secure Network Analytics as a network-detection-and-response platform that delivers broad telemetry visibility and security analytics.

Secure Cloud Analytics is also used to access and analyze the aggregated firewall logs supplied through SAL. It provides cloud-delivered visibility and threat detection capabilities, enabling analysts to review activity and investigate suspicious behavior without relying solely on individual firewall devices. Together, these solutions provide the analytics interfaces for the log data that SAL aggregates, supporting centralized operational visibility across protected environments. Cisco's product information for Secure Network Analytics and Secure Cloud Analytics describes their respective security-analytics capabilities and deployment models.

QUESTION NO: 43

Which two Security Intelligence policy elements can be used by Cisco FTD to block malicious activity before access control rule evaluation? (Choose two.)

A. network lists and feeds

B. DNS lists and feeds

C. intrusion rule groups

D. routing policy maps

E. SSL cipher suites

ANSWER: A B

Explanation:

Network lists and feeds can contain IP addresses, networks, and CIDR blocks that FTD evaluates against the source and destination of a connection. When a connection matches a blocked network intelligence entry, the device blocks it before it reaches access control policy processing.

DNS lists and feeds provide domain-based Security Intelligence enforcement. The device can inspect DNS requests and deny requests for domains that match blocked intelligence entries. This prevents clients from resolving known malicious or unwanted domains before they can establish connections to the associated destinations. Cisco documents network and DNS Security Intelligence as early traffic-filtering mechanisms in the Secure Firewall Security Intelligence documentation.

QUESTION NO: 44

A software development company hosts the website http:dev.company.com for contractors to share code for projects they are working on with internal developers. The web server is on premises and is protected by a Cisco Secure Firewall Threat Defense appliance. The network administrator is worried about someone trying to transmit infected files to internal users via this site. Which type of policy must be able associated with an access control policy to enable Cisco Secure Firewall Malware Defense to detect and block malware?

A. SSL policy

B. Prefilter policy

C. File policy

D. Network discovery policy

ANSWER: C

Explanation:

File policy is correct because Cisco Secure Firewall Malware Defense requires file inspection to identify and control malware carried in transferred files. In Secure Firewall Management Center, a file policy defines the file types and directions to inspect and the action to take when a file is detected as malicious. The policy can use cloud-based malware lookup through Cisco Secure Malware Analytics and, where configured, file analysis to make a disposition decision. A file policy is associated with an access control rule in the access control policy, so matching web traffic is subjected to the selected file and malware inspection settings. For this internal web application, applying the file policy to the rule that permits the relevant

HTTP traffic allows the Threat Defense device to inspect files sent through the site and block those with a malicious disposition. The access control policy must then be deployed to the managed Threat Defense appliance for enforcement. Cisco documents file policies as the mechanism for configuring file control and malware cloud lookup/file-analysis behavior in access-control processing. See the Cisco Secure Firewall file policy documentation and the Cisco access control rule documentation.

QUESTION NO: 45

An engineer is configuring a Cisco Secure Firewall Threat Defense device to operate in transparent mode between two switch stacks. VLAN 10 is used for in-band management on both switch stacks. Which two actions are required on the device to inspect traffic between the switch stacks without interrupting network traffic? (Choose two.)

A. Configure a BVI interface for VLAN 10.

B. Configure at least one bridge group.

C. Exempt BPDUs from advanced inspection.

D. Set the MTU to 9198 on all interfaces to support jumbo frames.

E. Add separate routes for data and management traffic.

ANSWER: B C

Explanation:

Configure at least one bridge group because transparent-mode Cisco Secure Firewall Threat Defense forwards transit traffic at Layer 2 through a bridge group. The physical interfaces connected to the respective switch stacks are assigned to the same bridge group, creating the inline forwarding path on which the device can apply access-control, intrusion, and other inspection policies. This preserves the transparent deployment model: the firewall inspects frames crossing between the two sides while the switching infrastructure continues to use its existing VLAN design, including VLAN 10.

