EXAMTOPICS

- Expert Verified, Online, **Free**.

Custom View Settings

Topic 1 - Single Topic

Question #1 *Topic 1*

What is a result of enabling Cisco FTD clustering?

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

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

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

D. All Firepower appliances support Cisco FTD clustering.

Question #2 *Topic 1*

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

A. The units must be the same version

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

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

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

E. The units must be the same model.

Question #3 *Topic 1*

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

A. transparent inline mode

B. TAP mode

C. strict TCP enforcement

D. propagate link state

Question #4 *Topic 1*

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

A. inline interfaces, security zones, MTU, and mode

B. passive interface, MTU, and mode

C. inline interfaces, MTU, and mode

D. passive interface, security zone, MTU, and mode

Question #5 *Topic 1*

What is the difference between inline and inline tap on Cisco Firepower?

A. Inline tap mode can send a copy of the traffic to another device.

B. Inline tap mode does full packet capture.

C. Inline mode cannot do SSL decryption.

D. Inline mode can drop malicious traffic.

Question #6 *Topic 1*

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

A. inline set

B. passive

C. routed

D. inline tap

Question #7 *Topic 1*

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

Question #8

Topic 1

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

A. STP

B. HSRP

C. GLBP

D. VRRP

Question #9

Topic 1

Which interface type allows packets to be dropped?

A. passive

B. inline

C. ERSPAN

D. TAP

Question #10

Topic 1

Which Cisco Firepower Threat Defense, which two interface settings are required when configuring a routed interface? (Choose two.)

A. Redundant Interface

B. EtherChannel

C. Speed

D. Media Type

E. Duplex

Question #11

Topic 1

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

Question #12 *Topic 1*

Which policy rule is included in the deployment of a local DMZ during the initial deployment of a Cisco NGFW through the Cisco FMC GUI?

A. a default DMZ policy for which only a user can change the IP addresses.

B. deny ip any

C. no policy rule is included

D. permit ip any

Question #13 *Topic 1*

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

A. CIFS

B. IMAP

C. SSL

D. DNP3

E. ICMP

Question #14 *Topic 1*

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

A. multi-instance

B. multiple deployment

C. single deployment

D. single-context

Question #15 *Topic 1*

A network engineer is extending a user segment through an FTD device for traffic inspection without creating another IP subnet. How is this accomplished on an
FTD device in routed mode?

A. by assigning an inline set interface

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

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

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

Question #16 *Topic 1*

An engineer is configuring a Cisco FTD appliance in IPS-only mode and needs to utilize fail-to-wire interfaces. Which interface mode should be used to meet these requirements?

A. passive

B. routed

C. transparent

D. inline set

Question #17 *Topic 1*

An organization has noticed that malware was downloaded from a website that does not currently have a known bad reputation. How will this issue be addressed globally in the quickest way possible and with the least amount of impact?

A. by creating a URL object in the policy to block the website.

B. Cisco Talos will automatically update the policies.

C. by denying outbound web access

D. by isolating the endpoint

Question #18 *Topic 1*

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

A. drop packet

B. generate events

C. drop connection

D. drop and generate

Question #19 *Topic 1*

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

A. subinterface

B. switch virtual

C. bridge virtual

D. bridge group member

Question #20 *Topic 1*

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

A. Balanced Security and Connectivity

B. Security Over Connectivity

C. Maximum Detection

D. Connectivity Over Security

Question #21 *Topic 1*

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

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

B. The licensing purchased does not include high availability.

C. The primary FMC currently has devices connected to it.

D. There is only 10 Mbps of bandwidth between the two devices.

Question #22 *Topic 1*

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

A. inline set

B. passive

C. transparent

D. inline tap

Question #23 *Topic 1*

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

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

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

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

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

Question #24 *Topic 1*

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

A. minor upgrade

B. local import of intrusion rules

C. Cisco Geolocation Database

D. local import of major upgrade

Question #25 *Topic 1*

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

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

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

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

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

Question #26 *Topic 1*

Network traffic coming from an organization's CEO must never be denied. Which access control policy configuration option should be used if the deployment engineer is not permitted to create a rule to allow all traffic?

A. Change the intrusion policy from security to balance.

B. Configure a trust policy for the CEO.

C. Configure firewall bypass.

D. Create a NAT policy just for the CEO.

Question #27 *Topic 1*

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

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

B. Routing between bridge groups is achieved only with a router-on-a-stick configuration on a connected router.

C. In routed firewall mode, routing between bridge groups must pass through a routed interface.

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

Question #28 *Topic 1*

A Cisco FTD device is running in transparent firewall mode with a VTEP bridge group member ingress interface. What must be considered by an engineer tasked with specifying a destination MAC address for a packet trace?

A. The output format option for the packet logs is unavailable.

B. Only the UDP packet type is supported.

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

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

Question #29 *Topic 1*

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

A. ERSPAN

B. firewall

C. tap

D. IPS-only

Question #30 *Topic 1*

An engineer is monitoring network traffic from their sales and product development departments, which are on two separate networks. What must be configured in order to maintain data privacy for both departments?

A. Use passive IDS ports for both departments.

B. Use a dedicated IPS inline set for each department to maintain traffic separation.

C. Use 802.1Q inline set Trunk interfaces with VLANs to maintain logical traffic separation.

D. Use one pair of inline set in TAP mode for both departments.

Question #31 *Topic 1*

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

A. Configure a second circuit to an ISP for added redundancy.

B. Keep a copy of the current configuration to use as backup.

C. Configure the Cisco FMCs for failover.

D. Configure the Cisco FMC managed devices for clustering.

Question #32 *Topic 1*

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

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

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

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

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

Question #33 *Topic 1*

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

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

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

C. Deploy the firewall in routed mode with NAT configured

D. Deploy the firewall in transparent mode with NAT configured

Question #34 *Topic 1*

An engineer must configure high availability for the Cisco Firepower devices. The current network topology does not allow for two devices to pass traffic concurrently. How must the devices be implemented in this environment?

A. in active/active mode

B. in a cluster span EtherChannel

C. in active/passive mode

D. in cluster interface mode

Question #35 *Topic 1*

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

A. inline tap monitor-only mode

B. passive monitor-only mode

C. passive tap monitor-only mode

D. inline mode

Question #36 *Topic 1*

An organization has a Cisco FTD that uses bridge groups to pass traffic from the inside interfaces to the outside interfaces. They are unable to gather information about neighboring Cisco devices or use multicast in their environment. What must be done to resolve this issue?

A. Create a firewall rule to allow CDP traffic

B. Create a bridge group with the firewall interfaces

C. Change the firewall mode to transparent

D. Change the firewall mode to routed

Question #37 *Topic 1*

A network engineer implements a new Cisco Firepower device on the network to take advantage of its intrusion detection functionality. There is a requirement to analyze the traffic going across the device, alert on any malicious traffic, and appear as a bump in the wire. How should this be implemented?

A. Specify the BVI IP address as the default gateway for connected devices

B. Enable routing on the Cisco Firepower

C. Add an IP address to the physical Cisco Firepower interfaces

D. Configure a bridge group in transparent mode

Question #38 *Topic 1*

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

A. same flash memory size

B. same NTP configuration

C. same DHCP/PPoE configuration

D. same host name

E. same number of interfaces

Question #39 *Topic 1*

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

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

B. Disable the default IPS policy and enable global logging

C. Configure an IPS policy and enable global logging

D. Disable the default IPS policy and enable per-rule logging

Question #40 *Topic 1*

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

A. OSPFv2 with IPv6 capabilities

B. virtual links

C. SHA authentication to OSPF packets

D. area boundary router type 1 LSA filtering

E. MD5 authentication to OSPF packets

Question #41 *Topic 1*

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

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

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

C. Add a Table View section to the report with the Search field defined as the network in CIDR format.

D. Select IP Address as the X-Axis in each section of the report.

Question #42 *Topic 1*

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

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

B. Smart License is required to maintain VPN connections simultaneously across all cluster units.

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

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

Question #43 *Topic 1*

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.

Question #44 *Topic 1*

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

A. configure manager local 10.0.0.10 Cisco123

B. configure manager add Cisco123 10.0.0.10

C. configure manager local Cisco123 10.0.0.10

D. configure manager add 10.0.0.10 Cisco123

Question #45 *Topic 1*

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

A. Block with Reset

B. Monitor

C. Analyze

D. Discover

E. Block ALL

Question #46 *Topic 1*

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

Question #47 *Topic 1*

Which object type supports object overrides?

A. time range

B. security group tag

C. network object

D. DNS server group

Question #48 *Topic 1*

Which Cisco Firepower rule action displays an HTTP warning page?

A. Monitor

B. Block

C. Interactive Block

D. Allow with Warning

Question #49 *Topic 1*

What is the result a specifying of QoS rule that has a rate limit that is greater than the maximum throughput of an interface?

A. The rate-limiting rule is disabled.

B. Matching traffic is not rate limited.

C. The system rate-limits all traffic.

D. The system repeatedly generates warnings.

Question #50 *Topic 1*

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

A. FlexConfig

B. BDI

C. SGT

D. IRB

Question #51 *Topic 1*

In which two places are thresholding settings configured? (Choose two.)

A. on each IPS rule

B. globally, within the network analysis policy

C. globally, per intrusion policy

D. on each access control rule

E. per preprocessor, within the network analysis policy

Question #52 *Topic 1*

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

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

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

C. They block traffic based on Security Intelligence data.

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

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

Question #53 *Topic 1*

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

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

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

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

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

E. reputation-based objects, such as URL categories

Question #54 *Topic 1*

A security engineer is configuring an Access Control Policy for multiple branch locations. These locations share a common rule set and utilize a network object called INSIDE_NET which contains the locally significant internal network subnets at each location. What technique will retain the policy consistency at each location but allow only the locally significant network subnet within the application rules?

A. utilizing a dynamic ACP that updates from Cisco Talos

B. creating a unique ACP per device

C. utilizing policy inheritance

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

Question #55 *Topic 1*

An organization has seen a lot of traffic congestion on their links going out to the internet. There is a Cisco Firepower device that processes all of the traffic going to the internet prior to leaving the enterprise. How is the congestion alleviated so that legitimate business traffic reaches the destination?

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

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

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

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

Question #56 *Topic 1*

An engineer configures an access control rule that deploys file policy configurations to security zone or tunnel zones, and it causes the device to restart. What is the reason for the restart?

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

B. The source tunnel zone in the rule does not match a tunnel zone that is assigned to a tunnel rule in the destination policy.

C. Source or destination security zones in the source tunnel zone do not match the security zones that are associated with interfaces on the target devices.

D. The source tunnel zone in the rule does not match a tunnel zone that is assigned to a tunnel rule in the source policy.

Question #57 *Topic 1*

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

Question #58 *Topic 1*

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

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

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

C. It has minimal performance impact.

D. It is not subject to any Privacy regulations.

Question #59 *Topic 1*

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

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

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

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

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

Question #60 *Topic 1*

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

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

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

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

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

Question #61 *Topic 1*

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

A. Prefilter

B. Intrusion

C. Access Control

D. Identity

Question #62 *Topic 1*

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

A. malware analysis

B. dynamic analysis

C. sandbox analysis

D. Spero analysis

Question #63 *Topic 1*

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

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

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

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

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

Question #64 *Topic 1*

An engineer is attempting to add a new FTD device to their FMC behind a NAT device with a NAT ID of ACME001 and a password of Cisco0391521107. Which command set must be used in order to accomplish this?

