Cisco.300-710.vJun-2024.by.Rickynoe.175q

Number: 300-710
Passing Score: 800
Time Limit: 120
File Version: 23.0

Exam Code: 300-710
Exam Name: Securing Networks with Cisco Firepower (SNCF)

Exam A

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

Correct Answer: C
Section:
Explanation:
https://www.cisco.com/c/en/us/td/docs/security/firepower/623/fdm/fptd-fdm-config-guide-623/fptd-fdm-intrusion.html

QUESTION 2
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. Delete and reregister the device to Cisco FMC
B. Update the IP addresses from IFV4 to IPv6 without deleting the device from Cisco FMC
C. Format and reregister the device to Cisco FMC.
D. Cisco FMC does not support devices that use IPv4 IP addresses.

Correct Answer: A
Section:

QUESTION 3
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 applicable rules?

A. utilizing policy inheritance
B. utilizing a dynamic ACP that updates from Cisco Talos
C. creating a unique ACP per device
D. creating an ACP with an INSIDE_NET network object and object overrides

Correct Answer: D
Section:

QUESTION 4
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. event viewer
B. reports

C. dashboards
D. context explorer

Correct Answer: B
Section:

QUESTION 5
With Cisco FTD integrated routing and bridging, which interface does the bridge group use to communicate with a routed interface?

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

Correct Answer: C
Section:
Explanation:
Reference:
https://www.cisco.com/c/en/us/td/docs/security/firepower/640/configuration/guide/fpmc-configguide-v64/transparent_or_routed_firewall_mode_for_firepower_threat_defense.html

QUESTION 6
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 intrusion policy must be disabled for port 80.
B. The access policy rule must be configured for the action trust.
C. The NAT policy must be modified to translate the source IP address as well as destination IP address.
D. The access policy must allow traffic to the internal web server IP address.

Correct Answer: D
Section:

QUESTION 7
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. Add a separate tab.
B. Adjust policy inheritance settings.
C. Add a separate widget.
D. Create a copy of the dashboard.

Correct Answer: D
Section:

QUESTION 8
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 Connection Events dashboard to check the block reason and adjust the inspection policy as needed.
B. Use the packet capture tool to check where the traffic is being blocked and adjust the access control or intrusion 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.

Correct Answer: A
Section:

QUESTION 9
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. Which technique will retain the policy consistency at each location but allow only the locally significant network subnet within the applicable rules?

A. utilizing a dynamic Access Control Policy that updates from Cisco Talos
B. utilizing policy inheritance
C. creating a unique Access Control Policy per device
D. creating an Access Control Policy with an INSIDE_NET network object and object overrides

Correct Answer: D
Section:

QUESTION 10
An engineer runs the command restore remote-manager-backup location 2.2.2.2 admin /Volume/home/admin FTD408566513.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 backup file is not in .cfg format.
B. The wrong IP address is used.
C. The backup file extension was changed from .tar to .zip.
D. The directory location is incorrect.

Correct Answer: C
Section:
Explanation:
Reference: https://www.ciscolive.com/c/dam/r/ciscolive/emea/docs/2019/pdf/BRKSEC-3455.pdf

QUESTION 11
While configuring FTD, a network engineer wants to ensure that traffic passing through the appliance does not require routing or Vlan rewriting. Which interface mode should the engineer implement to accomplish this task?

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

Correct Answer: B
Section:

QUESTION 12
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. generate events
B. drop packet
C. drop connection
D. drop and generate

Correct Answer: B
Section:
Explanation:
Reference"
https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-configguide-v62/working_with_intrusion_events.html

QUESTION 13
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. transparent
B. routed
C. passive
D. inline set

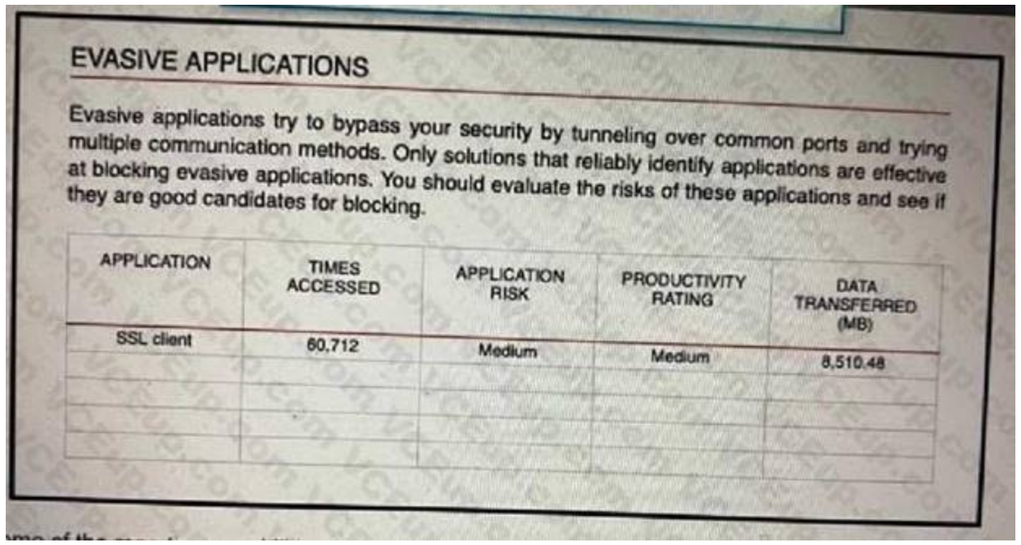
Correct Answer: D
Section:
Explanation:
Reference:
https://www.cisco.com/c/en/us/td/docs/security/firepower/630/configuration/guide/fpmc-configguide-v63/inline_sets_and_passive_interfaces_for_firepower_threat_defense.html

QUESTION 14
Which two considerations must be made when deleting and re-adding devices while managing them via Cisco FMC (Choose two).

A. Before re-adding the device In Cisco FMC, the manager must be added back.
B. The Cisco FMC web interface prompts users to re-apply access control policies.
C. Once a device has been deleted, It must be reconfigured before it is re-added to the Cisco FMC.
D. An option to re-apply NAT and VPN policies during registration is available, so users do not need to re-apply the polices after registration is completed.
E. There is no option to re-apply NAT and VPN policies during registration is available, so users need to re-apply the policies after registration is completed.

Correct Answer: B, E
Section:

QUESTION 15
Refer to the exhibit.



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

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 cloud be used for evasion. Which action will mitigate this risk?

A. Use SSL decryption to analyze the packets.
B. Use encrypted traffic analytics to detect attacks
C. Use Cisco AMP for Endpoints to block all SSL connection
D. Use Cisco Tetration to track SSL connections to servers.

Correct Answer: A
Section:

QUESTION 16
An engineer is troubleshooting application failures through a 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 application-identification-debug command to determine which rules the traffic matching and modify the rule accordingly
C. Use the system support firewall-engine-dump-user-f density-data command to change the policy and allow the application through the firewall.
D. Use the system support network-options command to fine tune the policy.

Correct Answer: A
Section:

QUESTION 17
An administrator is attempting to remotely log into a switch in the data centre using SSH and is unable to connect. How does the administrator confirm that traffic is reaching the firewall?

A. by running Wireshark on the administrator's PC
B. by performing a packet capture on the firewall.
C. by running a packet tracer on the firewall.
D. by attempting to access it from a different workstation.

Correct Answer: B
Section:

QUESTION 18
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. All types of Firepower devices are supported.
C. Supports all devices that are running supported versions of Firepower
D. An on-premises proxy server does not need to set up and maintained

Correct Answer: D
Section:
Explanation:
Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/integrations/CTR/Firepower_and_Cisco_Threat_Response_Integration_Guide.pdf

QUESTION 19

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 addresses globally in the quickest way possible and with the least amount of impact?

A. by denying outbound web access
B. Cisco Talos will automatically update the policies.
C. by Isolating the endpoint
D. by creating a URL object in the policy to block the website

Correct Answer: D
Section:

QUESTION 20
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. identity
B. Intrusion
C. Access Control
D. Prefilter

Correct Answer: C
Section:
Explanation:
Reference:
https://www.cisco.com/c/en/us/td/docs/security/firepower/migration-tool/migrationguide/ASA2FTD-with-FP-Migration-Tool/b_Migration_Guide_ASA2FTD_chapter_01011.html

QUESTION 21
Which two routing options are valid with Cisco FTD? (Choose Two)

A. BGPv6
B. ECMP with up to three equal cost paths across multiple interfaces
C. ECMP with up to three equal cost paths across a single interface
D. BGPv4 in transparent firewall mode
E. BGPv4 with nonstop forwarding

Correct Answer: A, C
Section:
Explanation:
Reference:
https://www.cisco.com/c/en/us/td/docs/security/firepower/601/configuration/guide/fpmc-configguide-v601/fpmc-config-guide-v60_chapter_01100011.html#ID-2101-0000000e

QUESTION 22
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.