Exempt BPDUs from advanced inspection to preserve normal Spanning Tree Protocol operation while the firewall is inline between switch stacks. BPDUs carry topology and loop-prevention information and must be handled promptly and predictably. Cisco documents the use of an EtherType access list on bridge-group member interfaces to trust BPDU EtherType traffic, preventing inspection processing from interfering with control-plane frames essential to maintaining the switched topology. Together, bridge-group forwarding and BPDU exemption enable inspected transparent traffic flow without disrupting the Layer 2 network. See Cisco's FTD interface configuration guide and transparent-mode configuration documentation.

QUESTION NO: 46

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: B E

Explanation:

OSPF and BGP are the dynamic routing protocols that Cisco FTD supports through its native routing configuration, without requiring FlexConfig. OSPF can be configured to exchange routes dynamically with neighboring routers, with settings such as process ID, router ID, areas, interfaces, authentication, and route redistribution managed through the supported FTD

configuration workflow. BGP is also natively supported for dynamic interdomain route exchange and can be configured with an autonomous system number, neighbors, address families, route policies, and redistribution as appropriate for the deployment.

The key distinction in the question is that both protocols are dynamic: they learn and advertise routes based on protocol exchanges rather than relying solely on manually defined paths. Cisco documents OSPF and BGP as available routing capabilities in the FTD management interface, whereas FlexConfig is intended for cases where a required configuration is not exposed through the standard user interface. See Cisco's FTD Device Manager Routing Configuration Guide and the Secure Firewall Threat Defense Routing documentation for supported routing configuration details.

QUESTION NO: 47

An engineer is deploying failover capabilities for a pair of Cisco Secure Firewall devices. The core switch keeps the MAC address of the previously active unit in the ARP table. Which action must the engineer take to minimize downtime and ensure that network users keep access to the internet after a Cisco Secure Firewall failover?

A. Set the same MAC address on both units.

B. Add the MAC address to the switch ARP table.

C. Run a script to send gratuitous ARP after a failover.

D. Use a virtual MAC address on both units.

ANSWER: D

Explanation:

Use a virtual MAC address on both units. In an active/standby high-availability deployment, Cisco Secure Firewall assigns a virtual MAC address to each monitored data interface. The active device uses that interface's virtual MAC address when forwarding traffic. When a failover occurs, the newly active device assumes the same virtual MAC address rather than exposing its own unique physical interface MAC address. Consequently, adjacent network devices and endpoint ARP caches can continue sending frames to the MAC address already associated with the firewall's IP address. This avoids waiting for cached ARP information to age out and substantially reduces the traffic interruption that could otherwise occur during the role transition. The newly active firewall also sends gratuitous ARP messages as part of failover processing, helping refresh neighboring devices' IP-to-MAC mappings; the persistent virtual MAC is the key configuration that makes the address identity consistent across both peers. Cisco documents virtual MAC addressing as part of interface configuration for high availability and explains that it enables the standby unit to take over interface identity after failover. See the Cisco Secure Firewall high-availability documentation and Cisco's Secure Firewall configuration guide list.

QUESTION NO: 48

An organization does not want to use the default Cisco Firepower block page when blocking HTTP traffic. The organization wants to include information about its policies and procedures to help educate the users whenever a block occurs. Which two steps must be taken to meet these requirements? (Choose two.)

A. Edit the HTTP request handling in the access control policy to customized block

B. Modify the system-provided block page result using Python

C. Create HTML code with the information for the policies and procedures

D. Change the HTTP response in the access control policy to custom

E. Write CSS code with the information for the policies and procedures

ANSWER: C D

Explanation:

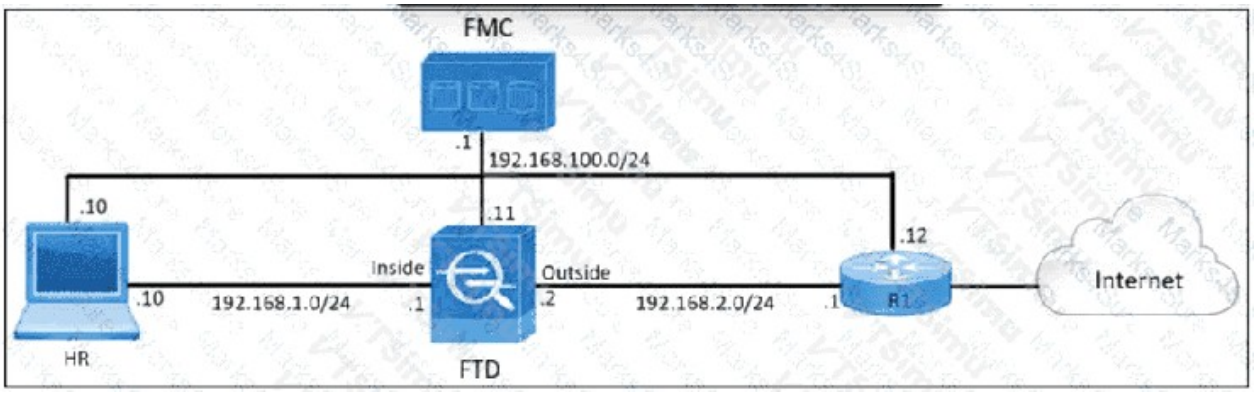
A custom HTTP response page must contain the organization-specific content that will be displayed to a user whose HTTP request is blocked. Creating HTML code with the policy and procedure information provides the content and layout for that page. The HTML can include explanatory text, links to acceptable-use guidance, and contact information so that the block event becomes an educational message rather than the standard system response.

The custom page must then be selected as the HTTP response behavior in the access control policy. Setting the HTTP response to custom associates the custom response page with traffic matched by the blocking rule, causing Firepower to return that organization-defined HTML page when it can issue an HTTP block response. This configuration applies to HTTP traffic because the device can inject an HTTP response only when it can inspect the applicable web request and response flow.

Cisco documents HTTP response pages as access-control policy components that can be customized and applied to rules. See the Cisco Secure Firewall Management Center guidance for HTTP response pages and the Cisco Firepower Management Center configuration guides.

QUESTION NO: 49 - (DRAG DROP)

Refer to the exhibit.



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


192.168.1.0/24
192.168.2.0/24
HTTP-HTTPS
HTTP-HTTPS-QoS
5 Mb/s
Interfaces in Destination Interface Objects
Name
Apply QoS On
Download/Upload Limit
Source Interface Networks
Destination Interface Networks
Destination Ports

ANSWER:



Explanation:

The QoS rule identifies and rate-limits web traffic initiated by the HR users. HR is attached to the FTD inside network, and the diagram labels that network as **192.168.1.0/24**. That value therefore belongs in **Source Interface Networks**, ensuring that the rule is scoped to connections originating from the HR subnet. The next hop from the FTD toward R1 and the Internet is the outside-side network labeled **192.168.2.0/24**, so it is used as **Destination Interface Networks**.

The rule must recognize both HTTP and HTTPS services. The **HTTP-HTTPS** object is consequently assigned to **Destination Ports**, which matches the destination service ports used by those web connections. The rule is named **HTTP-HTTPS-QoS**, providing an identifiable policy name that reflects the traffic being controlled.

QoS is enforced on the egress side selected by the rule, so **Interfaces in Destination Interface Objects** is placed in **Apply QoS On**. This aligns the QoS action with traffic leaving the firewall toward the outside route. Finally, Cisco Secure Firewall's QoS rule configuration provides one rate field for the download/upload limit; entering **5 Mb/s** fulfills the stated requirement that each direction be limited to 5 Mb/s. Cisco documents the use of source and destination interface objects, port matching, interface selection, and directional bandwidth limiting in its Secure Firewall QoS configuration guidance.