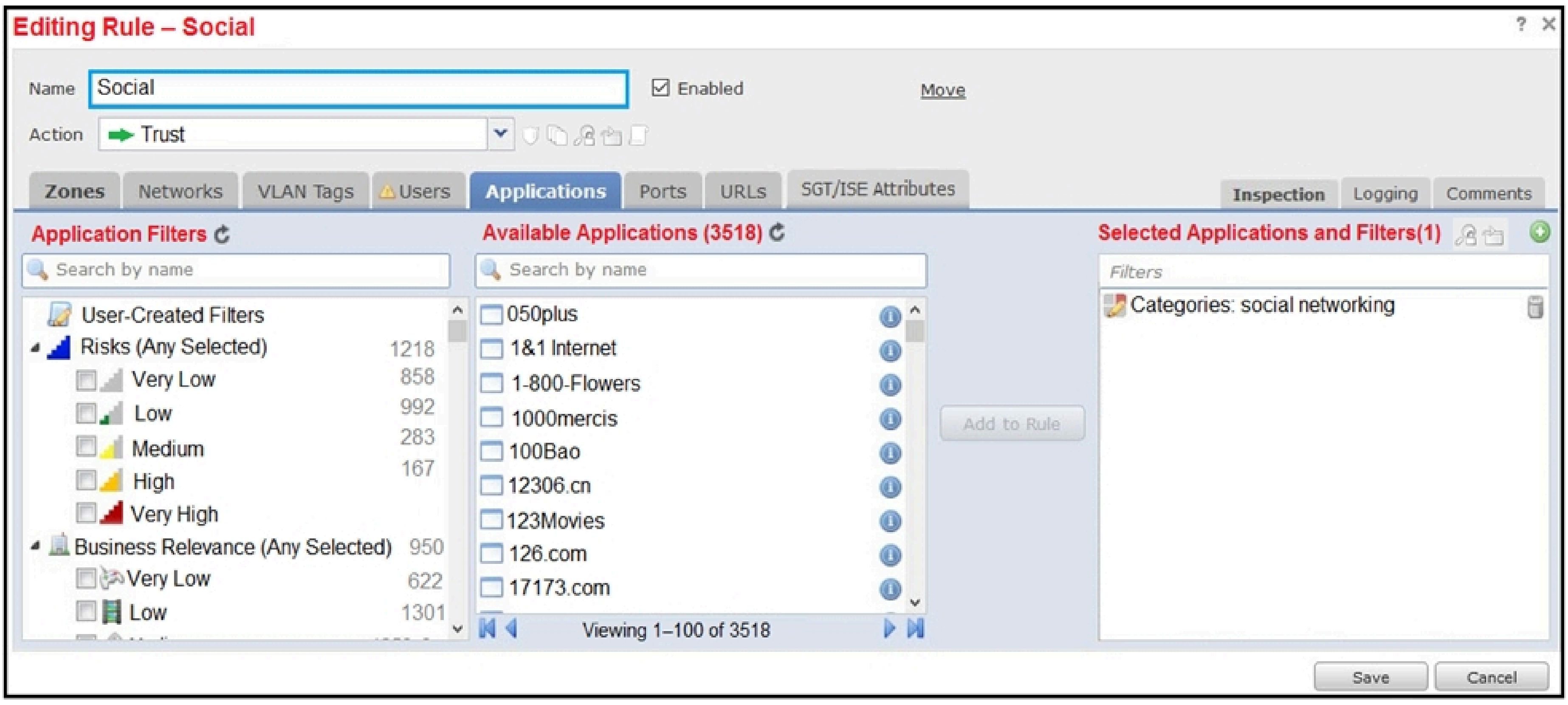
A. configure manager add<FMC IP> <registration key>ACME001

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

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

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

Question #65 *Topic 1*



Editing Rule – Social

Name: Social

☑ Enabled

Action: Trust

Selected Applications and Filters(1)

Categories: social networking

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

A. Add the social network URLs to the block list.

B. Change the intrusion policy to connectivity over security.

C. Modify the selected application within the rule.

D. Modify the rule action from trust to allow.

Question #66 *Topic 1*

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

A. Spero analysis

B. capacity handling

C. local malware analysis

D. dynamic analysis

Question #67 *Topic 1*

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

A. Exclude load balancers and NAT devices.

B. Leave default networks.

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

D. Change the method to TCP/SYN.

Question #68 *Topic 1*

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

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

B. An external NAT IP address is not configured

C. An external NAT IP address is configured to match the wrong interface

D. An object NAT exemption rule does not exist at the top of the NAT table

Question #69 *Topic 1*

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

A. The interfaces are being used for NAT for multiple networks

B. The administrator is adding interfaces of multiple types

C. The administrator is adding an interface that is in multiple zones

D. The interfaces belong to multiple interface groups

Question #70 *Topic 1*

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

A. Modify the Cisco ISE authorization policy to deny this access to the user

B. Modify Cisco ISE to send only legitimate usernames to the Cisco FTD

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

D. Add the unknown user in the Malware & File Policy in Cisco FTD

Question #71 *Topic 1*

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.

Question #72 *Topic 1*

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

A. /etc/sf/DCMIB.ALERT

B. /sf/etc/DCEALERT.MIB

C. /etc/sf/DCEALERT.MIB

D. system/etc/DCEALERT.MIB

Question #73 *Topic 1*

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

Question #74 *Topic 1*

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

A. configure coredump packet-engine enable

B. capture-traffic

C. capture

D. capture WORD

Question #75 *Topic 1*

How many report templates does the Cisco Firepower Management Center support?

A. 20

B. 10

C. 5

D. unlimited

Question #76 *Topic 1*

Which action should be taken after editing an object that is used inside an access control policy?

A. Delete the existing object in use.

B. Refresh the Cisco FMC GUI for the access control policy.

C. Redeploy the updated configuration.

D. Create another rule using a different object name.

Question #77 *Topic 1*

Which Cisco Firepower feature is used to reduce the number of events received in a period of time?

A. rate-limiting

B. suspending

C. correlation

D. thresholding

Question #78 *Topic 1*

Which report template field format is available in Cisco FMC?

A. box lever chart

B. arrow chart

C. bar chart

D. benchmark chart

Question #79 *Topic 1*

Which group within Cisco does the Threat Response team use for threat analysis and research?

A. Cisco Deep Analytics

B. OpenDNS Group

C. Cisco Network Response

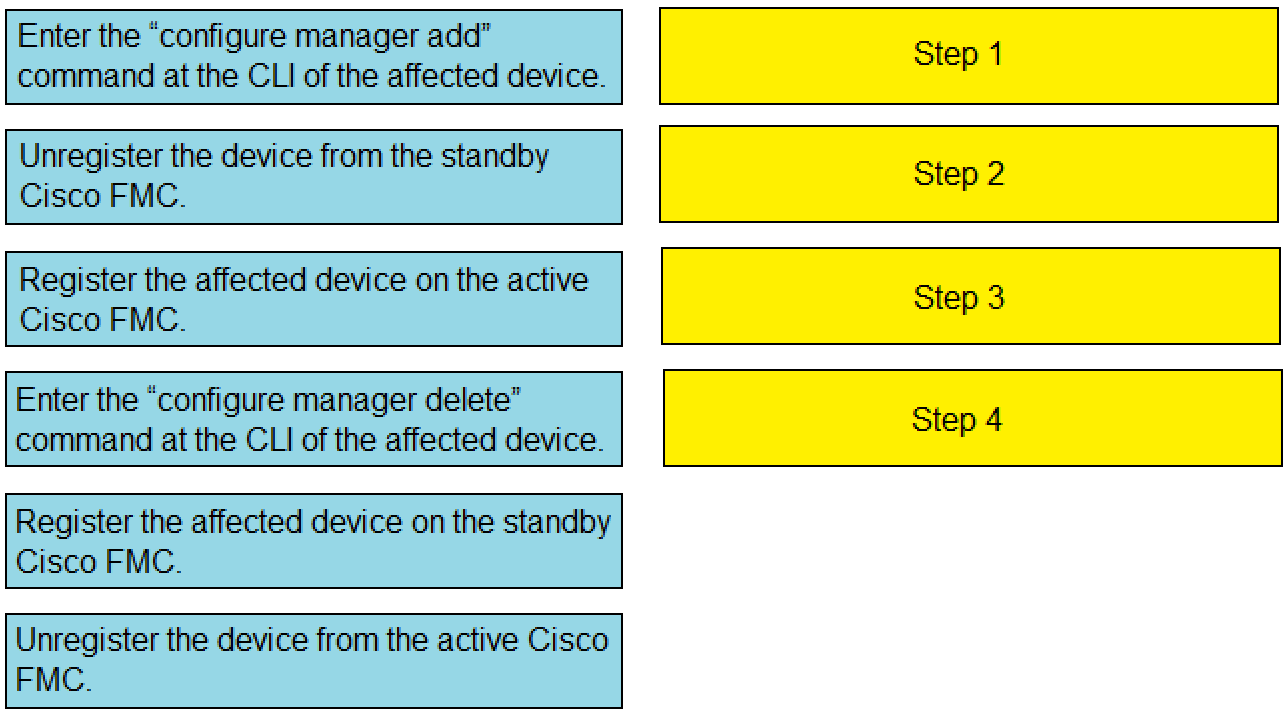
D. Cisco Talos

Question #80 *Topic 1*

DRAG DROP -

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

Select and Place:



Enter the "configure manager add" command at the CLI of the affected device.	Step 1
Unregister the device from the standby Cisco FMC.	Step 2
Register the affected device on the active Cisco FMC.	Step 3
Enter the "configure manager delete" command at the CLI of the affected device.	Step 4
Register the affected device on the standby Cisco FMC.	
Unregister the device from the active Cisco FMC.	

Question #81 *Topic 1*

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

A. system support firewall-engine-debug

B. system support ssl-debug

C. system support platform

D. system support dump-table

Question #82 *Topic 1*

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

A. privileged

B. user

C. configuration

D. admin

Question #83 *Topic 1*

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

Question #84 *Topic 1*

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

A. system support ssl-client-hello-tuning

B. system support ssl-client-hello-display

C. system support ssl-client-hello-force-reset

D. system support ssl-client-hello-reset

Question #85 *Topic 1*

Which command is typed at the CLI on the primary Cisco FTD unit to temporarily stop running high-availability?

A. configure high-availability resume

B. configure high-availability disable

C. system support network-options

D. configure high-availability suspend

Question #86 *Topic 1*

Which command must be run to generate troubleshooting files on an FTD?

A. system support view-files

B. sudo sf_troubleshoot.pl

C. system generate-troubleshoot all

D. show tech-support

Question #87 *Topic 1*

When is the file-size command needed while troubleshooting with packet capture?

A. when capture packets are less than 16 MB

B. when capture packets are restricted from the secondary memory

C. when capture packets exceed 10 GB

D. when capture packets exceed 32 MB

Question #88 *Topic 1*

What is a functionality of port objects in Cisco FMC?

A. to mix transport protocols when setting both source and destination port conditions in a rule

B. to represent protocols other than TCP, UDP, and ICMP

C. to represent all protocols in the same way

D. to add any protocol other than TCP or UDP for source port conditions in access control rules.

Question #89 *Topic 1*

Within Cisco Firepower Management Center, where does a user add or modify widgets?

A. dashboard

B. reporting

C. context explorer

D. summary tool

Question #90 *Topic 1*

A network engineer is configuring URL Filtering on Cisco FTD. Which two port requirements on the FMC 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

Question #91 *Topic 1*

What is the maximum bit size that Cisco FMC supports for HTTPS certificates?

A. 1024

B. 8192

C. 4096

D. 2048

Question #92 *Topic 1*

Which limitation applies to Cisco FMC dashboards in a multi-domain environment?

A. Child domains are able to view but not edit dashboards that originate from an ancestor domain.

B. Child domains have access to only a limited set of widgets from ancestor domains.

C. Only the administrator of the top ancestor domain is able to view dashboards.

D. Child domains are not able to view dashboards that originate from an ancestor domain.

Question #93 *Topic 1*

Which two considerations must be made when deleting and re-adding devices while managing them via Cisco FMC? (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, the manager must be added back.

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

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

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

Question #94 *Topic 1*

What is a behavior of a Cisco FMC database purge?

A. User login and history data are removed from the database if the User Activity check box is selected.

B. Data is recovered from the device.

C. The appropriate process is restarted.

D. The specified data is removed from Cisco FMC and kept for two weeks.

Question #95 *Topic 1*

Which two packet captures does the FTD LINA engine support? (Choose two.)

A. Layer 7 network ID

B. source IP

C. application ID

D. dynamic firewall importing

E. protocol

Question #96 *Topic 1*

An engineer currently has a Cisco FTD device registered to the Cisco FMC and is assigned the address of 10.10.50.12. The organization is upgrading the addressing schemes and there is a requirement to convert the addresses to a format that provides an adequate amount of addresses on the network. What should the engineer do to ensure that the new addressing takes effect and can be used for the Cisco FTD to Cisco FMC connection?