Correct Answer: A
Section:

QUESTION 23
With Cisco Firepower Threat Defense software, which interface mode must be configured to passively receive traffic that passes through the appliance?

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

Correct Answer: B
Section:
Explanation:
Reference:
https://www.cisco.com/c/en/us/td/docs/security/firepower/640/configuration/guide/fpmc-configguide-v64/interface_overview_for_firepower_threat_defense.html

QUESTION 24
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

Correct Answer: A, B
Section:
Explanation:
Reference:
https://www.cisco.com/c/en/us/td/docs/security/firepower/610/configuration/guide/fpmc-configguide-v61/firepower_threat_defense_high_availability.html

QUESTION 25
Which protocol establishes network redundancy in a switched Firepower device deployment?

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

Correct Answer: A
Section:
Explanation:
Reference:
https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-configguide-v62/firepower_threat_defense_high_availability.html

QUESTION 26
Which interface type allows packets to be dropped?

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

Correct Answer: B
Section:
Explanation:
Reference: https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/200908-configuring-firepower- threat-defense-int.html

QUESTION 27
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

Correct Answer: C, E
Section:
Explanation:
https://www.cisco.com/c/en/us/td/docs/security/firepower/610/fdm/fptd-fdm-config-guide-610/fptd-fdm- interfaces.html

QUESTION 28
Which two dynamic routing protocols are supported in Firepower Threat Defense without using FlexConfig? (Choose two.)

A. EIGRP
B. OSPF
C. static routing
D. IS-IS
E. BGP

Correct Answer: B, E
Section:
Explanation:
Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/660/fdm/fptd-fdm-configguide-660/fptd- fdm-routing.html

QUESTION 29
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

Correct Answer: C
Section:

QUESTION 30
What are two application layer preprocessors? (Choose two.)

A. CIFS
B. IMAP
C. SSL
D. DNP3
E. ICMP

Correct Answer: B, C
Section:
Explanation:
Reference:
https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-configguide-v60/Application_Layer_Preprocessors.html

QUESTION 31
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.

Correct Answer: C
Section:
Explanation:
Reference: https://www.cisco.com/c/en/us/td/docs/security/asa/asa96/configuration/general/asa-96-general-config/intro-fw.html

QUESTION 32
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

Correct Answer: C
Section:

QUESTION 33
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

Correct Answer: A
Section:
Explanation:
https://www.cisco.com/c/en/us/td/docs/security/asa/asa910/configuration/firewall/asa-910-firewall-config/access-sfr.htmlInline tap monitor-only mode (ASA inline)—In an inline tap monitor-only deployment, a copy of thetraffic is sent to the ASA FirePOWER module, but it is not returned to the ASA. Inline tap mode letsyou see what the ASA FirePOWER module would have done to traffic, and lets you evaluate thecontent of the traffic, without impacting the network.
However, in this mode, the ASA does apply itspolicies to the traffic, so traffic can be dropped due to access rules, TCP normalization, and so forth.

QUESTION 34
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 neighbouring 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.

Correct Answer: C
Section:
Explanation:
"In routed firewall mode, broadcast and multicast traffic is blocked even if you allow it in an access rule..." "The bridge group does not pass CDP packets packets..."
https://www.cisco.com/c/en/us/td/docs/security/asa/asa913/configuration/general/asa-913-general-config/intro-fw.htmlPassing Traffic Not Allowed in Routed ModeIn routed mode, some types of traffic cannot pass through the ASA even if you allow it in an accessrule. The bridge group, however, can allow almost any traffic through using either an access rule (forIP traffic) or an EtherType rule (for non-IP traffic):
IP traffic—In routed firewall mode, broadcast and "multicast traffic is blocked even if you allow it in an access rule," including unsupported dynamic routing protocols and DHCP (unless you configure DHCP relay). Within a bridge group, you can allow this traffic with an access rule (using an extended ACL).
Non-IP traffic—AppleTalk, IPX, BPDUs, and MPLS, for example, can be configured to go through using an EtherType rule.
Note
"The bridge group does not pass CDP packets packets, or any packets that do not have a valid EtherType greater than or equal to 0x600. An exception is made for BPDUs and IS-IS, which are supported. "

QUESTION 35

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 BVl 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.

Correct Answer: D
Section:
Explanation:
Traditionally, a firewall is a routed hop and acts as a default gateway for hosts that connect to one of its screened subnets. A transparent firewall, on the other hand, is a Layer 2 firewall that acts like a "bump in the wire," or a "stealth firewall," and is not seen as a router hop to connected devices.
However, like any other firewall, access control between interfaces is controlled, and all of the usual firewall checks are in place. Layer 2 connectivity is achieved by using a "bridge group" where you group together the inside and outside interfaces for a network, and the ASA uses bridging techniques to pass traffic between the interfaces. Each bridge group includes a Bridge Virtual Interface (BVI) to which you assign an IP address on the network. You can have multiple bridge groups for multiple networks. In transparent mode, these bridge groups cannot communicate with each other.
https://www.cisco.com/c/en/us/td/docs/security/asa/asa97/configuration/general/asa-97-generalconfig/intro-fw.html

QUESTION 36
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

Correct Answer: B, E
Section:
Explanation:
https://www.cisco.com/c/en/us/support/docs/security/firepower-management-center/212699-configure-ftd-high-availability-on-firep.htmlConditionsIn order to create an HA between 2 FTD devices, these conditions must be met:
Same model
Same version (this applies to FXOS and to FTD - (major (first number), minor (second number), and maintenance (third number) must be equal)) Same number of interfaces Same type of interfaces Both devices as part of same group/domain in FMC Have identical Network Time Protocol (NTP) configuration Be fully deployed on the FMC without uncommitted changes Be in the same firewall mode: routed or transparent.
Note that this must be checked on both FTD devices and FMC GUI since there have been cases where the FTDs had the same mode, but FMC does not reflect this.
Does not have DHCP/Point-to-Point Protocol over Ethernet (PPPoE) configured in any of the interface Different hostname (Fully Qualified Domain Name (FQDN)) for both chassis. In order to check the chassis hostname navigate to FTD CLI and run this command

QUESTION 37
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.

Correct Answer: C
Section:

QUESTION 38
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. span EtherChannel clustering
B. redundant interfaces
C. high availability active/standby firewalls
D. multi-instance firewalls

Correct Answer: D
Section:

QUESTION 39
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. Inline tap
B. passive
C. transparent
D. routed

Correct Answer: A
Section:

QUESTION 40
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. Shut down the Cisco FMC before powering up the replacement unit.
B. Ensure that the faulty Cisco FTD device remains registered to the Cisco FMC.
C. Unregister the faulty Cisco FTD device from the Cisco FMC
D. Shut down the active Cisco FTD device before powering up the replacement unit.

Correct Answer: C
Section:

QUESTION 41
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. prefilter
B. intrusion
C. identity
D. URL filtering

Correct Answer: A

Section:

QUESTION 42
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. active/active failover
B. transparent
C. routed
D. high availability clustering

Correct Answer: B
Section:

QUESTION 43
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. Add a native instance to distribute traffic to each Cisco FTD context.
B. Add the Cisco FTD device to the Cisco ASA port channels.
C. Configure a container instance in the Cisco FTD for each context in the Cisco ASA.
D. Configure the Cisco FTD to use port channels spanning multiple networks.

Correct Answer: C
Section:

QUESTION 44
Which firewall design allows a firewall to forward traffic at layer 2 and layer 3 for the same subnet?

A. Cisco Firepower Threat Defense mode
B. transparent mode
C. routed mode
D. integrated routing and bridging

Correct Answer: B
Section:
Explanation:
Topic 2, Configuration

QUESTION 45
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

Correct Answer: B, E
Section:
Explanation:
Reference:
https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-configguide-v62/ospf_for_firepower_threat_defense.html

QUESTION 46
When creating a report template, how can the results be limited to show only the activity of a specific subnet?

A. Create a custom search in Firepower Management Center 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.

Correct Answer: B
Section:
Explanation:
Reference: https://www.cisco.com/c/en/us/td/docs/security/firesight/541/user-guide/FireSIGHTSystem-UserGuide-v5401/Reports.html#87267

QUESTION 47
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.

