Atmic Networks

CERTIFICATION EXAM SUPPORT

EXAM PREPARATION MATERIAL

Practice files designed to help you understand exam patterns, question styles and the overall assessment format.

IMPORTANT NOTE

> **Please note that these files may not be up to date. However, the questions will help you understand the exam format and typical question patterns.**

Stay connected with our support team
for the latest file updates and exam-related information.

www.atmicnetworks.com

Knowledge that moves beyond memorization.

www.atmicnetworks.com

Question: 1

What is a result of enabling Cisco FTD clustering?

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

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

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

D. All Firepower appliances can support Cisco FTD clustering.

Answer: C

Explanation:

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

Question: 2

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

A. The units must be the same version

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

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

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

E. The units must be the same model.

Answer: AE

Explanation:

Reference: https://www.cisco.com/c/en/us/support/docs/security/firepower-management-

center/212699- configure-ftd-high-availability-on-firep.html

Question: 3

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

A. transparent inline mode

B. TAP mode

C. strict TCP enforcement

D. propagate link state

Answer: D

Explanation:

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

Question: 4

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

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

Answer: C

Explanation:

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

Question: 5

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

A. Inline tap mode can send a copy of the traffic to another device.
B. Inline tap mode does full packet capture.
C. Inline mode cannot do SSL decryption.
D. Inline mode can drop malicious traffic.

Answer: A

Explanation:

Question: 6

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

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

Answer: B

Explanation:

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

Question: 7

Which two deployment types support high availability? (Choose two.)

A. transparent
B. routed
C. clustered
D. intra-chassis multi-instance

E. virtual appliance in public cloud

Answer: AB

Explanation:

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

Question: 8

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

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

Answer: A

Explanation:

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

Question: 9

Which interface type allows packets to be dropped?

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

Answer: B

Explanation:

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

Question: 10

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

A. Redundant Interface
B. EtherChannel
C. Speed
D. Media Type
E. Duplex

Answer: CE

Explanation:

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

Question: 11

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

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

Answer: BE

Explanation:

Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/660/fdm/fptd-fdm-config- guide-660/fptd-fdm-routing.html

Question: 12

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

A. a default DMZ policy for which only a user can change the IP addresses.
B. deny ip any
C. no policy rule is included
D. permit ip any

Answer: C

Explanation:

Question: 13

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

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

Answer: BC

Explanation:

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

Question: 14

An engineer is tasked with deploying an internal perimeter firewall that will support multiple DMZs

Each DMZ has a unique private IP subnet range. How is this requirement satisfied?

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

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

C. Deploy the firewall in routed mode with NAT configured.

D. Deploy the firewall in transparent mode with NAT configured.

Answer: C

Explanation:

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

Question: 15

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

A. in active/active mode
B. in a cluster span EtherChannel
C. in active/passive mode
D. in cluster interface mode

Answer: C

Explanation:

Question: 16

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

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

Answer: A

Explanation:

https://www.cisco.com/c/en/us/td/docs/security/asa/asa910/configuration/firewall/asa-910- firewall-config/access-sfr.html

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

Question: 17

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.

Answer: C

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.html

Passing Traffic Not Allowed in Routed Mode

In routed mode, some types of traffic cannot pass through the ASA even if you allow it in an access rule. The bridge group, however, can allow almost any traffic through using either an access rule (for IP 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: 18

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

A. Specify the BVI IP address as the default gateway for connected devices.
B. Enable routing on the Cisco Firepower
C. Add an IP address to the physical Cisco Firepower interfaces.
D. Configure a bridge group in transparent mode.

Answer: D

Explanation:

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-general- config/intro-fw.html

Question: 19

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

A. same flash memory size

B. same NTP configuration

C. same DHCP/PPoE configuration

D. same host name

E. same number of interfaces

Answer: BE

Explanation:

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

Conditions

In 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: 20

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

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

B. Disable the default IPS policy and enable global logging.

C. Configure an IPS policy and enable global logging.

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

Answer: C

Explanation:

Question: 21

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

Answer: D

Explanation:

Question: 22

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

Answer: A

Explanation:

www.atmicnetworks.com

Question: 23

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.

Answer: C

Explanation:

Question: 24

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

Answer: A

Explanation:

Question: 25

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

Answer: B

Explanation:

Question: 26

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.

Answer: C

Explanation:

Question: 27

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

Answer: B

Explanation:

Topic 2, Configuration

Question: 28

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

A. OSPFv2 with IPv6 capabilities
B. virtual links
C. SHA authentication to OSPF packets
D. area boundary router type 1 LSA filtering
E. MD5 authentication to OSPF packets

Answer: BE

Explanation:

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

Question: 29

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.

Answer: B

Explanation:

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

Question: 30

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

A. VPN connections can be re-established only if the failed master unit recovers.
B. Smart License is required to maintain VPN connections simultaneously across all cluster units.
C. VPN connections must be re-established when a new master unit is elected.
D. Only established VPN connections are maintained when a new master unit is elected.

Answer: C

Explanation:

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

Question: 31

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

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

Answer: BE

Explanation:

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

Question: 32

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

A. configure manager local 10.0.0.10 Cisco123
B. configure manager add Cisco123 10.0.0.10
C. configure manager local Cisco123 10.0.0.10
D. configure manager add 10.0.0.10 Cisco123

Answer: D

Explanation:

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

Question: 33

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

A. Block with Reset

B. Monitor C. Analyze D. Discover E. Block ALL

Answer: AB

Explanation:

Reference: https://www.cisco.com/c/en/us/td/docs/security/firesight/541/firepower-module-user- guide/asa-firepower-module-user-guide-v541/AC-Rules-Tuning-Overview.html#71854

Question: 34

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

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

Answer: AC

Explanation:

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

Question: 35

Which object type supports object overrides?

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

Answer: C

Explanation:

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

Question: 36

Which Cisco Firepower rule action displays an HTTP warning page?

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

Answer: C

Explanation:

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

Question: 37

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.

Answer: B

Explanation:

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

Question: 38

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

A. FlexConfig
B. BDI
C. SGT
D. IRB

Answer: D

Explanation:

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: 39

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

Answer: AC

Explanation:

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

Question: 40

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.

Answer: AC

Explanation:

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

Question: 41

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

A. dynamic key mapping objects that help link HTTP and HTTPS GET requests to Layer 7 application protocols.
B. reputation-based objects that represent Security Intelligence feeds and lists, application filters based on category and reputation, and file lists
C. network-based objects that represent IP address and networks, port/protocols pairs, VLAN tags, security zones, and origin/destination country

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

E. reputation-based objects, such as URL categories

Answer: BC

Explanation:

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

Question: 42

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

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

B. An external NAT IP address is not configured.

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

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

Answer: A

Explanation:

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

Question: 43

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

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

B. The administrator is adding interfaces of multiple types.

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

D. The interfaces belong to multiple interface groups.

Answer: D

Explanation:

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

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 it contains."

Question: 44

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

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

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

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

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

Answer: C

Explanation:

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

Question: 45

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.

Answer: A

Explanation:

Question: 46

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

Answer: A

Explanation:

Question: 47

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

Answer: C

Explanation:

Question: 48

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.

Answer: D

Explanation:

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

Question: 49

An organization does not want to use the default Cisco Firepower block page when blocking HTTP

traffic. The organization wants to include information about its policies and procedures to help educate the users whenever a block occurs. Which two steps must be taken to meet these requirements? (Choose two.)

A. 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.

Answer: B, E

Explanation:

Question: 50

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.

Answer: C

Explanation:

Question: 51

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.

Answer: C

Explanation:

A file policy defines the actions that the Cisco Firepower Threat Defense (FTD) device should take when it encounters different types of files. The file policy is applied as part of an access control policy. If an access control policy does not include a file policy, the FTD device will not take any action on the files it encounters, resulting in a disposition of "unknown" for all file types except exe.

Reference: https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/219759-configure-bypass-policies-on-the-cisco-firepow.html

Topic 3, Management and Troubleshooting

Question: 52

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.

Answer: A

Explanation:

Question: 53

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

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

Answer: C

Explanation:

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

Question: 54

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

A. system generate-troubleshoot
B. show configuration session
C. show managers

D. show running-config | include manager

Answer: C

Explanation:

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: 55

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

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

Answer: C

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-with- firepower-threat-defense-f.html#anc10

The command is
firepower# capture DMZ interface dmz trace detail match ip host 192.168.76.14 host 192.168.76.100 firepower# capture INSIDE interface inside trace detail match ip host 192.168.76.14 host 192.168.75.14

Question: 56

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

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

Answer: D

Explanation:

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

Question: 57

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.

Answer: C

Explanation:

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

Question: 58

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

Answer: D

Explanation:

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

Question: 59

Which report template field format is available in Cisco FMC?

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

Answer: C

Explanation:

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

Question: 60

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

A. Cisco Deep Analytics
B. OpenDNS Group

C. Cisco Network Response

D. Cisco Talos

Answer: D

Explanation:

Reference: https://www.cisco.com/c/en/us/products/security/threat-response.html#~benefits

Question: 61

DRAG DROP

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

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

Answer:

Explanation:

Unregister the device from the active Cisco FMC.

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

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

Register the affected device on the active Cisco FMC.

Explanation

Reference:
https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-config- guide-v62/firepower_management_center_high_availability.html#id_32288

Question: 62

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

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

Answer: A

Explanation:

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

Question: 63

Which command-line mode is supported from the Cisco Firepower Management Center CLI?

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

Answer: C

Explanation:

Reference:

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

Question: 64

Which command is entered in the Cisco FMC CLI to generate a troubleshooting file?

A. show running-config
B. show tech-support chassis
C. system support diagnostic-cli
D. sudo sf_troubleshoot.pl

Answer: D

Explanation:

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

Question: 65

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-enabled

Answer: A

Explanation:

Question: 66

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

A. configure high-availability resume
B. configure high-availability disable
C. system support network-options
D. configure high-availability suspend

Answer: B

Explanation:

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

Question: 67

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

A. system support view-files
B. sudo sf_troubleshoot.pl
C. system generate-troubleshoot all
D. show tech-support

Answer: C

Explanation:

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

Question: 68

When do you need the file-size command option during troubleshooting with packet capture?

A. when capture packets are less than 16 MB
B. when capture packets are restricted from the secondary memory
C. when capture packets exceed 10 GB
D. when capture packets exceed 32 MB

Answer: D

Explanation:

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

Question: 69

What is a functionality of port objects in Cisco FMC?

A. to mix transport protocols when setting both source and destination port conditions in a rule
B. to represent protocols other than TCP, UDP, and ICMP
C. to represent all protocols in the same way
D. to add any protocol other than TCP or UDP for source port conditions in access control rules.

Answer: B

Explanation:

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

www.atmicnetworks.com

Question: 70

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

A. dashboard
B. reporting
C. context explorer
D. summary tool

Answer: A

Explanation:

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

Question: 71

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

A. outbound port TCP/443
B. inbound port TCP/80
C. outbound port TCP/8080
D. inbound port TCP/443
E. outbound port TCP/80

Answer: AE

Explanation:

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

Question: 72

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

A. 1024
B. 8192
C. 4096
D. 2048

Answer: C

Explanation:

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

Question: 73

Which limitation applies to Cisco Firepower Management Center dashboards in a multidomain environment?

A. Child domains can view but not edit dashboards that originate from an ancestor domain.
B. Child domains have access to only a limited set of widgets from ancestor domains.
C. Only the administrator of the top ancestor domain can view dashboards.
D. Child domains cannot view dashboards that originate from an ancestor domain.

Answer: D

Explanation:

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

Question: 74

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

A. An option to re-apply NAT and VPN policies during registration is available, so users do not need to re- apply the policies after registration is completed.
B. Before re-adding the device in Cisco FMC, you must add the manager back in the device.
C. No option to delete and re-add a device is available in the Cisco FMC web interface.
D. The Cisco FMC web interface prompts users to re-apply access control policies.
E. No option to re-apply NAT and VPN policies during registration is available, so users need to reapply the policies after registration is completed.

Answer: DE

Explanation:

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

Question: 75

What is a behavior of a Cisco FMC database purge?

A. User login and history data are removed from the database if the User Activity check box is selected.
B. Data can be recovered from the device.

C. The appropriate process is restarted.
D. The specified data is removed from Cisco FMC and kept for two weeks.

Answer: C

Explanation:

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

Question: 76

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

A. Layer 7 network ID
B. source IP
C. application ID
D. dynamic firewall importing
E. protocol

Answer: BE

Explanation:

Reference: https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/212474-working- with-firepower-threat-defense-f.html

Topic 4, Integration

Question: 77

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

A. application blocking
B. simple custom detection
C. file repository
D. exclusions
E. application whitelisting

Answer: AB

Explanation:

Question: 78

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.

Answer: A

Explanation:

Question: 79

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

Answer: B

Explanation:

Reference: https://www.cisco.com/c/en/us/support/docs/security/amp-endpoints/214933-amp-for- endpoints-deployment-methodology.html

Question: 80

What is a valid Cisco AMP file disposition?

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

Answer: B

Explanation:

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

Question: 81

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

Answer: A

Explanation:

Question: 82

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

Answer: CD

Explanation:

Reference: https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/210524- configure-firepower-6-1-pxgrid-remediati.html

Question: 83

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

Answer: A

Explanation:

Question: 84

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

Answer: D

Explanation:

Reference:

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

Topic 5, NEW Questions

Question: 85

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 now had WM added to the natwoik	36#
A dovK# dotted uung ■ now transport protocol	MI
A dowoo started using • now 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.

Answer: C

Explanation:

Ref: https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-

config-guide-v60/Tailoring_Intrusion_Protection_to_Your_Network_Assets.html

Question: 86

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

Answer: D

Explanation:

Question: 87

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

Answer: C

Explanation:

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

Question: 88

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.

Answer: B

Explanation:

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

Question: 89

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

Answer: A

Explanation:

Question: 90

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

Answer: B

Explanation:

Question: 91

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

Answer: C

Explanation:

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

Question: 92

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.

Answer: A

Explanation:

Question: 93

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

Answer: D

Explanation:

Question: 94

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.

Answer: A

Explanation:

Question: 95

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.

Answer: B

Explanation:

Question: 96

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

Answer: D

Explanation:

Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/integrations/CTR/Firepower_and_Cisco_Threat_Response_Integration_Guide.pdf

Question: 97

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

Answer: D

Explanation:

Question: 98

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

Answer: C

Explanation:

Reference:
https://www.cisco.com/c/en/us/td/docs/security/firepower/migration-tool/migration-

guide/ASA2FTD-with-FP-Migration-Tool/b_Migration_Guide_ASA2FTD_chapter_01011.html

Question: 99

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

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

Answer: AC

Explanation:

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

Question: 100

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

Answer: C

Explanation:

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

Question: 101

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

Answer: B

Explanation:

Question: 102

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

Answer: B

Explanation:

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

Question: 103

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

Answer: D

Explanation:

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

Question: 104

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

A. Before re-adding the device In Cisco FMC, the manager must be added back.
B. The Cisco FMC web interface prompts users to re-apply access control policies.
C. Once a device has been deleted, It must be reconfigured before it is re-added to the Cisco FMC.

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

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

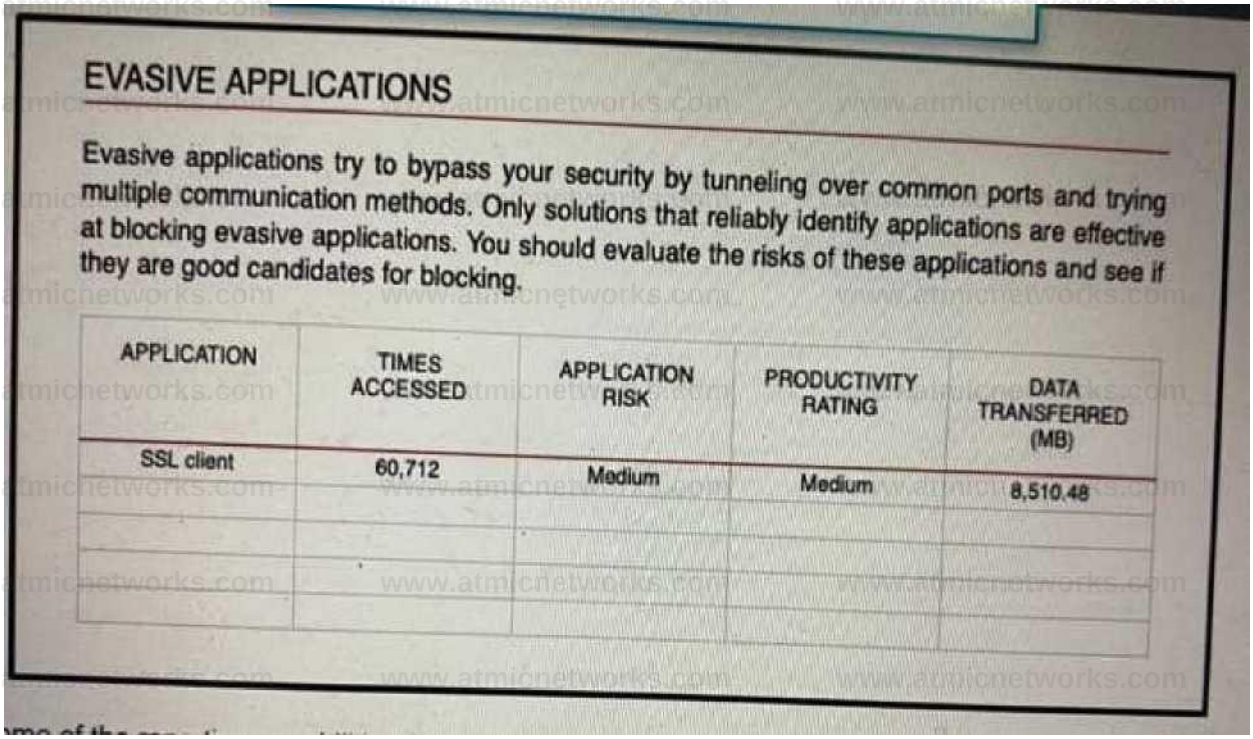
Answer: B, E

Explanation:

Question: 105

Refer to the exhibit.

www.atmicnetworks.com



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.

Answer: A

Explanation:

Question: 106

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

Answer: D

Explanation:

Question: 107

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

Answer: D

Explanation:

Question: 108

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

Answer:B

Question: 109

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

Answer: B

Explanation:

Question: 110

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

Answer: A

Explanation:

Question: 111

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.