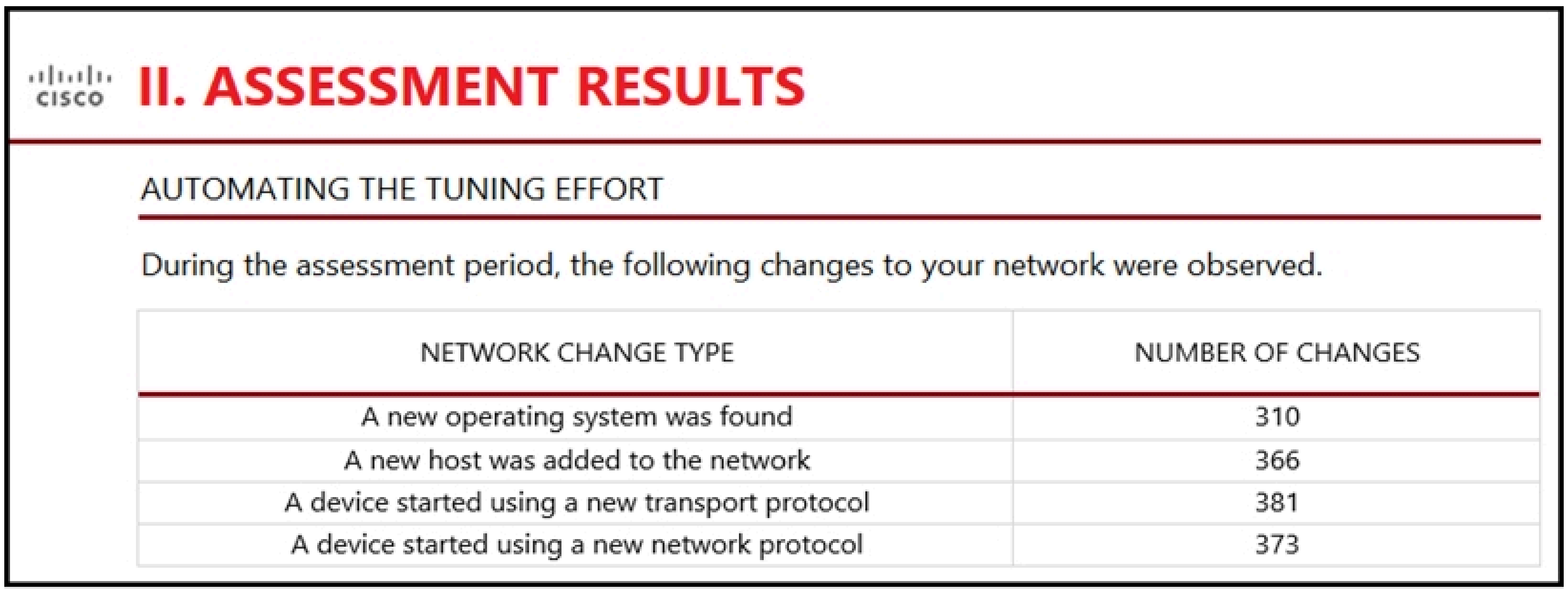
A. Update the IP addresses from IPv4 to IPv6 without deleting from Cisco FMC.

B. Format and reregister the device to Cisco FMC.

C. Cisco FMC does not support devices that use IPv4 IP addresses.

D. Delete and reregister the device to Cisco FMC.

Question #97 *Topic 1*



II. ASSESSMENT RESULTS

AUTOMATING THE TUNING EFFORT

During the assessment period, the following changes to your network were observed.

NETWORK CHANGE TYPE	NUMBER OF CHANGES
A new operating system was found	310
A new host was added to the network	366
A device started using a new transport protocol	381
A device started using a new network protocol	373

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

A. The administrator manually updates the policies.

B. The administrator requests a Remediation Recommendation Report from Cisco Firepower.

C. Cisco Firepower gives recommendations to update the policies.

D. Cisco Firepower automatically updates the policies.

Question #98 *Topic 1*

After using Firepower for some time and learning about how it interacts with the network, an administrator is trying to correlate malicious activity with a user. Which widget should be configured to provide this visibility on the Cisco Firepower dashboards?

A. Current Sessions

B. Correlation Events

C. Current Status

D. Custom Analysis

Question #99 *Topic 1*

An engineer is troubleshooting application failures through an FTD deployment. While using the FMC CLI, it has been determined that the traffic in question is not matching the desired policy. What should be done to correct this?

A. Use the system support firewall-engine-debug command to determine which rules the traffic matching and modify the rule accordingly.

B. Use the system support firewall-engine-dump-user-identity-data command to change the policy and allow the application though the firewall.

C. Use the system support application-identification-debug command to determine which rules the traffic matching and modify the rule accordingly.

D. Use the system support network-options command to fine tune the policy.

Question #100 *Topic 1*

An engineer has been asked to show application usages automatically on a monthly basis and send the information to management. What mechanism should be used to accomplish this task?

A. reports

B. context explorer

C. dashboards

D. event viewer

Question #101 *Topic 1*

A network administrator is configuring SNORT inspection policies and is seeing failed deployment messages in Cisco FMC. What information should the administrator generate for Cisco TAC to help troubleshoot?

A. A ג€troubleshootג€ file for the device in question.

B. A ג€show techג€ file for the device in question.

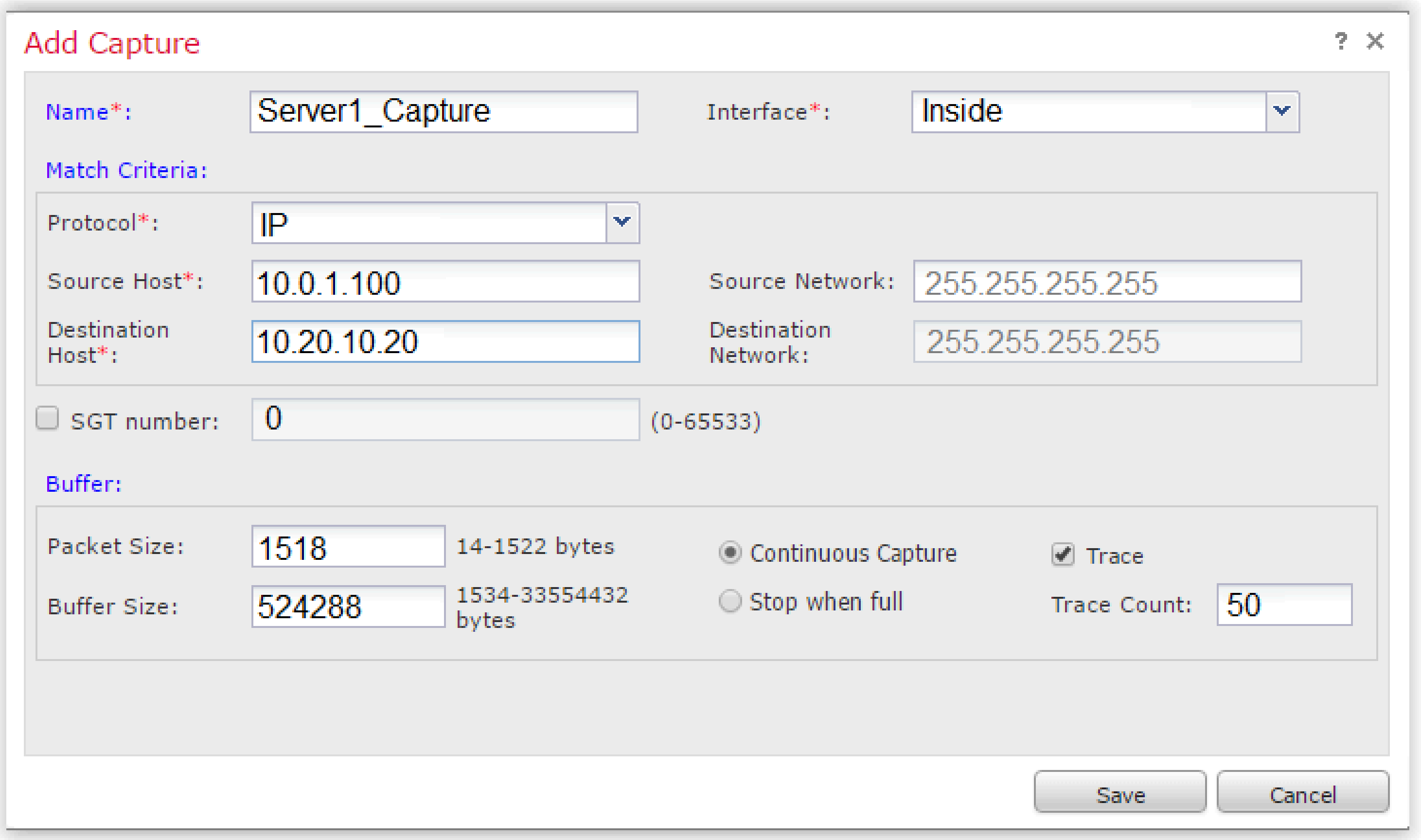
C. A ג€troubleshootג€ file for the Cisco FMC.

D. A ג€show techג€ for the Cisco FMC.

Question #102 *Topic 1*

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 the issue?

A.



Add Capture

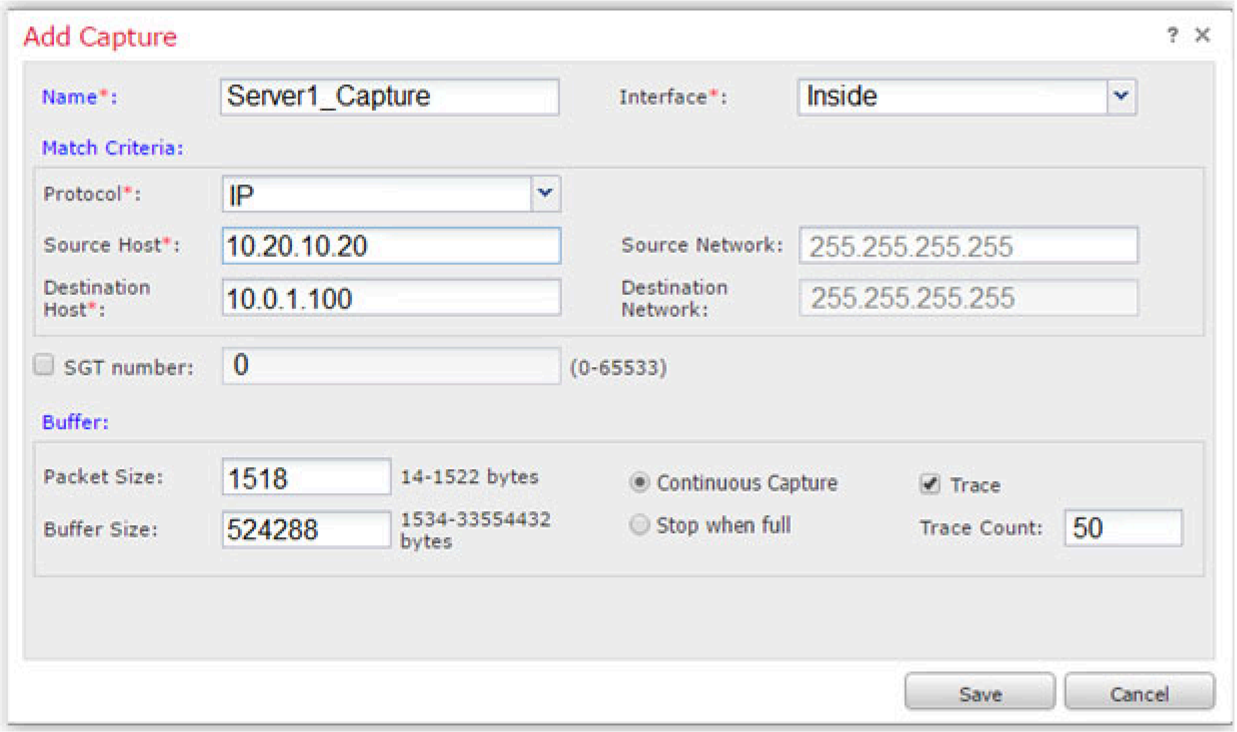
Name*: Server1_Capture
Interface*: Inside

Match Criteria:
Protocol*: IP
Source Host*: 10.0.1.100
Source Network: 255.255.255.255
Destination Host*: 10.20.10.20
Destination Network: 255.255.255.255

□ SGT number: 0 (0-65533)

Buffer:
Packet Size: 1518 14-1522 bytes
Buffer Size: 524288 1534-33554432 bytes
● Continuous Capture
○ Stop when full
☑ Trace
Trace Count: 50

B.



