Cisco.300-710.vSep-2023.by.Yan.126q

Number: 300-710
Passing Score: 800.0
Time Limit: 120.0
File Version: 5.0

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

Exam A

QUESTION 1
When deploying a Cisco ASA Firepower module, an organization wants to evaluate the contents of the traffic without affecting the network. It is currently configured to have more than one instance of the same device on the physical appliance Which deployment mode meets the needs of the organization?

A. inline tap monitor-only mode
B. passive monitor-only mode
C. passive tap monitor-only mode
D. inline mode

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 2
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 3

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 4
Which two remediation options are available when Cisco FMC is integrated with Cisco ISE? (Choose two.)

A. dynamic null route configured
B. DHCP pool disablement
C. quarantine
D. port shutdown
E. host shutdown

Correct Answer: C, D
Section:
Explanation:
Reference: https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/210524-configure- firepower-6-1-pxgrid-remediati.html

QUESTION 5
Which connector is used to integrate Cisco ISE with Cisco FMC for Rapid Threat Containment?

A. pxGrid
B. FTD RTC
C. FMC RTC
D. ISEGrid

Correct Answer: A
Section:

QUESTION 6
What is the maximum SHA level of filtering that Threat Intelligence Director supports?

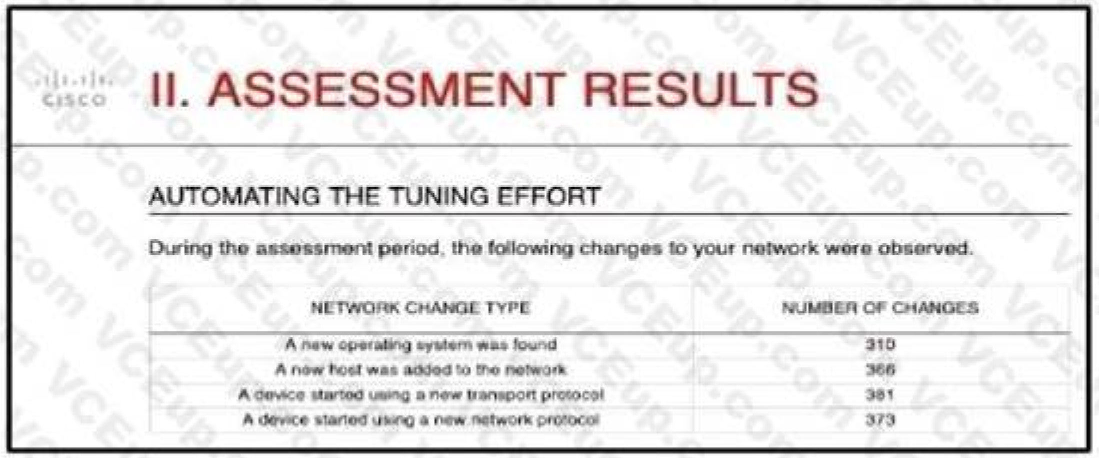
A. SHA-1024
B. SHA-4096

C. SHA-512
D. SHA-256

Correct Answer: D
Section:
Explanation:
Reference:
https://www.cisco.com/c/en/us/td/docs/security/firepower/623/configuration/guide/fpmc-configguide-v623/cisco_threat_intelligence_directortid_.html

Topic 5, Misc. Questions

QUESTION 7
Refer to the exhibit.



II. ASSESSMENT RESULTS

AUTOMATING THE TUNING EFFORT

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

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

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

A. Cisco Firepower automatically updates the policies.
B. The administrator requests a Remediation Recommendation Report from Cisco Firepower
C. Cisco Firepower gives recommendations to update the policies.
D. The administrator manually updates the policies.

Correct Answer: C
Section:
Explanation:
Ref: https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmcQuestions& Answers PDF P-35config-guide-v60/Tailoring_Intrusion_Protection_to_Your_Network_Assets.html

QUESTION 8
An engineer is implementing Cisco FTD in the network and is determining which Firepower mode to use. The organization needs to have multiple virtual Firepower devices working separately inside of the FTD appliance to provide traffic segmentation Which deployment mode should be configured in the Cisco Firepower Management Console to support these requirements?

A. multiple deployment
B. single-context
C. single deployment
D. multi-instance

Correct Answer: D
Section:

QUESTION 9
A network engineer is extending a user segment through an FTD device for traffic inspection without creating another IP subnet How is this accomplished on an FTD device in routed mode?

A. by leveraging the ARP to direct traffic through the firewall
B. by assigning an inline set interface
C. by using a BVI and create a BVI IP address in the same subnet as the user segment
D. by bypassing protocol inspection by leveraging pre-filter rules

Correct Answer: C
Section:
Explanation:
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 10
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 11
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 12
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 13
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 14
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 15
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 16
What are the minimum requirements to deploy a managed device inline?

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

Correct Answer: C
Section:
Explanation:
Reference:
https://www.cisco.com/c/en/us/td/docs/security/firepower/650/configuration/guide/fpmc-configguide-v65/ips_device_deployments_and_configuration.html

QUESTION 17
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 18
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 19
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 20
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 21
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 22
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 23

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 24
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 25
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 26
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 27
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 28
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 29
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 30
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 31
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 32
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 33
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 34
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 35
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 36
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 37
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 38
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 39
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 40
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 41

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 42
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 43
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 44
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 45
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 46
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 47
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 48
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 49
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 50
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 51
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 52
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 53
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 54
Which action should you take when Cisco Threat Response notifies you that AMP has identified a file as malware?

A. Add the malicious file to the block list.
B. Send a snapshot to Cisco for technical support.
C. Forward the result of the investigation to an external threat-analysis engine.
D. Wait for Cisco Threat Response to automatically block the malware.

Correct Answer: A
Section:

QUESTION 55
Which Cisco Advanced Malware Protection for Endpoints policy is used only for monitoring endpoint actively?

A. Windows domain controller
B. audit
C. triage
D. protection

Correct Answer: B
Section:
Explanation:
Reference: https://www.cisco.com/c/en/us/support/docs/security/amp-endpoints/214933-amp-forendpoints-deployment-methodology.html

QUESTION 56
What is a valid Cisco AMP file disposition?