Correct Answer: C
Section:
Explanation:
Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/fxos/clustering/ftd-clustersolution.html#concept_g32_yml_y2b

QUESTION 48
Which two statements about bridge-group interfaces in Cisco FTD are true? (Choose two.)

A. The BVI IP address must be in a separate subnet from the connected network.
B. Bridge groups are supported in both transparent and routed firewall modes.
C. Bridge groups are supported only in transparent firewall mode.
D. Bidirectional Forwarding Detection echo packets are allowed through the FTD when using bridgegroup members.
E. Each directly connected network must be on the same subnet.

Correct Answer: B, E
Section:
Explanation:
Reference:
https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-configguide-v62/transparent_or_routed_firewall_mode_for_firepower_threat_defense.html

QUESTION 49

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

Correct Answer: D
Section:
Explanation:
Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/misc/fmc-ftd-mgmt-nw/fmcftd-mgmt- nw.html#id_106101

QUESTION 50
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

Correct Answer: A, B
Section:
Explanation:
Reference: https://www.cisco.com/c/en/us/td/docs/security/firesight/541/firepower-module-userguide/asa- firepower-module-user-guide-v541/AC-Rules-Tuning-Overview.html#71854

QUESTION 51
Which two routing options are valid with Cisco Firepower Threat Defense? (Choose two.)

A. BGPv6
B. ECMP with up to three equal cost paths across multiple interfaces
C. ECMP with up to three equal cost paths across a single interface
D. BGPv4 in transparent firewall mode
E. BGPv4 with nonstop forwarding

Correct Answer: A, C
Section:
Explanation:
Reference:
https://www.cisco.com/c/en/us/td/docs/security/firepower/601/configuration/guide/fpmc-configguide-v601/fpmc-config-guide-v60_chapter_01100011.html#ID-2101-0000000e

QUESTION 52
Which object type supports object overrides?

A. time range
B. security group tag
C. network object

D. DNS server group

Correct Answer: C
Section:
Explanation:
Reference:
https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-configguide-v60/Reusable_Objects.html#concept_8BFE8B9A83D742D9B647A74F7AD50053

QUESTION 53
Which Cisco Firepower rule action displays an HTTP warning page?

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

Correct Answer: C
Section:
Explanation:
Reference: https://www.cisco.com/c/en/us/td/docs/security/firesight/541/user-guide/FireSIGHTSystem-UserGuide-v5401/AC-Rules-Tuning-Overview.html#76698

QUESTION 54
What is the result of 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.

Correct Answer: B
Section:
Explanation:
Reference:
https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-configguide-v62/quality_of_service_qos.pdf

QUESTION 55
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

Correct Answer: D
Section:
Explanation:
Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/620/relnotes/Firepower_System_Release_Notes_Version_620/new_features_and_functionality.html

QUESTION 56
In which two places can thresholding settings be 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

Correct Answer: A, C
Section:
Explanation:
Reference: https://www.cisco.com/c/en/us/td/docs/security/firesight/541/firepower-module-userguide/asa- firepower-module-user-guide-v541/Intrusion-Global-Threshold.pdf

QUESTION 57
In which two ways do access control policies operate on a Cisco Firepower system? (Choose two.)

A. Traffic inspection can be interrupted temporarily when configuration changes are deployed.
B. The system performs intrusion inspection followed by file inspection.
C. They can 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.

Correct Answer: A, C
Section:
Explanation:
Reference:
https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-configguide-v60/Access_Control_Using_Intrusion_and_File_Policies.html

QUESTION 58
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 applicationprotocols.
B. reputation-based objects that represent Security Intelligence feeds and lists, application filters based on category and reputation, and file lists
C. network-based objects that represent IP address and networks, port/protocols pairs, VLAN tags, security zones, and origin/destination country
D. network-based objects that represent FQDN mappings and networks, port/protocol pairs, VXLAN tags, security zones and origin/destination country
E. reputation-based objects, such as URL categories

Correct Answer: B, C
Section:
Explanation:
Reference:
https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-configguide-v62/reusable_objects.html#ID-2243-00000414

QUESTION 59
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.

Correct Answer: A
Section:
Explanation:
https://www.cisco.com/c/en/us/support/docs/security/firepower-management-center/212702-configure-and-verify-nat-on-ftd.html

QUESTION 60
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.

Correct Answer: D
Section:
Explanation:
https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-configguide-v62/reusable_objects.html#ID-2243-000009b4"All interfaces in an interface object must be of the same type: all inline, passive, switched, routed,or ASA FirePOWER. After you create an interface object, you cannot change the type of interfaces itcontains."

QUESTION 61
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.

Correct Answer: C
Section:
Explanation:
Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/640/fdm/fptd-fdm-configguide-640/fptd-fdm-identity.html#concept_655B055575E04CA49B10186DEBDA301A

QUESTION 62
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 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.
B. 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.
C. 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.
D. 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.

Correct Answer: A
Section:

QUESTION 63
An engineer is using the configure manager add <FMC IP> Cisc402098527 command to add a new Cisco FTD device to the Cisco FMC; however, the device is not being added. Why Is this occurring?

A. The NAT ID is required since the Cisco FMC is behind a NAT device.
B. The IP address used should be that of the Cisco FTD. not the Cisco FMC.
C. DONOTRESOLVE must be added to the command
D. The registration key is missing from the command

Correct Answer: A
Section:

QUESTION 64
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. interface-based VLAN switching
B. inter-chassis clustering VLAN
C. integrated routing and bridging
D. Cisco ISE Security Group Tag

Correct Answer: C
Section:

QUESTION 65
An engineer configures a network discovery policy on Cisco FMC. Upon configuration, it is noticed that excessive and misleading events filing the database and overloading the Cisco FMC. A monitored NAT device is executing multiple updates of its operating system in a short period of time.
What configuration change must be made to alleviate this issue?

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

Correct Answer: D
Section:
Explanation:
Reference:
https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-configguide-v60/Network_Discovery_Policies.html

QUESTION 66
An organization does not want to use the default Cisco Firepower block page when blocking HTTPtraffic. The organization wants to include information about its policies and procedures to helpeducate the users whenever a block occurs.
Which two steps must be taken to meet theserequirements? (Choose two.)

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

B. Create HTML code with the information for the policies and procedures.
C. Edit the HTTP request handling in the access control policy to customized block.
D. Write CSS code with the information for the policies and procedures.
E. Change the HTTP response in the access control policy to custom.

Correct Answer: B, E
Section:

QUESTION 67
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 this concern?

A. Send Cisco FTD connection events and security events directly to SIEM system for storage and analysis.
B. Send Cisco FTD connection events and security events to a cluster of Cisco FMC devices for storage and analysis.
C. Send Cisco FTD connection events and security events to Cisco FMC and configure it to forward logs to SIEM for storage and analysis.
D. 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.

Correct Answer: C
Section:

QUESTION 68
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. The malware license has not been applied to the Cisco FTD.
B. The Cisco FMC cannot reach the Internet to analyze files.
C. A file policy has not been applied to the access policy.
D. Only Spero file analysis is enabled.

Correct Answer: C
Section:
Explanation:
A file policy defines the actions that the Cisco Firepower Threat Defense (FTD) device should take whenit encounters different types of files. The file policy is applied as part of an access control policy. If anaccess control policy does not include a file policy, the FTD device will not take any action on the files itencounters, resulting in a disposition of 'unknown' for all file types except exe

QUESTION 69
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 indicated 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.

Correct Answer: A
Section:

QUESTION 70
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

Correct Answer: C
Section:
Explanation:
Reference: https://www.cisco.com/c/en/us/td/docs/security/firesight/541/firepower-module-userguide/asa- firepower-module-user-guide-v541/Intrusion-External-Responses.pdf

QUESTION 71
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

Correct Answer: C
Section:
Explanation:
Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/command_ref/b_Command_Reference_for_Firepower_Threat_Defense/c_3.html

QUESTION 72
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

Correct Answer: C
Section:
Explanation:
Reason: the command "capture-traffic" is used for SNORT Engine Captures. To capture a LINA Engine Capture, you use the "capture" command. Since the Lina Engine represents the actual physical interface of the device, "capture" is the only reasonable choice Reference:
https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/212474-working-withfirepower-threat-defense-f.html#anc10The command isfirepower# capture DMZ interface dmz trace detail match ip host 192.168.76.14 host 192.168.76.100firepower# capture INSIDE interface inside trace detail match ip host 192.168.76.14 host192.168.75.14

QUESTION 73
How many report templates does the Cisco Firepower Management Center support?