Add Capture

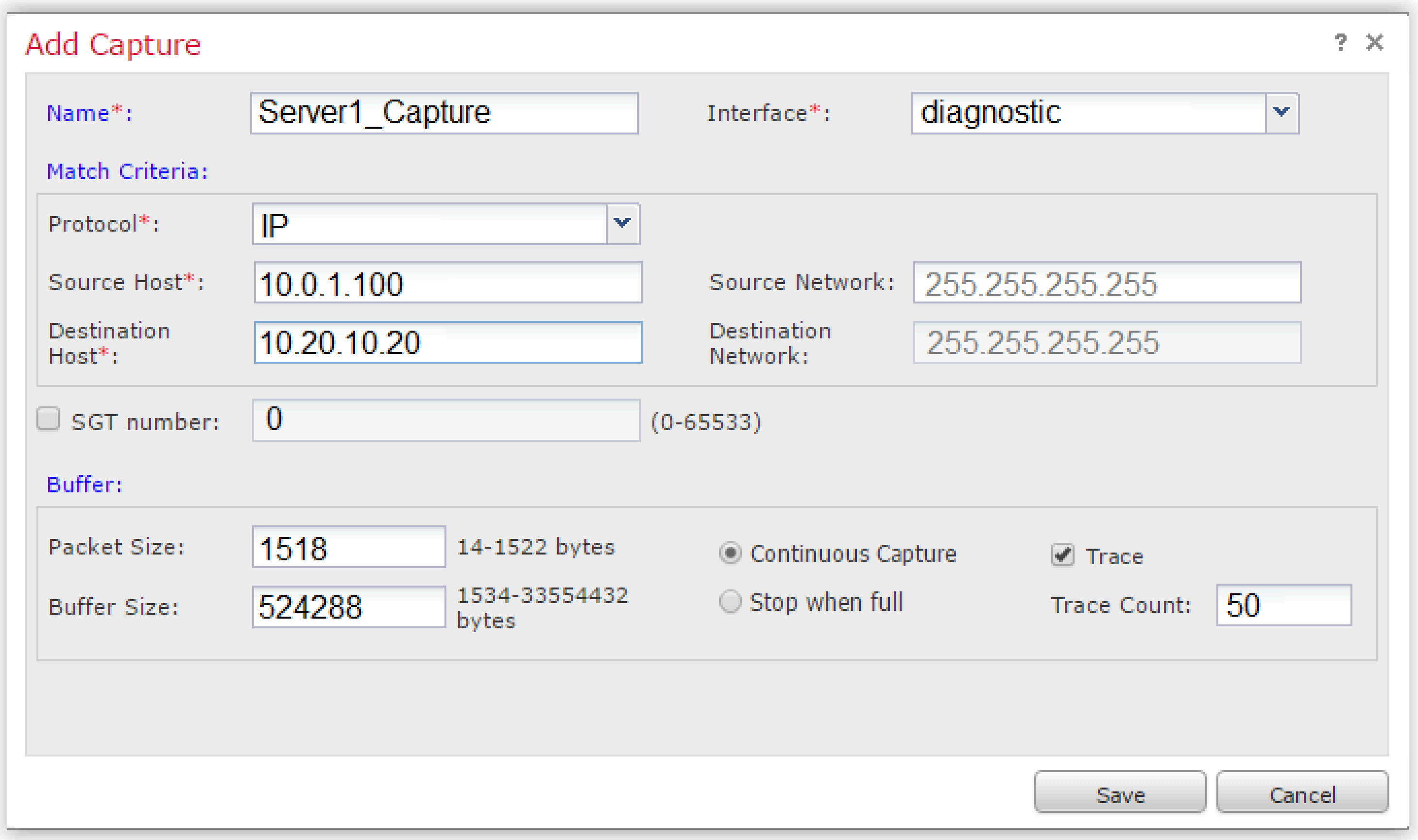
Name*: Server1_Capture
Interface*: Inside

Match Criteria:
Protocol*: IP
Source Host*: 10.20.10.20
Source Network: 255.255.255.255
Destination Host*: 10.0.1.100
Destination Network: 255.255.255.255

□ SGT number: 0 (0-65533)

Buffer:
Packet Size: 1518 14-1522 bytes
Buffer Size: 524288 1534-33554432 bytes
● Continuous Capture
○ Stop when full
☑ Trace
Trace Count: 50

C.



Add Capture

Name*: Server1_Capture

Interface*: diagnostic

Match Criteria:

Protocol*: IP

Source Host*: 10.0.1.100

Source Network: 255.255.255.255

Destination Host*: 10.20.10.20

Destination Network: 255.255.255.255

□ SGT number: 0 (0-65533)

Buffer:

Packet Size: 1518 14-1522 bytes

Buffer Size: 524288 1534-33554432 bytes

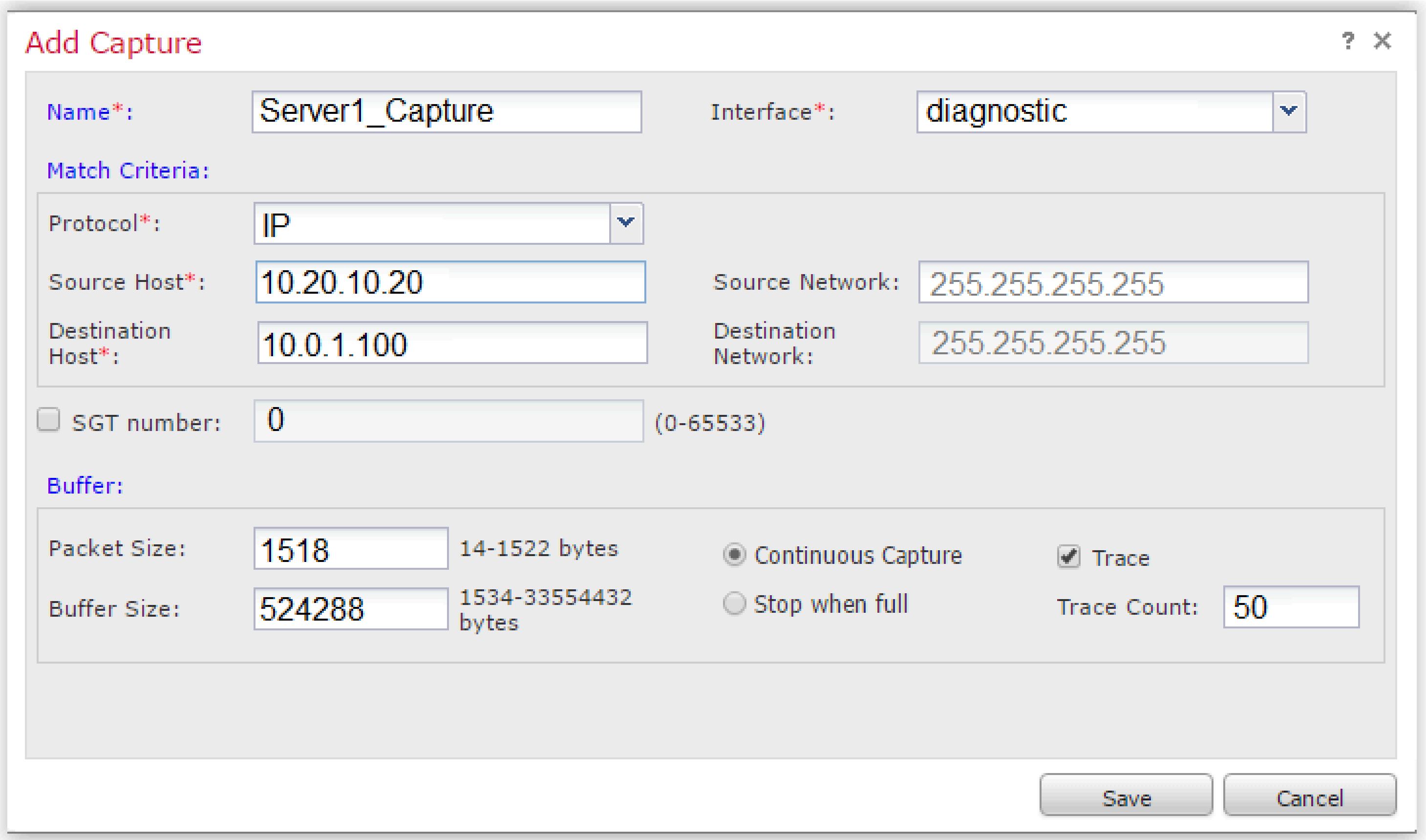
● Continuous Capture

○ Stop when full

☑ Trace

Trace Count: 50

D.



Add Capture

Name*: Server1_Capture

Interface*: diagnostic

Match Criteria:

Protocol*: IP

Source Host*: 10.20.10.20

Source Network: 255.255.255.255

Destination Host*: 10.0.1.100

Destination Network: 255.255.255.255

□ SGT number: 0 (0-65533)

Buffer:

Packet Size: 1518 14-1522 bytes

Buffer Size: 524288 1534-33554432 bytes

● Continuous Capture

○ Stop when full

☑ Trace

Trace Count: 50

Question #103 *Topic 1*

A network engineer is receiving reports of users randomly getting disconnected from their corporate applications which traverse the data center FTD appliance.
Network monitoring tools show that the FTD appliance utilization is peaking above 90% of total capacity. What must be done in order to further analyze this issue?

A. Use the Packet Export feature to save data onto external drives.

B. Use the Packet Capture feature to collect real-time network traffic.

C. Use the Packet Tracer feature for traffic policy analysis.

D. Use the Packet Analysis feature for capturing network data.

Question #104 *Topic 1*

An administrator is attempting to remotely log into a switch in the data center using SSH and is unable to connect. How does the administrator confirm that traffic is reaching the firewall?

A. by performing a packet capture on the firewall

B. by attempting to access it from a different workstation

C. by running Wireshark on the administrator's PC

D. by running a packet tracer on the firewall

Question #105 *Topic 1*

IT management is asking the network engineer to provide high-level summary statistics of the Cisco FTD appliance in the network. The business is approaching a peak season so the need to maintain business uptime is high. Which report type should be used to gather this information?

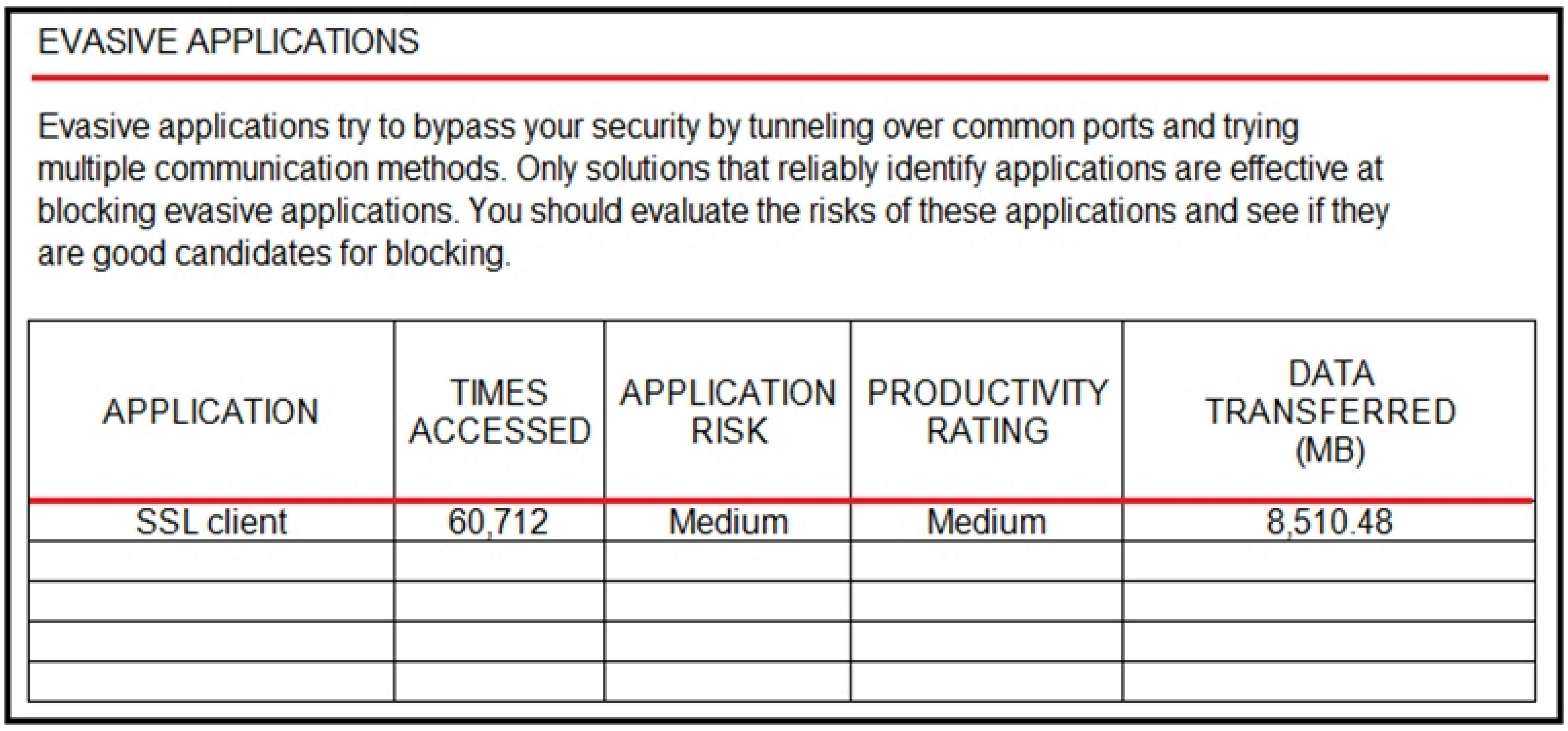
A. Risk Report

B. SNMP Report

C. Standard Report

D. Malware Report

Question #106 *Topic 1*



EVASIVE APPLICATIONS

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

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

Refer to the exhibit. An administrator is looking at some of the reporting capabilities for Cisco Firepower and noticed this section of the Network Risk Report showing a lot of SSL activity that could be used for evasion. Which action will mitigate this risk?