A. non-malicious
B. malware
C. known-good
D. pristine

Correct Answer: B
Section:
Explanation:
Reference:
https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-configQuestions& Answers PDF P-33guide- v60/Reference_a_wrapper_Chapter_topic_here.html

QUESTION 57
In a Cisco AMP for Networks deployment, which disposition is returned if the cloud cannot be reached?

A. unavailable
B. unknown
C. clean
D. disconnected

Correct Answer: A
Section:

QUESTION 58
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 59
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 60
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 61
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 62
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 63

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 64

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 65

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 66

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 67
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 68
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 69
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 70
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 71
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 72
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

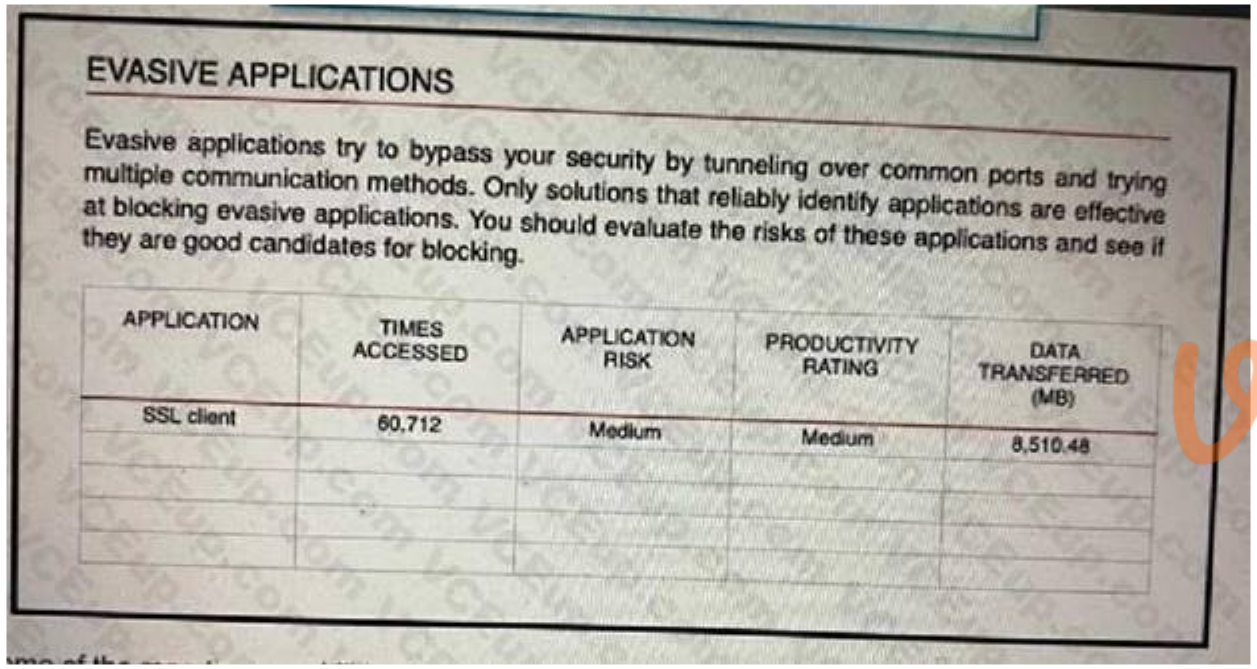
Correct Answer: D
Section:
Explanation:
Reference:
https://www.cisco.com/c/en/us/td/docs/security/firepower/630/configuration/guide/fpmc-configguide-v63/inline_sets_and_passive_interfaces_for_firepower_threat_defense.html

QUESTION 73
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 74
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 75
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

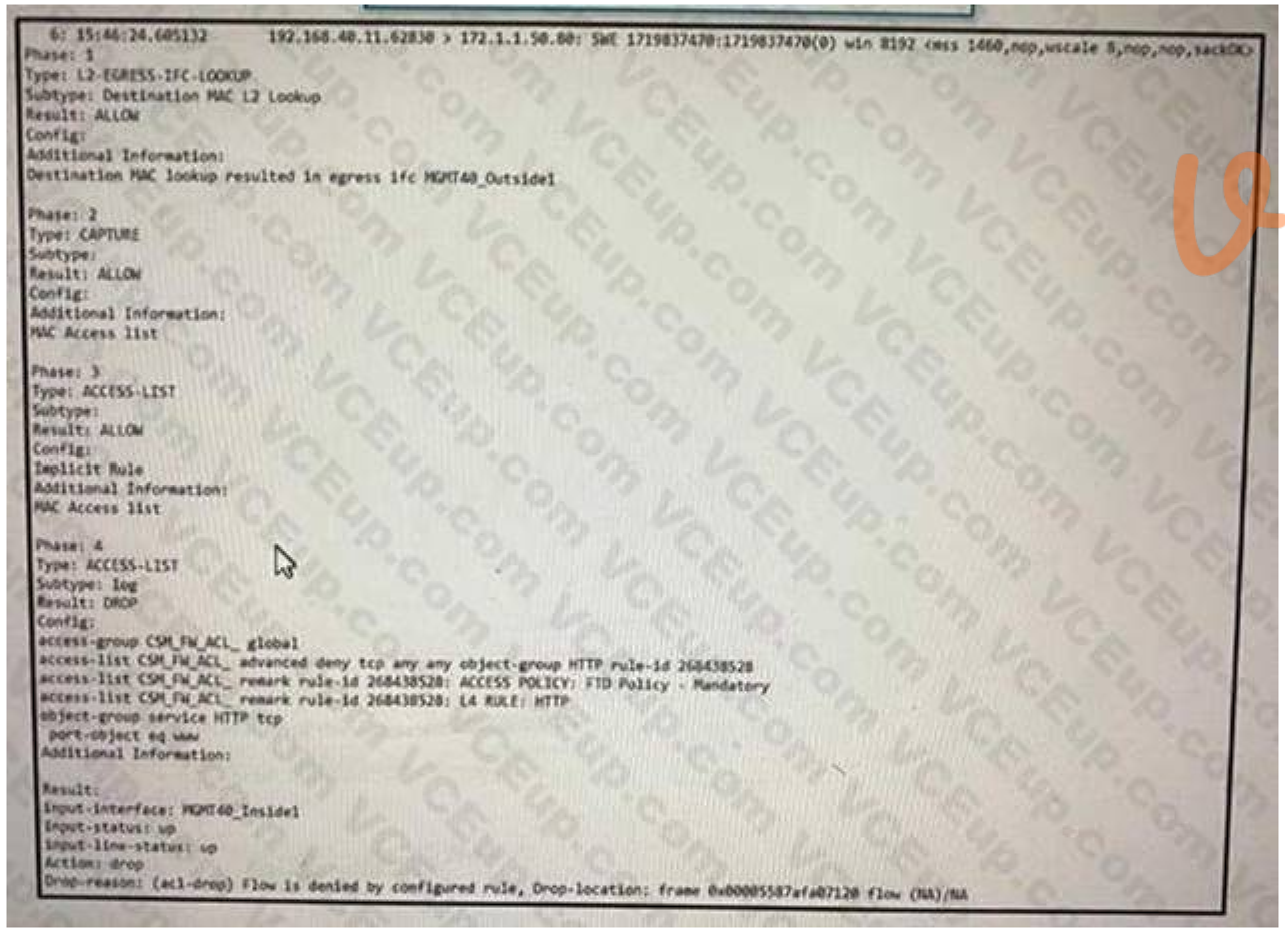
Correct Answer: D
Section:

QUESTION 76
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 77
Refer to the exhibit.



```
  6: 15:46:24.605132       192.168.40.11.62830 > 172.1.1.50.80: SWE 1719837470:1719837470(0) win 8192 <mss 1460,nop,wscale 8,nop,nop,sackOK>
Phase: 1
Type: L2-EGRESS-IFC-LOOKUP
Subtype: Destination MAC L2 Lookup
Result: ALLOW
Config:
Additional Information:
Destination MAC lookup resulted in egress ifc MGMT40_Outside1

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

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

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

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

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 78
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 79
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 80
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 81
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 82

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 83

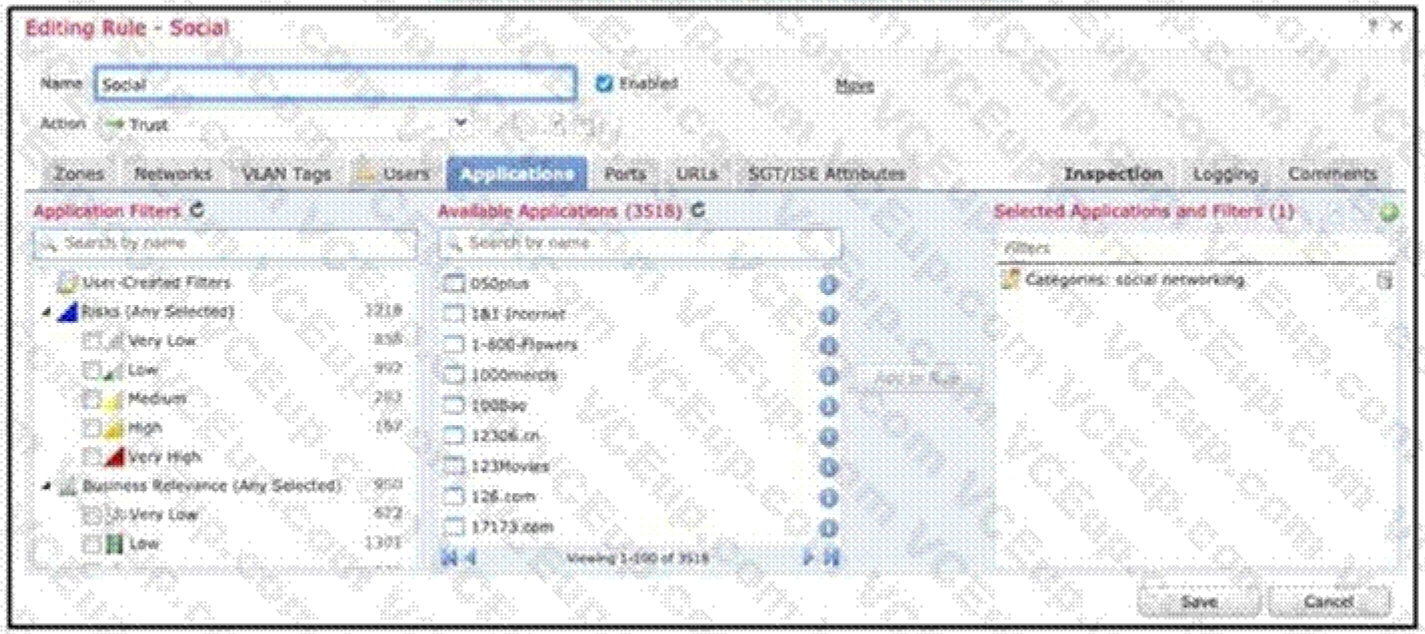
An organization has implemented Cisco Firepower without IPS capabilities and now wants to enable inspection for their traffic. They need to be able to detect protocol anomalies and utilize the Snort rule sets to detect malicious behaviour.
How is this accomplished?

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 84

Refer to the exhibit.



Editing Rule - Social

Name: Social ☑ Enabled

Action: Trust

Selected Applications and Filters (1)

Categories: social networking

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 85
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 86
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 87
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 88
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

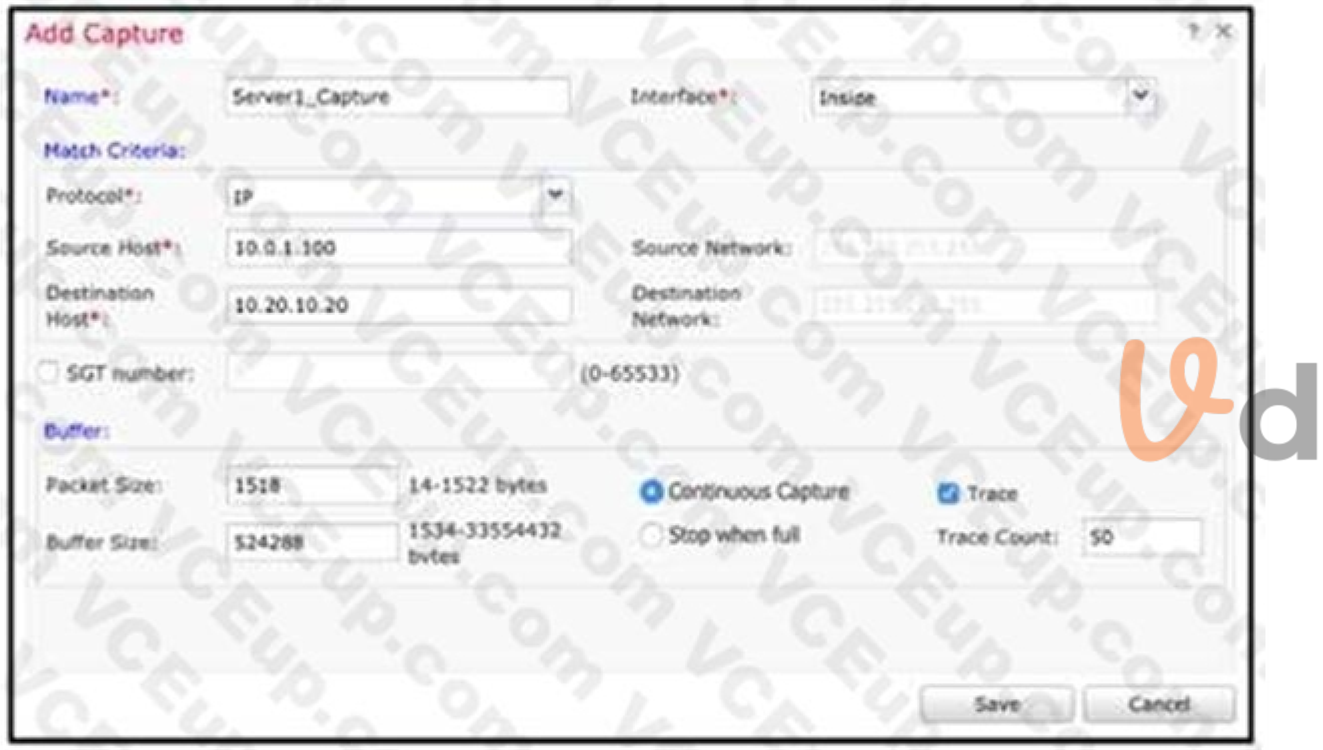
C. Use the Packet Tracer feature for traffic policy analysis

D. Use the Packet Analysis feature for capturing network data

Correct Answer: B
Section:

QUESTION 89
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.



Add Capture

Name*: Server1_Capture
Interface*: Inside

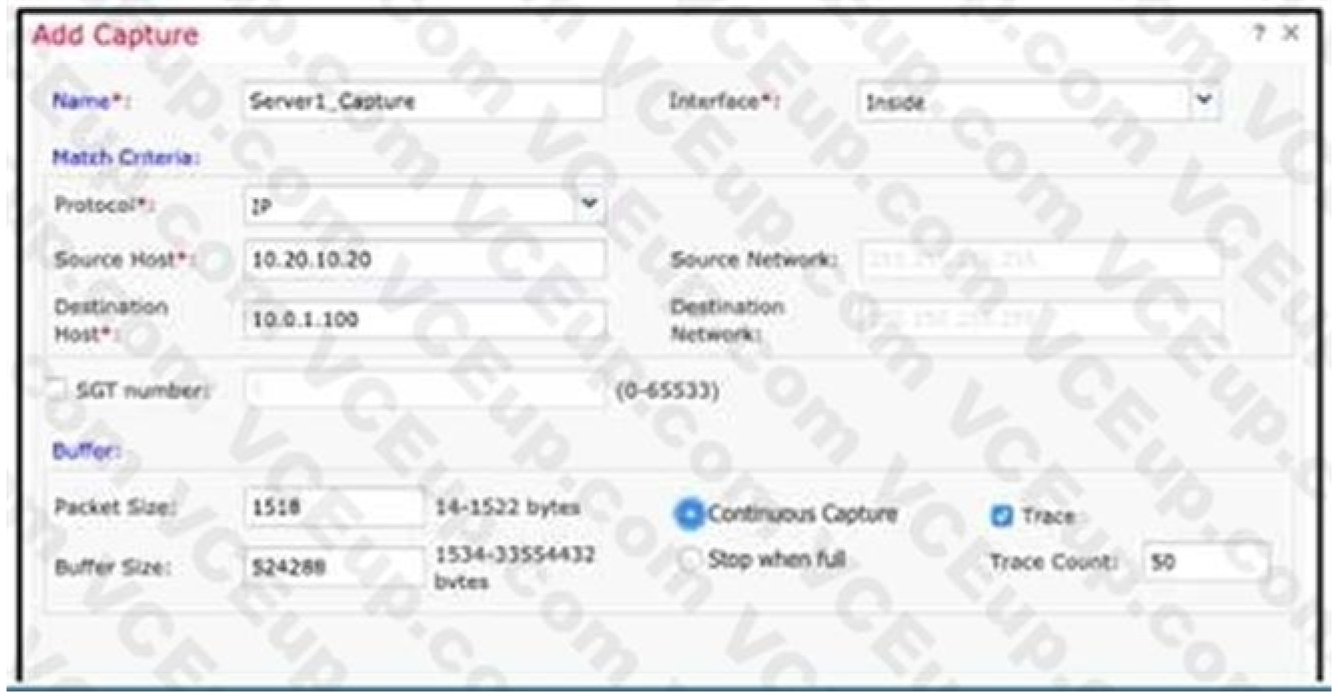
Match Criteria:

Protocol*: IP
Source Host*: 10.0.1.100
Source Network:
Destination Host*: 10.20.10.20
Destination Network:
□ SGT number: (0-65533)

Buffer:

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

B.



Add Capture

Name*: Server1_Capture

Interface*: Inside

Match Criteria:

Protocol*: IP

Source Host*: 10.20.10.20

Source Network: 255.255.255.255

Destination Host*: 10.0.1.100

Destination Network: 255.255.255.255

□ SGT number: 0 (0-65533)

Buffer:

Packet Size: 1518 14-1522 bytes

Buffer Size: 524288 1534-33554432 bytes

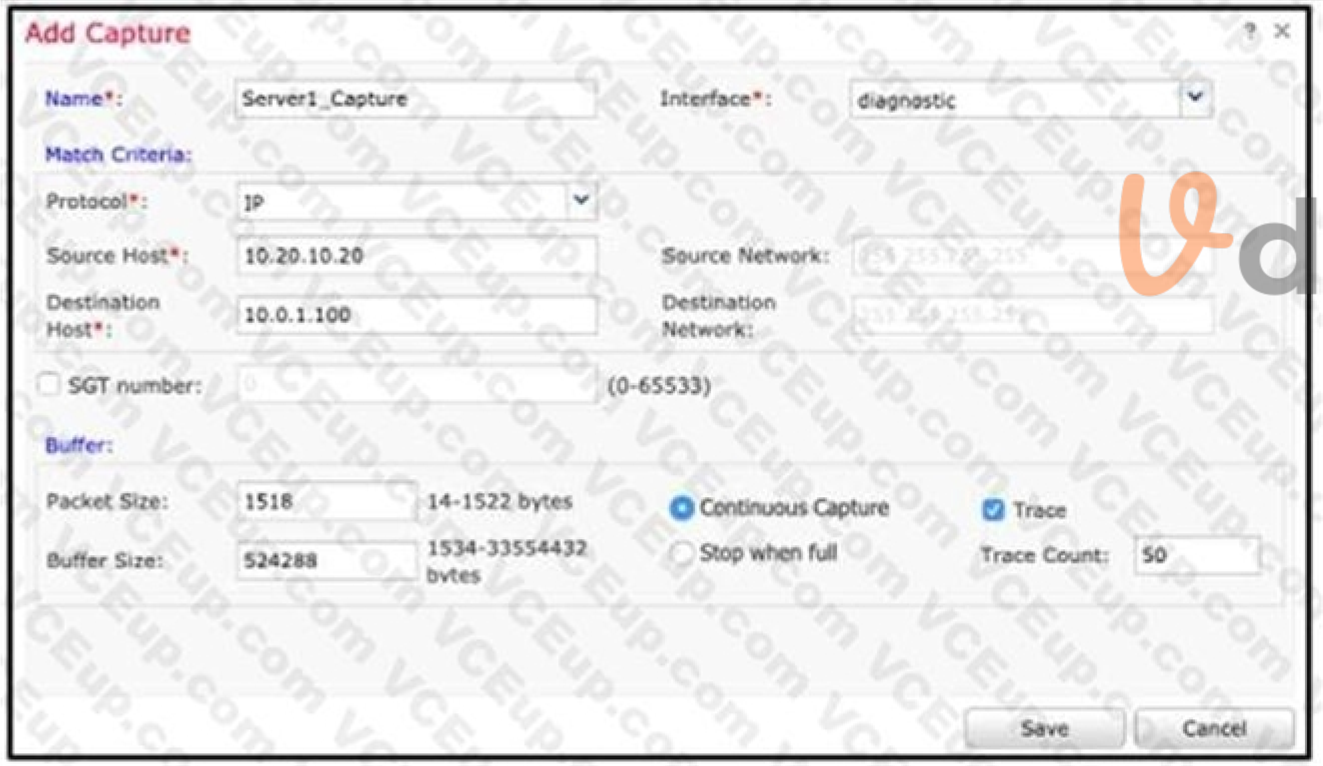
● Continuous Capture

○ Stop when full

☑ Trace

Trace Count: 50

C.



Add Capture

Name*: Server1_Capture

Interface*: diagnostic

Match Criteria:

Protocol*: IP

Source Host*: 10.20.10.20

Source Network: 255.255.255.255

Destination Host*: 10.0.1.100

Destination Network: 255.255.255.255

□ SGT number: 0 (0-65533)

Buffer:

Packet Size: 1518 14-1522 bytes

Buffer Size: 524288 1534-33554432 bytes

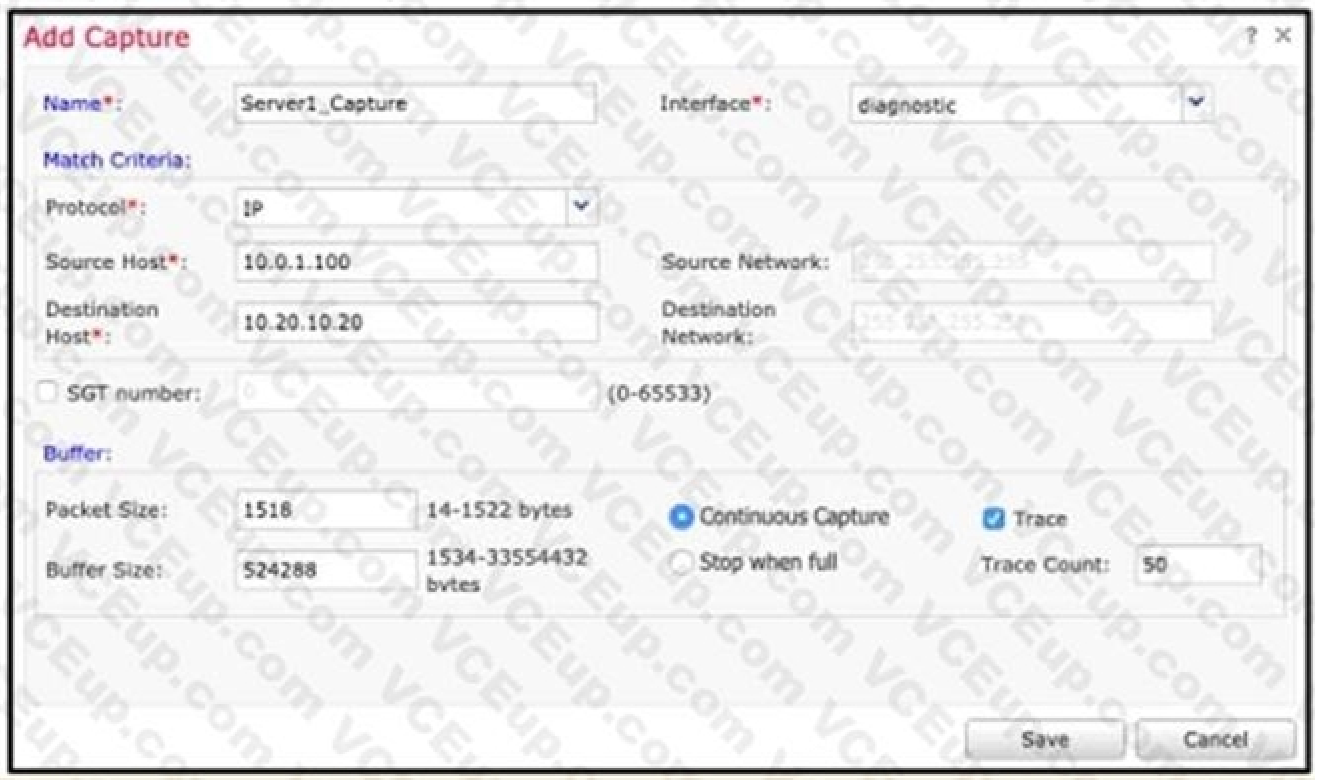
● Continuous Capture

○ Stop when full

☑ Trace

Trace Count: 50

D.



Add Capture

Name*: Server1_Capture

Interface*: diagnostic

Match Criteria:

Protocol*: IP

Source Host*: 10.0.1.100

Source Network:

Destination Host*: 10.20.10.20

Destination Network:

☐ SGT number: 0 (0-65533)

Buffer:

Packet Size: 1518 14-1522 bytes

Buffer Size: 524288 1534-33554432 bytes

● Continuous Capture

○ Stop when full

☑ Trace

Trace Count: 50

Correct Answer: B
Section:

QUESTION 90
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 91
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 92