Answer: C

Explanation:

Question: 112

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

Answer: D

Explanation:

Question: 113

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

Answer: C

Explanation:

When you configure the Cisco Firepower devices to bypass the access control policies for VPN traffic, the devices will not inspect the VPN traffic and thus will not waste resources on it. This is the best option to ensure that the VPN traffic is not wasting resources on the Cisco Firepower devices.

Reference: https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/219759-configure-bypass-policies-on-the-cisco-firepow.html

Question: 114

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?

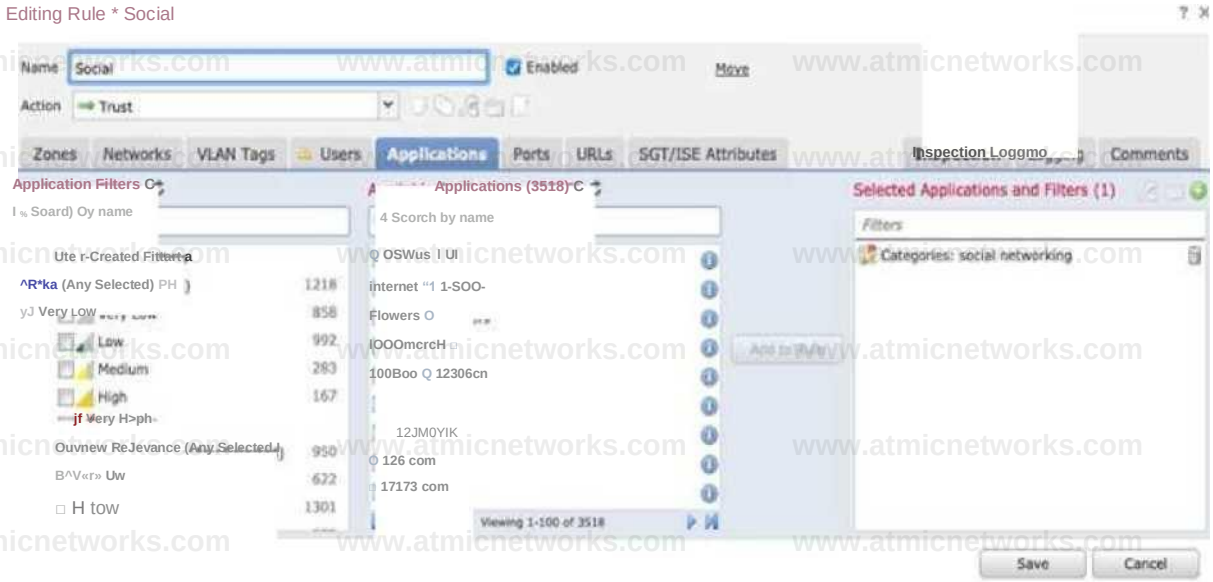
A. Modify the access control policy to redirect interesting traffic to the engine
B. Modify the network discovery policy to detect new hosts to inspect
C. Modify the network analysis policy to process the packets for inspection
D. Modify the intrusion policy to determine the minimum severity of an event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

Answer: D

Explanation:

Question: 115

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

Answer: A

Explanation:

Question: 116

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

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

Answer: C

Explanation:

Question: 117

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

Answer: B

Explanation:

Question: 118

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

Answer: A

Explanation:

Question: 119

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

Answer: B

Explanation:

Question: 120

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

Answer: D

Explanation:

Question: 121

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

Answer: B

Explanation:

Question: 122

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

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

Answer: B

Explanation:

Question: 123

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

Answer: A

Explanation:

Question: 124

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

Answer: B

Explanation:

Question: 125

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

Answer: A

Explanation:

Question: 126

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

Answer: A

Explanation:

Question: 127

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

Answer: A

Explanation:

Question: 128

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

Answer: D

Explanation:

Question: 129

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

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

Answer: B

Explanation:

Question: 130

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

Answer: B

Explanation:

Question: 131

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

Answer: B

Explanation:

Question: 132

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

Answer: C

Explanation:

Question: 133

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

Answer: A

Explanation:

Question: 134

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

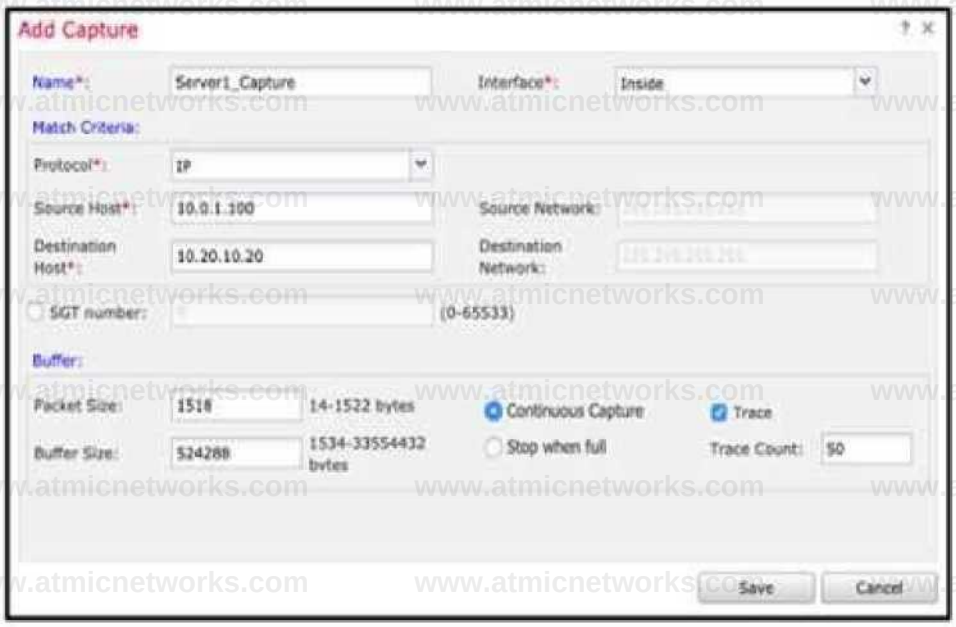
Answer: D

Explanation:

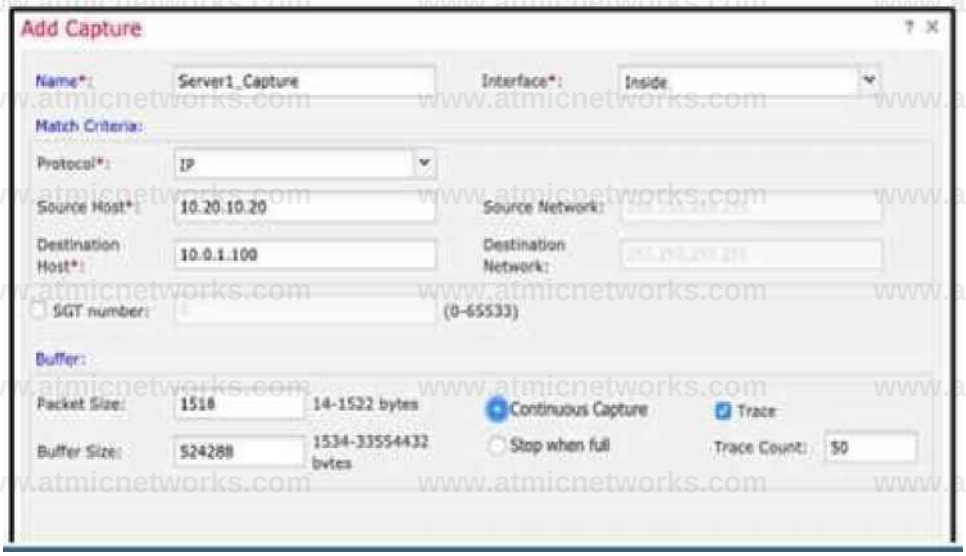
Question: 135

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?

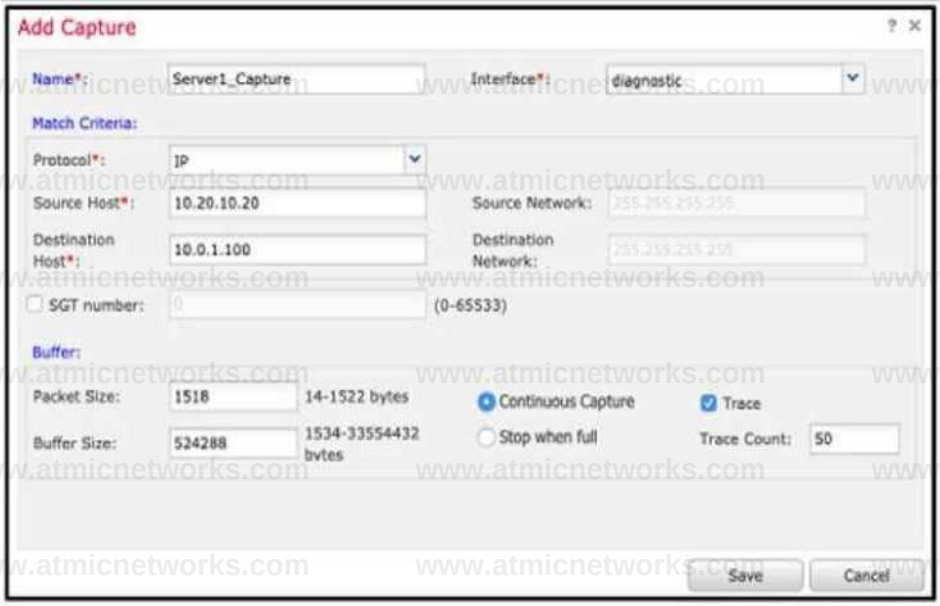
A)



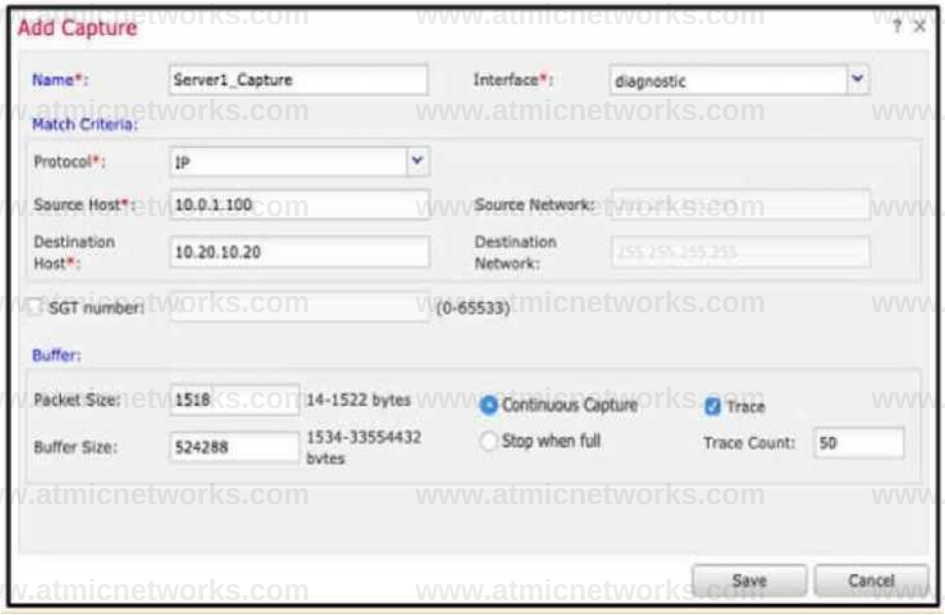
B)



C)



D)



A. Option A B. Option B C. Option C D. Option D

Answer: B

Explanation:

Question: 136

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

Answer: B

Explanation:

Question: 137

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

Answer: B

Explanation:

Question: 138

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

A. Intrusion Events
B. Correlation Information
C. Appliance Status
D. Current Sessions
E. Network Compliance

Answer: A, E

Explanation:

Question: 139

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.

Answer: BE

Explanation:

Question: 140

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.

Answer: A

Explanation:

Question: 141

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.

Answer: DE

Explanation:

Question: 142

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

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

Answer: D

Explanation:

Question: 143

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

Answer: C

Explanation:

Question: 144

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.

Answer: A

Explanation:

Question: 145

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.

Answer: A

Explanation:

Question: 146

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.

Answer: A

Explanation:

Question: 147

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.

Answer: D

Explanation:

Question: 148

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

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

Answer: C

Explanation:

Question: 149

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.

Answer: D

Explanation:

Question: 150

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

Answer: A

Explanation:

Question: 151

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

Answer: D

Explanation:

Reference: https://www.ciscolive.com/c/dam/r/ciscolive/us/docs/2018/pdf/BRKSEC-2020.pdf

Question: 152

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.

Answer: B

Explanation:

Question: 153

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.

Answer: A

Explanation:

Question: 154

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.

Answer: B

Explanation:

Question: 155

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.

Answer: B

Explanation:

Question: 156

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.

Answer: D

Explanation:

Question: 157

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

Answer: B

Explanation:

Question: 158

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

Answer: C

Explanation:

Question: 159

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.

Answer: D

Explanation:

Question: 160

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.

Answer: C

Explanation:

Question: 161

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.

Answer: B

Explanation:

Question: 162

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.

Answer: C

Explanation:

Question: 163

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

Answer: C

Explanation:

Question: 164

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.

Answer: A

Explanation:

Question: 165

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.

Answer: C

Explanation:

Question: 166

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.

Answer: D

Explanation:

Question: 167

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

www.atmicnetworks.com

Answer: C

Explanation:

Question: 168

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.

Answer: B

Explanation:

Question: 169

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

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

C. The rule Is configured with the wrong setting for the source port.

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

Answer: A

Explanation:

www.atmicnetworks.com

Question: 170

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

Answer: D

Explanation:

Question: 171

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.

Answer: C

Explanation:

Question: 172

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

Answer: CD

Explanation:

Question: 173

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.

Answer: C

Explanation:

Question: 174

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.

Answer: D

Explanation:

Question: 175

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.

Answer: D

Explanation:

Question: 176

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.

Answer: A

Explanation:

Question: 177

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

Answer: D

Explanation:

Question: 178

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.

Answer: C

Explanation:

Reference: https://www.ciscolive.com/c/dam/r/ciscolive/emea/docs/2019/pdf/BRKSEC-3455.pdf

Question: 179

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.

Answer: B

Explanation:

Question: 180

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.

Answer: B

Explanation:

Question: 181

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

Answer: A

Explanation:

Question: 182

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

Answer: C

Explanation:

Question: 183

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.

Answer: A

Explanation:

Question: 184

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.

Answer: B

Explanation:

Question: 185

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

Answer: C

Explanation:

Question: 186

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

Answer: D

Explanation:

Question: 187

An engineer is working 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

Answer: D

Explanation:

Question: 188

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

Answer: C

Explanation:

Question: 189

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

Answer: A

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: 190

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

Answer: B

Explanation:

Question: 191

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.

Answer: D

Explanation:

Question: 192

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

Answer: C

Explanation:

Question: 193

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

Answer: B

Explanation:

Question: 194

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

Answer: A

Explanation:

Question: 195

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

A. The switches do not have Layer 3 connectivity to the FTD device for GRE traffic transmission.
B. The switches were not set up with a monitor session ID that matches the flow ID defined on the Cisco FTD.
C. The Cisco FTD must be in routed mode to process ERSPAN traffic.
D. The Cisco FTD must be configured with an ERSPAN port not a passive port.

Answer: C

Explanation:

Question: 196

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.

Answer: A

Explanation:

https://www.cisco.com/c/en/us/td/docs/security/firepower/601/configuration/guide/fpmc-config- guide-v601/fpmc-config-guide-v60_chapter_01011010.pdf

Question: 197

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.

Answer: A

Explanation:

Question: 198

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.

Answer: B

Explanation:

Question: 199

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.

Answer: A

Explanation:

Question: 200

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.

Answer: B

Explanation:

Question: 201

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

Answer: D

Explanation:

Question: 202

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

Answer: A

Explanation:

Question: 203

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

Answer: A

Explanation:

Question: 204

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.

Answer: A

Explanation:

Question: 205

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.

Answer: D

Explanation:

Question: 206

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.

Answer: A

Explanation:

Question: 207

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

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

Answer: D

Explanation:

Question: 208

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.

Answer: A

Explanation:

Question: 209

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.

Answer: C

Explanation:

Question: 210

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.

Answer: B

Explanation:

Question: 211

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.

Answer: D

Explanation:

Question: 212

Which feature is supported by IRB on Cisco FTD devices?

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

Answer: B

Explanation:

Question: 213

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.

Answer: D

Explanation:

Question: 214

Refer to the exhibit.

r*>l«i It !^«l !M«l Mijtc: MWlt! DROP C«MW AMKIOMl taforwtlaiu IMH text; Packet i IOV teitIOtv Mw IMM bMtM* MreNIli ttani<s n«W MTcning. nat 4 -» 1. #N • -• ♦, tian #. tor «. ir< ^t t,K •. MV.W.TN •. •** W ¹VM •* w#n»N 'Mo iMMacicMiaR RnulfM* « , IOOTIN 4. tcwCNt • ri retell; #UU rota. 'rH' . 4'N (MMI Irocerred N<Mer atarii or act lent <ueN« drop (MM 14 •. w* 14). IK 14 », VPf«ut MKXIW. #l«w« By HNM#H Snort Verdict; (fel«k-ll«O Black <Ht Mill flow

Multi !M«t-|MUrfM<c ACttS$41jM»Oa| inOvt-statmi M> iri^jt-tIM-Mat-C: up actl#A: draa
Dr«p*r«Mon; (VIrtMIIl 4lettrd er BtackUatN by the firewall prNrecoMr, Oro#-localIMl fraae e»eNOii<Jt4t44>fc# flov iNAl/MA

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

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

Answer: A

Explanation:

Question: 215

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.

Answer: D

Explanation:

Question: 216

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

Answer: A

Explanation:

Question: 217

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

Answer: C

Explanation:

Question: 218

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

redundancy configuration? (Choose two.)

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

Answer: A, C

Explanation:

www.atmicnetworks.com

Question: 219

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.

Answer: C

Explanation:

Question: 220

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.

Answer: B

Explanation:

Question: 221

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

Answer: B, C

Explanation:

Question: 222

Due to an Increase in malicious events, a security engineer must generate a threat report to include intrusion in 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.

Answer: D

Explanation:

Question: 223

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 CLI for the device is managed by Cisco FMC to which the engineer has access. Which action in Cisco FMC grants access to the CLI 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.