A. Use SSL decryption to analyze the packets.

B. Use Cisco Tetration to track SSL connections to servers.

C. Use encrypted traffic analytics to detect attacks.

D. Use Cisco AMP for Endpoints to block all SSL connection.

Question #107 *Topic 1*

An administrator is setting up Cisco FirePower to send data to the Cisco Stealthwatch appliances. The NetFlow_Set_Parameters objet is already created, but
NetFlow is not being sent to the flow collector. What must be done to prevent this from occurring?

A. Create a service identifier to enable the NetFlow service.

B. Add the NetFlow_Send_Destination object to the configuration.

C. Create a Security Intelligence object to send the data to Cisco Stealthwatch.

D. Add the NetFlow_Add_Destination object to the configuration.

Question #108 *Topic 1*

With a recent summer time change, system logs are showing activity that occurred to be an hour behind real time. Which action should be taken to resolve this issue?

A. Manually adjust the time to the correct hour on all managed devices.

B. Configure the system clock settings to use NTP with Daylight Savings checked.

C. Configure the system clock settings to use NTP.

D. Manually adjust the time to the correct hour on the Cisco FMC.

Question #109 *Topic 1*

A network administrator notices that SI events are not being updated. The Cisco FTD device is unable to load all of the SI event entries and traffic is not being blocked as expected. What must be done to correct this issue?

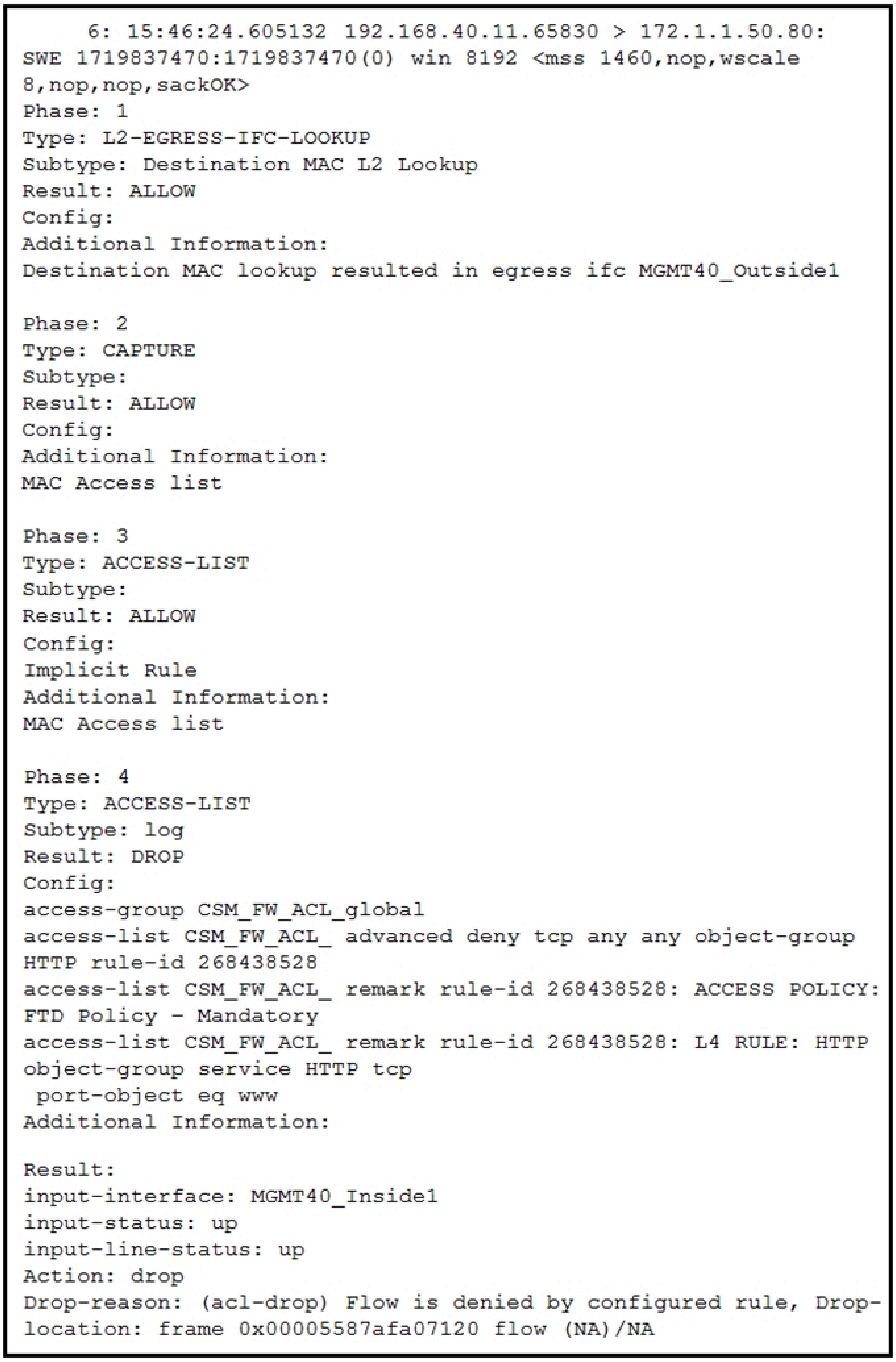
A. Restart the affected devices in order to reset the configurations.

B. Redeploy configurations to affected devices so that additional memory is allocated to the SI module.

C. Replace the affected devices with devices that provide more memory.

D. Manually update the SI event entries to that the appropriate traffic is blocked.

Question #110 Topic 1



```
     6: 15:46:24.605132 192.168.40.11.65830 > 172.1.1.50.80:
SWE 1719837470:1719837470(0) win 8192 <mss 1460,nop,wscale
8,nop,nop,sackOK>
Phase: 1
Type: L2-EGRESS-IFC-LOOKUP
Subtype: Destination MAC L2 Lookup
Result: ALLOW
Config:
Additional Information:
Destination MAC lookup resulted in egress ifc MGMT40_Outside1

Phase: 2
Type: CAPTURE
Subtype:
Result: ALLOW
Config:
Additional Information:
MAC Access list

Phase: 3
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
MAC Access list

Phase: 4
Type: ACCESS-LIST
Subtype: log
Result: DROP
Config:
access-group CSM_FW_ACL_global
access-list CSM_FW_ACL_ advanced deny tcp any any object-group
HTTP rule-id 268438528
access-list CSM_FW_ACL_ remark rule-id 268438528: ACCESS POLICY:
FTD Policy - Mandatory
access-list CSM_FW_ACL_ remark rule-id 268438528: L4 RULE: HTTP
object-group service HTTP tcp
 port-object eq www
Additional Information:

Result:
input-interface: MGMT40_Inside1
input-status: up
input-line-status: up
Action: drop
Drop-reason: (acl-drop) Flow is denied by configured rule, Drop-
location: frame 0x00005587afa07120 flow (NA)/NA
```

Refer to the exhibit. What must be done to fix access to this website while preventing the same communication to all other websites?

A. Create an intrusion policy rule to have Snort allow port 80 to only 172.1.1.50.

B. Create an intrusion policy rule to have Snort allow port 443 to only 172.1.1.50.

C. Create an access control policy rule to allow port 443 to only 172.1.1.50.

D. Create an access control policy rule to allow port 80 to only 172.1.1.50.

Question #111 *Topic 1*

A connectivity issue is occurring between a client and a server which are communicating through a Cisco Firepower device. While troubleshooting, a network administrator sees that traffic is reaching the server, but the client is not getting a response. Which step must be taken to resolve this issue without initiating traffic from the client?

A. Use packet-tracer to ensure that traffic is not being blocked by an access list

B. Use packet capture to ensure that traffic is not being blocked by an access list

C. Use packet capture to validate that the packet passes through the firewall and is NATed to the corrected IP address

D. Use packet-tracer to validate that the packet passes through the firewall and is NATed to the corrected IP address

Question #112 *Topic 1*

A VPN user is unable to connect to web resources behind the Cisco FTD device terminating the connection. While troubleshooting, the network administrator determines that the DNS response are not getting through the Cisco FTD. What must be done to address this issue while still utilizing Snort IPS rules?

A. Uncheck the ג€Drop when Inlineג€ box in the intrusion policy to allow the traffic

B. Modify the Snort rules to allow legitimate DNS traffic to the VPN users

C. Disable the intrusion rule thresholds to optimize the Snort processing

D. Decrypt the packet after the VPN flow so the DNS queries are not inspected

Question #113 *Topic 1*

An engineer is restoring a Cisco FTD configuration from a remote backup using the command restore remote-manager-backup location 1.1.1.1 admin /
Volume/home/admin BACKUP_Cisc394602314.zip on a Cisco FMC. After connecting to the repository, an error occurred that prevents the FTD device from accepting the backup file. What is the problem?

A. The backup file is not in .cfg format

B. The backup file is too large for the Cisco FTD device

C. The backup file extension was changed from .tar to .zip

D. The backup file was not enabled prior to being applied

Question #114 *Topic 1*

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

Question #115 *Topic 1*

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

Question #116 *Topic 1*

An organization must be able to ingest NetFlow traffic from their Cisco FTD device to Cisco Stealthwatch for behavioral analysis. What must be configured on the
Cisco FTD to meet this requirement?

A. flexconfig object for NetFlow

B. interface object to export NetFlow

C. security intelligence object for NetFlow

D. variable set object for NetFlow

Question #117 *Topic 1*

An engineer must build redundancy into the network and traffic must continuously flow if a redundant switch in front of the firewall goes down. What must be configured to accomplish this task?

A. redundant interfaces on the firewall cluster mode and switches

B. redundant interfaces on the firewall noncluster mode and switches

C. vPC on the switches to the interface mode on the firewall cluster

D. vPC on the switches to the span EtherChannel on the firewall cluster

Question #118 *Topic 1*

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

A. The value of the highest MTU assigned to any non-management interface was changed

B. The value of the highest MSS assigned to any non-management interface was changed

C. A passive interface was associated with a security zone

D. Multiple inline interface pairs were added to the same inline interface

Question #119 *Topic 1*

A network administrator needs to create a policy on Cisco Firepower to fast-path traffic to avoid Layer 7 inspection. The rate at which traffic is inspected must be optimized. What must be done to achieve this goal?

A. Enable the FXOS for multi-instance

B. Configure a prefilter policy

C. Configure modular policy framework

D. Disable TCP inspection

Question #120 *Topic 1*

A network engineer is tasked with minimizing traffic interruption during peak traffic times. When the SNORT inspection engine is overwhelmed, what must be configured to alleviate this issue?

A. Enable IPS inline link state propagation

B. Enable Pre-filter policies before the SNORT engine failure

C. Set a Trust ALL access control policy

D. Enable Automatic Application Bypass

Question #121 *Topic 1*

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

A. application blocking

B. simple custom detection

C. file repository

D. exclusions

E. application allow listing

Question #122 *Topic 1*

Which action should you take when Cisco Threat Response notifies you that AMP has identified a file as malware?

A. Add the malicious file to the block list.

B. Send a snapshot to Cisco for technical support.

C. Forward the result of the investigation to an external threat-analysis engine.

D. Wait for Cisco Threat Response to automatically block the malware.

Question #123 *Topic 1*

Which Cisco AMP for Endpoints policy is used only for monitoring endpoint activity?

A. Windows domain controller

B. audit

C. triage

D. protection

Question #124 *Topic 1*

What is a valid Cisco AMP file disposition?

A. non-malicious

B. malware

C. known-good

D. pristine

Question #125 *Topic 1*

In a Cisco AMP for Networks deployment, which disposition is returned if the cloud cannot be reached?

A. unavailable

B. unknown

C. clean

D. disconnected

Question #126 *Topic 1*

Which two remediation options are available when Cisco FMC is integrated with Cisco ISE? (Choose two.)

A. dynamic null route configured

B. DHCP pool disablement

C. quarantine

D. port shutdown

E. host shutdown

Question #127 *Topic 1*

Which connector is used to integrate Cisco ISE with Cisco FMC for Rapid Threat Containment?

A. pxGrid

B. FTD RTC

C. FMC RTC

D. ISEGrid

Question #128 *Topic 1*

What is the maximum SHA level of filtering that Threat Intelligence Director supports?

A. SHA-1024

B. SHA-4096

C. SHA-512

D. SHA-256

Question #129 *Topic 1*

What is the advantage of having Cisco Firepower devices send events to Cisco Threat Response via the security services exchange portal directly as opposed to using syslog?

A. Firepower devices do not need to be connected to the Internet.

B. An on-premises proxy server does not need to set up and maintained.

C. All types of Firepower devices are supported.

D. Supports all devices that are running supported versions of Firepower

Question #130 *Topic 1*

Which license type is required on Cisco ISE to integrate with Cisco FMC pxGrid?

A. apex

B. plus

C. base

D. mobility

Question #131 *Topic 1*

What is a feature of Cisco AMP private cloud?