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 93
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 94
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 95
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 96
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 97

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

A. The backup file is not in .cfg format.
B. The backup file is too large for the Cisco FTD device
C. The backup file extension was changed from tar to zip
D. The backup file was not enabled prior to being applied

Correct Answer: C
Section:

QUESTION 98
An engineer has been tasked with providing disaster recovery for an organization's primary Cisco FMC. What must be done on the primary and secondary Cisco FMCs to ensure that a copy of the original corporate policy is available if the primary Cisco FMC fails?

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

Correct Answer: A
Section:

QUESTION 99
A network engineer is logged into the Cisco AMP for Endpoints console and sees a malicious verdict for an identified SHA-256 hash. Which configuration is needed to mitigate this threat?

A. Add the hash to the simple custom deletion list.
B. Use regular expressions to block the malicious file.
C. Enable a personal firewall in the infected endpoint.
D. Add the hash from the infected endpoint to the network block list.

Correct Answer: A
Section:

QUESTION 100
An organization has a Cisco IPS running in inline mode and is inspecting traffic for malicious activity.
When traffic is received by the Cisco IRS, if it is not dropped, how does the traffic get to its destination?

A. It is retransmitted from the Cisco IPS inline set.
B. The packets are duplicated and a copy is sent to the destination.
C. It is transmitted out of the Cisco IPS outside interface.
D. It is routed back to the Cisco ASA interfaces for transmission.

Correct Answer: A
Section:

QUESTION 101
A network administrator is concerned about (he high number of malware files affecting users' machines. What must be done within the access control policy in Cisco FMC to address this concern?

A. Create an intrusion policy and set the access control policy to block.
B. Create an intrusion policy and set the access control policy to allow.
C. Create a file policy and set the access control policy to allow.
D. Create a file policy and set the access control policy to block.

Correct Answer: D
Section:

QUESTION 102
An engineer is investigating connectivity problems on Cisco Firepower that is using service group tags. Specific devices are not being tagged correctly, which is preventing clients from using the proper policies when going through the firewall How is this issue resolved?

A. Use traceroute with advanced options.
B. Use Wireshark with an IP subnet filter.
C. Use a packet capture with match criteria.
D. Use a packet sniffer with correct filtering

Correct Answer: C
Section:

QUESTION 103
A connectivity issue is occurring between a client and a server which are communicating through a Cisco Firepower device While troubleshooting, a network administrator sees that traffic is reaching the server, but the client is not getting a response Which step must be taken to resolve this issue without initiating traffic from the client?

A. Use packet-tracer to ensure that traffic is not being blocked by an access list.
B. Use packet capture to ensure that traffic is not being blocked by an access list.
C. Use packet capture to validate that the packet passes through the firewall and is NATed to the corrected IP address.
D. Use packet-tracer to validate that the packet passes through the firewall and is NATed to the corrected IP address.

Correct Answer: D
Section:

QUESTION 104