A. 20
B. 10
C. 5
D. unlimited

Correct Answer: D
Section:
Explanation:
Reference:
https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-configguide-v60/Working_with_Reports.html

QUESTION 74
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.

Correct Answer: C
Section:
Explanation:
Reference:
https://www.cisco.com/c/en/us/td/docs/security/firepower/630/configuration/guide/fpmc-configguide-v63/reusable_objects.html

QUESTION 75
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

Correct Answer: D
Section:
Explanation:
Reference: https://www.cisco.com/c/en/us/td/docs/security/firesight/541/firepower-module-userguide/asa- firepower-module-user-guide-v541/Intrusion-Global-Threshold.html

QUESTION 76
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 primary FMC currently has devices connected to it.
B. The code versions running on the Cisco FMC devices are different
C. The licensing purchased does not include high availability
D. There is only 10 Mbps of bandwidth between the two devices.

Correct Answer: B
Section:
Explanation:
https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-configguide-v62/firepower_management_center_high_availability.html

QUESTION 77
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. Custom Analysis
B. Current Status
C. Current Sessions
D. Correlation Events

Correct Answer: A
Section:

QUESTION 78
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 Cisco388267669. Which command set must be used in order to accomplish this?

A. configure manager add ACME001 <registration key> <FMC IP>
B. configure manager add <FMC IP> ACME0O1 <registration key>
C. configure manager add DONTRESOLVE <FMC IP> AMCE001 <registration key>
D. configure manager add <FMC IP> registration key> ACME001

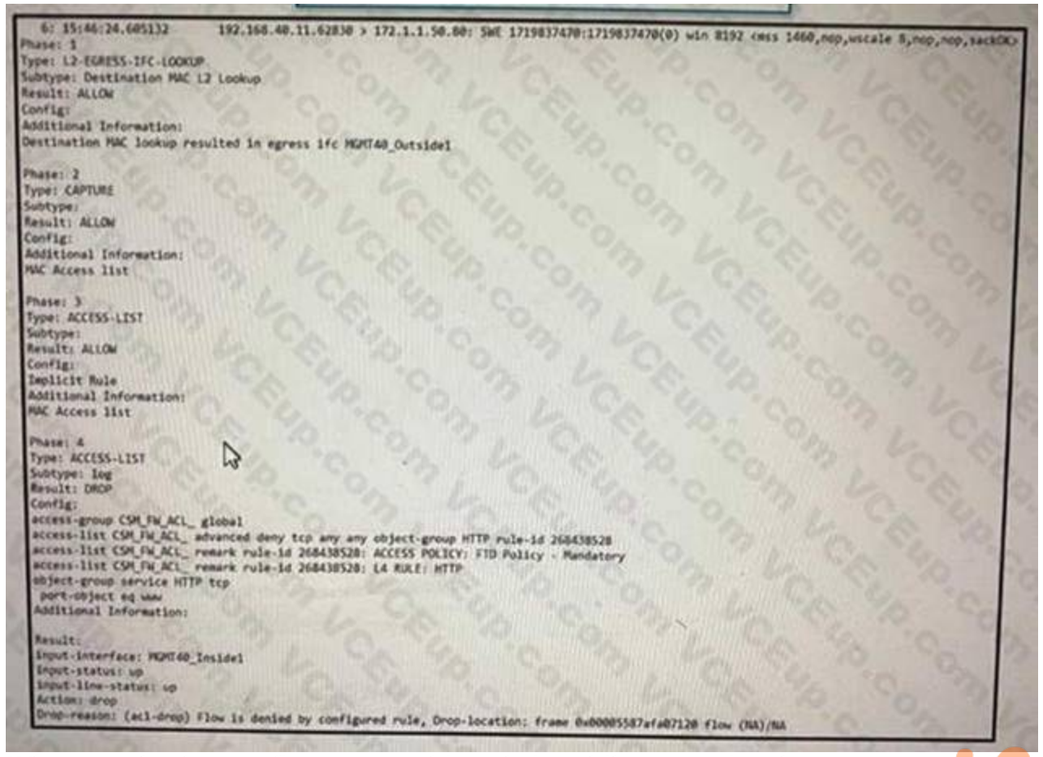
Correct Answer: D
Section:

QUESTION 79
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. Capacity handling
B. Local malware analysis
C. Spere analysis
D. Dynamic analysis

Correct Answer: D
Section:

QUESTION 80
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 access control policy rule to allow port 80 to only 172.1.1 50.
C. Create an intrusion policy rule to have Snort allow port 443 to only 172.1.1.50
D. Create an access control policy rule to allow port 443 to only 172.1.1 50

Correct Answer: B
Section:

QUESTION 81
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 analyse the file in the Talos cloud?

A. Spero analysis
B. Malware analysis
C. Dynamic analysis
D. Sandbox analysis

Correct Answer: B
Section:

QUESTION 82
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 Troubleshoot" file for the device in question.

B. A "show tech" file for the device in question
C. A "show tech" for the Cisco FMC.
D. A "troubleshoot" file for the Cisco FMC

Correct Answer: A
Section:

QUESTION 83
Network traffic coining 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. Configure firewall bypass.
B. Change the intrusion policy from security to balance.
C. Configure a trust policy for the CEO.
D. Create a NAT policy just for the CEO.

Correct Answer: C
Section:

QUESTION 84
A network administrator discovers that a user connected to a file server and downloaded a malware file. The Cisc FMC generated an alert for the malware event, however the user still remained connected. Which Cisco APM file rule action within the Cisco FMC must be set to resolve this issue?

A. Detect Files
B. Malware Cloud Lookup
C. Local Malware Analysis
D. Reset Connection

Correct Answer: D
Section:

QUESTION 85
An organization wants to secure traffic from their branch office to the headquarter 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 ignore the VPN traffic using prefilter policies
B. Enable a flexconfig policy to re-classify VPN traffic so that it no longer appears as interesting traffic
C. Configure the Cisco Firepower devices to bypass the access control policies for VPN traffic.
D. Tune the intrusion policies in order to allow the VPN traffic through without inspection

Correct Answer: C
Section:
Explanation:
When you configure the Cisco Firepower devices to bypass the access control policies for VPN traffic, thedevices will not inspect the VPN traffic and thus will not waste resources on it. This is the best option toensure that the VPN traffic is not wasting resources on the Cisco Firepower devices.

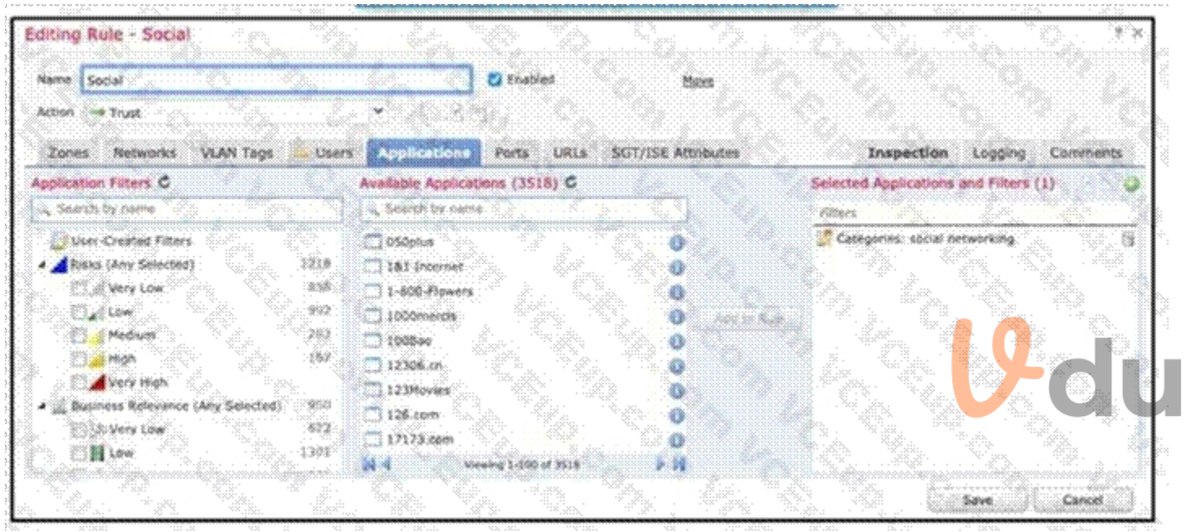
QUESTION 86
An organization has implemented Cisco Firepower without IPS capabilities and now wants to enable inspection for their traffic. They need to be able to detect protocol anomalies and utilize the Snort rule sets to detect

malicious behaviour.
How is this accomplished?