QUESTION NO: 50

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

A. IPsec

B. SSH

C. SSL

D. MACsec

ANSWER: A

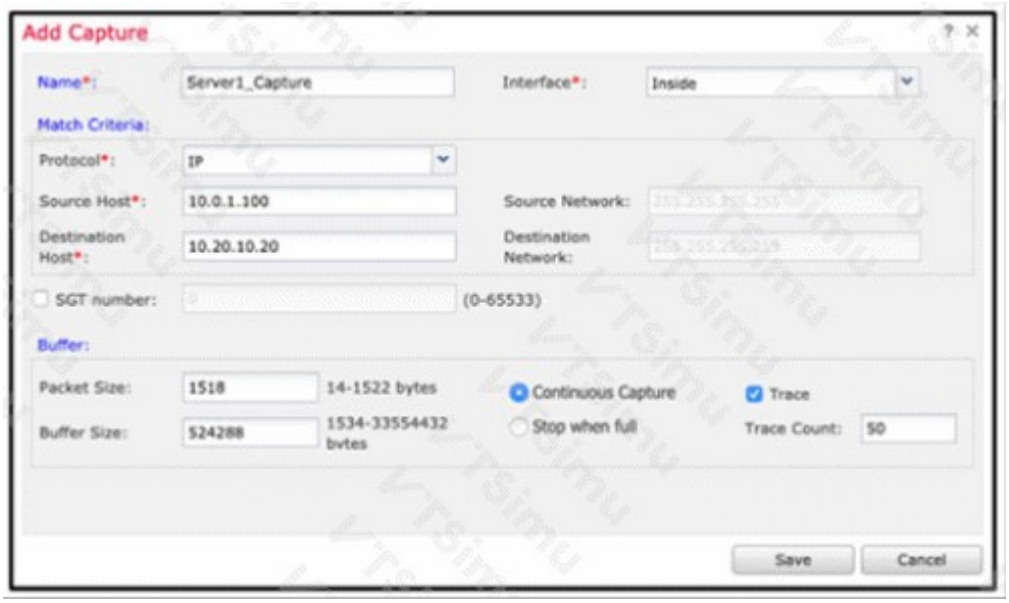
Explanation:

IPsec is correct because Cisco Secure Firewall Threat Defense uses IPsec to protect high-availability communication between the two peers. An FTD high-availability pair exchanges operational information across its failover/control link, including state and configuration-related synchronization data needed for reliable active/standby operation. Enabling IPsec encryption protects the confidentiality and integrity of this device-to-device traffic while it traverses the network connecting the HA peers. This is particularly important when the failover link is carried through shared switching infrastructure or any network segment that is not considered physically isolated and trusted. Cisco documents IPsec as the mechanism used to encrypt communications between high-availability devices, with the required HA configuration performed through the applicable management method, such as Firepower Management Center or the device manager. The protocol is designed for network-layer protection and is therefore appropriate for securing the traffic exchanged over the FTD failover link. See Cisco's High Availability for FMC-Managed Devices documentation and the Secure Communications guidance.