An organization must be able to ingest NetFlow traffic from their Cisco FTD device to Cisco Stealthwatch for behavioral analysis. What must be configured on the Cisco FTD to meet this requirement?

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

Correct Answer: A
Section:

QUESTION 105
An engineer must build redundancy into the network and traffic must continuously flow if a redundant switch in front of the firewall goes down. What must be configured to accomplish this task?

A. redundant interfaces on the firewall cluster mode and switches
B. redundant interfaces on the firewall noncluster mode and switches
C. vPC on the switches to the interface mode on the firewall duster
D. vPC on the switches to the span EtherChannel on the firewall cluster

Correct Answer: D
Section:
Explanation:
Reference: https://www.ciscolive.com/c/dam/r/ciscolive/us/docs/2018/pdf/BRKSEC-2020.pdf

QUESTION 106
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. All types of Cisco Firepower devices are supported.
B. An on-premises proxy server does not need to be set up and maintained.
C. Cisco Firepower devices do not need to be connected to the Internet.
D. Supports all devices that are running supported versions of Cisco Firepower.

Correct Answer: B
Section:

QUESTION 107
A network administrator notices that inspection has been interrupted on all non-managed interfaces of a device. What is the cause of this?

A. The value of the highest MTU assigned to any non-management interface was changed.
B. The value of the highest MSS assigned to any non-management interface was changed.
C. A passive interface was associated with a security zone.
D. Multiple inline interface pairs were added to the same inline interface.

Correct Answer: A
Section:

QUESTION 108
A network administrator is configuring Snort inspection policies and is seeing failed deployment messages in Cisco FMC. What information should the administrator generate for Cisco TAC to help troubleshoot?

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

Correct Answer: B
Section:

QUESTION 109
A network administrator needs to create a policy on Cisco Firepower to fast-path traffic to avoid Layer 7 inspection. The rate at which traffic is inspected must be optimized. What must be done to achieve this goal?

A. Enable lhe FXOS for multi-instance.

B. Configure a prefilter policy.
C. Configure modular policy framework.
D. Disable TCP inspection.

Correct Answer: B
Section:

QUESTION 110
A network engineer is tasked with minimising traffic interruption during peak traffic limes. When the SNORT inspection engine is overwhelmed, what must be configured to alleviate this issue?

A. Enable IPS inline link state propagation
B. Enable Pre-filter policies before the SNORT engine failure.
C. Set a Trust ALL access control policy.
D. Enable Automatic Application Bypass.

Correct Answer: D
Section:

QUESTION 111
A VPN user is unable to conned lo web resources behind the Cisco FTD device terminating the connection. While troubleshooting, the network administrator determines that the DNS responses are not getting through the Cisco FTD What must be done to address this issue while still utilizing Snort IPS rules?

A. Uncheck the "Drop when Inline" box in the intrusion policy to allow the traffic.
B. Modify the Snort rules to allow legitimate DNS traffic to the VPN users.
C. Disable the intrusion rule threshes to optimize the Snort processing.
D. Decrypt the packet after the VPN flow so the DNS queries are not inspected

Correct Answer: B
Section:

QUESTION 112
An analyst is investigating a potentially compromised endpoint within the network and pulls a host report for the endpoint in question to collect metrics and documentation. What information should be taken from this report for the investigation?