A. It disables direct connections to the public cloud.

B. It supports security intelligence filtering.

C. It support anonymized retrieval of threat intelligence.

D. It performs dynamic analysis.

Question #132 *Topic 1*

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 Networks

C. file policies

D. Cisco AMP for Endpoints

Question #133 *Topic 1*

A network administrator discovers that a user connected to a file server and downloaded a malware file. The Cisco FMC generated an alert for the malware event, however the user still remained connected. Which Cisco AMP file rule action within the Cisco FMC must be set to resolve this issue?

A. Malware Cloud Lookup

B. Reset Connection

C. Detect Files

D. Local Malware Analysis

Question #134 *Topic 1*

An engineer has been tasked with using Cisco FMC to determine if files being sent through the network are malware. Which two configuration tasks must be performed to achieve this file lookup? (Choose two.)

A. The Cisco FMC needs to include a SSL decryption policy.

B. The Cisco FMC needs to connect to the Cisco AMP for Endpoints service.

C. The Cisco FMC needs to connect to the Cisco ThreatGrid service directly for sandboxing.

D. The Cisco FMC needs to connect with the FireAMP Cloud.

E. The Cisco FMC needs to include a file inspection policy for malware lookup.

Question #135

Topic 1

A network engineer wants to add a third-party threat feed into the Cisco FMC for enhanced threat detection. Which action should be taken to accomplish this goal?

A. Enable Rapid Threat Containment using REST APIs.

B. Enable Rapid Threat Containment using STIX and TAXII.

C. Enable Threat Intelligence Director using REST APIs.

D. Enable Threat Intelligence Director using STIX and TAXII.

Question #136

Topic 1

A network engineer is logged into the Cisco AMP for Endpoints console and sees a malicious verdict for an identified SHA-256 hash. Which configuration is needed to mitigate this threat?

A. Add the hash to the simple custom detection list

B. Use regular expressions to block the malicious file

C. Enable a personal firewall in the infected endpoint

D. Add the hash from the infected endpoint to the network block list

Question #137

Topic 1

A network administrator is concerned about the high number of malware files affecting users' machines. What must be done within the access control policy in
Cisco FMC to address this concern?

A. Create an intrusion policy and set the access control policy to block

B. Create an intrusion policy and set the access control policy to allow

C. Create a file policy and set the access control policy to allow

D. Create a file policy and set the access control policy to block

Question #138

Topic 1

Within an organization's high availability environment where both firewalls are passing traffic, traffic must be segmented based on which department it is destined for. Each department is situated on a different LAN. What must be configured to meet these requirements?

A. redundant interfaces

B. span EtherChannel clustering

C. high availability active/standby firewalls

D. multi-instance firewalls

Question #139 *Topic 1*

An engineer is configuring a Cisco IPS to protect the network and wants to test a policy before deploying it. A copy of each incoming packet needs to be monitored while traffic flow remains constant. Which IPS mode should be implemented to meet these requirements?

A. routed

B. passive

C. transparent

D. inline tap

Question #140 *Topic 1*

A network security engineer must replace a faulty Cisco FTD device in a high availability pair. Which action must be taken while replacing the faulty unit?

A. Ensure that the faulty Cisco FTD device remains registered to the Cisco FMC

B. Shut down the active Cisco FTD device before powering up the replacement unit

C. Shut down the Cisco FMC before powering up the replacement unit

D. Unregister the faulty Cisco FTD device from the Cisco FMC

Question #141 *Topic 1*

An administrator is optimizing the Cisco FTD rules to improve network performance, and wants to bypass inspection for certain traffic types to reduce the load on the Cisco FTD. Which policy must be configured to accomplish this goal?

A. intrusion

B. prefilter

C. URL filtering

D. identity

Question #142 *Topic 1*

A Cisco FTD has two physical interfaces assigned to a BVI. Each interface is connected to a different VLAN on the same switch. Which firewall mode is the Cisco FTD set up to support?

A. high availability clustering

B. active/active failover

C. transparent

D. routed

Question #143 *Topic 1*

An organization is migrating their Cisco ASA devices running in multicontext mode to Cisco FTD devices. Which action must be taken to ensure that each context on the Cisco ASA is logically separated in the Cisco FTD devices?

A. Configure a container instance in the Cisco FTD for each context in the Cisco ASA.

B. Add the Cisco FTD device to the Cisco ASA port channels.

C. Configure the Cisco FTD to use port channels spanning multiple networks.

D. Add a native instance to distribute traffic to each Cisco FTD context.

Question #144 *Topic 1*

An engineer wants to change an existing transparent Cisco FTD to routed mode. The device controls traffic between two network segments. Which action is mandatory to allow hosts to reestablish communication between these two segments after the change?

A. Remove the existing dynamic routing protocol settings.

B. Configure multiple BVIs to route between segments.

C. Assign unique VLAN IDs to each firewall interface.

D. Implement non-overlapping IP subnets on each segment.

Question #145 *Topic 1*

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

A. transparent firewall mode with IRB only

B. routed firewall mode with BVI and routed interfaces

C. transparent firewall mode with multiple BVIs

D. routed firewall mode with routed interfaces only

Question #146 *Topic 1*

A network administrator is deploying a Cisco IPS appliance and needs it to operate initially without affecting traffic flows. It must also collect data to provide a baseline of unwanted traffic before being reconfigured to drop it. Which Cisco IPS mode meets these requirements?

A. failsafe

B. inline tap

C. promiscuous

D. bypass

Question #147 *Topic 1*

A network administrator is implementing an active/passive high availability Cisco FTD pair. When adding the high availability pair, the administrator cannot select the secondary peer. What is the cause?

A. The second Cisco FTD is not the same model as the primary Cisco FTD.

B. An high availability license must be added to the Cisco FMC before adding the high availability pair.

C. The failover link must be defined on each Cisco FTD before adding the high availability pair.

D. Both Cisco FTD devices are not at the same software version.

Question #148 *Topic 1*

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.

Question #149 *Topic 1*

What is an advantage of adding multiple inline interface pairs to the same inline interface set when deploying an asynchronous routing configuration?

A. Allows the IPS to identify inbound and outbound traffic as part of the same traffic flow.

B. The interfaces disable autonegotiation and interface speed is hard coded set to 1000 Mbps.

C. Allows traffic inspection to continue without interruption during the Snort process restart.

D. The interfaces are automatically configured as a media-independent interface crossover.

Question #150 *Topic 1*

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

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

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

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

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

Question #151 *Topic 1*

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.

Question #152 *Topic 1*

Which firewall design will allow it to forward traffic at layers 2 and 3 for the same subnet?

A. routed mode

B. Cisco Firepower Threat Defense mode

C. transparent mode

D. integrated routing and bridging

Question #153 *Topic 1*

An organization is configuring a new Cisco Firepower High Availability deployment. Which action must be taken to ensure that failover is as seamless as possible to end users?

A. Set the same FQDN for both chassis.

B. Set up a virtual failover MAC address between chassis.

C. Load the same software version on both chassis.

D. Use a dedicated stateful link between chassis.

Question #154 *Topic 1*

A company is in the process of deploying intrusion prevention with Cisco FTDs managed by a Cisco FMC. An engineer must configure policies to detect potential intrusions but not block the suspicious traffic. Which action accomplishes this task?

A. Configure IPS mode when creating or editing a policy rule under the Cisco FMC Intrusion tab in Access Policies section by checking the “Drop when inline” option.

B. Configure IPS mode when creating or editing a policy rule under the Cisco FMC Intrusion tab in Access Policies section by unchecking the “Drop when inline” option.

C. Configure IDS mode when creating or editing a policy rule under the Cisco FMC Intrusion tab in Access Policies section by checking the “Drop when inline” option.

D. Configure IDS mode when creating or editing a policy rule under the Cisco FMC Intrusion tab in Access Policies section by unchecking the “Drop when inline” option.

Question #155

Topic 1

An engineer is using the configure manager add Cisc404225383 command to add a new Cisco FTD device to the Cisco FMC; however, the device is not being added. Why is this occurring?

A. DONOTRESOLVE must be added to the command

B. The IP address used should be that of the Cisco FTD, not the Cisco FMC

C. The registration key is missing from the command

D. The NAT ID is required since the Cisco FMC is behind a NAT device

Question #156

Topic 1

An engineer is configuring Cisco FMC and wants to allow multiple physical interfaces to be part of the same VLAN. The managed devices must be able to perform Layer 2 switching between interfaces, including sub-interfaces. What must be configured to meet these requirements?

A. inter-chassis clustering VLAN

B. Cisco ISE Security Group Tag

C. interface-based VLAN switching

D. integrated routing and bridging

Question #157

Topic 1

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

Question #158

Topic 1

A company has many Cisco FTD devices managed by a Cisco FMC. The security model requires that access control rule logs be collected for analysis. The security engineer is concerned that the Cisco FMC will not be able to process the volume of logging that will be generated. Which configuration addresses concern this?

A. Send Cisco FTD connection events directly to a SIEM system and forward security events from Cisco FMC to the SIEM system for storage and analysis

B. Send Cisco FTD connection events and security events directly to SIEM system for storage and analysis

C. Send Cisco FTD connection events and security events to a cluster of Cisco FMC devices for storage and analysis

D. Send Cisco FTD connection events and security events to Cisco FMC and configure it to forward logs to SIEM for storage and analysis

Question #159 *Topic 1*

A network administrator reviews the file report for the last month and notices that all file types, except exe, show a disposition of unknown. What is the cause of this issue?

A. Only Spero file analysis is enabled.

B. The Cisco FMC cannot reach the Internet to analyze files.

C. A file policy has not been applied to the access policy.

D. The malware license has not been applied to the Cisco FTD.

Question #160 *Topic 1*

An engineer wants to connect a single IP subnet through a Cisco FTD firewall and enforce policy. There is a requirement to present the internal IP subnet to the outside as a different IP address. What must be configured to meet these requirements?

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

B. Configure the upstream router to perform NAT.

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

D. Configure the downstream router to perform NAT.

Question #161 *Topic 1*

A security engineer is configuring a remote Cisco FTD that has limited resources and internet bandwidth. Which malware action and protection option should be configured to reduce the requirement for cloud lookups?

A. Block File action and local malware analysis

B. Malware Cloud Lookup and dynamic analysis

C. Block Malware action and dynamic analysis

D. Block Malware action and local malware analysis

Question #162 *Topic 1*

An administrator must use Cisco FMC to install a backup route within the Cisco FTD to route traffic in case of a routing failure with primary route. Which action accomplish this task?

A. Install the static backup route and modify the metric to be less than the primary route

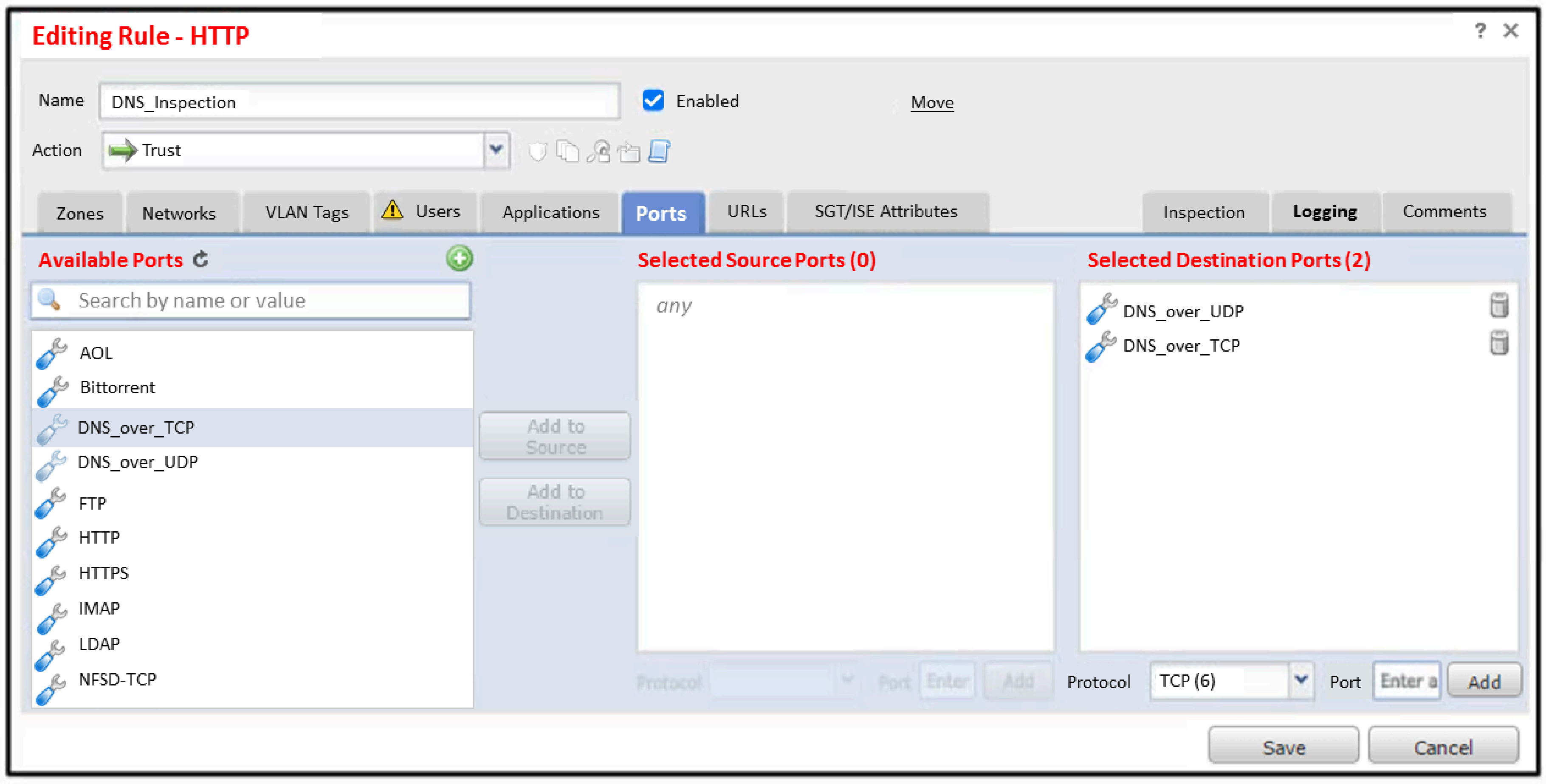
B. Use a default route in the FMC instead of having multiple routes contending for priority

C. Configure EIGRP routing on the FMC to ensure that dynamic routes are always updated

D. Create the backup route and use route tracking on both routes to a destination IP address in the network

Question #163 *Topic 1*

Refer to the exhibit.