Answer: A

Explanation:

Question: 224

An administrator is attempting to add a new FTD device to their FMC behind a NAT device with a NAT ID of NAT001 and a password of Cisco0420l06525. The private IP address of the FMC server is 192.168.45.45. which is being translated to the public IP address of 209.165.200.225/27. Which command set must be used in order to accomplish this task?

A. configure manager add 209.165.200.225 <reg_key> <nat_id>
B. configure manager add 192.168.45,45 <reg_key> <nat_id>
C. configure manager add 209.165.200.225 255.255.255.224 <reg_key> <nat_id>
D. configure manager add 209.165.200.225/27 <reg_key> <nat_id>

Answer: A

Explanation:

Question: 225

A security analyst must create a new report within Cisco FMC to show an overview of the daily attacks, vulnerabilities, and connections. The analyst wants to reuse specific dashboards from other reports to create this consolidated one. Which action accomplishes this task?

A. Create a new dashboard object via Object Management to represent the desired views.
B. Modify the Custom Workflows within the Cisco FMC to feed the desired data into the new report.

C. Copy the Malware Report and modify the sections to pull components from other reports.
D. Use the import feature in the newly created report to select which dashboards to add.

Answer: D

Explanation:

Question: 226

A network administrator has converted a Cisco FTD from using LDAP to LDAPS for VPN authentication. The Cisco FMC can connect to the LDAPS server, but the Cisco FTD is not connecting. Which configuration must be enabled on the Cisco FTD?

A. SSL must be set to a use TLSv1.2 or lower.
B. The LDAPS must be allowed through the access control policy.
C. DNS servers must be defined for name resolution.
D. The RADIUS server must be defined.

Answer: B

Explanation:

Question: 227

When using Cisco Threat Response, which phase of the Intelligence Cycle publishes the results of the investigation?

A. direction
B. dissemination
C. processing
D. analysis

Answer: B

Explanation:

Disseminate: The dissemination phase publishes the results of the investigation or threat hunt. This information is disseminated with a focus on the receivers of the information. At the tactical level, this information feeds back into the beginning of the F3EAD model, Find. Figure 3 illustrates the F3EAD model.

Question: 228

A security engineer must integrate an external feed containing STIX/TAXII data with Cisco FMC. Which feature must be enabled on the Cisco FMC to support this connection?

A. Cisco Success Network
B. Cisco Secure Endpoint Integration

C. Threat Intelligence Director
D. Security Intelligence Feeds

Answer: C

Explanation:

Question: 229

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

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

Answer: D

Explanation:

Question: 230

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

A. Prefilter policy
B. SSL policy
C. DNS policy
D. Access Control policy with URL filtering

Answer: D

Explanation:

Question: 231

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

A. Set up a virtual failover MAC address between chassis.
B. Use a dedicated stateful link between chassis.
C. Load the same software version on both chassis.
D. Set the same FQDN for both chassis.

Answer: B

Explanation:

Question: 232

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

A. Set to passive, and configure an access control policy with an intrusion policy and a file policy defined
B. Set to passive, and configure an access control policy with a prefilter policy defined
C. Set to none, and configure an access control policy with a prefilter policy defined
D. Set to none, and configure an access control policy with an intrusion policy and a file policy defined

Answer: A

Explanation:

Question: 233

DRAG DROP

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

www.atmicnetworks.com

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

Answer:

Explanation:
4, 1, 2, 3

Question: 234

HIGH BANDWIDTH APPLICATIONS

Son* apotcahont uM • aubatartoM amoura & naTwor* MnMdbi TWa btndandtl M*0* <4* ba CMS* * row argamcMan ar# can nagaMn •'Md warn* raw* partonHanca *M ma* oara to raatHCt rw uaaga at MM acMubona 1s partoMi naw** tor natanca a MMM Matt ma* not ba wot wtad tor MM vatiwig (k. yew can arwt Man MM aoatcatana ar*«y or caw gal ***** •* "a* *•* banbarM to ban* MS#

•aaMM— MM

'touTMa	MS	**•	Wry 10*	ntm>
Pandora AM«	•	MB0UIB	WVUe	t40t0
Scotto	44	IMum	Wr»LMi	snt?
bkcroaMUpMa	m	ItoMn	LM	2M!7
Aaati VtoM	HO	Uw	14*	2WM

ENCRYPTED APPLICATIONS

aora* at*Aeaaon* ancr*t« Mu Ma* MCbM £*•»<() MCWty ttotonaaraaar* « b* oam) 9 *tac*a ana map panama Wan ML aacryytoan aMaMbaton can Mb awM MM appteaacna and abeam Mr MM An ML OKtopaoa apptarc* men at a Qtco SSL Accaarca can daoypc SSL MAC nbauno ano oaMotM MouM be ■ta>«* M canftcato* to onawa nab tanar*. an# autoerr# by actng at in MarmaMry n brawaan csnnacbant to toa l<M>>at a to "wortort to MM SSL Oacrypton to abeam naMb Ma ancryptao apptcMona to bat "Mgato PM tWM Mae* MCtor

Qtotototo AMMMBB bate rM«M*wa

Cto*M	NM	Madum	Madex*	msm
Mamta Ej*«r ar	11 OJO	UMurn	UMur*	JJS1M6
torataa	»rw	UMM	VMM*	MM10
War	t Mt	Matoum	ttaMaai	44 HL*
Karbama	17U	Vary Lon	K*[1]	4#4»

EVASIVE APPLICATIONS

Erttna tcaacMona try ■ »>MM roar MC vray by *mnatr# ever camw MTH W naif MM* coMweaMn naVMa Only tabibana M Matty Mntty apyAcaacna era oStcbM to ttodang Mania aantcaaona Itou MoM arMMa *<• nak* el traa* aacneatona anO aaa * bay art paoo caMMaa tor taocarr*

t Mawa ayflcaaena try M OyoaM MM Moray by wwtrg «MV cowmen gem M tryrig muayae ceoamaacaaer mafteM My aoMtona tut r**attf rOaroty *rr******** ar* *•*(•«• M Uocamg evaatrw aaMcaaar* Ibu ataM <MM* Ma rata at #WM aM*caa«>w an* W* 4twy ar* gw* caMMata* IM Mw*»w

fbvM ACMMO# ^v-*-**** ®H# **Q£W*M*V M**(0**B T**X*V>W4

BtVanW	0	VaryH^X[1]	Vary lew	1 »M
	»	Ma«MB	LOW	0 000#
	to too	Matfrm	MaOMai	*• *1M
SSI eft#*				
•*w#	•44	Uadum	UMuai	>0 IMS
CURL	MO	Madura	MarMza	04440

Refer to the exhibit. An engineer is analyzing a Network Risk Report from Cisco FMC. Which application must the engineer take immediate action against to prevent unauthorized network use?

A. Kerberos
B. YouTube
C. Chrome
D. TOR

Answer: D

Explanation:

Question: 235

An engineer wants to perform a packet capture on the Cisco FTD to confirm that the host using IP address 192 168.100.100 has the MAC address of 0042 7734.103 to help troubleshoot a connectivity issue What is the correct tcpdump command syntax to ensure that the MAC address appears in the packet capture output?

A. -nm src 192.168.100.100
B. -ne src 192.168.100.100
D. -w capture.pcap -s 1518 host 192.168.100.100 mac
D. -w capture.pcap -s 1518 host 192.168.100.100 ether

Answer: B

Explanation:

Reference: https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/212474-working- with-firepower-threat-defense-f.html

Question: 236

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

A. The FTD is out of available resources lor use. so QoS cannot be added
B. The network segments that the interfaces are on do not have contiguous IP space
C. QoS is available only on routed interfaces, and this device is in transparent mode.
D. A conflict exists between the destination interface types that is preventing QoS from being added

Answer: C

Explanation:

Question: 237

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

A. Identity policy
B. Prefilter policy
C. Network Analysis policy
D. Intrusion policy

Answer: B

Explanation:

Question: 238

A network administrator is troubleshooting access to a website hosted behind a Cisco FTD device External clients cannot access the web server via HTTPS The IP address configured on the web server is 192 168 7.46 The administrator is running the command capture CAP interface outside match ip any 192.168.7.46 255.255.255.255 but cannot see any traffic in the capture Why is this occurring?

A. The capture must use the public IP address of the web server.
B. The FTD has no route to the web server.
C. The access policy is blocking the traffic.
D. The packet capture shows only blocked traffic

Answer: A

Explanation:

Question: 239

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

A. The hairpinning feature is not available on FTD.
B. Split tunneling is enabled for the Remote Access VPN on FTD
C. FTD has no NAT policy that allows outside to outside communication
D. The Enable Spoke to Spoke Connectivity through Hub option is not selected on FTD.

Answer: A

Explanation:

Question: 240

An engineer must configure the firewall to monitor traffic within a single subnet without increasing the hop count of

that traffic. How would the engineer achieve this?

A. Configure Cisco Firepower as a transparent firewall
B. Set up Cisco Firepower as managed by Cisco FDM
C. Configure Cisco Firepower in FXOS monitor only mode.
D. Set up Cisco Firepower in intrusion prevention mode

Answer: A

Explanation:

Question: 241

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

A. Enable Inspect Local Router Traffic
B. Enable Automatic Application Bypass
C. Configure Fastpath rules to bypass inspection
D. Add a Bypass Threshold policy for failures

Answer: B

Explanation:

Question: 242

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

A. An interface cannot belong to a security zone and an interface group
B. Interface groups can contain multiple interface types
C. Interface groups can contain interfaces from many devices.
D. Two security zones can contain the same interface

Answer: C

Explanation:

Question: 243

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

A. Specify the protocol to match (HTTP or HTTPS).
B. Use the FQDN including the subdomain for the website
C. Define the path to the individual webpage that uses HTTPS.
D. Use the subject common name from the website certificate

Answer: B

Explanation:

Question: 244

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

A. Add it as a separate widget.
B. Copy it to the current domain
C. Assign themselves ownership of it
D. Change the document attributes.

Answer: B

Explanation:

Question: 245

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

A. Add at least two container instances from the same module.
B. Set up a cluster control link between all logical devices
C. Add one shared management interface on all logical devices.
D. Define VLAN subinterfaces for each logical device.

Answer: C

Explanation:

Question: 246

An administrator is configuring a transparent Cisco FTD device to receive ERSPAN traffic from multiple switches on a passive port but the 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 FTD must be configured with an ERSPAN port, not a passive port.
C. The FTD must &e in routed mode to process ERSPAN traffic.
D. The switches were not set up with a monitor session ID (hat matches the flow ID defined on the FTD

Answer: C

Explanation:

Question: 247

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

A. ARP inspection is enabled by default.
B. Multicast and broadcast packets are denied by default.
C. STP BPDU packets are allowed by default.
D. ARP packets are allowed by default.

Answer: B

Explanation:

Question: 248

An organization is installing a new Cisco FTD appliance in the network. An engineer is tasked with configuring access between two network segments within the same IP subnet. Which step is needed to accomplish this task?

A. Assign an IP address to the Bridge Virtual Interface.
B. Permit BPDU packets to prevent loops.
C. Specify a name for the bridge group.
D. Add a separate bridge group for each segment.

Answer: A

Explanation:

Question: 249

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

A. Diagnostic
B. EtherChannel
C. BVI
D. Physical
E. Subinterface

Answer: AC

Explanation:

Question: 250

An administrator needs to configure Cisco FMC to send a notification email when a data transfer larger than 10 MB is initiated from an internal host outside of standard business hours. Which Cisco FMC feature must be configured to accomplish this task?

A. file and malware policy
B. application detector
C. intrusion policy
D. correlation policy

Answer: A

Explanation:

Question: 251

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

A. Reconfigure the Cisco FMC lo use the device's private IP address instead of the WAN address.
B. Configure a NAT ID on both the Cisco FMC and the device.
C. Add the port number being used for PAT on the router to the device's IP address in the Cisco FMC.
D. Reconfigure the Cisco FMC to use the device's hostname instead of IP address.
E. Remove the IP address defined for the device in the Cisco FMC.

Answer: BE

Explanation:

Question: 252

An engineer defines a new rule while configuring an Access Control Policy. After deploying the policy, the rule is not working as expected and the hit counters associated with the rule are showing zero.
What is causing this error?

A. Logging is not enabled for the rule.
B. The rule was not enabled after being created.
C. The wrong source interface for Snort was selected in the rule.
D. An incorrect application signature was used in the rule.

Answer: B

Explanation:

Question: 253

A network administrator is configuring a site-to-site IPsec VPN to a router sitting behind a Cisco FTD. The administrator has configured an access policy to allow traffic to this device on UDP 500, 4500, and ESP VPN traffic is not working. Which action resolves this issue?

A. Set the allow action in the access policy to trust.
B. Enable IPsec inspection on the access policy.
C. Modify the NAT policy to use the interface PAT.

D. Change the access policy to allow all ports.

Answer: B

Explanation:

Question: 254

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

A. IPsec
B. SSH
C. SSL
D. MACsec

Answer: A

Explanation:

Question: 255

An engineer is troubleshooting HTTP traffic to a web server using the packet capture tool on Cisco FMC. When reviewing the captures, the engineer notices that there are a lot of packets that are not sourced from or destined to the web server being captured. How can the engineer reduce the strain of capturing packets for irrelevant traffic on the Cisco FTD device?

A. Use the host filter in the packet capture to capture traffic to or from a specific host.
B. Redirect the packet capture output to a. pcap file that can be opened with Wireshark.
C. Use the -c option to restrict the packet capture to only the first 100 packets.
D. Use an access-list within the packet capture to permit only HTTP traffic to and from the web server.

Answer: A

Explanation:

Question: 256

A security engineer needs to configure a network discovery policy on a Cisco FMC appliance and prevent excessive network discovery events from overloading the FMC database? Which action must be taken to accomplish this task?

A. Change the network discovery method to TCP/SYN.
B. Configure NetFlow exporters for monitored networks.
C. Monitor only the default IPv4 and IPv6 network ranges.
D. Exclude load balancers and NAT devices in the policy.

Answer: D

Explanation:

Question: 257

An engineer is setting up a remote access VPN on a Cisco FTD device and wants to define which traffic gets sent over the VPN tunnel. Which named object type in Cisco FMC must be used to accomplish this task?

A. split tunnel
B. crypto map
C. access list
D. route map

Answer: A

Explanation:

Question: 258

Which process should be checked when troubleshooting registration issues between Cisco FMC and managed devices to verify that secure communication is occurring?

A. fpcollect
B. dhclient
C. sfmgr
D. sftunnel

Answer: D

Explanation:

Question: 259

An engineer needs to configure remote storage on Cisco FMC. Configuration backups must be

available from a secure location on the network for disaster recovery. Reports need to back up to a shared location that auditors can access with their Active Directory logins. Which strategy must the engineer use to meet these objectives?

A. Use SMB for backups and NFS for reports.
B. Use NFS for both backups and reports.
C. Use SMB for both backups and reports.
D. Use SSH for backups and NFS for reports.

Answer: C

Explanation:

https://www.cisco.com/c/en/us/td/docs/security/firepower/640/configuration/guide/fpmc-config- guide-v64/system_configuration.html#ID-2241-00000551

"You cannot send backups to one remote system and reports to another, but you can choose to send either to a remote system and store the other on the Firepower Management Center."

Question: 260

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

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

Answer: D

Explanation:

Transparent mode is a firewall configuration in which the firewall acts as a "bump in the wire" or a "stealth firewall" and is not seen as a router hop to connected devices. In transparent mode, the firewall can forward traffic at both layer 2 and layer 3 for the same subnet, as it does not perform any address translation or routing. The firewall inspects the traffic and applies security policies based on the source and destination IP addresses, ports, and protocols. Transparent mode is useful when you want to deploy a firewall without changing the existing network topology or addressing scheme1.

Question: 261

What is a limitation to consider when running a dynamic routing protocol on a Cisco FTD device in IRB mode?

A. Only link-stale routing protocols are supported.
B. Only distance vector routing protocols are supported.
C. Only EtherChannel interfaces are supposed.
D. Only nonbridge interfaces are supported.

Answer: D

Explanation:

Integrated routing and bridging (IRB) is a feature that allows you to route between different bridge groups on a Cisco FTD device. A bridge group is a logical interface that acts as a container for one or more physical or logical interfaces that belong to the same layer 2 broadcast domain. You can assign an IP address to a bridge group interface (BVI) and enable routing protocols on it, just like a regular routed interface. However, when you run a dynamic routing protocol on a Cisco FTD device in IRB mode, you can only use nonbridge interfaces as routing peers. You cannot use bridge group interfaces or bridge group member interfaces as routing peers2. This is because the routing protocol packets are sent and received on the nonbridge interfaces, and the bridge group interfaces are used only for forwarding data traffic3.

Question: 262

DRAG DROP

A network engineer is deploying a Cisco Firepower 4100 appliance and must configure a multiinstance environment for

high availability. Drag and drop me actions from the left into sequence on the right far this configuration.

Answer:

Explanation:

The correct sequence of actions for configuring a multi-instance environment for high availability on a Cisco Firepower 4100 appliance is as follows:

Add a resource profile for container instances. A resource profile defines the CPU, RAM, and disk space allocation for each container instance. You can create multiple resource profiles with different resource settings and assign them to different container instances1.

Add a MAC pool prefix and view the MAC address for the container instance interfaces. A MAC pool prefix is a 24-bit prefix that is used to generate MAC addresses for the container instance interfaces.

You can specify a custom MAC pool prefix or use the default one. You can also view the MAC addresses that are assigned to each container instance interface1.

Configure interfaces. You need to configure the physical interfaces, EtherChannels, and VLAN subinterfaces that will be used by the container instances. You can also configure shared interfaces that can be used by multiple container instances on the same security module/engine1.

Add a Standalone Firepower Threat Defense for Cisco Secure Firewall Management Center. You need to add a logical device that runs a standalone Firepower Threat Defense (FTD) application instance and register it with the Cisco Secure Firewall Management Center (FMC). This logical device will act as the management interface for the container instances1.

Add a high-availability pair. You need to add another logical device that runs a standalone FTD application instance and register it with the FMC as well. Then, you need to configure high availability (HA) between the two standalone FTD logical devices. This will enable HA for the container instances that are associated with them1.

Question: 263

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

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

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

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

D. Configure an access control rule that matches the Adult URL category and se: the action to interactive Block.

E. Configure an access control rule that matches an URL object for http://www.badaduitslte.com; and set the action to interactive Block.

Answer: BE

Explanation:

To configure URL filtering for a Cisco FTD device in Cisco FMC, and to meet the requirements of the question, the engineer must do the following:

On the HTTP Responses tab of the access control policy editor, set the Interactive Block Response Page to system-provided. This will enable the system to display a warning page to the users when they try to access a blocked URL, and give them the option to continue or cancel. The system- provided page is a default page that contains a generic message and a logo1.