A. client applications by user, web applications, and user connections
B. number of attacked machines, sources of the attack, and traffic patterns
C. intrusion events, host connections, and user sessions
D. threat detections over time and application protocols transferring malware

Correct Answer: C
Section:

QUESTION 113
A company wants a solution to aggregate the capacity of two Cisco FTD devices to make the best use of resources such as bandwidth and connections per second. Which order of steps must be taken across the Cisco FTDs with Cisco FMC to meet this requirement?

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

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

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

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

Correct Answer: D
Section:

QUESTION 114
An analyst is reviewing the Cisco FMC reports for the week. They notice that some peer-to-peer applications are being used on the network and they must identify which poses the greatest risk to the environment. Which report gives the analyst this information?

A. Attacks Risk Report

B. User Risk Report

C. Network Risk Report

D. Advanced Malware Risk Report

Correct Answer: C
Section:

QUESTION 115
An administrator is adding a new URL-based category feed to the Cisco FMC for use within the policies. The intelligence source does not use STIX. but instead uses a .txt file format. Which action ensures that regular updates are provided?

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

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

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

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

Correct Answer: A
Section:

QUESTION 116
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. Only the UDP packet type is supported.

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

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

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

Correct Answer: C
Section:

QUESTION 117
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 118
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

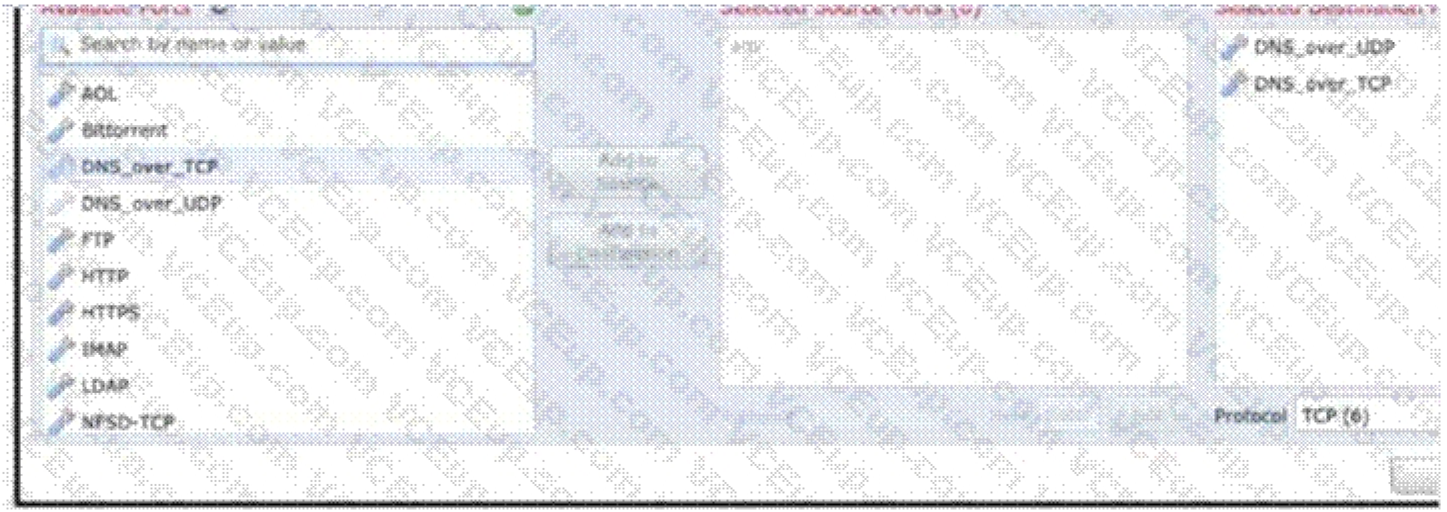
Correct Answer: C
Section:

QUESTION 119
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 120
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 121
A network engineer is logged into the Cisco AMP for Endpoints console and sees a malicious verdict for an identified SHA-256 hash. Which configuration is needed to mitigate this threat?

A. Use regular expressions to block the malicious file.
B. Add the hash from the infected endpoint to the network block list.
C. Add the hash to the simple custom detection list.
D. Enable a personal firewall in the infected endpoint.

Correct Answer: C
Section:

QUESTION 122
An engineer must define a URL object on Cisco FMC. What is the correct method to specify the URL without performing SSL inspection?

A. Use Subject Common Name value.
B. Specify all subdomains in the object group.
C. Specify the protocol in the object.
D. Include all URLs from CRL Distribution Points.

Correct Answer: B
Section:

QUESTION 123
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 routed.
D. Change the firewall mode to transparent.

Correct Answer: C
Section:

QUESTION 124
A network administrator is reviewing a monthly advanced malware risk report and notices a host that Is listed as CnC Connected. Where must the administrator look within Cisco FMC to further determine if this host is infected with malware?

A. Analysis > Hosts > indications of Compromise

B. Analysts > Files > Malware Events
C. Analysis > Hosts > Host Attributes
D. Analysis > Flies > Network File Trajectory