Editing Rule - HTTP

Name: DNS_Inspection ☑ Enabled

Action: Trust

Available Ports

Search by name or value

- AOL
- Bittorrent
- DNS_over_TCP
- DNS_over_UDP
- FTP
- HTTP
- HTTPS
- IMAP
- LDAP
- NFSD-TCP

Selected Source Ports (0)

any

Selected Destination Ports (2)

- DNS_over_UDP
- DNS_over_TCP

Protocol: TCP (6) Port: Enter a

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

A. The action of the rule is set to trust instead of allow.

B. The rule is configured with the wrong setting for the source port.

C. The rule must define the source network for inspection as well as the port.

D. The rule must specify the security zone that originates the traffic.

Question #164 *Topic 1*

A network administrator configured a NAT policy that translates a public IP address to an internal web server IP address. An access policy has also been created that allows any source to reach the public IP address on port 80. The web server is still not reachable from the Internet on port 80. Which configuration change is needed?

A. The NAT policy must be modified to translate the source IP address as well as destination IP address.

B. The access policy must allow traffic to the internal web server IP address.

C. The intrusion policy must be disabled for port 80.

D. The access policy rule must be configured for the action trust.

Question #165 *Topic 1*

An administrator is adding a new URL-based category feed to the Cisco FMC for use within the policies. The intelligence source does not use STIX, but instead uses a .txt file format. Which action ensures that regular updates are provided?

A. Add a URL source and select the flat file type within Cisco FMC.

B. Add a TAXII feed source and input the URL for the feed.

C. Upload the .txt file and configure automatic updates using the embedded URL.

D. Convert the .txt file to STIX and upload it to the Cisco FMC.

Question #166 *Topic 1*

An engineer is configuring Cisco FMC and wants to limit the time allowed for processing packets through the interface. However, if the time is exceeded, the configuration must allow packets to bypass detection. What must be configured on the Cisco FMC to accomplish this task?

A. Cisco ISE Security Group Tag

B. Automatic Application Bypass

C. Inspect Local Traffic Bypass

D. Fast-Path Rules Bypass

Question #167 *Topic 1*

An engineer must define a URL object on Cisco FMC. What is the correct method to specify the URL without performing SSL inspection?

A. Include all URLs from CRL Distribution Points.

B. Use Subject Common Name value.

C. Specify all subdomains in the object group.

D. Specify the protocol in the object.

Question #168 *Topic 1*

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.

Question #169 *Topic 1*

A network administrator is migrating from a Cisco ASA to a Cisco FTD. EIGRP is configured on the Cisco ASA but it is not available in the Cisco FMC. Which action must the administrator take to enable this feature on the Cisco FTD?

A. Configure EIGRP parameters using FlexConfig objects.

B. Add the command feature eigrp via the FTD CLI.

C. Create a custom variable set and enable the feature in the variable set.

D. Enable advanced configuration options in the FMC.

Question #170 *Topic 1*

A Cisco FMC administrator wants to configure fastpathing of trusted network traffic to increase performance. In which type of policy would the administrator configure this feature?

A. Network Analysis policy

B. Identity policy

C. Prefilter policy

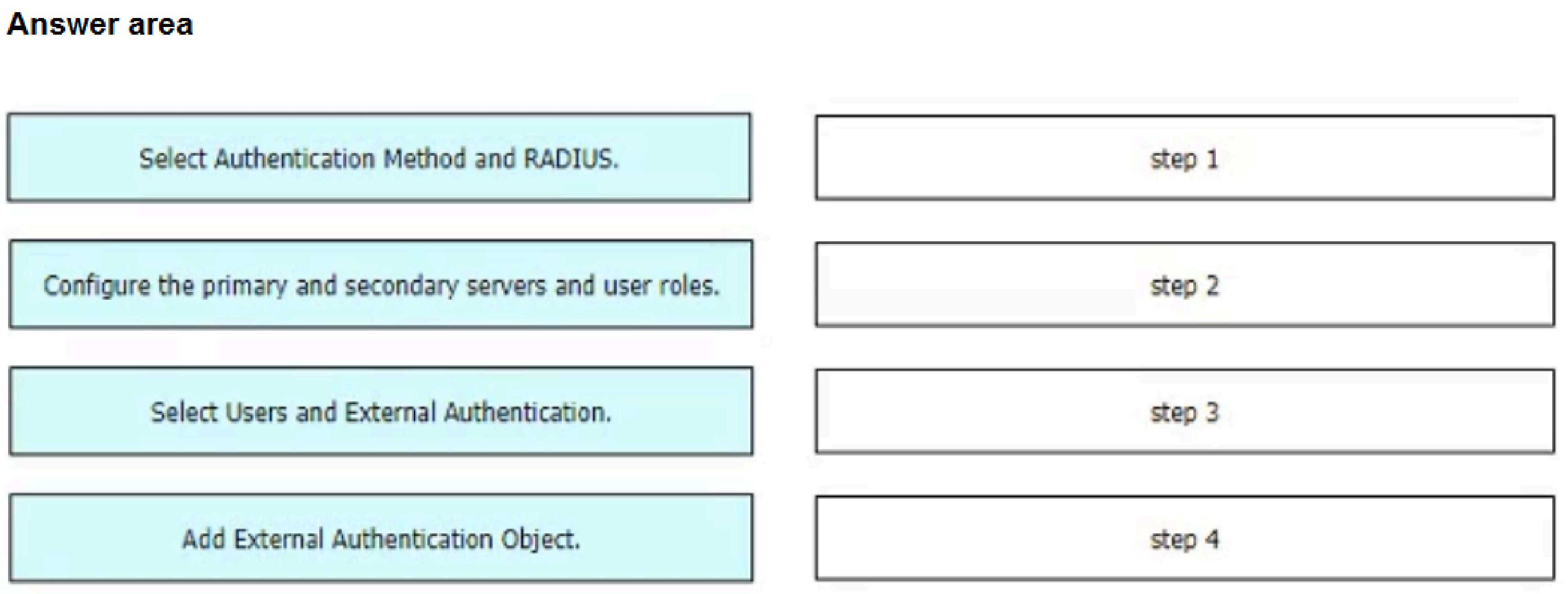
D. Intrusion policy

Question #171 *Topic 1*

DRAG DROP

-

Drag and drop the configuration steps from the left into the sequence on the right to enable external authentication on Cisco FMC to a RADIUS server.



Answer area

Select Authentication Method and RADIUS.	step 1
Configure the primary and secondary servers and user roles.	step 2
Select Users and External Authentication.	step 3
Add External Authentication Object.	step 4

Question #172 *Topic 1*

An engineer is creating an URL object on Cisco FMC. How must it be configured so that the object will match for HTTPS traffic in an access control policy?

A. Specify the protocol to match (HTTP or HTTPS).

B. Use the FQDN including the subdomain for the website.

C. Use the subject common name from the website certificate.

D. Define the path to the individual webpage that uses HTTPS.

Question #173 *Topic 1*

Which action must be taken on the Cisco FMC when a packet bypass is configured in case the Snort engine is down or a packet takes too long to process?

A. Enable Automatic Application Bypass.

B. Add a Bypass Threshold policy for failures.

C. Configure Fastpath rules to bypass inspection.

D. Enable Inspect Local Router Traffic.

Question #174 *Topic 1*

An engineer is configuring multiple Cisco FTD appliances for use in the network. Which rule must the engineer follow while defining interface objects in Cisco FMC for use with interfaces across multiple devices?

A. Two security zones can contain the same interface.

B. Interface groups can contain interfaces from many devices.

C. An interface cannot belong to a security zone and an interface group.

D. Interface groups can contain multiple interface types.

Question #175 *Topic 1*

An administrator is adding a QoS policy to a Cisco FTD deployment. When a new rule is added to the policy and QoS is applied on “Interfaces in Destination Interface Objects”, no interface objects are available. What is the problem?

A. The FTD is out of available resources for use, so QoS cannot be added.

B. The network segments that the interfaces are on do not have contiguous IP space.

C. A conflict exists between the destination interface types that is preventing QoS from being added.

D. QoS is available only on routed interfaces, and this device is in transparent mode.

Question #176 *Topic 1*

A network administrator wants to block traffic to a known malware site at https:/www.badsite.com and all subdomains while ensuring no packets from any internal client are sent to that site. Which type of policy must the network administrator use to accomplish this goal?

A. Access Control policy with URL filtering

B. Prefilter policy

C. DNS policy

D. SSL policy

Question #177 *Topic 1*

A network security engineer must export packet captures from the Cisco FMC web browser while troubleshooting an issue. When navigating to the address https:///capture/CAPI/pcap/test.pcap, an error 403: Forbidden is given instead of the PCAP file. Which action must the engineer take to resolve this issue?

A. Disable the proxy setting on the browser

B. Disable the HTTPS server and use HTTP instead

C. Use the Cisco FTD IP address as the proxy server setting on the browser

D. Enable the HTTPS server for the device platform policy

Question #178 *Topic 1*

An analyst is investigating a potentially compromised endpoint within the network and pulls a host report for the endpoint in question to collect metrics and documentation. What information should be taken from this report for the investigation?

A. client applications by user, web applications, and user connections

B. number of attacked machines, sources of the attack, and traffic patterns

C. threat detections over time and application protocols transferring malware

D. intrusion events, host connections, and user sessions

Question #179 *Topic 1*

An engineer must investigate a connectivity issue and decides to use the packet capture feature on Cisco FTD. The goal is to see the real packet going through the Cisco FTD device and see Snort detection actions as a part of the output. After the capture-traffic command is issued, only the packets are displayed. Which action resolves this issue?

A. Specify the trace using the -T option after the capture-traffic command

B. Perform the trace within the Cisco FMC GUI instead of the Cisco FMC CLI

C. Use the verbose option as a part of the capture-traffic command

D. Use the capture command and specify the trace option to get the required information

Question #180 *Topic 1*

An analyst using the security analyst account permissions is trying to view the Correlations Events Widget but is not able to access it. However, other dashboards are accessible. Why is this occurring?

A. The widget is configured to display only when active events are present

B. The security analyst role does not have permission to view this widget

C. An API restriction within the Cisco FMC is preventing the widget from displaying

D. The widget is not configured within the Cisco FMC

Question #181 *Topic 1*

An engineer is troubleshooting connectivity to the DNS servers from hosts behind a new Cisco FTD device. The hosts cannot send DNS queries to servers in the DMZ. Which action should the engineer take to troubleshoot this issue using the real DNS packets?

A. Use the packet capture tool to check where the traffic is being blocked and adjust the access control or intrusion policy as needed

B. Use the Connection Events dashboard to check the block reason and adjust the inspection policy as needed

C. Use the packet tracer tool to determine at which hop the packet is being dropped

D. Use the show blocks command in the Threat Defense CLI tool and create a policy to allow the blocked traffic

Question #182 *Topic 1*

An engineer must configure a Cisco FMC dashboard in a child domain. Which action must be taken so that the dashboard is visible to the parent domain?

A. Adjust policy inheritance settings

B. Add a separate widget

C. Create a copy of the dashboard

D. Add a separate tab

Question #183 *Topic 1*

A network engineer sets up a secondary Cisco FMC that is integrated with Cisco Security Packet Analyzer. What occurs when the secondary Cisco FMC synchronizes with the primary Cisco FMC?