A. Modify the access control policy to redirect interesting traffic to the engine
B. Modify the network discovery policy to detect new hosts to inspect
C. Modify the network analysis policy to process the packets for inspection
D. Modify the intrusion policy to determine the minimum severity of an event to inspect.

Correct Answer: D
Section:

QUESTION 87
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. Modify the selected application within the rule
B. Change the intrusion policy to connectivity over security.
C. Modify the rule action from trust to allow
D. Add the social network URLs to the block list

Correct Answer: A
Section:

QUESTION 88
Which feature within the Cisco FMC web interface allows for detecting, analyzing and blocking malware in network traffic?

A. intrusion and file events
B. Cisco AMP for Endpoints
C. Cisco AMP for Networks
D. file policies

Correct Answer: C
Section:

QUESTION 89
An administrator is setting up Cisco Firepower to send data to the Cisco Stealthwatch appliances. The NetFlow_Set_Parameters object is already created, but NetFlow is not being sent to the flow collector. What must be done to prevent this from occurring?

A. Add the NetFlow_Send_Destination object to the configuration
B. Create a Security Intelligence object to send the data to Cisco Stealthwatch
C. Create a service identifier to enable the NetFlow service
D. Add the NetFlow_Add_Destination object to the configuration

Correct Answer: B
Section:

QUESTION 90
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 has minimal performance impact
C. It is not subject to any Privacy regulations
D. It will fail if certificate pinning is not enforced

Correct Answer: A
Section:

QUESTION 91
A network engineer is receiving reports of users randomly getting disconnected from their corporate applications which traverses 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

Correct Answer: B
Section:

QUESTION 92
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. Configure high-availability in both the primary and secondary Cisco FMCs
B. Connect the primary and secondary Cisco FMC devices with Category 6 cables of not more than 10 meters in length.
C. Place the active Cisco FMC device on the same trusted management network as the standby device
D. Restore the primary Cisco FMC backup configuration to the secondary Cisco FMC device when the primary device fails

Correct Answer: D

Section:

QUESTION 93
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 a dedicated IPS inline set for each department to maintain traffic separation
B. Use 802 1Q mime set Trunk interfaces with VLANs to maintain logical traffic separation
C. Use passive IDS ports for both departments
D. Use one pair of inline set in TAP mode for both departments

Correct Answer: B
Section:

QUESTION 94
Which license type is required on Cisco ISE to integrate with Cisco FMC pxGrid?

A. mobility
B. plus
C. base
D. apex

Correct Answer: B
Section:

QUESTION 95
With Cisco FTD software, which interface mode must be configured to passively receive traffic that passes through the appliance?

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

Correct Answer: A
Section:

QUESTION 96
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 have the same port-channel numbering
B. Confirm that both devices are running the same software version
C. Confirm that both devices are configured with the same types of interfaces
D. Confirm that both devices have the same flash memory sizes

Correct Answer: B
Section:

QUESTION 97
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 Threat Intelligence Director using STIX and TAXII
B. Enable Rapid Threat Containment using REST APIs
C. Enable Threat Intelligence Director using REST APIs
D. Enable Rapid Threat Containment using STIX and TAXII

Correct Answer: A
Section:

QUESTION 98
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 destination MAC address is optional if a VLAN ID value is entered
B. Only the UDP packet type is supported
C. The output format option for the packet logs unavailable
D. The VLAN ID and destination MAC address are optional

Correct Answer: A
Section:

QUESTION 99
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. Deploy a firewall in transparent mode between the clients and servers.
B. Change the IP addresses of the clients, while remaining on the same subnet.
C. Deploy a firewall in routed mode between the clients and servers
D. Change the IP addresses of the servers, while remaining on the same subnet

Correct Answer: A
Section:

QUESTION 100
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. Manually update the SI event entries to that the appropriate traffic is blocked
C. Replace the affected devices with devices that provide more memory
D. Redeploy configurations to affected devices so that additional memory is allocated to the SI module

Correct Answer: D
Section:

QUESTION 101
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.

Correct Answer: B
Section:

QUESTION 102
In a multi-tennent 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

Correct Answer: B
Section:

QUESTION 103
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. Malware Report
B. Standard Report
C. SNMP Report
D. Risk Report

Correct Answer: B
Section:

QUESTION 104
What is a feature of Cisco AMP private cloud?

A. It supports anonymized retrieval of threat intelligence
B. It supports security intelligence filtering.
C. It disables direct connections to the public cloud.
D. It performs dynamic analysis

Correct Answer: C
Section:

QUESTION 105
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 appliances in firewall clustering mode to increase performance.
B. Deploy multiple Cisco FTD appliances using VPN load-balancing to scale performance.
C. Deploy multiple Cisco FTD HA pairs to increase performance
D. Deploy multiple Cisco FTD HA pairs in clustering mode to increase performance

Correct Answer: A
Section:

QUESTION 106
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 flexconfig policy to use WCCP for application aware bandwidth limiting
B. Create a VPN policy so that direct tunnels are established to the business applications
C. Create a NAT policy so that the Cisco Firepower device does not have to translate as many addresses
D. Create a QoS policy rate-limiting high bandwidth applications

Correct Answer: D
Section:

QUESTION 107
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 nonstandard port of 9443 The host the engineer is attempting the connection from is at the IP address of 10.20.10.20. In order to determine what is happening to the packets on the network, the engineer decides to use the FTD packet capture tool Which capture configuration should be used to gather the information needed to troubleshoot this issue?

A.

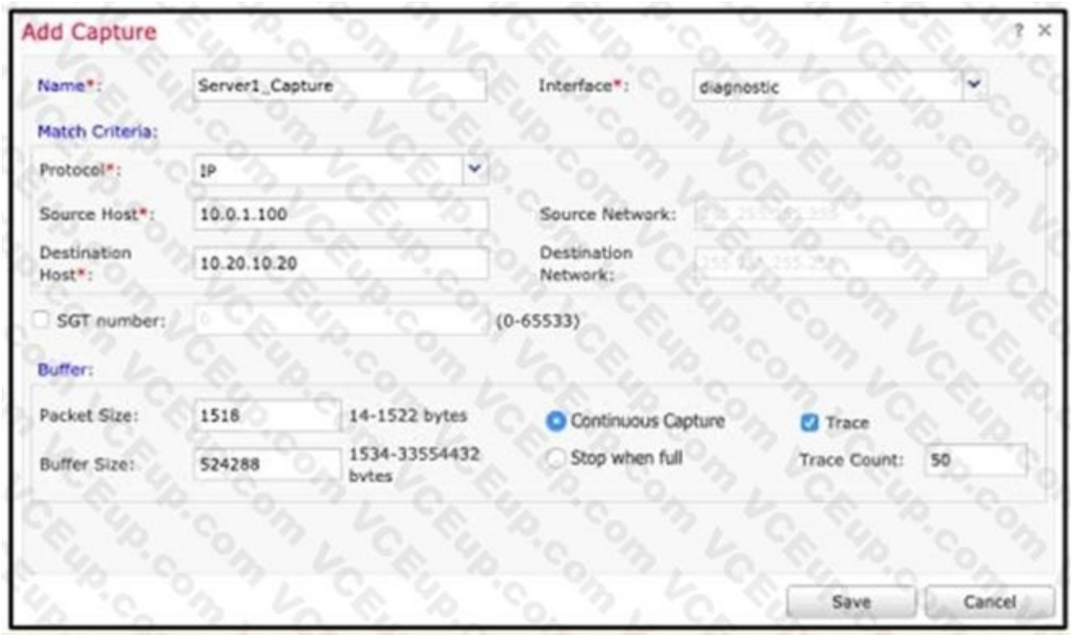
B.


C.


Add Capture
Name*: Server1_Capture
Interface*: Inside
Match Criteria:
Protocol*: IP
Source Host*: 10.20.10.20
Source Network:
Destination Host*: 10.0.1.100
Destination Network:
SGT number:
(0-65533)
Buffer:
Packet Size: 1518
14-1522 bytes
Continuous Capture
Trace
Buffer Size: 524288
1534-33554432 bytes
Stop when full
Trace Count: 50

D.


Add Capture
Name*: Server1_Capture
Interface*: diagnostic
Match Criteria:
Protocol*: IP
Source Host*: 10.20.10.20
Source Network:
Destination Host*: 10.0.1.100
Destination Network:
SGT number:
(0-65533)
Buffer:
Packet Size: 1518
14-1522 bytes
Continuous Capture
Trace
Buffer Size: 524288
1534-33554432 bytes
Stop when full
Trace Count: 50
Save
Cancel



Correct Answer: B
Section:

QUESTION 108
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. Manually adjust the time to the correct hour on the Cisco FMC.
D. Configure the system clock settings to use NTP

Correct Answer: B
Section:

QUESTION 109
What is a characteristic of bridge groups on a Cisco FTD?