Correct Answer: A
Section:
Explanation:
To determine if a host is infected with malware, the network administrator can look at the Indications of Compromise (IOC) feature in Cisco FMC. The IOC feature analyzes network and endpoint data collected by Firepower sensors and AMP for Endpoints connectors, and identifies hosts that exhibit signs of compromise or infection. The IOC feature uses predefined rules based on Cisco Talos intelligence and other sources to detect IOCs on hosts.One of these rules is CnC Connected, which indicates that a host has communicated with a command-and-control (CnC) server that is known to be associated with malware activity2.
To view the IOC information for a host, the network administrator can navigate to Analysis > Hosts > Indications of Compromise in Cisco FMC, and select a host from the table. The IOC Details page will show the IOC events for that host, including the CnC Connected event, along with other information such as severity, timestamp, source, destination, protocol, and rule name.The network administrator can also view more details about each IOC event by clicking on it2.
The other options are incorrect because:
Analysis > Files > Malware Events shows information about files that have been detected as malware by Firepower sensors or AMP for Endpoints connectors.This does not show information about hosts that are infected with malware or have communicated with CnC servers3.
Analysis > Hosts > Host Attributes shows information about hosts that have been discovered by Firepower sensors, such as IP address, MAC address, operating system, applications, users, vulnerabilities, and so on.This does not show information about IOCs or CnC connections on hosts4.
Analysis > Files > Network File Trajectory shows information about files that have traversed your network and have been detected by Firepower sensors or AMP for Endpoints connectors. This allows you to track where a file came from, where it went, and what happened to it along the way.This does not show information about hosts that are infected with malware or have communicated with CnC servers5.

QUESTION 125
An engineer is configuring a custom application detector for HTTP traffic and wants to import a file that was provided by a third party. Which type of flies are advanced application detectors creates and uploaded as?

A. Perl script
B. NBAR protocol
C. LUA script
D. Python program

Correct Answer: C
Section:
Explanation:
A custom application detector is a user-defined script that can detect web applications, clients, and application protocols based on patterns in network traffic. Custom application detectors are written in LUA, which is a lightweight and embeddable scripting language.LUA scripts can use predefined functions and variables provided by the Firepower System to access packet data and metadata, and to specify the detection criteria and the application information1.
To import a custom application detector file that was provided by a third party, you need to follow these steps1:
In the FMC web interface, navigate to Objects > Object Management > Application Detectors.
Click Import.
Browse to the location of the LUA script file and select it.
Click Upload.
Review the detector details and click Save.
The other options are incorrect because:
Perl script is not a supported format for custom application detectors. Perl is a general-purpose programming language that is not embedded in the Firepower System.
NBAR protocol is not a file type, but a feature of Cisco IOS routers that can classify and monitor network traffic based on application types. NBAR protocols are predefined and cannot be imported as custom application detectors.