Configure an access control rule that matches an URL object for http://www.badadultsite.com; and set the action to Interactive Block. This will apply the interactive block action to the specific URL that is defined in the URL object. The interactive block action will trigger the interactive block response page that was configured in the previous step1.

The other options are incorrect because:

On the HTTP Responses tab of the access control policy editor, setting the Block Response Page to Custom will not affect the interactive block action. The block response page is used when the action is set to Block, not Interactive Block1.

Configuring the default action for the access control policy to Interactive Block will apply the interactive block action to all URLs that are not matched by any access control rule. This will not meet the requirement of blocking no other websites1.

Configuring an access control rule that matches the Adult URL category and sets the action to Interactive Block will apply the interactive block action to all URLs that belong to the Adult category. This will not meet the requirement of blocking only http://www.badadultsite.com1.

Question: 264

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

Answer: A

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: 265

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

Answer: C

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 generalpurpose programming language that is not embedded in the Firepower System.

Question: 266

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.

Answer: B

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 commandline 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 firewallengine-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.

Question: 267

A security engineer must configure policies tor a recently deployed Cisco FTD. The security policy for the company dictates that when five or more connections from external sources are initiated within 2 minutes, there is cause for concern. Which type of policy must be configured in Cisco FMC \z
generate an alert when this condition is triggered?

A. application detector
B. access control
C. intrusion
D. correlation

Answer: D

Explanation:

A correlation policy is a feature that allows you to respond in real time to threats or specific conditions on your network, using correlation rules. A correlation rule can trigger when the system generates a specific type of event, or when your network traffic deviates from its normal profile1. When a correlation rule triggers, the system generates a correlation event and can also launch a response, such as sending an alert, blocking an IP address, or scanning a host1.

In this case, the security engineer can configure a correlation rule that triggers when the system detects five or more connections from external sources within 2 minutes. The engineer can also configure a response that sends an alert to the FMC or an email recipient when this condition is triggered. The engineer can then create a correlation policy that includes this rule and activate it on the FTD device1.

The other options are incorrect because:

An application detector is a feature that allows you to detect web applications, clients, and application protocols based on patterns in network traffic. An application detector does not generate alerts based on the number of connections from external sources2.

An access control policy is a feature that allows you to control traffic flow through your network and inspect traffic for intrusions, malware, and files. An access control policy does not generate alerts based on the number of connections from external sources3.

An intrusion policy is a feature that allows you to detect and prevent malicious network activity using Snort rules. An intrusion policy does not generate alerts based on the number of connections from external sources4.

Question: 268

Which default action setting in a Cisco FTD Access Control Policy allows all traffic from an undefined application to pass without Snort Inspection?

A. Trust All Traffic
B. Inherit from Base Policy
C. Network Discovery Only
D. Intrusion Prevention

Answer: A

Explanation:

The default action setting in a Cisco FTD Access Control Policy determines how the system handles and logs traffic that is not handled by any other access control configuration. The default action can block or trust all traffic without further inspection, or inspect traffic for intrusions and discovery data3.

The Trust All Traffic option allows all traffic from an undefined application to pass without Snort inspection. This option also disables Security Intelligence filtering, file and malware inspection, and URL filtering for all traffic handled by the default action. This option is useful when you want to minimize the performance impact of access control on your network3.

The other options are incorrect because:

The Inherit from Base Policy option inherits the default action setting from the base policy. The base policy is the predefined access control policy that you use as a starting point for creating your own policies. Depending on which base policy you choose, the inherited default action setting can be different3.

The Network Discovery Only option inspects all traffic for discovery data only. This option enables Security Intelligence filtering for all traffic handled by the default action, but disables file and malware inspection, URL filtering, and intrusion inspection. This option is useful when you want to collect information about your network before you configure access control rules3.

The Intrusion Prevention option inspects all traffic for intrusions and discovery data. This option enables Security Intelligence filtering, file and malware inspection, URL filtering, and intrusion inspection for all traffic handled by the default action. This option provides the most comprehensive protection for your network, but also has the most performance impact3.

Question: 269

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

A. FMC CLI
B. FTD CLI
C. FXOS CLI
D. FMC GUI

Answer: C

Explanation:

An EtherChannel interface is a logical interface that consists of a bundle of individual Ethernet links that act as a single network link. An EtherChannel interface can increase the bandwidth and reliability of a network connection5.

On a Cisco Firepower 9300 appliance registered with an FMC for high availability, the network administrator must create the EtherChannel interface on the FXOS CLI. The FXOS is the operating system that runs on the Firepower 9300 chassis and provides hardware management functions such as interface configuration, power supply status, fan speed control, and so on6.

To create an EtherChannel interface on the FXOS CLI, the network administrator can follow these steps5:

Connect to the FXOS CLI using SSH or console.

Enter scope eth-uplink command to enter Ethernet uplink mode.

Enter create port-channel command to create an EtherChannel interface.

Enter a port-channel ID (1-48) and a mode (on or active) for the EtherChannel interface.

Enter add interface command to add physical interfaces to the EtherChannel interface.

Enter one or more interface IDs (for example, 1/1) for the physical interfaces.

Enter commit-buffer command to save the changes.

The other options are incorrect because:

The FMC CLI does not provide any commands to create an EtherChannel interface on a Firepower 9300 appliance. The FMC CLI is mainly used for managing FMC settings such as backup, restore, upgrade, troubleshoot, and so on7.

The FTD CLI does not provide any commands to create an EtherChannel interface on a Firepower 9300 appliance. The FTD CLI is mainly used for managing FTD settings such as routing, NAT, VPN, access control, and so on8.

The FMC GUI does not provide any options to create an EtherChannel interface on a Firepower 9300 appliance. The FMC GUI is mainly used for managing FTD policies such as access control, intrusion, file, malware, and so on9.

Question: 270

An engineer Is configuring a Cisco FTD device to place on the Finance VLAN to provide additional protection tor company financial dat

a. The device must be deployed without requiring any changes on the end user workstations, which currently use DHCP lo obtain an IP address. How must the engineer deploy the device to meet this requirement?

A. Deploy the device in routed mode and allow DHCP traffic in the access control policies.

B. Deploy the device in routed made aid enable the DHCP Relay feature.

C. Deploy the device in transparent mode and allow DHCP traffic in the access control policies

D. Deploy the device in transparent mode and enable the DHCP Server feature.

Answer: C

Explanation:

Transparent mode allows the FTD device to act as a “bump in the wire” that does not affect the IP addressing of the network. The end user workstations will not need any changes to their configuration, as they will still receive an IP address from the same DHCP server. However, the FTD device must allow DHCP traffic in the access control policies, otherwise it will block the DHCP requests and replies1

Question: 271

A consultant Is working on a project where the customer is upgrading from a single Cisco Firepower 2130 managed by FDM to a pair of Cisco Firepower 2130s managed oy FMC tor nigh availability. The customer wants the configures of the existing device being managed by FDM to be carried over to FMC and then replicated to the additional: device being added to create the high availability pair. Which action must the consultant take to meet this requirement?

A. The current FDM configuration must be configured by hand into FMC before the devices are registered.

B. The current FDM configuration will be converted automatically into FMC when the device registers.

C. The current FDM configuration must be migrated to FMC using the Secure Firewall Migration Tool. D. The FTD configuration must be converted to ASA command format, which can then be migrated to FMC.

Answer: B

Explanation:

When an FTD device that is managed by FDM is registered to FMC, the existing configuration is automatically converted and imported into FMC. The FMC then pushes the configuration back to the device. This process preserves most of the FDM configuration, except for some features that are not supported by FMC, such as VPN wizards and certificates.

Question: 272

An engineer plans to reconfigure an existing Cisco FTD from transparent mode to routed mode. Which additional action must be taken to maintain communication Between me two network segments?

A. Configure a NAT rule so mat traffic between the segments is exempt from NAT.
B. Update the IP addressing so that each segment is a unique IP subnet.
C. Deploy inbound ACLs on each interface to allow traffic between the segments.
D. Assign a unique VLAN ID for the interface in each segment.

Answer: B

Explanation:

When reconfiguring an existing Cisco FTD from transparent mode to routed mode, an additional action that must be taken to maintain communication between the two network segments is to update the IP addressing so that each segment is a unique IP subnet. This is because in routed mode, the FTD device acts as a router hop in the network and requires each interface to be on a different subnet. In transparent mode, the FTD device acts as a layer 2 firewall and does not require different subnets for each interface1.

The other options are incorrect because:

Configuring a NAT rule so that traffic between the segments is exempt from NAT is not necessary to maintain communication between the two network segments. NAT is used to translate IP addresses between different networks, but it does not affect the routing of packets. Moreover, NAT is optional in routed mode and can be disabled if not needed2.

Deploying inbound ACLs on each interface to allow traffic between the segments is not required to maintain communication between the two network segments. ACLs are used to control access to network resources based on source and destination addresses, protocols, and ports. They do not affect the routing of packets. Furthermore, ACLs are optional in routed mode and can be configured as needed3.

Assigning a unique VLAN ID for the interface in each segment is not relevant to maintain communication between the two network segments. VLANs are used to create logical groups of hosts that share the same broadcast domain, regardless of their physical location or connection. They do not affect the routing of packets. Besides, VLANs are not supported in routed mode and can only be used in transparent mode4.

Question: 273

A network administrator reviews me attack risk report and notices several Low-Impact attacks. What does this type of attack indicate?

A. All attacks are listed as low until manually categorized.
B. The host is not vulnerable to those attacks.
C. The attacks are not dangerous to the network.
D. The host is not within the administrator's environment.

Answer: B

Explanation:

A low-impact attack indicates that the host is not vulnerable to those attacks. A low-impact attack is an attack that does not exploit any known vulnerability on the target host or does not match any signature or anomaly rule on the FTD device5. A low-impact attack does not mean that the attack is not dangerous to the network or that the host is not within the administrator's environment. It simply means that the attack did not succeed in compromising or affecting the host.

The other options are incorrect because:

All attacks are not listed as low until manually categorized. The FTD device automatically assigns an impact level to each attack based on various factors, such as vulnerability information, threat score, and confidence rating5. The impact level can be high, medium, or low, depending on how likely and how severe the attack is.

The attacks are not necessarily harmless to the network. A low-impact attack may still cause some damage or disruption to the network, such as consuming bandwidth, generating noise, or distracting attention from other attacks6. A low-impact attack may also indicate that the attacker is probing or scanning the network for potential vulnerabilities or weaknesses7.

The host is not necessarily outside the administrator's environment. A low-impact attack can target any host on the network, regardless of its location or ownership. A low-impact attack does not imply that the host is external or irrelevant to the administrator's environment.

Question: 274

When an engineer captures traffic on a Cisco FTD to troubleshoot a connectivity problem, they receive a large amount of output data in the GUI tool. The engineer found that viewing the Captures this way is time-consuming and difficult lo son and filter. Which file type must the engineer export the data in so that it can be reviewed using a tool built for this type of analysis?

A. NetFlow v9

B. PCAP

C. NetFlow v5

D. IPFIX

Answer: B

Explanation:

When capturing traffic on a Cisco FTD device to troubleshoot a connectivity problem, a file type that can be exported for reviewing using a tool built for this type of analysis is PCAP. PCAP stands for Packet Capture and it is a file format used to store network packet data captured from a network interface8. PCAP files contain the raw data of network packets, including the headers and payloads of each packet8.

PCAP files are widely used in network analysis and troubleshooting tasks. They enable network administrators, analysts, and researchers to inspect and analyze network traffic for various purposes, such as diagnosing network issues, detecting malicious activity, measuring network performance, and understanding network protocols8. PCAP files can be read by applications that understand that format, such as Wireshark, tcpdump, CA NetMaster, or Microsoft Network Monitor8.

The other options are incorrect because:

NetFlow v9 is not a file type, but a protocol for collecting and exporting information about network flows. A network flow is a sequence of packets that share common attributes such as source and destination IP addresses, ports, and protocols9. NetFlow v9 records contain summary information about network flows, such as start and end times, byte

counts, packet counts, and so on9. NetFlow v9 records do not contain the raw data of network packets.

NetFlow v5 is not a file type, but an earlier version of the NetFlow protocol for collecting and exporting information about network flows. NetFlow v5 records contain similar information as NetFlow v9 records, but with fewer fields and less flexibility10. NetFlow v5 records do not contain the raw data of network packets.

IPFIX is not a file type, but a protocol for collecting and exporting information about network flows. IPFIX stands for IP Flow Information Export and it is based on NetFlow v9, but with some extensions and improvements11. IPFIX records contain similar information as NetFlow v9 records, but with more fields and more flexibility11. IPFIX records do not contain the raw data of network packets.

Question: 275

Network users are experiencing Intermittent issues with internet access. An engineer ident med mat the issue Is being caused by NAT exhaustion. How must the engineer change the dynamic NAT configuration to provide internet access for more users without running out of resources?

A. Define an additional static NAT for the network object in use.
B. Configure fallthrough to interface PAT on 'he Advanced tab.
C. Convert the dynamic auto NAT rule to dynamic manual NAT.
D. Add an identity NAT rule to handle the overflow of users.

Answer: B

Explanation:

Fallthrough to interface PAT is a feature that allows the dynamic NAT configuration to use the interface IP address as a last resort when the NAT pool is exhausted. This way, more users can access the internet without running out of resources. To enable this feature, the engineer must check the Enable PAT Fallback check box on the Advanced tab of the NAT rule editor1

Question: 276

An engineer is configuring a custom intrusion rule on Cisco FMC. The engineer needs the rule to search the payload or stream for the string "|45 5* 26 27 4 0A|*. Which Keyword must the engineer

use with this stung lo create an argument for packed inspection?

A. metadata
B. Content
C. Protected _ content
D. data

Answer: B

Explanation:

The content keyword is used to specify a string or pattern to search for in the payload or stream of a packet. The string must be enclosed in quotation marks and can use modifiers such as nocase, depth, offset, and so on. The string can also use hexadecimal notation by using a pipe symbol (|) before and after the hexadecimal characters. For example, content:"|45 5* 26 27 4 0A|" will match any payload or stream that contains the hexadecimal bytes 45 5 26 27 4 0A followed by any number of bytes2

www.atmicnetworks.com

Question: 277

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

A. Analysis > Lookup > Whols
B. Analysis > Correlation > Correlation Events
C. Analysis > Hosts > Vulnerabilities
D. Analysis > Hosts > Host Attributes

Answer: C

Explanation:

The Analysis > Hosts > Vulnerabilities page in Cisco FMC displays information about the hosts on the network and their associated vulnerabilities. The administrator can filter the hosts by impact level, which indicates how likely an attack is to succeed against a host. An impact level of 2 means that the host was attacked and is potentially vulnerable, but no exploit was confirmed. The administrator can click on a host to view more details, such as its IP address, operating system, applications, protocols, and intrusion events. The administrator can also view the details of each vulnerability, such as its CVE ID, description, severity, and recommended actions3

Question: 278

An engineer must deploy a Cisco FTD device. Management wants to examine traffic without requiring network changes that will disrupt end users. Corporate security policy requires the separation of management traffic from data traffic and the use of SSH over Telnet for remote administration. How must the device be deployed to meet these requirements?

A. in routed mode with a diagnostic interface
B. in transparent mode with a management Interface

C. in transparent made with a data interface
D. in routed mode with a bridge virtual interface

Answer: B

Explanation:

To deploy a Cisco FTD device that meets the requirements of the question, the engineer must use transparent mode with a management interface. Transparent mode is a firewall configuration in which the FTD device acts as a "bump in the wire" or a "stealth firewall" and is not seen as a router hop to connected devices. In transparent mode, the FTD device can examine traffic without requiring network changes that will disrupt end users, such as changing IP addresses or routing configurations1. A management interface is a dedicated interface that is used for managing the FTD device and separating management traffic from data traffic. A management interface can be configured to allow SSH access for remote administration, which is more secure than Telnet2.

The other options are incorrect because:

Routed mode is a firewall configuration in which the FTD device acts as a router and performs address translation and routing for connected networks. Routed mode requires network changes that may disrupt end users, such as changing IP addresses or routing configurations1. A diagnostic interface is a special interface that is used for troubleshooting and capturing traffic on the FTD device. A diagnostic interface does not separate management traffic from data traffic or

allow SSH access for remote administration.

Transparent mode with a data interface does not meet the requirement of separating management traffic from data traffic. A data interface is a regular interface that is used for passing and inspecting traffic on the FTD device. A data interface does not allow SSH access for remote administration2. Routed mode with a bridge virtual interface (BVI) does not meet the requirement of examining traffic without requiring network changes that will disrupt end users. A BVI is a logical interface that acts as a container for one or more physical or logical interfaces that belong to the same layer 2 broadcast domain. A BVI allows the FTD device to route between different bridge groups on the same security module/engine. However, routed mode still requires network changes that may disrupt end users, such as changing IP addresses or routing configurations.

Question: 279

A network administrator is trying to configure Active Directory authentication for VPN authentication to a Cisco Secure Firewall Threat Defence instance that is registered with Cisco Secure Firewall Management Center. Which system settings must be configured first in Secure Firewall Management Center to accomplish the goal?

A. Device, Remote Access VPN
B. System, Realms
C. Policies, Authentication
D. Authentication, Device

Answer: B

Explanation:

To configure Active Directory authentication for VPN authentication on a Cisco Secure Firewall Threat Defense (FTD) instance registered with Cisco Secure Firewall Management Center (FMC), the administrator needs to configure Realms in the System settings of the FMC. Realms in FMC are used to define the directory servers (e.g., Active Directory) and how they are used for user authentication. Steps to configure this in FMC:

Navigate to System > Integration > Realms and Directory.

Add a new realm and configure the necessary details such as the directory server type (e.g., Active Directory), server address, and bind credentials.

Test the connection to ensure it works correctly.

This setup allows the FMC to authenticate VPN users against the Active Directory, thereby enabling secure access control for VPN connections.

Reference: Cisco Secure Firewall Management Center Administrator Guide, Chapter on Realms Configuration.

Question: 280

A network administrator is trying to configure an access rule to allow access to a specific banking site over HTTPS. Which method must the administrator use to meet the requirement?

A. Enable SSL decryption and specify the URL.
B. Define the URL to be blocked and set the application to HTTP.
C. Define the URL to be blocked and disable SSL inspection.
D. Block the category of banking and define the application of WWW.