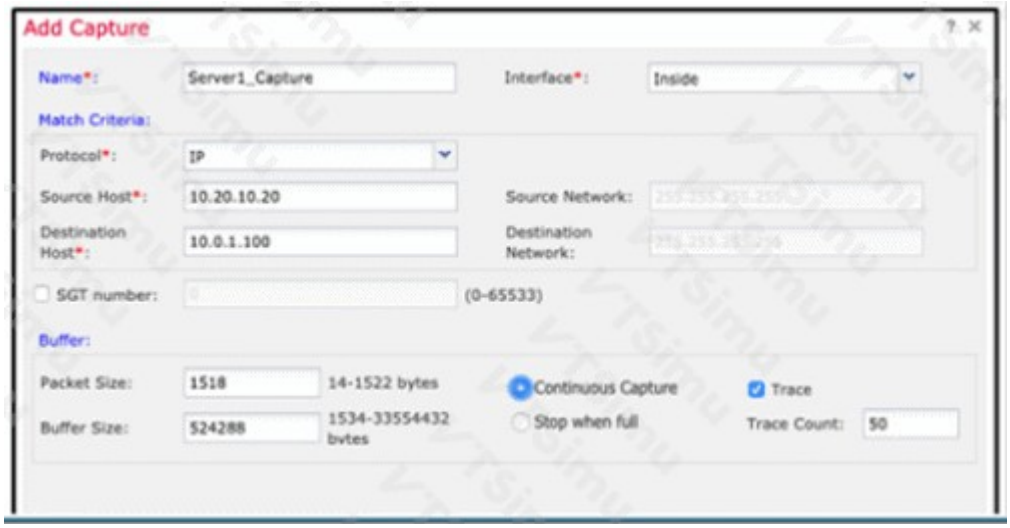
QUESTION NO: 51

An engineer is troubleshooting a device that cannot connect to a web server. The connection is initiated from the Cisco FTD inside interface and attempting to reach 10.0.1.100 over the non-standard port of 9443 The host the engineer is attempting the connection from is at the IP address of 10.20.10.20. In order to determine what is happening to the packets on the network, the engineer decides to use the FTD packet capture tool Which capture configuration should be used to gather the information needed to troubleshoot this issue?

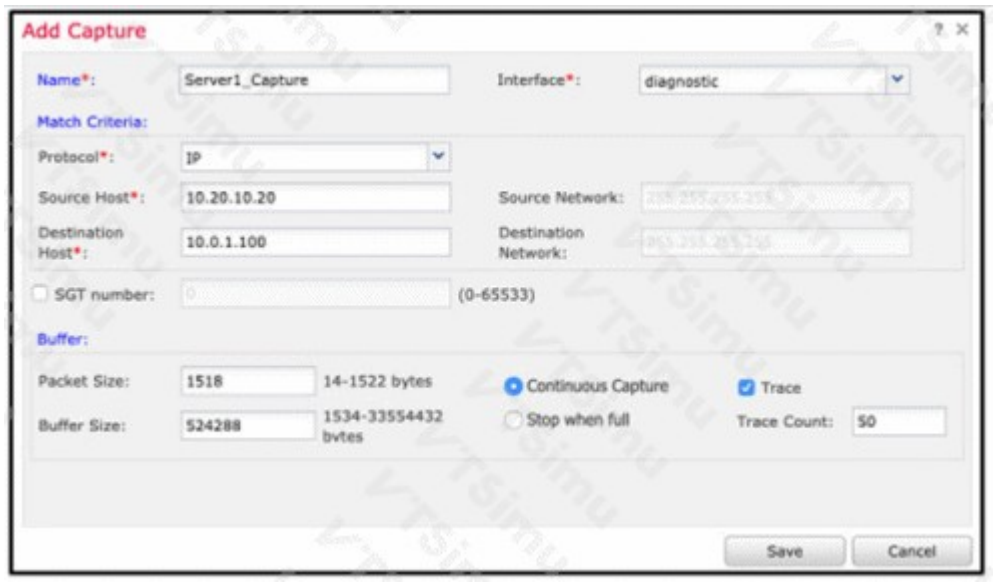
A)



B)



C)



D)



A. Option A

B. Option B

C. Option C

D. Option D

ANSWER: B

Explanation:

The correct capture configuration is the one that captures traffic on the inside interface and applies a filter for the affected connection: source host 10.20.10.20, destination host 10.0.1.100, and TCP port 9443. This scope directly matches the reported client-to-server flow while avoiding unrelated traffic that can make a packet capture difficult to interpret. Because 9443 is a nonstandard web port, the port must be explicitly included in the capture filter rather than relying on a predefined HTTP or HTTPS application assumption. Capturing at the inside interface also verifies whether the FTD receives the initial TCP packets from the client and permits inspection of the TCP handshake, retransmissions, resets, or other packet behavior relevant to the failed connection. Cisco Secure Firewall packet captures use capture filters to limit collected packets to the hosts, protocols, and ports relevant to a troubleshooting case. The resulting capture can be downloaded and examined in a packet-analysis tool when deeper protocol-level inspection is required. See Cisco's Secure Firewall packet capture documentation and the Secure Firewall Threat Defense command reference.