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

Correct Answer: B
Section:

QUESTION 110
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

Correct Answer: A, E
Section:

QUESTION 111
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.

Correct Answer: B, E
Section:

QUESTION 112
An engineer configures an access control rule that deploys file policy configurations to security zones 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.

Correct Answer: A
Section:

QUESTION 113
An engineer has been tasked with using Cisco FMC to determine if files being sent through the network are malware. Which two configuration takes 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.

Correct Answer: D, E
Section:

QUESTION 114
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

Correct Answer: A
Section:

QUESTION 115
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.

Correct Answer: A
Section:

QUESTION 116
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.

Correct Answer: D
Section:

QUESTION 117

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.

Correct Answer: A
Section:

QUESTION 118
Which protocol is needed to exchange threat details in rapid threat containment on Cisco FMC?

A. SGT
B. SNMP v3
C. BFD
D. pxGrid

Correct Answer: D
Section:

QUESTION 119
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

Correct Answer: D
Section:

QUESTION 120
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. Use the context explorer to see the destination port blocks
C. Filter the connection events by the source port 8699/udp.
D. Filter the connection events by the destination port 8699/udp.

Correct Answer: D
Section:

QUESTION 121
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. Malware Cloud Lookup and dynamic analysis
B. Block Malware action and dynamic analysis
C. Block Malware action and local malware analysis
D. Block File action and local malware analysis

Correct Answer: C
Section:

QUESTION 122
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. Create a new access control policy rule to allow ports 80 and 443 to the FQDN of the web 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. Verify the blocks using the packet capture tool and create a rule with the action monitor for the traffic.
D. 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.

Correct Answer: B
Section:

QUESTION 123
Refer to the exhibit.

An engineer is modifying an access control policy to add a rule to Inspect all DNS traffic that passes it making the change and deploying the policy, they see that DNS traffic Is not being Inspected by the Snort engine. What is.....

A. The rule must specify the security zone that originates the traffic.
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 action of the rule is set to trust instead of allow.

Correct Answer: D
Section:

QUESTION 124

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 Umbrell a. Which API meets this requirement?

A. investigate
B. reporting
C. enforcement
D. REST

Correct Answer: D
Section:

QUESTION 125
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 downstream router to perform NAT.
B. Configure the upstream router to perform NAT.
C. Configure the Cisco FTD firewall in routed mode with NAT enabled.
D. Configure the Cisco FTD firewall in transparent mode with NAT enabled.

Correct Answer: C
Section:

QUESTION 126
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 ASA 5500 Series
B. Cisco FMC
C. Cisco AMP
D. Cisco Stealthwatch
E. Cisco ASR 7200 Series

Correct Answer: C, D
Section:

QUESTION 127
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. An API restriction within the Cisco FMC is preventing the widget from displaying.
B. The widget is configured to display only when active events are present.
C. The widget is not configured within the Cisco FMC.
D. The security analyst role does not have permission to view this widget.

Correct Answer: C
Section:

QUESTION 128
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. Cisco AMP for Networks is unable to contact Cisco Threat Grid Cloud.
C. There is a host limit set.
D. The user agent status is set to monitor.

Correct Answer: B
Section:

QUESTION 129
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 the 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. Use the verbose option as a part of the capture-traffic command
B. Use the capture command and specify the trace option to get the required information.
C. Specify the trace using the -T option after the capture-traffic command.
D. Perform the trace within the Cisco FMC GUI instead of the Cisco FTD CLI.

Correct Answer: B
Section:

QUESTION 130
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. prevalence
B. threat root cause
C. vulnerable software
D. file analysis

Correct Answer: A
Section:

QUESTION 131
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. interface object to export NetFlow
B. security intelligence object for NetFlow
C. flexconfig object for NetFlow
D. variable set object for NetFlow

Correct Answer: C
Section:

QUESTION 132
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 the primary route. Which action accomplishes this task?

A. Install the static backup route and modify the metric to be less than the primary route.
B. Configure EIGRP routing on the FMC to ensure that dynamic routes are always updated.
C. Use a default route on the FMC instead of having multiple routes contending for priority.
D. Create the backup route and use route tracking on both routes to a destination IP address in the network.

Correct Answer: A
Section:

QUESTION 133
A network security engineer must export packet captures from the Cisco FMC web browser while troubleshooting an issue. When navigating to the address https://<FMC IP>/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 HTTPS server and use HTTP instead.
B. Enable the HTTPS server for the device platform policy.
C. Disable the proxy setting on the browser.
D. Use the Cisco FTD IP address as the proxy server setting on the browser.

Correct Answer: B
Section:
Explanation:
When you configure the Cisco Firepower devices to bypass the access control policies for VPN traffic, thedevices will not inspect the VPN traffic and thus will not waste resources on it. This is the best option toensure that the VPN traffic is not wasting resources on the Cisco Firepower devices.

QUESTION 134
An engineer integrates Cisco FMC and Cisco ISE using pxGrid. Which role is assigned for Cisco FMC?

A. controller
B. publisher
C. client
D. server

Correct Answer: C
Section:

QUESTION 135
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. Fast-Path Rules Bypass
B. Cisco ISE Security Group Tag
C. Inspect Local Traffic Bypass
D. Automatic Application Bypass

Correct Answer: D
Section:

QUESTION 136

An engineer is »vorlang on a LAN switch and has noticed that its network connection to the mime 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

Correct Answer: D
Section:

QUESTION 137

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

A. The rule must specify the security zone that originates the traffic
B. The rule must define the source network for inspection as well as the port
C. The action of the rule is set to trust instead of allow.
D. The rule is configured with the wrong setting for the source port

Correct Answer: C
Section:

QUESTION 138
What is the role of the casebook feature in Cisco Threat Response?

A. sharing threat analysts
B. pulling data via the browser extension
C. triage automaton with alerting
D. alert prioritization

Correct Answer: A
Section:
Explanation:
The casebook and pivot menu are widgets available in Cisco Threat Response. Casebook - It is used to record, organize, and share sets of observables of interest primarily during an investigation and threat analysis. You can use a casebook to get the current verdicts or dispositions on the observables.
https://www.cisco.com/c/en/us/td/docs/security/ces/user_guide/esa_user_guide_13-5-1/b_ESA_Admin_Guide_ces_13-5-1/b_ESA_Admin_Guide_13-0_chapter_0110001.pdf

QUESTION 139
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 integration configuration is replicated to the primary Cisco FMC
B. The existing configuration for integration of the secondary Cisco FMC the Cisco Security Packet Analyzer is overwritten.
C. The synchronization between the primary and secondary Cisco FMC fails
D. The secondary Cisco FMC must be reintegrated with the Cisco Security Packet Analyzer after the synchronization

Correct Answer: B
Section:

QUESTION 140
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.

Correct Answer: D
Section:

QUESTION 141
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

Correct Answer: C
Section:

QUESTION 142
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

Correct Answer: B
Section:

QUESTION 143
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

Correct Answer: A
Section:

QUESTION 144
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.

Correct Answer: C
Section:

QUESTION 145
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.

Correct Answer: A
Section:

QUESTION 146
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.

Correct Answer: A
Section:

QUESTION 147
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 the 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.

Correct Answer: B
Section:

QUESTION 148
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.

Correct Answer: A
Section:

QUESTION 149
The CEO ask 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.

Correct Answer: B
Section:

QUESTION 150
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

Correct Answer: D
Section:

QUESTION 151
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

Correct Answer: A
Section:

QUESTION 152
An administrator Is setting up a Cisco PMC and must provide expert mode access for a security engineer. The engineer Is permitted to use only a secured out-of-band network workstation with a static IP address to access the Cisco FMC.
What must be configured to enable this access?

A. Enable SSH and define an access list.
B. Enable HTTP and define an access list.
C. Enable SCP under the Access List section.
D. Enable HTTPS and SNMP under the Access List section.

Correct Answer: A
Section:

QUESTION 153
An engainer must add DNS-specific rules to me Cisco FTD intrusion policy. The engineer wants to use the rules currently in the Cisco FTD Snort database that are not already enabled but does not want to enable more than are needed.
Which action meets these requirements?

A. Change the dynamic state of the rule within the policy.
B. Change the base policy to Security over Connectivity.
C. Change the rule state within the policy being used.
D. Change the rules using the Generate and Use Recommendations feature.