Answer: A

Explanation:

To allow access to a specific banking site over HTTPS, the network administrator must use SSL decryption (also known as SSL/TLS inspection) and specify the URL. This is because HTTPS traffic is encrypted, and the firewall needs to decrypt the traffic to inspect the URL and enforce the access rule.

Steps:

Enable SSL Decryption: Configure SSL policies to decrypt the HTTPS traffic.

Specify the URL: Define the URL of the banking site in the access control policy, ensuring that the decrypted traffic is inspected and allowed based on the specified URL.

This method ensures that only the desired banking site is accessed over HTTPS, while other HTTPS traffic can be filtered or blocked according to the organization's security policies.

Reference: Cisco Secure Firewall Management Center Configuration Guide, Chapter on SSL Decryption.

Question: 281

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.

Answer: C

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. Reference: Cisco Secure Firewall Management Center and Cisco Secure Endpoint Integration Guide.

Question: 282

A software development company hosts the website http:dev.company.com for contractors to share code for projects they are working on with internal developers. The web server is on premises and is protected by a Cisco Secure Firewall

Threat Defense appliance. The network administrator is worried about someone trying to transmit infected files to internal users via this site. Which type of policy must be able associated with an access control policy to enable Cisco Secure Firewall Malware Defense to detect and block malware?

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

Answer: C

Explanation:

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.
Reference: Cisco Secure Firewall Management Center Administrator Guide, Chapter on File Policies.

Question: 283

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.

Answer: B

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.

Reference: Cisco Secure Firewall Management Center Device Configuration Guide, Chapter on Routed Mode Configuration.

Question: 284

Which file format can standard reports from Cisco Secure Firewall Management Center be downloaded in?

A. ppt
B. csv
C. xis
D. doc

Answer: B

Explanation:

Standard reports from Cisco Secure Firewall Management Center can be downloaded in CSV (Comma-Separated Values) format. This format is widely used for data exchange and can be opened in various applications such as Microsoft Excel.

Steps to download reports:

Navigate to Reports > Report Designer in the FMC.

Select or create the report you wish to download.

Choose the CSV format option when exporting the report.

This allows the network engineer to analyze and manipulate the report data easily.

Reference: Cisco Secure Firewall Management Center Administrator Guide, Chapter on Report Generation.

Question: 285

An engineer is configuring a Cisco Secure Firewall Threat Defence device managed by Cisco Secure Firewall Management Centre. The device must have SSH enabled and the accessible from the inside interface for remote administration. Which type of policy must the engineer configure to accomplish this?

A. Identify
B. Access control
C. Prefilter
D. Platform settings

Answer: D

Explanation:

To enable SSH access to a Cisco Secure Firewall Threat Defense (FTD) device from the inside interface for remote administration, the engineer needs to configure a Platform Settings policy in Cisco Secure Firewall Management Center (FMC). The Platform Settings policy allows the configuration of various system-related settings, including enabling SSH,

specifying the allowed interfaces, and defining the SSH access parameters.

Steps:

In FMC, navigate to Policies > Access Control > Platform Settings.

Create a new Platform Settings policy or edit an existing one.

In the policy settings, go to the SSH section.

Enable SSH and specify the inside interface as the allowed interface for SSH access.

Define the SSH parameters such as allowed IP addresses, user credentials, and other security settings.

Save and deploy the policy to the FTD device.

This configuration ensures that SSH access is enabled on the specified interface, allowing secure remote administration.

Reference: Cisco Secure Firewall Management Center Administrator Guide, Chapter on Platform Settings.

Question: 286

Which component simplifies incident investigation with Cisco Threat Response?

A. Cisco AMP client
B. local CVE database
C. Cisco Secure Firewall appliance
D. browser plug-in

Answer: D

Explanation:

Cisco Threat Response (CTR) is a security solution that helps simplify incident investigation and threat hunting. One of its components that significantly simplifies the investigation process is the browser plug-in. The browser plug-in integrates with CTR to provide contextual information directly within the browser, allowing security analysts to quickly view threat details, pivot to related information, and take appropriate actions without switching between multiple tools.

Features of the browser plug-in:

Provides real-time threat intelligence and context from various Cisco security products.

Allows security analysts to investigate incidents directly from web-based consoles.

Enhances efficiency by streamlining the workflow and reducing the time needed to gather and correlate information.

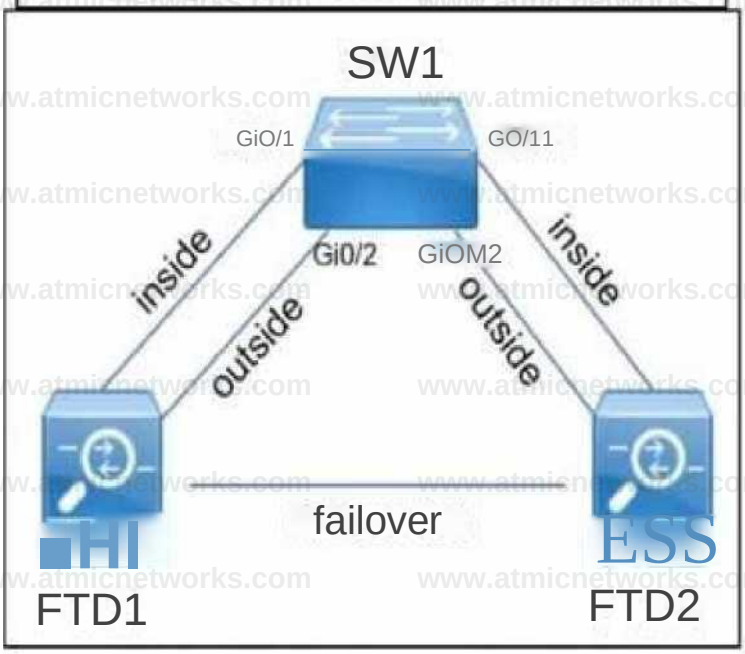
Reference: Cisco Threat Response Documentation, Browser Plug-in Section.

Question: 287

Refer to the exhibit.

tr r1 and - GiC/11 configuratica:
syitchpOxt EC-1* «CCeS3 access vl<c 10
switchport port-security pzrt - recur it y
switchport saxiansr. 1 per: recur icy
switchptrt violation
5witcr.pt re shutdown

3ij 1/and GiC/12 configuEatisn: switzr.pt rt nice access switzhpcrt access vlwj 2' switchport port-security suitcftport port-security saxirtun 1 switchport pert-security violation shutdown



A company is deploying a pair of Cisco Secure Firewall Threat defence devices named FTD1 and FTD2. FTD1 and FTD2 have been configured as an active/standby pair with a failover link but without a stateful link. What must be implemented next to ensure that users on the internal network still communicate with outside devices if FTD1 fails?

A. Disable port security on the switch interfaces connected to FTD1 and FTD2.
B. Set maximum secured addresses to two on the switch interfaces on FTD1 and FTD2.
C. Connect and configure a stateful link and thon deploy the changes.
D. Configure the spanning-tree PortFasl feature on SW1 and FTD2

Answer: C

Explanation:

In a failover configuration with Cisco Secure Firewall Threat Defense (FTD) devices, ensuring that users on the internal network can continue to communicate with outside devices if the primary device (FTD1) fails requires the implementation of a stateful failover link. The stateful failover link allows the secondary device (FTD2) to maintain session information and state data, ensuring seamless failover and minimizing disruptions.

Steps to implement a stateful failover link:

Physically connect a stateful failover link between FTD1 and FTD2.

Configure the stateful failover link in the FMC.

Ensure that both devices are properly synchronized and that stateful failover is enabled.

Deploy the changes to both FTD devices.

By configuring a stateful link, the secondary FTD can take over active sessions without requiring users to re-establish their connections, thus ensuring continuous communication.

Reference: Cisco Secure Firewall Threat Defense Configuration Guide, Chapter on Failover Configuration.

Question: 288

A network engineer must configure IPS mode on a Cisco Secure firewall Threat Defense device to inspect traffic and act as an IDS. The engineer already configured the passive-interface on the secure firewall threat Defence device and SPAN on the switch. What must be configured next by the engineer?

A. intrusion policy on the Secure Firewall Threat Defense device
B. active Interface on me Secure Firewall threat Defense device
C. DHCP on the switch
D. active SPAN port on the switch

Answer: A

Explanation:

To configure IPS mode on a Cisco Secure Firewall Threat Defense (FTD) device to inspect traffic and act as an IDS, the network engineer must configure an intrusion policy on the FTD device. The passive-interface and SPAN on the switch have already been configured, which means the traffic is being mirrored to the FTD. The next step is to set up an intrusion policy that defines the rules and actions for detecting and responding to malicious traffic.

Steps:

In FMC, navigate to Policies > Intrusion.

Create a new intrusion policy or edit an existing one.

Define the rules and actions for detecting threats.

Apply the intrusion policy to the relevant interfaces or access control policies.

This configuration enables the FTD to inspect the mirrored traffic and take appropriate actions based on the defined intrusion policy.

Reference: Cisco Secure Firewall Management Center Administrator Guide, Chapter on Intrusion Policies.

Question: 289

An administrator is attempting to add a Cisco Secure Firewall Threat Defence device to Cisco Secure Firewall Management Center with a password of Cisco0480846211 480846211. The private IP address of the FMC server is 192.168.75.201. Which command must be used in order to accomplish this task?

A. configure manager add 192.168.75.201/24 <reg_key>
B. configure manager add 192.16875.201 <reg_key>
C. configure manager add 192.168.45.45 <reg_key> <nal-ld>
D. configure manager add 192.168.75.201 255.255.255.0 <reg_key>

Answer: B

Explanation:

To add a Cisco Secure Firewall Threat Defense (FTD) device to Cisco Secure Firewall Management Center (FMC), the correct command to use is configure manager add 192.168.75.201 <reg_key>. This command registers the FTD device

with the FMC using the FMC's IP address and the registration key provided during the FMC setup.

Command structure:

configure manager add <FMC_IP> <reg_key>

For the given scenario:

FMC IP address: 192.168.75.201

Registration key: provided during FMC setup

Thus, the correct command is:

configure manager add 192.168.75.201 <reg_key>

Reference: Cisco Secure Firewall Management Center Device Configuration Guide, Chapter on Device Registration.

Question: 290

A cisco Secure firewall Threat Defence device is configured in inline IPS mode to inspect all traffic that passes through the interfaces in the inline set. Which setting in the inline set configuration must be connected to allow traffic to pass through uninterrupted when VDB updates are being applied?

A. Propagate Link State
B. Short Fall Open
C. Strict TCP Enforcement
D. Tap Mode

Answer: B

Explanation:

In inline IPS mode, to ensure that traffic passes through uninterrupted when VDB (Vulnerability Database) updates are being applied, the "Short Fall Open" setting must be configured. This setting allows traffic to continue to flow through the firewall even if there are issues with the inspection process, such as during updates or if the inspection engine fails.

Steps:

In FMC, navigate to the inline set configuration.

Enable the "Short Fall Open" option.

Deploy the configuration to the FTD device.

This ensures that network traffic is not disrupted during updates or other issues with the inspection process.

Reference: Cisco Secure Firewall Threat Defense Configuration Guide, Chapter on Inline IPS Mode Configuration.

Question: 291

When packet capture is used on a Cisco Secure Firewall Threat Defense device and the packet flow is wailing on the malware query, which Snort verdict appears?

A. retry
B. replace
C. block
D. blocfcflow

Answer: A

Explanation:

When packet capture is used on a Cisco Secure Firewall Threat Defense (FTD) device and the packet flow is waiting on the malware query, the Snort verdict appears as "retry." This indicates that the device is still processing the malware analysis and has not yet determined the final action for the packet.

The "retry" verdict signifies that the packet is in a holding state while awaiting the result of the malware inspection, which helps in maintaining the security posture until a definitive decision is made.

Reference: Cisco Secure Firewall Management Center Administrator Guide, Chapter on Packet Capture and Malware Inspection.

Question: 292

An engineer is configuring URL filtering tor a Cisco Secure Firewall Threat Defense device in Cisco Secure Firewall Management Centre. Use's must receive a warning when they access ..wwww badaduitsito com with the option of continuing to the website if they choose to No other websites should he blocked. Which two actions must the engineer take to moot these requirements?

A. Configure an access control rule that matches an URL object for http://www.Dadadullsile.com' and set the action to Interactive Block.

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

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

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

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

Answer: AB

Explanation:

To configure URL filtering such that users receive a warning when they access a specific website (e.g., http://www.badadultsite.com) and have the option to continue to the site, the engineer needs to perform the following actions:

Configure an access control rule:

Create a URL object for http://www.badadultsite.com.

Set the action for this URL object to "Interactive Block," which prompts the user with a warning and allows them to proceed if they choose to.

Set the Interactive Block Response Page:

Navigate to the HTTP Responses tab in the access control policy editor.

Set the Interactive Block Response Page to "System-provided" to ensure that users see the default warning page provided by Cisco Secure Firewall Management Center.

These actions ensure that only the specified website triggers an interactive block, while other websites are not blocked.

Reference: Cisco Secure Firewall Management Center Administrator Guide, Chapter on Access Control and URL Filtering.

Question: 293

Encrypted Visibility Engine (EVE) is enabled under which lab on an access control policy in Cisco Secure Firewall Management Centre?

A. Network Analysis Policy
B. Advanced
C. Security Intelligence
D. SSL

Answer: D

Explanation:

The Encrypted Visibility Engine (EVE) in Cisco Secure Firewall Management Center is enabled under the SSL tab of an access control policy. EVE provides visibility into encrypted traffic, allowing the firewall to detect threats even when traffic is encrypted.

Steps to enable EVE:

Navigate to the access control policy in FMC.

Go to the SSL tab.

Enable Encrypted Visibility Engine (EVE) to analyze encrypted traffic.

This configuration helps in identifying and mitigating threats within encrypted traffic without the need for full decryption.

Reference: Cisco Secure Firewall Management Center Configuration Guide, Chapter on SSL and Encrypted Traffic Visibility.

Question: 294

A company is deploying Cisco Secure Endpoint private cloud. The Secure Endpoint private cloud instance has already been deployed by the server administrator. The server administrator provided the hostname of the private cloud instance to the network engineer via email. What additional information does the network engineer require from the server administrator to be able to make the connection to Secure Endpoint private cloud in Cisco Secure Firewall Management Centre?

A. SSL certificate for the Secure Endpoint ornate cloud instance
B. Internet access for the Secure End point private cloud to reach the Secure Endpoint public cloud
C. Username and password to the Secure Endpoint private cloud instance
D. IP address and port number for the connection proxy

Answer: A

Explanation:

To connect to a Secure Endpoint private cloud instance from Cisco Secure Firewall Management Center (FMC), the network engineer requires the SSL certificate for the Secure Endpoint private cloud instance. This SSL certificate is necessary to establish a secure, trusted connection between the FMC and the private cloud instance.

Steps:

Obtain the SSL certificate from the server administrator.

Import the SSL certificate into the FMC.

Configure the connection to the Secure Endpoint private cloud instance using the provided hostname and SSL certificate.

This ensures a secure and authenticated connection to the private cloud instance.

Reference: Cisco Secure Firewall Management Center Integration Guide, Chapter on Secure Endpoint Integration.

Question: 295

Network users experience issues when accessing a server on a different network segment. An engineer investigates the issue by performing packet capture on Cisco Secure Firewall Threat Defense. The engineer expects more data and suspects that not all the traffic was collected during a 15-minute can't captured session. Which action must the engineer take to resolve the issue?

A. Forward the captured data lo an FTP server
B. Increase the amount of RAM allocated for the capture.
C. Provide a file name to save the data.
D. Ensure that the allocated memory is sufficient.

Answer: D

Explanation:

When performing packet capture on a Cisco Secure Firewall Threat Defense (FTD) device, ensuring that the allocated memory is sufficient is crucial for capturing all necessary traffic during a specified capture session. If users experience issues accessing a server and the engineer suspects not all traffic was collected, it indicates that the current memory allocation might not be enough to store the entire capture data for the 15-minute session.

Steps:

Check the current memory allocation for packet captures on the FTD device.

Increase the memory allocation if it is insufficient to handle the volume of traffic expected during the capture session.

This ensures that all relevant traffic is captured and can be analyzed to diagnose and resolve the network issue.

Reference: Cisco Secure Firewall Threat Defense Configuration Guide, Chapter on Packet Capture.

Question: 296

Users report that Cisco Duo 2FA fails when they attempt to connect to the VPN on a Cisco Secure Firewall Threat Defense (FTD) device IT staff have VPN profiles that do not require multifactor authentication and they can connect to the VPN without any issues When viewing the VPN troubleshooting log in Cisco Secure Firewall Management Centre (FMC), the network administrator sees an error in the Cisco Duo AAA server has been marked as tailed. What is the root cause of the Issue?

A. Multifactor authentication Is not supported on Secure FMC managed devices.
B. Duo trust certificates are missing from the Secure FTD device.
C. The internal AD server is unreachable from the Secure FTD device.
D. AD Trust certificates are missing from the Secure FTD device.

Answer: B

Explanation:

If users report that Cisco Duo 2FA fails when attempting to connect to the VPN on a Cisco Secure Firewall Threat Defense (FTD) device, and the VPN troubleshooting log in FMC shows an error indicating that the Cisco Duo AAA server has been marked as failed, the root cause is likely missing Duo trust certificates on the FTD device. Trust certificates are essential for establishing a secure and trusted connection between the FTD and the Duo authentication service.

Steps:

Obtain the necessary Duo trust certificates.

Install the certificates on the FTD device.

Verify the configuration to ensure that the FTD device can properly communicate with the Duo AAA server.

This resolves the authentication failure by ensuring that the FTD device can trust the Duo server. Reference: Cisco Secure Firewall Management Center Administrator Guide, Chapter on Certificate Management.

Question: 297

An engineer must change the mode of a Cisco Secure Firewall Threat Defense (FTD) firewall in the Cisco Secure Firewall Management Center (FMC) inventory. The engineer must take these actions: • Register Secure FTD with Secure FMC.

- Change the firewall mode.
- Deregister the Secure FTD device from Secure FMC.

How must the engineer take FTD take the actions?

A. Reload the Secure FTD device.
B. Configure the management IP address.
C. Access the Secure FTD CLI from the console port.
D. Erase the Secure FTD configuration

Answer: C

Explanation:
To change the mode of a Cisco Secure Firewall Threat Defense (FTD) device in the Cisco Secure Firewall Management Center (FMC) inventory, the engineer must follow these steps: Register the Secure FTD with Secure FMC.

Change the firewall mode.