Python program is not a supported format for custom application detectors. Python is a general-purpose programming language that is not embedded in the Firepower System.

QUESTION 126
An engineer must investigate a connectivity issue from an endpoint behind a Cisco FTD device and a public DNS server. The endpoint cannot perform name resolution queries. Which action must the engineer perform to

troubleshoot the issue by simulating real DNS traffic on the Cisco FTD while verifying the Snarl verdict?

A. Perform a Snort engine capture using tcpdump from the FTD CLI.
B. Use the Capture w/Trace wizard in Cisco FMC.
C. Create a Custom Workflow in Cisco FMC.
D. Run me system support firewall-engine-debug command from me FTD CLI.

Correct Answer: B
Section:
Explanation:
The Capture w/Trace wizard in Cisco FMC allows you to capture packets on an FTD device and trace their path through the Snort engine. This can help you troubleshoot connectivity issues from an endpoint behind an FTD device and a public DNS server, as well as verify the Snort verdict for the DNS traffic. The Capture w/Trace wizard lets you specify the source and destination IP addresses, ports, and protocols for the packets you want to capture and trace, as well as the FTD device and interface where you want to perform the capture. You can also apply filters to limit the capture size and duration.After you start the capture, you can ping the DNS server from the endpoint and then view the captured packets and their Snort verdicts in the FMC web interface2.
To use the Capture w/Trace wizard in Cisco FMC, you need to follow these steps2:
In the FMC web interface, navigate to Troubleshooting > Capture/Trace.
Click New Capture.
Choose an FTD device from the Device drop-down list.
Choose an interface from the Interface drop-down list.
Enter the source and destination IP addresses, ports, and protocols for the packets you want to capture and trace. For example, if you want to capture DNS queries from an endpoint with IP address 10.1.1.100 to a DNS server with IP address 8.8.8.8, you can enter these values:
Source IP: 10.1.1.100
Source Port: any
Destination IP: 8.8.8.8
Destination Port: 53
Protocol: UDP
Optionally, apply filters to limit the capture size and duration. For example, you can set the maximum number of packets to capture, the maximum capture file size, or the maximum capture time.
Click Start.
Ping the DNS server from the endpoint and wait for some packets to be captured.
Click Stop to stop the capture.
Click View Capture to see the captured packets and their Snort verdicts.
The other options are incorrect because:
Performing a Snort engine capture using tcpdump from the FTD CLI will not allow you to trace the path of the packets through the Snort engine or verify their Snort verdicts.Tcpdump is a command-line tool that can capture packets on an FTD device, but it does not provide any information about how Snort processes those packets or what actions Snort takes on them2.
Creating a Custom Workflow in Cisco FMC will not help you troubleshoot a connectivity issue from an endpoint behind an FTD device and a public DNS server. A Custom Workflow is a user-defined set of pages that display event data in different formats, such as tables, charts, maps, and so on.A Custom Workflow does not allow you to capture or trace packets on an FTD device3.
Running the system support firewall-engine-debug command from the FTD CLI will not allow you to simulate real DNS traffic on the FTD device or verify the Snort verdict for that traffic. The firewall-engine-debug command is a diagnostic tool that can generate synthetic packets and send them through the Snort engine on an FTD device.The synthetic packets are not real network traffic and do not affect any connections or policies on the FTD device4.