Correct Answer: C
Section:

QUESTION 154
A network administrator is trying to convert from LDAP to LDAPS for VPN user authentication on a Cisco FTD. Which action must be taken on the Cisco FTD objects to accomplish this task?

A. Add a Key Chain object to acquire the LDAPS certificate.

B. Create a Certificate Enrollment object to get the LDAPS certificate needed.
C. Identify the LDAPS cipher suite and use a Cipher Suite List object to define the Cisco FTD connection requirements.
D. Modify the Policy List object to define the session requirements for LDAPS.

Correct Answer: B
Section:

QUESTION 155
What is the RTC workflow when the infected endpoint is identified?

A. Cisco ISE instructs Cisco AMP to contain the infected endpoint.
B. Cisco ISE instructs Cisco FMC to contain the infected endpoint.
C. Cisco AMP instructs Cisco FMC to contain the infected endpoint.
D. Cisco FMC instructs Cisco ISE to contain the infected endpoint.

Correct Answer: D
Section:

QUESTION 156
Which feature is supported by IRB on Cisco FTD devices?

A. redundant interface
B. dynamic routing protocol
C. EtherChannel interface
D. high-availability cluster

Correct Answer: B
Section:

QUESTION 157
A security engineer is deploying a pair of primary and secondary Cisco FMC devices. The secondary must also receive updates from Cisco Talos. Which action achieves this goal?

A. Force failover for the secondary Cisco FMC to synchronize the rule updates from the primary.
B. Configure the secondary Cisco FMC so that it receives updates from Cisco Talos.
C. Manually import rule updates onto the secondary Cisco FMC device.
D. Configure the primary Cisco FMC so that the rules are updated.

Correct Answer: D
Section:

QUESTION 158
Refer to the exhibit.

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

A. Create an access control policy rule that allows ICMP traffic.
B. Configure a custom Snort signature to allow ICMP traffic after Inspection.
C. Modify the Snort rules to allow ICMP traffic.
D. Create an ICMP allow list and add the ICMP destination to remove it from the implicit deny list.

Correct Answer: A
Section:

QUESTION 159
A security engineer must configure a Cisco FTD appliance to inspect traffic coming from the internet.
The Internet traffic will be mirrored from the Cisco Catalyst 9300 Switch. Which configuration accomplishes the task?

A. Set interface configuration mode to none.
B. Set the firewall mode to transparent.
C. Set the firewall mode to routed.
D. Set interface configuration mode to passive.

Correct Answer: D
Section:

QUESTION 160
The network administrator wants to enhance the network security posture by enabling machine learning tor malware detection due to a concern with suspicious Microsoft executable file types that were seen while creating monthly security reports for the CIO. Which feature must be enabled to accomplish this goal?

A. Spero
B. dynamic analysis
C. static analysis
D. Ethos

Correct Answer: A
Section:

QUESTION 161
A network administrator is configuring a Cisco AMP public cloud instance and wants to capture infections and polymorphic variants of a threat to help detect families of malware. Which detection engine meets this

requirement?

A. RBAC
B. Tetra
C. Ethos
D. Spero

Correct Answer: C
Section:

QUESTION 162
A network engineer must provide redundancy between two Cisco FTD devices. The redundancy configuration must include automatic configuration, translation, and connection updates. After the initial configuration of the two appliances, which two steps must be taken to proceed with the redundancy configuration? (Choose two.)

A. Configure the virtual MAC address on the failover link.
B. Disable hellos on the inside interface.
C. Configure the standby IP addresses.
D. Ensure the high availability license is enabled.
E. Configure the failover link with stateful properties.

Correct Answer: A, C
Section:

QUESTION 163
A network administrator is configuring an FTD in transparent mode. A bridge group is set up and an access policy has been set up to allow all IP traffic. Traffic is not passing through the FTD. What additional configuration is needed?

A. The security levels of the interfaces must be set.
B. A default route must be added to the FTD.
C. An IP address must be assigned to the BVI.
D. A mac-access control list must be added to allow all MAC addresses.

Correct Answer: C
Section:

QUESTION 164
A network administrator registered a new FTD to an existing FMC. The administrator cannot place the FTD in transparent mode. Which action enables transparent mode?

A. Add a Bridge Group Interface to the FTD before transparent mode is configured.
B. Dereglster the FTD device from FMC and configure transparent mode via the CLI.
C. Obtain an FTD model that supports transparent mode.
D. Assign an IP address to two physical interfaces.

Correct Answer: B
Section:

QUESTION 165

A security engineer must deploy a Cisco FTD appliance as a bump in the wire to detect intrusion events without disrupting the flow of network traffic. Which two features must be configured to accomplish the task? (Choose two.)

A. inline set pair
B. transparent mode
C. tapemode
D. passive interfaces
E. bridged mode

Correct Answer: B, C
Section:

QUESTION 166
Due to an Increase in malicious events, a security engineer must generate a threat report to include intrusion events, malware events, and security intelligence events. How Is this information collected in a single report?

A. Run the default Firepower report.
B. Export the Attacks Risk report.
C. Generate a malware report.
D. Create a Custom report.

Correct Answer: D
Section:

QUESTION 167
An engineer attempts to pull the configuration for a Cisco FTD sensor to review with Cisco TAC but does not have direct access to the CU for the device. The CLl for the device is managed by Cisco FMC to which the engineer has access.
Which action in Cisco FMC grants access to the CLl for the device?

A. Export the configuration using the Import/Export tool within Cisco FMC.
B. Create a backup of the configuration within the Cisco FMC.
C. Use the show run all command in the Cisco FTD CLI feature within Cisco FMC.
D. Download the configuration file within the File Download section of Cisco FMC.

Correct Answer: A
Section:

QUESTION 168
A network engineer detects a connectivity issue between Cisco Secure Firewall Management Centre and Cisco Secure Firewall Threat Defense Initial troubleshooting indicates that heartbeats and events not being received. The engineer re-establishes the secure channels between both peers Which two commands must the engineer run to resolve the issue? (Choose two.)

A. manage_procs.pl
B. sudo stats_unified.pl
C. sudo perfstats -Cq < /var/sf/rna/correlator-stats/now
D. show history
E. show disk-manager

Correct Answer: A, B

Section:
Explanation:
When connectivity issues are detected between Cisco Secure Firewall Management Center (FMC) and Cisco Secure Firewall Threat Defense (FTD) devices, and initial troubleshooting indicates that heartbeats and events are not being received, the engineer can run the following commands to resolve the issue by re-establishing secure channels and checking process statuses:
manage_procs.pl: This script is used to manage and restart processes on the FTD device. Running this script can help restart any malfunctioning processes and re-establish connectivity between the FMC and FTD.
sudo stats_unified.pl: This command provides detailed statistics and status of the unified system processes. It helps in diagnosing and resolving issues related to the secure channel and event reporting.
Steps:
Access the FTD CLI.
Run the command manage_procs.pl to restart processes.
Run the command sudo stats_unified.pl to gather detailed process statistics and verify the status.
These commands help resolve connectivity issues by ensuring that all necessary processes are running correctly and secure channels are re-established.

QUESTION 169
An engineer must replace a Cisco Secure Firewall high-availability device due to a failure. When the replacement device arrives, the engineer must separate the high-availability pair from Cisco Secure Firewall Management Center Which action must the engineer take first to restore high availability?

A. Register the secondary device
B. Force a break between the devices.
C. Unregister the secondary device.
D. Configure NTP time synchronization.

Correct Answer: C
Section:
Explanation:
When replacing a Cisco Secure Firewall high-availability (HA) device due to a failure, the first step the engineer must take is to unregister the secondary (failed) device from the Cisco Secure Firewall Management Center (FMC). This action separates the HA pair and ensures that the new replacement device can be registered and configured correctly.
Steps:
Access the FMC and navigate to the device management section.
Unregister the failed secondary device to remove it from the HA pair.
Register the replacement device to the FMC.
Reconfigure the HA settings to restore the high-availability configuration.
By unregistering the failed device first, the engineer ensures a clean setup for the replacement device, avoiding potential conflicts or issues in the HA configuration.