A. The existing configuration for integration of the secondary Cisco FMC the Cisco Security Packet Analyzer is overwritten.

B. The synchronization between the primary and secondary Cisco FMC fails.

C. The existing integration configuration is replicated to the primary Cisco FMC.

D. The secondary Cisco FMC must be reintegrated with the Cisco Security Packet Analyzer after the synchronization.

Question #184 *Topic 1*

An analyst is reviewing the Cisco FMC reports for the week. They notice that some peer-to-peer applications are being used on the network and they must identify which poses the greatest risk to the environment. Which report gives the analyst this information?

A. User Risk Report

B. Advanced Malware Risk Report

C. Attacks Risk Report

D. Network Risk Report

Question #185 *Topic 1*

An administrator receives reports that users cannot access a cloud-hosted web server. The access control policy was recently updated with several new policy additions and URL filtering. What must be done to troubleshoot the issue and restore access without sacrificing the organization's security posture?

A. Download a PCAP of the traffic attempts to verify the blocks and use the flexconfig objects to create a rule that allows only the required traffic to the destination server.

B. Identify the blocked traffic in the Cisco FMC connection events to validate the block, and modify the policy to allow the traffic to the web server.

C. Create a new access control policy rule to allow ports 80 and 443 to the FQDN of the web server.

D. Verify the blocks using the packet capture tool and create a rule with the action monitor for the traffic.

Question #186 *Topic 1*

An engineer is reviewing a ticket that requests to allow traffic for some devices that must connect to a server over 8699/udp. The request mentions only one IP address, 172.16.18.15, but the requestor asked for the engineer to open the port for all machines that have been trying to connect to it over the last week. Which action must the engineer take to troubleshoot this issue?

A. Use the context explorer to see the application blocks by protocol.

B. Filter the connection events by the source port 8699/udp.

C. Filter the connection events by the destination port 8699/udp.

D. Use the context explorer to see the destination port blocks.

Question #187 *Topic 1*

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

A. investigate

B. REST

C. reporting

D. enforcement

Question #188 *Topic 1*

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.

Question #189 *Topic 1*

An engineer runs the command restore remote-manager-backup location 2.2.2.2 admin/Volume/home/admin FTD411247145.zip on a Cisco FMC. After connecting to the repository, the Cisco FTD device is unable to accept the backup file. What is the reason for this failure?

A. The wrong IP address is used.

B. The directory location is incorrect.

C. The backup file is not in .cfg format.

D. The backup file extension was changed from .tar to .zip.

Question #190 *Topic 1*

The CIO asks a network administrator to present to management a dashboard that shows custom analysis tables for the top DNS queries URL category statistics, and the URL reputation statistics. Which action must the administrator take to quickly produce this information for management?

A. Run the Attack report and filter on DNS to show this information.

B. Create a new dashboard and add three custom analysis widgets that specify the tables needed.

C. Modify the Connection Events dashboard to display the information in a view for management.

D. Copy the intrusion events dashboard tab and modify each widget to show the correct charts.

Question #191 *Topic 1*

Which Cisco FMC report gives the analyst information about the ports and protocols that are related to the configured sensitive network for analysis?

A. Malware Report

B. Host Report

C. Firepower Report

D. Network Report

Question #192 *Topic 1*

An engineer is investigating connectivity problems on Cisco Firepower for a specific SGT. Which command allows the engineer to capture real packets that pass through the firewall using an SGT of 64?

A. capture CAP type inline-tag 64 match ip any any

B. capture CAP match 64 type inline-tag ip any any

C. capture CAP headers-only type inline-tag 64 match ip any any

D. capture CAP buffer 64 match ip any any

Question #193 *Topic 1*

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

A. Connectivity Over Security

B. Balanced Security and Connectivity

C. Maximum Detection

D. No Rules Active

Question #194 *Topic 1*

An engineer wants to add an additional Cisco FTD Version 6.2.3 device to their current 6.2.3 deployment to create a high availability pair. The currently deployed Cisco FTD device is using local management and identical hardware including the available port density to enable the failover and stateful links required in a proper high availability deployment. Which action ensures that the environment is ready to pair the new Cisco FTD with the old one?

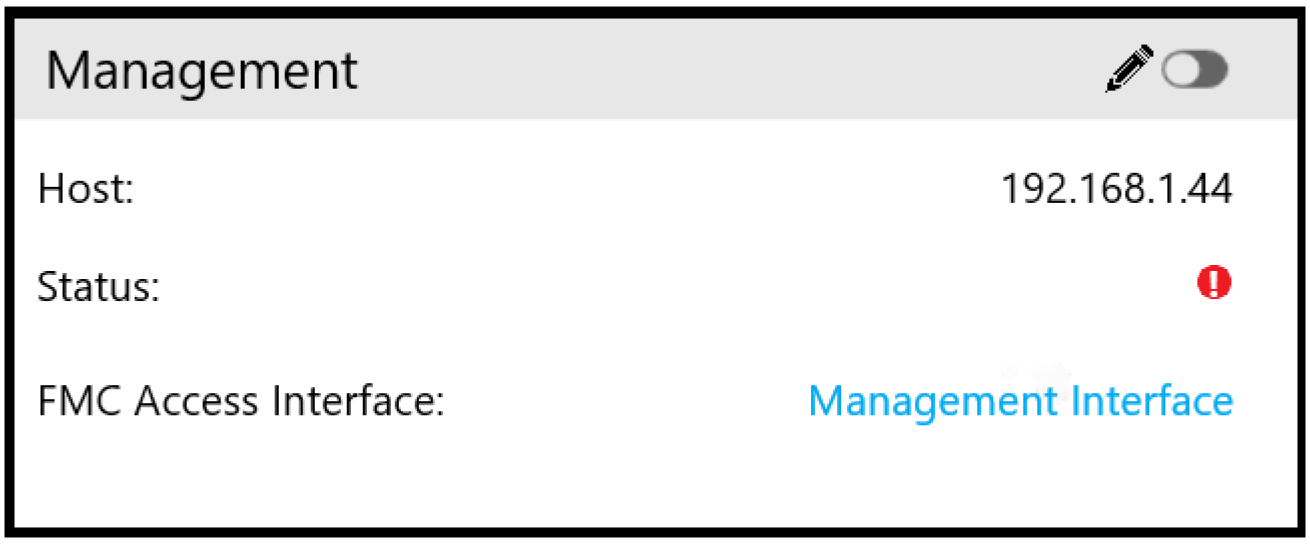
A. Change from Cisco FDM management to Cisco FMC management on both devices and register them to FMC.

B. Ensure that the two devices are assigned IP addresses from the 169.254.0.0/16 range for failover interfaces.

C. Factory reset the current Cisco FTD so that it can synchronize configurations with the new Cisco FTD device.

D. Ensure that the configured DNS servers match on the two devices for name resolution.

Question #195 *Topic 1*



Management

Host: 192.168.1.44

Status: ❗

FMC Access Interface: Management Interface

Refer to the exhibit. What is the effect of the existing Cisco FMC configuration?

A. The remote management port for communication between the Cisco FMC and the managed device changes to port 8443.

B. The managed device is deleted from the Cisco FMC.

C. The SSL-encrypted communication channel between the Cisco FMC and the managed device becomes plain-text communication channel.

D. The management connection between the Cisco FMC and the Cisco FTD is disabled.

Question #196 *Topic 1*

Remote users who connect via Cisco AnyConnect to the corporate network behind a Cisco FTD device report that they get no audio when calling between remote users using their softphones. These same users can call internal users on the corporate network without any issues. What is the cause of this issue?

A. FTD has no NAT policy that allows outside to outside communication.

B. Split tunneling is enabled for the Remote Access VPN on FTD.

C. The hairpinning feature is not available on FTD.

D. The Enable Spoke to Spoke Connectivity through Hub option is not selected on FTD.

Question #197 *Topic 1*

A network administrator is troubleshooting access to a website hosted behind a Cisco FTD device. External clients cannot access the web server via HTTPS. The IP address configured on the web server is 192.168.7.46. The administrator is running the command capture CAP interface outside match ip any 192.168.7.46 255.255.255.255 but cannot see any traffic in the capture. Why is this occurring?

A. The capture must use the public IP address of the web server.

B. The packet capture shows only blocked traffic.

C. The FTD has no route to the web server.

D. The access policy is blocking the traffic.

Question #198 *Topic 1*

An engineer must deploy a Cisco FTD appliance via Cisco FMC to span a network segment to detect malware and threats. When setting the Cisco FTD interface mode, which sequence of actions meets this requirement?

A. Set to passive, and configure an access control policy with an intrusion policy and a file policy defined.

B. Set to passive, and configure an access control policy with a prefilter policy defined.

C. Set to none, and configure an access control policy with an intrusion policy and a file policy defined.

D. Set to none, and configure an access control policy with a prefilter policy defined.

Question #199 *Topic 1*

An engineer wants to perform a packet capture on the Cisco FTD to confirm that the host using IP address 192.168.100.100 has the MAC address of 1234.5678.901 to help troubleshoot a connectivity issue. What is the correct tcpdump command syntax to ensure that the MAC address appears in the packet capture output?

A. -w capture.pcap -s 1518 host 192.168.100.100 ether

B. -w capture.pcap -s 1518 host 192.168.100.100 mac

C. -nm src 192.168.100.100

D. -ne src 192.168.100.100

Question #200 *Topic 1*

What must be implemented on Cisco Firepower to allow multiple logical devices on a single physical device to have access to external hosts?

A. Add at least two container instances from the same module.

B. Set up a cluster control link between all logical devices.

C. Define VLAN subinterfaces for each logical device.

D. Add one shared management interface on all logical devices.

Question #201 *Topic 1*

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. Copy it to the current domain.

B. Add it as a separate widget.

C. Change the document attributes.

D. Assign themselves ownership of it.

Question #202 *Topic 1*

A company is deploying intrusion protection on multiple Cisco FTD appliances managed by Cisco FMC. Which system-provided policy must be selected if speed and detection are priorities?

A. Maximum Detection

B. Connectivity Over Security

C. Security Over Connectivity

D. Balanced Security and Connectivity

Question #203 *Topic 1*

An engineer integrates Cisco FMC and Cisco ISE using pxGrid. Which role is assigned for Cisco FMC?

A. server

B. controller

C. publisher

D. client

Question #204 *Topic 1*

A company wants a solution to aggregate the capacity of two Cisco FTD devices to make the best use of resources such as bandwidth and connections per second. Which order of steps must be taken across the Cisco FTDs with Cisco FMC to meet this requirement?

A. Add members to the Cisco FMC, configure Cisco FTD interfaces, create the cluster in Cisco FMC, and configure cluster members in Cisco FMC

B. Add members to Cisco FMC, configure Cisco FTD interfaces in Cisco FMC, configure cluster members in Cisco FMC, create cluster in Cisco FMC, and configure cluster members in Cisco FMC

C. Configure the Cisco FTD interfaces, add members to FMC, configure cluster members in FMC, and create cluster in Cisco FMC

D. Configure the Cisco FTD interfaces and cluster members, add members to Cisco FMC, and create the cluster in Cisco FMC

Question #205 *Topic 1*

The administrator notices that there is malware present with an .exe extension and needs to verify if any of the systems on the network are running the executable file. What must be configured within Cisco AMP for Endpoints to show this data?

A. vulnerable software

B. file analysis

C. threat root cause

D. prevalence

Question #206 *Topic 1*

Upon detecting a flagrant threat on an endpoint, which two technologies instruct Cisco Identity Services Engine to contain the infected endpoint either manually or automatically? (Choose two.)

A. Cisco Stealthwatch

B. Cisco ASA 5500 Series

C. Cisco FMC

D. Cisco ASR 7200 Series

E. Cisco AMP

Question #207 *Topic 1*

A security engineer found a suspicious file from an employee email address and is trying to upload it for analysis, however the upload is failing. The last registration status is still active. What is the cause for this issue?

A. Cisco AMP for Networks is unable to contact Cisco Threat Grid on premise.

B. There is a host limit set.

C. The user agent status is set to monitor.

D. Cisco AMP for Networks is unable to contact Cisco Threat Grid Cloud.

Question #208 *Topic 1*

What is the role of the casebook feature in Cisco Threat Response?

A. pulling data via the browser extension

B. alert prioritization

C. sharing threat analysis

D. triage automation with alerting

Question #209 *Topic 1*

An engineer is troubleshooting a file that is being blocked by a Cisco FTD device on the network. The user is reporting that the file is not malicious. Which action does the engineer take to identify the file and validate whether or not it is malicious?

A. Identify the file in the intrusion events and submit it to Threat Grid for analysis.

B. Use FMC file analysis to look for the file and select Analyze to determine its disposition.

C. Use the context explorer to find the file and download it to the local machine for investigation.

D. Right click the connection event and send the file to AMP for Endpoints to see if the hash is malicious.