Deregister the Secure FTD device from Secure FMC.

To perform these actions, accessing the Secure FTD CLI from the console port is necessary. This allows the engineer to execute the required commands to change the firewall mode and manage the registration status of the FTD device.

Steps:

Connect to the Secure FTD device via the console port.

Access the CLI and execute the command to change the firewall mode (configure firewall-mode).

Deregister the device from FMC if needed.

Register or re-register the device with FMC as required.

Reference: Cisco Secure Firewall Threat Defense Configuration Guide, Chapter on Device Management and CLI Access.

Question: 298

A network administrator wants to configure a Cisco Secure Firewall Threat Defense instance managed by Cisco Secure Firewall Management Center to block traffic to known cryptomning networks. Which system settings must the administrator configure in Secure Firewall Management Center to meet the requirement?

A. Access Policy. Security Intelligence
B. Malware Policy.
C. Rules Intrusion Policy. Security Intelligence
D. Access Policy. Rules

Answer: A

Explanation:

To block traffic to known cryptomining networks using Cisco Secure Firewall Threat Defense (FTD) managed by Cisco

Secure Firewall Management Center (FMC), the network administrator needs to configure Security Intelligence in an Access Control Policy. Security Intelligence allows administrators to block traffic based on threat intelligence feeds, which include known malicious IP addresses, domains, and URLs.

Steps:

Navigate to Policies > Access Control > Access Control Policy in FMC.

Edit or create an Access Control Policy.

Go to the Security Intelligence tab.

Enable the relevant threat intelligence feeds that include cryptomining networks.

Apply the policy to the FTD device.

This configuration ensures that traffic to known cryptomining networks is blocked, enhancing the network's security posture against cryptomining threats.

Reference: Cisco Secure Firewall Management Center Configuration Guide, Chapter on Security Intelligence.

Question: 299

An administrator is configuring the interface of a Cisco Secure Firewall Threat Defense device in a passive IPS deployment. The device and interface have been identified. Which set of configuration steps of the administrator take next to complete the implementation?

A. Set the interface mode to passive. Associate the interface with a security zone. Set the MTU parameter. Reset the interface.

B. Modify the interface to retransmit received traffic. Associate the interface with a security zone Enable the interface. Sat the MTU parameter.

C. Modify the interface to retransmit received traffic. Associate the interface with a security zone. Set the MTU parameter.

D. Set the interface mode to passive. Associate the interface with a security zone. Enable the interface. Set the MTU parameter.

Answer: D

Explanation:

In a passive IPS deployment for a Cisco Secure Firewall Threat Defense (FTD) device, the administrator must configure the interface to operate in passive mode. This involves setting the interface mode, associating it with a security zone, enabling the interface, and setting the MTU parameter.

Steps:

Set the interface mode to passive:

In FMC, navigate to Devices > Device Management.

Select the FTD device and configure the relevant interface.

Set the interface mode to "Passive."

Associate the interface with a security zone:

Create or select an appropriate security zone.

Assign the passive interface to this security zone.

Enable the interface:

Ensure the interface is enabled to receive traffic.

Set the MTU parameter:

Configure the Maximum Transmission Unit (MTU) parameter as required.

This ensures that the FTD device can inspect traffic passively without impacting the network flow. Reference: Cisco Secure Firewall Management Center Device Configuration Guide, Chapter on Interface Settings

www.atmicnetworks.com

Question: 300

Refer to the exhibit.

An engineer generates troubleshooting files in Cisco Secure Firewall Management Center (FMC). A successfully completed task Is removed before the files are downloaded. Which two actions must be taken to determine the filename and obtain the generated troubleshooting files without regenerating them? (Choose two.)

A. Use an FTP client Hi expert mode on Secure FMC lo upload the files to the FTP server.

B. Go to the same screen as shown in the exhibit, click Advanced Troubleshooting, enter the rile name, and then start the download

C. Connect to CU on the FTD67 and FTD66 devices and copy the tiles from flash to the PIP server.

D. Go to expert mode on Secure FMC. list the contents of/Var/common, and determine the correct filename from the output

E. Click System Monitoring, men Audit to determine the correct filename from the line containing the Generate Troubleshooting Files string.

Answer: DE

Explanation:

If a task to generate troubleshooting files in Cisco Secure Firewall Management Center (FMC) is completed successfully but removed before the files are downloaded, the following steps can be taken to determine the filename and obtain the generated troubleshooting files without regenerating them:

Go to expert mode on Secure FMC:

Access expert mode on the FMC via SSH or the console.

List the contents of the directory /var/common to locate the generated troubleshooting files. Use the command ls /var/common.

Use the System Monitoring Audit logs:

In FMC, navigate to System > Monitoring > Audit.

Find the line containing the "Generate Troubleshooting Files" string to determine the correct filename.

These actions help identify and retrieve the generated troubleshooting files without the need to regenerate them, saving time and resources.

Reference: Cisco Secure Firewall Management Center Administrator Guide, Chapter on Troubleshooting and File Management.

Question: 301

An administrator is configuring a new report template off. of a saved search within Cisco Secure

Firewall Management Centre. The goal is to use the malware analysis report template, but use a different type saved search as the basis. The report is not working. What must be considered when configuring this report template?

A. Saved searches can be used for the same report template only
B. Saved searches are available freely for all report templates within the same domain.
C. Saved searches from a different report template must be used.
D. Saved searches must be renamed before using for different report template.

Answer: A

Explanation:

When configuring a new report template based on a saved search in Cisco Secure Firewall Management Center (FMC), it is important to note that saved searches are specific to the report template they were created with. Saved searches cannot be freely used across different report templates.
To use a different type of saved search, you must ensure that it aligns with the specific report template being used. This restriction ensures that the saved search parameters match the report's data requirements.
Reference: Cisco Secure Firewall Management Center Administrator Guide, Chapter on Reporting and Saved Searches.

Question: 302

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

A. KVM
B. Azure
C. ESXi
D. AWS
E. Openstack

Answer: CD

Explanation:

Cisco Secure Firewall Threat Defense Virtual (FTDv) appliances support High Availability (HA) configurations in specific virtual environments. The supported environments for HA setups include: ESXi: VMware's ESXi is a widely supported platform for deploying FTDv appliances in HA configurations.
AWS: Amazon Web Services (AWS) supports FTDv appliances and allows for HA configurations to ensure redundancy and reliability in cloud deployments.
These environments provide the necessary infrastructure and capabilities to support the high availability requirements for FTDv appliances.
Reference: Cisco Secure Firewall Threat Defense Virtual Configuration Guide, Chapter on High Availability and Supported Platforms.

Question: 303

An engineer must export a packet capture from Cisco Secure Firewall Management Center to assist in troubleshooting an

issue an a Secure Firewall Threat Defense device. When the engineer navigates to URL for Secure Firewall Management Center at:

..<FMC IP>/capture/CAP/pcap/sample.pcap

An engineer receives a 403: Forbidden error instead of being provided with the PCAP file. Which action resolves the issue?

A. Disable the HTTPS server and use HTTP.
B. Enable the proxy setting in the device platform policy.
C. Enable HTTPS in the device platform policy.
D. Disable the proxy setting on the client browser.

Answer: C

Explanation:

If an engineer receives a 403: Forbidden error when attempting to download a packet capture file from Cisco Secure Firewall Management Center (FMC), the issue is likely due to HTTPS not being enabled in the device platform policy. To resolve this issue, the engineer must enable HTTPS in the platform policy.

Steps:

In FMC, navigate to Policies > Device Management > Platform Settings.

Edit the relevant platform policy.

Enable HTTPS for the device.

Deploy the changes to the FTD device.

This ensures that the FMC and FTD device can securely transfer the packet capture file over HTTPS, resolving the 403 error.

Reference: Cisco Secure Firewall Management Center Administrator Guide, Chapter on Platform Settings and HTTPS Configuration.

Question: 304

Cisco Security Analytics and Logging SaaS licenses come with how many days of data retention by default?

A. 60
B. 365
C. 90
D. 120

Answer: C

Explanation:

Cisco Security Analytics and Logging (SaaS) licenses come with a default data retention period of 90 days. This retention period allows organizations to store and analyze their security event data for up
to 90 days, providing sufficient time for security monitoring and forensic investigations.

Reference: Cisco Security Analytics and Logging Documentation, Chapter on License Information and Data Retention.

Question: 305

An engineer is implementing a new Cisco Secure Firewall. The firewall must filler traffic between the three subnets:

- LAN 192.168.101.0724
- DMZ 192.168 200.0/24
- WAN 10.0.0.0/30

Which firewall mode must the engineer implement?

A. transparent
B. network
C. routed
D. gateway

Answer: C

Explanation:

To filter traffic between multiple subnets, the engineer must implement the firewall in routed mode. In routed mode, the firewall operates as a Layer 3 device, capable of routing traffic between different IP subnets. This mode is appropriate for filtering traffic between LAN, DMZ, and WAN subnets.

Steps to configure routed mode:

Access the firewall's management interface.

Configure interfaces for each subnet (LAN, DMZ, WAN) with appropriate IP addresses and network masks.

Define security zones and apply access control policies to filter traffic as required.

This ensures that the firewall can inspect and route traffic between the different subnets, providing the necessary security and control.

Reference: Cisco Secure Firewall Threat Defense Configuration Guide, Chapter on Routed Mode Configuration.

Question: 306

An engineer is configuring a new dashboard within Cisco Secure Firewall Management Center and is having trouble implementing a custom widget. When a custom analysis widget is configured which option is mandatory for the system to display the information?

A. table
B. filter
C. title
D. results

Answer: C

Explanation:

When configuring a custom widget on a dashboard within Cisco Secure Firewall Management Center (FMC), it is mandatory to provide a title for the system to display the information correctly. The title helps in identifying and organizing the widget on the dashboard.

Steps:

Navigate to the dashboard section in FMC.

Add a new custom widget.

Configure the widget settings and provide a title.

Save and apply the widget to the dashboard.

Providing a title ensures that the widget is correctly displayed and easily identifiable on the dashboard.

Reference: Cisco Secure Firewall Management Center User Guide, Chapter on Dashboard and Custom Widgets.

Question: 307

An engineer has been tasked with performing an audit of network projects to determine which objects are duplicated across the various firewall models (Cisco Secure Firewall Threat Defense Cisco Secure firewall ASA, and Meraki MX Series) deployed throughout the company Which tool will assist the engineer in performing that audit?

A. Cisco Firepower Device Manager
B. Cisco SecureX
C. Cisco Defense Orchestrator
D. Cisco Secure Firewall Management Center

Answer: C

Explanation:

Cisco Defense Orchestrator (CDO) is the tool that assists engineers in performing an audit of network projects to determine which objects are duplicated across various firewall models, including Cisco Secure Firewall Threat Defense, Cisco Secure Firewall ASA, and Meraki MX Series. CDO provides a unified management interface for managing multiple security devices and can identify duplicate objects across these devices.

Steps:

Access Cisco Defense Orchestrator.

Connect and synchronize all relevant firewall devices (FTD, ASA, Meraki MX).

Use the audit and reporting features in CDO to identify and manage duplicate objects.

This helps ensure consistency and efficient management across the organization's firewall deployments.

Reference: Cisco Defense Orchestrator Documentation, Chapter on Device Management and Object Auditing.

Question: 308

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.

Answer: C

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.
Reference: Cisco Secure Firewall Management Center Administrator Guide, Chapter on High Availability Configuration.

Question: 309

Refer to the exhibit.

A Cisco Secure Firewall Threat Defense (FTD) device is deployed in inline mode with an inline set. The network engineer wants router R2 to remove the directly connected route M 68.1.0/24 from its routing table when the cable between routed R1 and the Secure FTD device Is disconnected. Which action must the engineer take?
1

A. Implement the Propagate Link Stale option on the Secure FTD device
B. Establish a routing protocol between R1 and R2.
C. Disable hardware bypass on the Secure FTD device.
D. Implement autostate functionality on the Gi0/2 interface of R2

Answer: A

Explanation:
To ensure that router R2 removes the directly connected route for 192.168.1.0/24 from its routing table when the cable between router R1 and the Secure FTD device is disconnected, the network engineer must implement the "Propagate Link State" option on the Secure FTD device. This option allows the FTD to propagate the link state changes to adjacent devices, ensuring that the disconnection is recognized and the routing table is updated accordingly.
Steps:
Access the FTD device configuration via FMC.
Navigate to the interface settings for the relevant interfaces.
Enable the "Propagate Link State" option for the interfaces connected to R1 and R2.
Deploy the changes to the FTD device.
This configuration ensures that the link state changes are communicated to router R2, prompting it to remove the disconnected route from its routing table.
Reference: Cisco Secure Firewall Threat Defense Configuration Guide, Chapter on Interface Settings and Link State Propagation.

Question: 310

Which component is needed to perform rapid threat containment with Cisco FMC?

A. ISE
B. RESTful API
C. SIEM
D. DDI

Answer: A

Explanation:

To perform rapid threat containment with Cisco FMC, the necessary component is Cisco Identity Services Engine (ISE). ISE integrates with FMC to provide dynamic network access control and enforcement, allowing for quick isolation of compromised endpoints based on security events detected by FMC.

Steps:

Integrate FMC with ISE by configuring the necessary settings in both platforms.

Define security policies in FMC that trigger rapid threat containment actions via ISE.

When a threat is detected, FMC can instruct ISE to isolate the affected endpoint, limiting its access to the network.

This integration enables automated and efficient threat containment, reducing the response time and mitigating the impact of security incidents.

Reference: Cisco Secure Firewall Management Center Integration Guide, Chapter on ISE Integration for Rapid Threat Containment.

Question: 311

A security engineer must create a malware and file policy on a Cisco Secure Firewall Threat Defense device. The solution must ensure that PDF. DOCX, and XLSX files are not sent lo Cisco Secure Malware analytics. What must do configured to meet the requirements''

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

Answer: D

Explanation:

To create a malware and file policy on a Cisco Secure Firewall Threat Defense (FTD) device that ensures PDF, DOCX, and XLSX files are not sent to Cisco Secure Malware Analytics, the security engineer must configure local malware analysis. Local malware analysis allows the FTD to inspect and analyze files locally without sending them to the cloud-based Cisco Secure Malware Analytics. Steps to configure local malware analysis:

In FMC, navigate to Policies > Access Control > Malware & File Policies.

Create a new malware and file policy or edit an existing one.

Define rules to inspect specific file types, ensuring that PDF, DOCX, and XLSX files are handled locally.

Set the action for these file types to "Local Analysis."

Apply the policy to the relevant access control policy.

This configuration ensures that the specified file types are analyzed locally, meeting the requirement to avoid sending them to Cisco Secure Malware Analytics.

Reference: Cisco Secure Firewall Management Center Configuration Guide, Chapter on Malware and File Policies

Question: 312

An engineer must integrate a thud-party security Intelligence teed with Cisco Secure Firewall Management Center. Secure Firewall Management Center is running Version 6.2 3 and has 8 GB of memory. Which two actions must be taken to implement Throat Intelligence Director? (Choose two.)

A. Upgrade to version 6.6.
B. Enable REST API access.
C. Add the URL of the TAXII server.
D. Add 7 GB of memory.
E. Add a TAXII server

Answer: AC

Explanation:

To integrate a third-party security intelligence feed with Cisco Secure Firewall Management Center (FMC) using Threat Intelligence Director (TID), the following actions are necessary:
Upgrade to version 6.6: The FMC must be running at least version 6.6 to support Threat Intelligence Director. Version 6.2.3 does not support the necessary features for this integration.
Add the URL of the TAXII server: Threat Intelligence Director uses TAXII (Trusted Automated eXchange of Indicator Information) to pull threat intelligence data from third-party sources. The URL of the TAXII server must be added to the TID configuration in FMC.
Steps:
Upgrade FMC to version 6.6 or later.
In FMC, navigate to Integration > Threat Intelligence Director.
Add a new TAXII server by entering the URL of the TAXII server.
These actions enable the integration of third-party threat intelligence feeds, enhancing the security capabilities of the FMC.
Reference: Cisco Secure Firewall Management Center Administrator Guide, Chapter on Threat Intelligence Director.

Question: 313

An administrator configures the interfaces of a Cisco Secure Firewall Threat Defence device in an inline IPS deployment. The administrator completes these actions:
* identifies the device and the interfaces
* sets the interface mode to inline
* enables the interlaces
Which configuration step must the administrator take next to complete the implementation?

A. Enable spanning-tree PortFast on the interfaces.
B. Configure an inline set
C. Set the interface to Transparent mode.
D. Set the interface to routed mode.

Answer: B

Explanation:

After setting the interface mode to inline and enabling the interfaces on a Cisco Secure Firewall Threat Defense (FTD) device in an inline IPS deployment, the next step is to configure an inline set. An inline set groups two interfaces that work together to inspect traffic passing between them. Steps to configure an inline set:
In FMC, navigate to Devices > Device Management.
Select the FTD device and configure the interfaces.
Create a new inline set, adding the relevant interfaces that have been set to inline mode.
Deploy the configuration to the FTD device.
Configuring an inline set ensures that the traffic between the specified interfaces is inspected and processed according to the IPS policies, completing the implementation of the inline IPS deployment. Reference: Cisco Secure Firewall Management Center Configuration Guide, Chapter on Inline Sets.

Question: 314

A network engineer is deploying a pair of Cisco Secure Firewall Threat Defense devices managed by Cisco Secure Firewall Management Center tor High Availability Internet access is a high priority for the business and therefore they have invested in internet circuits from two different ISPs. The requirement from the customer Is that Internet access must do available to their user's oven if one of the ISPs is down. Which two features must be deployed to achieve this requirement? (Choose two.)

A. EtherChannel interfaces
B. Route Tracking
C. SLA Monitor
D. Redundant interfaces
E. BGP

Answer: BC

Explanation:

To ensure high availability of internet access when deploying a pair of Cisco Secure Firewall Threat Defense (FTD) devices managed by Cisco Secure Firewall Management Center (FMC), the following features must be deployed:
Route Tracking: This feature monitors the reachability of a specified target (such as an external IP address) through the configured routes. If the route to the target is lost, the FTD can dynamically adjust the routing to use an alternate path, ensuring continuous internet access.
SLA Monitor: Service Level Agreement (SLA) monitoring works alongside route tracking to continuously verify the status and performance of the internet links. If the SLA for one of the ISP links fails (indicating the link is down or underperforming), the FTD can switch traffic to the secondary ISP link.
Steps to configure:
In FMC, navigate to Devices > Device Management.
Select the FTD device and configure route tracking to monitor the ISP links.
Configure SLA monitors to continuously check the health and performance of the internet circuits. These configurations ensure that internet access remains available to users even if one of the ISPs goes down.
Reference: Cisco Secure Firewall Management Center Configuration Guide, Chapter on High Availability and SLA Monitoring.