QUESTION NO: 52

An engineer must configure a new identity policy in Cisco Firepower Management Center. Active authentication must be configured by using a Kerberos connection. Which two realms must be configured? (Choose two.)

A. Directory password

B. Active directory join password

C. Active directory primary domain

D. Active directory join username

E. Directory username

ANSWER: C D

Explanation:

Active directory primary domain is required because it identifies the AD DNS domain to which the Secure Firewall Management Center will join and in which it will obtain Kerberos service tickets. The domain value establishes the Kerberos authentication context used when the system validates an actively authenticated user.

Active directory join username is also required because FMC uses an AD account with permission to join the appliance to the specified domain. Joining the domain creates and maintains the computer-account relationship needed for Kerberos-based active authentication. In an actual FMC configuration, the associated join password must be supplied as well; however, the requested realm configuration selections identify the primary AD domain and the account used for the join operation. Cisco documents that Active Directory realms support Kerberos authentication and require the management system to join the configured AD domain. See the Cisco Secure Firewall Management Center identity sources documentation and the Cisco Secure Firewall Management Center support documentation.

QUESTION NO: 53

A network engineer must configure the cabling between a Cisco Secure Firewall Threat Defense appliance and a network so the Secure Firewall Threat Defense appliance performs inline to analyze and tune generated intrusion events before going live. Which Secure Firewall Threat Defense interface mode must the engineer use?

A. bypass

B. link state propagation

C. tap mode

D. strict TCP enforcement

ANSWER: C

Explanation:

tap mode is the appropriate choice for evaluating intrusion events and tuning intrusion policies before enforcing traffic inspection inline. In tap mode, the Secure Firewall Threat Defense appliance receives a copy of network traffic from a network TAP or switch SPAN session and performs passive inspection. This provides visibility into the traffic patterns, detected intrusion events, and potential false positives without placing the appliance in the forwarding path or disrupting production traffic. The engineer can use the resulting event data to tune rules, suppress known-benign events where appropriate, and refine the intrusion policy for the environment. After validation and tuning are complete, the deployment can be recabled and configured for inline inspection, where the appliance can actively enforce the selected security policy. Cisco documents passive deployments as a practical method to monitor and assess traffic before introducing active enforcement into a production path. See Cisco's Secure Firewall Threat Defense documentation and the Cisco Secure Firewall product information for deployment and inspection capabilities.

QUESTION NO: 54

Which feature within the Cisco FMC web interface allows for detecting, analyzing and blocking malware in network traffic?

A. intrusion and file events

B. Cisco AMP for Endpoints

C. Cisco AMP for Networks

D. file policies

ANSWER: C

Explanation:

Cisco AMP for Networks is the Cisco Secure Firewall/FMC capability that provides network-based malware protection for files observed in inspected traffic. It integrates file inspection with cloud-based malware analysis and threat intelligence, allowing the system to identify files, calculate or look up file dispositions, and enforce a blocking decision before a malicious file is delivered when the access-control and file-policy configuration is set to do so. It also supports retrospective detection: if a file initially appears clean but is later identified as malicious, FMC can generate an event and provide visibility into where that file was seen in the network. In current Cisco terminology, this functionality is commonly described as Secure Firewall malware defense or file/malware inspection, while Cisco AMP for Networks is the established name used in many FMC interfaces, documentation versions, and certification materials. Administrators apply the capability through file policies associated with access-control rules, but the malware-analysis feature itself is Cisco AMP for Networks. Cisco documents file-policy configuration and malware-cloud lookups in the Secure Firewall Management Center File Policies guide; Cisco's overview of the broader malware-protection platform is available at Cisco Advanced Malware Protection.