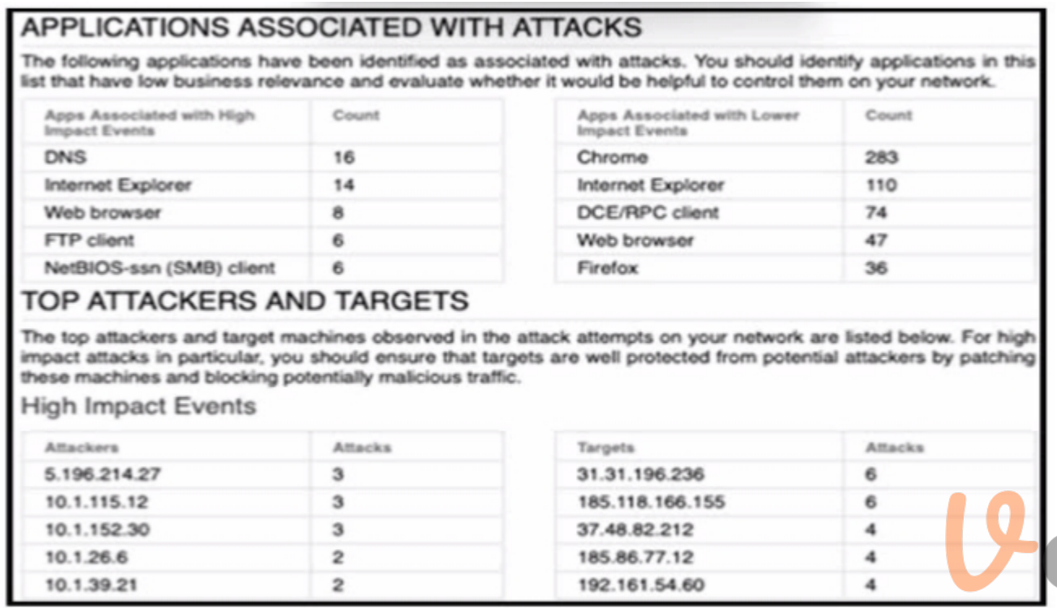
QUESTION 170
An engineer is configuring a Cisco Secure Firewall Threat Defense device and warns to create a new intrusion rule based on the detection of a specific pattern in the data payload for a new zero-day exploit. Which keyword type must be used to add a Line that identifies the author of the rule and the date it was created?

A. metadata
B. content
C. reference
D. gtp_info

Correct Answer: A
Section:
Explanation:
When creating a new intrusion rule in a Cisco Secure Firewall Threat Defense (FTD) device, the keyword type 'metadata' must be used to add a line that identifies the author of the rule and the date it was created. The metadata keyword is used to store additional information about the rule, such as authorship and creation date.
Steps:
In FMC, navigate to Policies > Intrusion > Rules.

Create a new rule or edit an existing one.
Use the 'metadata' keyword to add information about the author and date.
Example:
metadata: created_at 2023-06-15, author 'John Doe';
By using the metadata keyword, you ensure that the rule contains relevant information for tracking its creation and authorship, which is essential for maintaining rule documentation and accountability.

QUESTION 171
Refer to the Exhibit.



APPLICATIONS ASSOCIATED WITH ATTACKS

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

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

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

TOP ATTACKERS AND TARGETS

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

High Impact Events

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

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

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

A. Inspect DNS traffic
B. Block NetBIOS.
C. Block Internal Explorer
D. Inspect TCP port 80 traffic

Correct Answer: A
Section:
Explanation:
Based on the Attacks Risk Report, DNS is associated with a high number of impact events (16). DNS traffic is critical for network operations but can also be exploited for malicious activities such as DNS tunneling, DDoS attacks, and data exfiltration. To improve security, the security engineer should focus on inspecting DNS traffic. This involves deploying DNS security solutions and monitoring DNS traffic for anomalies to detect and mitigate potential threats.
Steps:
Implement DNS security tools such as DNS filtering, DNSSEC, and DNS anomaly detection.
Configure the firewall to inspect DNS traffic for malicious activities.
Regularly analyze DNS logs to identify and respond to threats.
This action addresses a significant risk identified in the report and helps to mitigate potential attacks exploiting DNS.

QUESTION 172
An engineer is troubleshooting an intermittent connectivity issue on a Cisco Secure Firewall Threat Defense appliance and must collect 24 hours' worth of data. The engineer started a packet capture. Whenever it stops prematurely during this time period. The engineer notices that the packet capture butter size is set to the default of 32 MB Which butter S170 is the maximum that the engineer must sot to able the packet capture to run

successfully?

A. 64 MB
B. 1 GB
C. 10 GB
D. 100 GB

Correct Answer: B
Section:
Explanation:
To collect 24 hours' worth of data using a packet capture on a Cisco Secure Firewall Threat Defense (FTD) appliance without prematurely stopping due to buffer size limitations, the engineer should increase the packet capture buffer size. The default buffer size is 32 MB, which is insufficient for extended captures.
Steps:
Access the packet capture configuration on the FTD device.
Increase the buffer size to 1 GB, which provides a significantly larger capacity for capturing packets over a 24-hour period.
Setting the buffer size to 1 GB should accommodate a substantial amount of traffic and prevent the capture from stopping prematurely.

QUESTION 173
A security engineer manages a firewall console and an endpoint console and finds it challenging and the consuming to review events and modify blocking of specific files in both consoles. Which action must the engineer take to streamline this process?

A. From the Secure FMC. create a Cisco Secure Endpoint object and reference the object in the Cisco Secure Endpoint console.
B. From the Cisco Secure Endpoint console, Croats and copy an API key and paste into the Cisco Secure AMP tab
C. initiate the integration between Secure FMC and Cisco Secure Endpoint from the Secure FMC using the AMP tab
D. Within the Cisco Secure Endpoint console, copy the connector GUID and paste into the Cisco Secure Firewall Management Center (FMC) AMP tab.

Correct Answer: C
Section:
Explanation:
To streamline the process of reviewing events and modifying blocking of specific files across both the firewall console and the endpoint console, the security engineer should initiate the integration between Secure FMC and Cisco Secure Endpoint (formerly AMP for Endpoints) from the Secure FMC using the AMP tab.
Steps:
In the FMC, navigate to Devices > Device Management.
Select the device and go to the AMP tab.
Initiate the integration by configuring the necessary API credentials and linking the FMC to the Cisco Secure Endpoint console.
This integration allows the security engineer to view endpoint events and apply blocking actions directly from the FMC, consolidating the management tasks.
This approach simplifies the workflow by providing a single interface to manage both network and endpoint security, reducing the time and effort required to maintain security across the organization.

QUESTION 174
A software development company hosts the website http:dev.company.com for contractors to share code for projects they are working on with internal developers. The web server is on premises and is protected by a Cisco Secure Firewall Threat Defense appliance. The network administrator is worried about someone trying to transmit infected files to internal users via this site. Which type of policy must be able associated with an access control policy to enable Cisco Secure Firewall Malware Defense to detect and block malware?

A. SSL policy
B. Prefilter policy
C. File policy
D. Network discovery policy

Correct Answer: C
Section:
Explanation:
To enable Cisco Secure Firewall Malware Defense to detect and block malware, the network administrator must associate a File policy with an access control policy. File policies allow administrators to configure malware detection and file analysis capabilities on the Cisco Secure Firewall Threat Defense appliance.
Steps to configure File policy:
Navigate to Policies > Access Control > File Policies in the FMC.
Create a new file policy or edit an existing one to include malware detection and blocking settings.
Associate the file policy with the relevant access control policy.
Ensure that the access control policy is deployed to the FTD appliance.
By associating a file policy, the firewall will inspect files being transmitted through the web server for malware and take appropriate actions (block, allow, or alert) based on the configured rules.

QUESTION 175
A network engineer must configure an existing firewall to have a NAT configuration. The now configuration must support more than two interlaces per context. The firewall has previously boon operating transparent mode. The Cisco Secure Firewall Throat Defense (FTD) device has been deregistered from Cisco Secure Firewall Management Center (FMC). Which set of configuration actions must the network engineer take next to meet the requirements?

A. Run the configure manager add routed command from the Secure FTD device CL1, and reregister with Secure FMC.
B. Run the configure firewall routed command from the Secure FTD device CD, and reregister with Secure FMC.
C. Run the configure manager add routed command from the Secure FMC CLI. and reregister with Secure FMC.
D. Run the configure firewall routed command from the Secure FMC CLI. and reregister with Secure FMC.

Correct Answer: B
Section:
Explanation:
To support more than two interfaces per context and enable NAT configurations, the firewall must operate in routed mode. Since the firewall was previously in transparent mode, the network engineer needs to change it to routed mode.
Steps:
Access the CLI of the Secure FTD device.
Run the command configure firewall routed to switch the firewall from transparent mode to routed mode.
Reregister the FTD device with the FMC by running the configure manager add <FMC_IP> <Registration_Key> command from the FTD device CLI.
This will ensure that the firewall can support the required NAT configurations and more than two interfaces per context.