Question: 315

A network engineer detects a connectivity issue between Cisco Secure Firewall Management Centre and Cisco Secure Firewall Threat Defense Initial troubleshooting indicates that heartbeats and events not being received. The engineer re-

establishes the secure channels between both peers Which two commands must the engineer run to resolve the issue? (Choose two.)

A. manage_procs.pl

B. sudo stats_unified.pl

C. sudo perfstats -Cq < /var/sf/rna/correlator-stats/now

D. show history

E. show disk-manager

Answer: AB

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.

Reference: Cisco Secure Firewall Threat Defense Configuration Guide, Chapter on Troubleshooting and CLI Commands.

Question: 316

A network administrator is deploying a new Cisco Secure Firewall Threat Defense (FTD) firewall After Cisco Secure FTD is deployed, inside clients nave intermittent connectivity to each other. When … the packet capture on the Secure FTD firewall, the administrator sees that Secure FID is responding to all the AW requests on the inside network. Which action must the network administrator e to resolve the issue''

A. Review NAT policy and disable incorrect proxy ARP configuration.
B. Hardcode the MAC address of the FTD to IP mapping on client machines.
C. Review the access policy and verify that ARP is allowed from inside to inside.
D. Convert the FTD to transparent mode to allow ARP requests.

Answer: A

Explanation:

If inside clients have intermittent connectivity issues and the Cisco Secure FTD is responding to all ARP requests on the inside network, it indicates that there may be an incorrect proxy ARP configuration in the NAT policy. Proxy ARP can cause the FTD to respond to ARP requests on behalf of other devices, leading to connectivity issues.

Steps to resolve:

Review the NAT policy on the FTD to identify any incorrect proxy ARP configurations.

Disable the proxy ARP setting for the relevant NAT rules that are causing the issue.

This ensures that the FTD only responds to ARP requests as needed, preventing it from interfering with normal ARP traffic on the inside network.

Reference: Cisco Secure Firewall Management Center Configuration Guide, Chapter on NAT and ARP Configuration.

Question: 317

An organization created a custom application that is being flagged by Cisco Secure Endpoint. The application must be exempt from being flagged. What is the process to meet the requirement?

A. Modify the custom detection list to exclude me custom application.
B. Preculculate the hash value of the custom application and add it to the allowed applications.
C. Configure the custom application to use the information-store paths.
D. Add the custom application to the DFC 1st and update the policy.

Answer: B

Explanation:

To exempt a custom application from being flagged by Cisco Secure Endpoint, the organization must precalculate the hash value of the custom application and add it to the allowed applications list. This process involves creating a hash of the executable file, which uniquely identifies it, and then configuring Cisco Secure Endpoint to recognize this hash as trusted.

Steps:

Calculate the hash value (e.g., SHA-256) of the custom application executable.

In the Cisco Secure Endpoint management console, navigate to the policy configuration.

Add the calculated hash value to the list of allowed applications or exclusions.

Save and deploy the updated policy.

By adding the hash value to the allowed applications, Cisco Secure Endpoint will recognize the custom application as trusted and will no longer flag it.

Reference: Cisco Secure Endpoint User Guide, Chapter on Policy Configuration and Application Whitelisting.

Question: 318

What is the result when two users modify a VPN policy at the same lime on a Cisco Secure Firewall Management Center managed device?

A. Both users can edit the policy arid the last saved configuration persists.
B. The first user locks the configuration when selecting edit on the policy.
C. The changes from both users will be merged together into the policy.
D. The system prevents modifications to the policy by multiple users.

Answer: B

Explanation:

In Cisco Secure Firewall Management Center (FMC), when two users attempt to modify a VPN policy simultaneously, the system implements a locking mechanism to prevent conflicts. The first user who selects edit on the policy locks the configuration, preventing other users from making changes until the lock is released.

Steps:

When the first user selects edit on the VPN policy, FMC locks the policy for editing.

The lock ensures that only the first user can make changes.

Once the first user saves or cancels their changes, the lock is released.

Other users can then edit the policy.

This locking mechanism ensures that configuration conflicts are avoided and only one set of changes is applied at a time.

Reference: Cisco Secure Firewall Management Center Configuration Guide, Chapter on Policy Management and User Permissions.

Question: 319

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

Answer: A

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. Reference: Cisco Secure Firewall Management Center Intrusion Policy Guide, Chapter on Custom Rule Creation and Metadata Usage.

Question: 320

Refer to the Exhibit.

APPLICATIONS ASSOCIATED WITH ATTACKS

M M h«t tow buwwM relevance and evaluate whether N would bo MtoM to control Vwm or* your network

aee* A«MCMM« ■■* re^ *w*eM Iveaea IFRRMI (WMI* •we*

oets	IS	Chromo	
Mamet Lepor or	14	Internet Explorer	110
Web browser	fl	DC C WC cheer	74
FTP chore	•	Web browser	47
NetBIOS-*** (SMB) Cfcere	0	Rretoa	30

TOP ATTACKERS AND TARGETS

enpoci attache •* patteuiar. you ahouid emure that target* are we* protected from potartoal attacUra by patching

High Impact Events

010021427	3	31 31 190230	fl
10 1 110 12	3	106 110 160 156	«
10 1 102 30	3	37 4fl 82 212	4
10 1200	2	105 00 77.12	4
10 1 30 21	2	192 101 54 00	

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

Answer: A

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.

Reference: Cisco Secure Firewall Management Center Administrator Guide, Chapter on DNS Security and Traffic Inspection.

Question: 321

An engineer is troubleshooting an intermittent connectivity issue on a Cisco Secure Firewall Threat Defense appliance and must collect 24 hours' worth of dat

a. 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

Answer: B

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.

Reference: Cisco Secure Firewall Threat Defense Configuration Guide, Chapter on Packet Capture Configuration and Management.

Question: 322

An engineer must create an access control policy on a Cisco Secure Firewall Threat Defense device. The company has a contact center that utilizes VoIP heavily, and it is critical that this traffic is not …. by performance issues after deploying the access control policy Which access control Action rule must be configured to handle the VoIP traffic?

A. monitor
B. trust
C. block
D. allow

Answer: B

Explanation:

To ensure that VoIP traffic in a contact center is not impacted by performance issues after deploying an access control policy on a Cisco Secure Firewall Threat Defense (FTD) device, the engineer should configure the access control rule with the "trust" action. The "trust" action allows traffic to bypass inspection and policy enforcement, ensuring that critical VoIP traffic is not delayed or degraded. Steps:

In FMC, navigate to Policies > Access Control > Access Control Policy.

Create a new rule or edit an existing rule.

Set the source and destination for the VoIP traffic.

Set the action to "trust" to ensure the VoIP traffic is not inspected.

By configuring the rule with the "trust" action, the VoIP traffic will be prioritized, maintaining the quality and performance required for the contact center operations.

Reference: Cisco Secure Firewall Management Center Configuration Guide, Chapter on Access Control Policies and Traffic Management.

www.atmicnetworks.com

Question: 323

Which action must be taken to configure an isolated bridge group for IRB mode on a Cisco Secure Firewall device?

A. Add the restricted segment to the ACL.
B. Leave BVI interface name empty.
C. Define the NAT pool for the blocked traffic.
D. Remove the route from the routing table.

Answer: B

Explanation:

To configure an isolated bridge group for Integrated Routing and Bridging (IRB) mode on a Cisco Secure Firewall device, the action to take is to leave the BVI (Bridge Virtual Interface) interface name empty. This ensures that the bridge group operates in an isolated manner, where Layer 3 routing is not applied to the bridged interfaces, effectively isolating the traffic within the bridge group.

Steps:

Access the firewall's configuration interface.

Configure the bridge group interfaces.

Ensure that the BVI interface name is left empty to isolate the bridge group.

This configuration prevents Layer 3 routing for the isolated bridge group, ensuring that traffic remains contained within the bridge group.

Reference: Cisco Secure Firewall Management Center Configuration Guide, Chapter on Bridge Groups and IRB Mode.

Question: 324

An administrator must fix a network problem whereby traffic from the inside network to a webserver is not getting through an instance of Cisco Secure Firewall Threat Defense. Which command must the administrator use to capture packets to the webserver that are dropped by Secure Firewall Throat Defense and resold the issue?

A. capture CAP int OUTSIDE match ip any host WEBSERVERIP
B. capture CAP type asp-drop all headers-only
C. capture CAP int INSIDE match ip any host WEBSERVERIP
D. capture CAP int INSIDE match tcp any 80 host WEBSERVERIP 80

Answer: B

Explanation:

To capture packets that are dropped by Cisco Secure Firewall Threat Defense (FTD) and troubleshoot the issue of traffic from the inside network to a webserver not getting through, the administrator should use the command to capture packets dropped by the accelerated security path (ASP) engine. The correct command is:

capture CAP type asp-drop all headers-only

This command captures all packets dropped by the ASP engine, which includes packets that are being blocked by access control policies, NAT issues, or other security checks.

Steps:

Access the FTD CLI.

Run the command capture CAP type asp-drop all headers-only to capture dropped packets.

Analyze the captured data to identify the cause of the drops.

This command provides detailed information on why packets are being dropped, helping the administrator resolve the issue.

Reference: Cisco Secure Firewall Threat Defense Configuration Guide, Chapter on Packet Capture and ASP Drop Captures.

Question: 325

What is the role of realms in the Cisco ISE and Cisco FMC integration?

A. AD definition
B. TACACS+ database
C. Cisco ISE context
D. Cisco Secure Firewall VDC

Answer: A

Explanation:

In the integration between Cisco Identity Services Engine (ISE) and Cisco Firewall Management Center (FMC), realms are used to define the Active Directory (AD) configuration. Realms in FMC specify the AD servers, domain, and other authentication settings necessary to authenticate and authorize users.

Steps to configure realms:

In FMC, navigate to System > Integration > Realms and Directory.

Add a new realm and configure the AD settings.

Ensure the realm settings match the AD environment for seamless integration.

Realms are essential for integrating AD with FMC, allowing the firewall to use AD for user authentication and policy enforcement.

Reference: Cisco Secure Firewall Management Center Administrator Guide, Chapter on Realms and Directory Integration.

Question: 326

An engineer is troubleshooting the upgrade of a Cisco Secure Firewall Threat Defense device on the Secure Firewall Management Center 7.0 GUI. The engineer wants to collect the upgrade data and logs. Which two actions must the engineer take? (Choose two.)

A. View the system and troubleshooting details.
B. Select the Secure Firewall Threat Defense device properties.
C. Select the Secure Firewall Management Center device.
D. Access the Health Events page.
E. Access the Health Monitor page.

Answer: B, E

Question: 327

An engineer is configuring two new Cisco Secure Firewall Threat Defense devices to replace the existing firewalls.

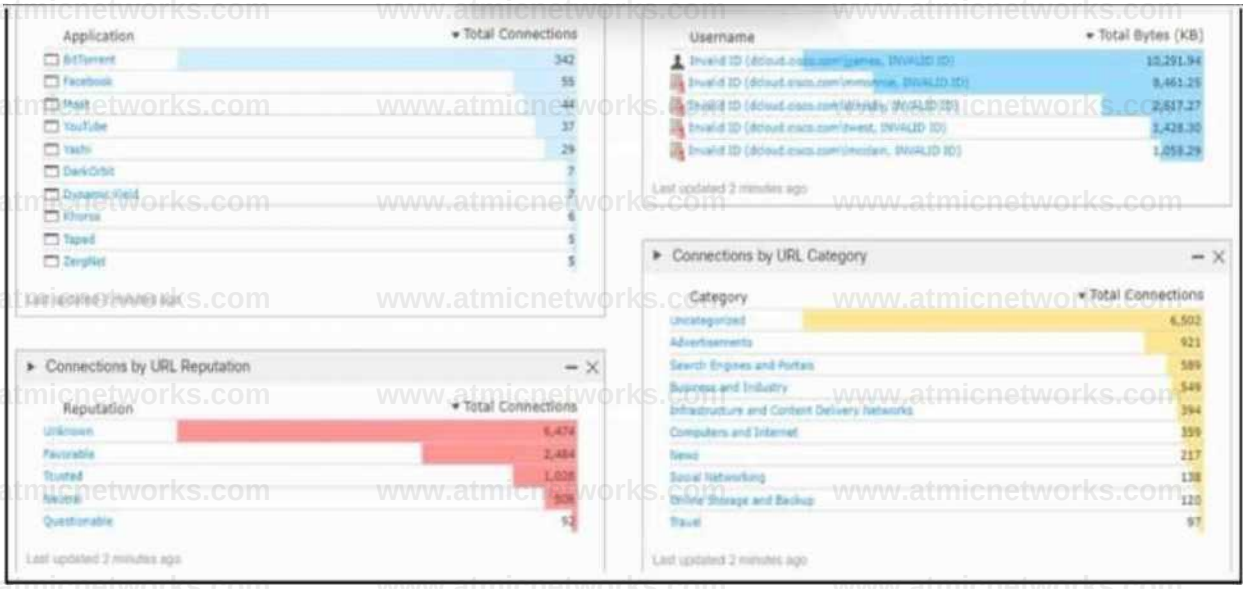
Network traffic must be analyzed for intrusion events without impacting the traffic. What must the engineer implement next to accomplish the goal?

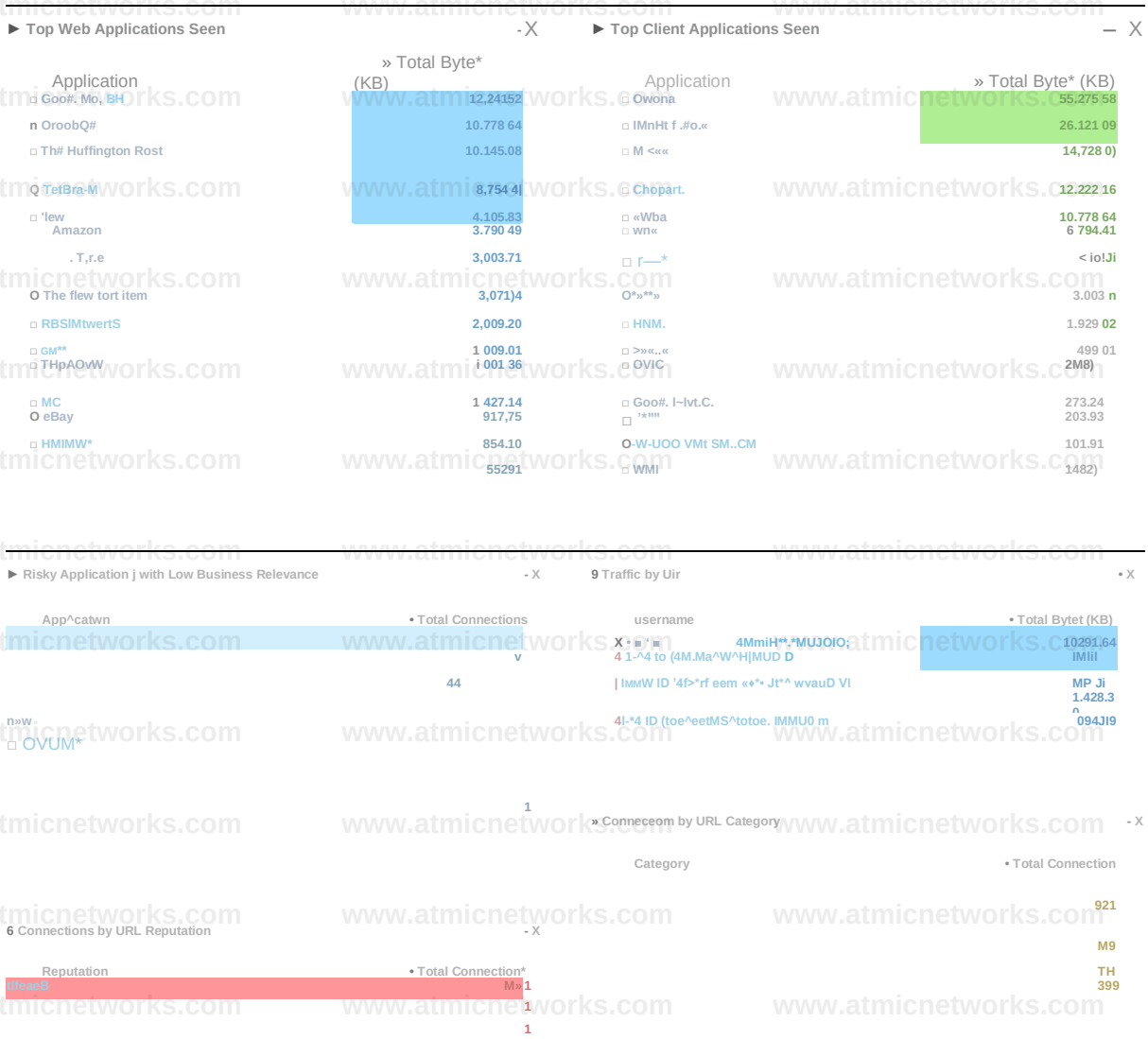
A. Passive mode
B. Inline Pair in Tap mode
C. ERSPAN Passive mode
D. Inline Pair mode

Answer: A

Question: 328

Refer to the exhibit.





Refer to the exhibit. An engineer analyzes a Cisco Firepower Management Center dashboard. Which action must be taken by the user to decrease the risk of data loss?

A. Stop all URLs that have an unknown reputation.
B. Block the use of Dropbox.
C. Stop all the URLs that are uncategorized.
D. Block all the BitTorrent applications.

Answer: C

Question: 329

An engineer must configure email notifications on Cisco Secure Firewall Management Center. TLS encryption must be used to protect the messages from unauthorized access. The engineer adds the IP address of the mail relay host and must set the port number. Which TCP port must the engineer use?

A. 25
B. 389
C. 465
D. 587

Answer: D

Question: 330

An engineer must implement Cisco Secure Firewall transparent mode due to a new server recently being added that must communicate with an existing server that is currently separated by the firewall. Which implementation action must be taken next by the engineer to accomplish the goal?

A. Enable both servers to share the same VXLAN segment.
B. Configure the same default gateway for both servers.
C. Ensure that both servers are in the same bridge domain.
D. Assign the same subnet to both servers.

Answer: C

Question: 331

An engineer is configuring a multidomain instance of Cisco Secure Firewall Management Center. The instance must be integrated with Cisco Secure Endpoint. What must the engineer configure to allow multiple domains to have hosts with the same IP-MAC address pairs?

A. second-level domain
B. leaf domain
C. global domain
D. subdomain

Answer: B

Question: 332

An engineer is deploying a Cisco Secure Firewall Management Center appliance. The company must send data to Cisco Secure Network Analytics appliances. Which two actions must the engineer take? (Choose two.)

A. Configure Security Intelligence object to send data to Cisco Secure Network Analytics.
B. Add the Netflow_Send_Destination object to the configuration.
C. Add the Netflow_Add_Destination object to the configuration.
D. Add the Netflow_Set_Parameters object to the configuration.
E. Create a service identifier to enable the NetFlow service.

Answer: C, D

Question: 333

A network administrator is configuring an instance of Cisco Secure Firewall Threat Defense, which is registered to Cisco Secure Firewall Management Center, to prevent internal users from downloading executable files from the internet. What must be created and configured by the administrator to meet the requirement?

A. Access policy rule that allows users to reach the internet and assigns a file policy that blocks executable downloads to the rule.
B. File policy that blocks downloads of all executable files and applies the file policy to the default action in the access policy.
C. File policy rule that allows users to reach the internet with a second rule applied that blocks application use of FTP.
D. Access policy rule that allows users to reach the internet with a second rule that blocks application executables.

Answer: A

Question: 334

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

A. Set the same MAC address on both units.
B. Add the MAC address to the switch ARP table.
C. Run a script to send gratuitous ARP after a failover.
D. Use a virtual MAC address on both units.

Answer: D

Question: 335

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

A. Define the transport protocol and the mandatory port range.
B. Add the transport number and specify the type and code.
C. Add the corresponding IP protocol number for UDP and TCP.
D. Specify the transport protocol and leave the port number empty.

Answer: A

Question: 336

Refer to the exhibit.

Refer to the exhibit. An engineer is configuring an instance of Cisco Secure Firewall Threat Defense with interfaces in IPS Inline Pair mode. What must be configured on interface e1/6 to accomplish the requirement?

A. propagate link state disabled
B. inline set MTU set to 1500
C. FailSafe disabled
D. security zone set to OUTSIDE_ZONE

Answer: B

Question: 337

A network administrator is trying to configure a previously created file policy on a new access policy. Which action must the administrator take before applying the file policy?

A. Set up an inspection policy.
B. Create a new access control rule.
C. Assign the file policy to the default action.
D. Apply an application to an access control rule.

Answer: B

Question: 338

An engineer is deploying a Cisco ASA Secure Firewall module. The engineer must be able to examine traffic without impacting the network, and the ASA has been deployed with a single context. Which ASA Secure Firewall module deployment mode must be implemented to meet the requirements?

A. Transparent mode with inline tap monitor-only mode
B. Routed mode with passive monitor-only mode

C. Transparent mode with passive monitor-only mode
D. Routed mode with inline tap monitor-only mode

Answer: C

Question: 339

Refer to the exhibit.

```
Network_l;Internal network;192.168.1.0/24;
FQDN_1;£amain Names;FQDN;www.example.cam;ipv4_ipv€
Network_2;Internal network2;192.168.2.0/24;
```

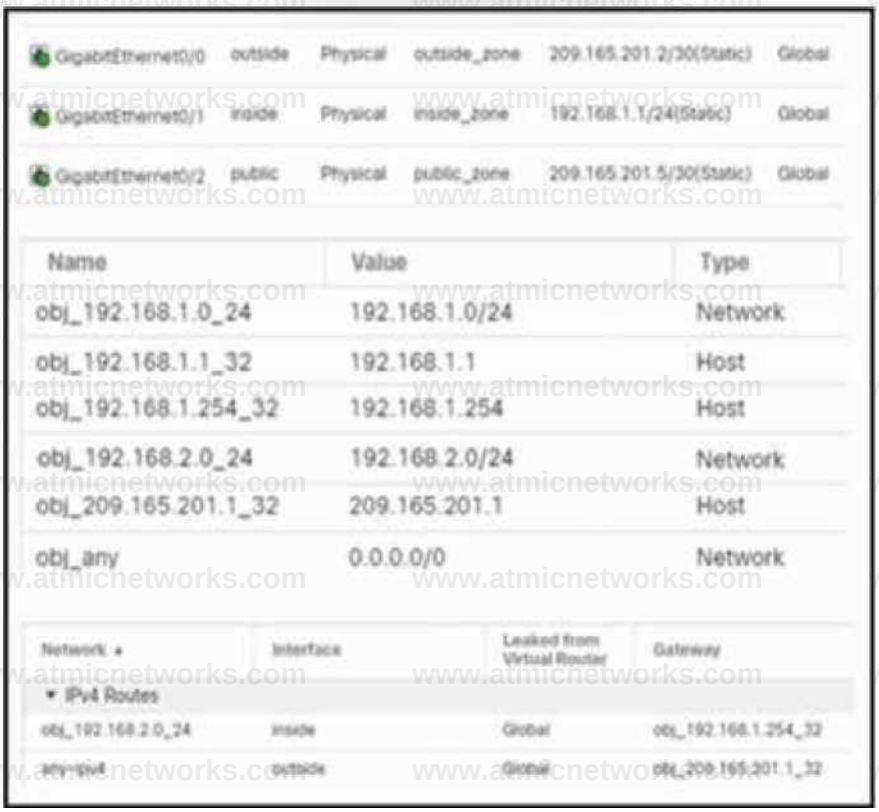
Refer to the exhibit. An engineer must import three network objects into the Cisco Secure Firewall Management Center by using a CSV file. Which header must be configured in the CSV file to accomplish the task?

A. NAME;DESCRIPTION;TYPE;VALUE;LOOKUP;
B. Name; Description; Type;Value;Lookup;
C. Name; Description; Type;Value;DN;
D. NAME;DESCRIPTION; TYPE;VALUE;DN;

Answer: A

Question: 340

DRAG DROP
Refer to the exhibit.



GigabitEthernet0/0	outside	Physical	outside_zone	209.165.201.2/30(Static)	Global
GigabitEthernet0/1	inside	Physical	inside_zone	192.168.1.1/24(Static)	Global
GigabitEthernet0/2	public	Physical	public_zone	209.165.201.5/30(Static)	Global

Name	Value	Type
obj_192.168.1.0_24	192.168.1.0/24	Network
obj_192.168.1.1_32	192.168.1.1	Host
obj_192.168.1.254_32	192.168.1.254	Host
obj_192.168.2.0_24	192.168.2.0/24	Network
obj_209.165.201.1_32	209.165.201.1	Host
obj_any	0.0.0.0/0	Network

Network	Interface	Leaked from Virtual Router	Gateway
IPv4 Routes			
obj_192.168.2.0_24	inside	Global	obj_192.168.1.254_32
any-ipv4	outside	Global	obj_209.165.201.1_32

Refer to the exhibit. An engineer configures a NAT rule allowing clients to use the internet only if clients are located on the directly connected internal network. Dynamic auto PAT must be configured. Drag and drop the NAT rules from the left onto the corresponding targets on the right. Not all options are used.

Answer:

Explanation:

NAT Rule Component	Corresponding Target
auto NAT	Nat Rule
obj_192.168.1.0_24	original source
inside_zone	source interface objects
outside_zone	destination interface objects
dynamic	type

Destination interface IP

Translated source

Question: 341

A network engineer detects a connectivity issue between Cisco Secure Firewall Management Center and Cisco Secure Firewall Threat Defense. Initial troubleshooting indicates that heartbeats and events are 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. show disk-manager
B. show history
C. sudo stats_unified.pl
D. manage_procs.pl
E. sudo perfstats -Cq < /var/sf/rna/correlator-stats/now

Answer: C, D

Question: 342

An administrator configures a Cisco Secure Firewall Threat Defense device in transparent mode. To configure the BVI (Bridge Virtual Interface), the administrator must:

Add a bridge-group interface

Configure a bridge-group ID

Configure the bridge-group interface description

Add bridge-group member interfaces

How must the engineer perform these actions?

A. Configure a name for the bridge-group interface
B. Set a security zone for the bridge-group interface
C. Set the bridge-group interface mode to transparent
D. Configure an IP address for the bridge-group interface

Answer: D

Question: 343

An engineer must implement static route tracking on a Cisco Secure Firewall Threat Defense appliance. Static route and IP

SLA operation has already been configured. Static route must be removed from the routing table if the tracked object is unreachable. Which action must the engineer take next to meet the requirement?

A. Implement a secondary route that has a higher precedence.
B. Enable the IP SLA Responder on the backup path interface.
C. Assign a tracking object to the static route and the IP SLA operation.
D. Enable an ICMP redirect message on the interface connected to the backup path.

Answer: C

Question: 344

What is a method used by Cisco Rapid Threat Containment to contain the threat in the network?

A. change of authentication
B. share context data
C. TACACS+
D. trustsec segmentation

Answer: D

Question: 345

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

A. Cisco Secure Network Analytics
B. Cisco Defense Orchestrator
C. Cisco Catalyst Center
D. Secure Cloud Analytics
E. Cisco Prime Infrastructure

Answer: A, D

Question: 346

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

A. bypass
B. link state propagation
C. tap mode
D. strict TCP enforcement

Answer: C

Question: 347

An engineer is configuring Cisco Secure Firewall Threat Defense managed by a Secure Firewall Management Center appliance. The company wants remote access VPN users to be reachable from the inside network. What must the engineer configure to meet the requirements?

A. manual NAT exemption rule at the top of the NAT policy
B. manual NAT exemption rule at the bottom of the NAT policy
C. auto NAT exemption rule at the top of the NAT policy
D. auto NAT exemption rule at the bottom of the NAT policy

Answer: A

Question: 348

A network engineer must monitor threat events from the console of Cisco Secure Firewall Management Center. The engineer integrates the Cisco Secure Firewall Malware Defense in Secure Firewall Management Center. Which action must the engineer take next?

A. Log in to Cisco Secure Endpoint, click Allow to authorize the Secure Firewall Malware Defense to Secure FMC connection, and add a Secure Firewall Malware Defense cloud connection to Secure FMC.
B. Log in to Secure Endpoint, click Allow to authorize the Secure Firewall Malware Defense to Secure FMC connection, add a Secure Firewall Malware Defense cloud connection to Secure FMC, and select the Secure Firewall Malware Defense cloud for Secure Endpoint.
C. Add a Secure Firewall Malware Defense cloud connection in Secure FMC, log in to Secure Endpoint, and click Allow to authorize the Secure Firewall Malware Defense to Secure FMC connection.
D. Add a Secure Firewall Malware Defense cloud connection in Secure FMC, select the Secure Firewall Malware Defense cloud for Secure Endpoint, log in to Secure Endpoint, and click Allow to authorize the Secure Firewall Malware Defense to Secure FMC connection.

Answer: D

Question: 349

An engineer must configure a correlation policy in Cisco Secure Firewall Management Center to detect when an IP address from an internal network communicates with a known malicious host. Connections made by the internal IP addresses must be tracked, and an external dynamic list must be used for the condition. Which type of event must the engineer configure on the correlation policy?

A. Intrusion Impact Alert
B. Connection tracker
C. Network discovery

D. Malware

Answer: B

Question: 350

Which firewall mode is Cisco Secure Firewall Threat Defense in when two physical interfaces are assigned to a named BVI?

A. Routed
B. Transparent
C. In-line
D. IPS only

Answer: B

Question: 351

An engineer is deploying Cisco Secure Endpoint for the first time and on endpoint with MAC address 50:54:15:04:0:AB. The engineer must make sure that during the testing phase no files are isolated and network connections must not be blocked. Which policy type must be configured to accomplish the task?

A. Triage
B. Quarantine
C. Protect
D. Audit

Answer: D

Question: 352

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 Low Impact Events	Count
Chrome	283
Internet Explorer	110
DCE/RPC client	74
Web browser Firefox	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
10.1.115.12	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

Refer to the exhibit. 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. Block Internet Explorer.
B. Block NetBIOS.
C. Inspect TCP port 80 traffic.
D. Inspect DNS traffic.

Answer: C

Question: 353

What is an attribute of the risk reporting capability in Cisco Secure Firewall Management Center?

A. Includes all domains in a multidomain system

B. Uses the same templates available to standard reports C. Includes the current domain in a multidomain system D. Uses the XML format to export all reporting

Answer: C

Question: 354

An engineer must deny ICMP traffic to the networks of separate departments that use Cisco Secure Firewall Management Center. The engineer must use the same object on the relevant device for each network. What must be configured in Secure Firewall Management Center?

A. IP address

B. IP range

C. Deny ICMP check box

D. Allow Overrides check box

Answer: D

Question: 355

Refer to the exhibit.

COMMON INDICATIONS OF COMPROMISE FOUND

Mcatona of ctsrnpomrte take many Mm), semap* • Mi hae been wan to execute mateere. bt connected to ■ Command 4 Contra) term ba targeted w* a high enpaci attack, or actrveh toakarg data ACTOM lha monitored network thaw are a aanMe a) different 1OC1 detected agaatat tee ryttenn

Most Common IOC Types Discovered

Category	Description	Count
Mew ere Detected	The hoot Ma encountered mateere	M
CnC Connected	The MM may bo under tornote control	n
Milwtfw Dowr*o*d	The hoot may connect to a mateere hoot	30
Fjpio« KI	The MM may have encountered an npot kit	20
Ptyetwig Target	The hoot may connect to a ptwhmg MM	20
Impact 1 Mac*	The hootarea attacked and to teary vulnerable	14
HMTWIQ tug*	The hoot may connect to a pinning URL	14
UAU«T« Ownnad	The Met may connect to a malware UK	J
ripaci 2 Attack	The hoot area attacked and to potentially vulnerable	4

HOSTS CONNECTED TO COMMAND AND CONTROL SERVERS

The tokOenng dencae have been toenafed aa bong connected to command and control (OCI aervere Crete derocti CnC defection* through a blend M deed taewon toacket coreont) nepectron. network comrmawaboni to hMla ide«Med by Ctacs Tain aa hoeeng CnC MraadmeMa and cannecbena oubeond from proceaaea on an endoort teal are known to be maicroue

* AIftVMa	BMM1**B	Lan 1MM
to t to* IB?	Mutton Event malware cnc	2022 03 04 221)44
101.104 JO	Multon Evert! mateare-cne	2022 03 44 22.14 08
tot 115 12	Mutton Ever) malearecnc	2022 03 44 2' 41 St
101 105.31	Ininntan Event - maheant-cnc	2022-0304 21 M M
101 10217	Mutton Event malarare-cnc	2022-03 04 2< 21 45

Refer to the exhibit. An engineer analyzes a Network Risk Report from Cisco Secure Firewall Management Center. What should the engineer recommend implementing to mitigate the risk?

A. IP address and URL blacklisting

B. Trend analysis

C. Network-based detection

D. Virtual protection

Answer: C

Question: 356

Refer to the exhibit.

```
adninJSourcefire3D:'$ cat /var/log/messages
Sourcefire3D SF-IMS[2OC4]: [2011] CloudAgent:lFReputation [HARN] Cannot download
  Sourcefire_Intelligence_Feed
Sourcefire3D SF-IMS[24085]: [24090] CloudAgent:IPReputation [WARN] Download unsucessful: Failure when
  receiving data from the peer
```

Refer to the exhibit. A Cisco Secure Firewall Management Center, 7.0 device fails to receive intelligence feed updates. The Cisco Secure Firewall Management Center is configured to use a proxy server that performs SSL inspection. Which action allows the Cisco Secure Firewall Management Center device to download the intelligence feed updates?

A. Install a self-signed certificate on the proxy server for intelligence.sourcefire.com.
B. Verify that the proxy server can use HTTPS to communicate to the internet.
C. Ensure that proxy authentication is disabled for the Cisco Secure Firewall Management Center device.
D. Bypass the proxy server for intelligence.sourcefire.com.

Answer: D

Question: 357

Refer to the exhibit.

```
fMC: System > Mzr.it      or > [FTDv] > Advanced Troubleshooting > Capture      //Trace

1: 209.165.201.6€.4       3413 > 2 39.165.202.13:. 3:::: S 134909:467:1349:3:      467(0) win
£4240 <mss 1382,sac 2:    kOK,timestamp 1421692252 O.ncp.wscale 7> .8080 >
209.165.202.100           209.165.201.66.43410: R 0:0(0) ack 134939               3468 win 0
3: 209.165.201.66.        36438 > 209.165.202.143.8081: S 2008074308:200807       4308(0) win
64240 <3*s 1390.3a 4:     ckOK,timestamp 1425272499 O.ncp.wscale 7> >
209.165.202.143           209.165.201.66 icmp: host 209.165.202.143 unre          achable -
admin prohibited f 5:     liter
209.165.201.66.           36438 > 209.165.202.143.8.91: S 2008074338:20083'       4308(G) win
64240 <mss 1390,3a        ckOK,timestamp 14252'3501 O.ncp.wscale 7>
6: 2 39.165.202.143       > 209.165.201.66 loop: host 209.165.202.143 unre        achat1€ •
admin prohibited f
                          36438 > 209.165.202.143.8081: S 2008074308:200807
64240 <mss 1330.3a        CkOK,timestamp 1425275517 O.ncp.wscale 7> >
6: 209.165.202.143        209.165.201.66 icmp: host 209.165.202.143 unre          achable -
admin prohibited f 9:     liter
209.165.201.66.           36438 > 209.165.202.143.SCSI: 3 2008074308:2008 2-7     4308(0) win
64240 <mss 1390,38        ckOK,timestamp 1425279677 O.ncp.wscale 7> >
10: 209.165.202.143       209.165.201.66 icmp: best 209.165.202.143 unre          achatle -
attain prohibited fi 11:
209.165.201.66.           36436 > 209.165.202.143.8081: S 2008074308:200807       4308(0) win
64240 <333 1360,sac       kOK,timestamp 1425287869 O.ncp.wscale 7>
12: 209.165.202.143       > 209.165.201.66 iemp: hest 209.165.202.143 unre        dCodvi^ •
attain prohibited fi
13: 209.165.201.66.       36436 > 2.9.165.202.143,:.81: S 16.4482258:16344s       2258(0) win
64242 <a33 1380,sac 14?   kOK,timestamp 1425333997 0,ncp,wscala 7> > 209.165.201.66
205.Ic5.202.143           icmp: hest 209.165.202.143 unre                         achable -
admin prohibited fi 15:
209.165.201.66.           36438 > 209.165.202.143.8081: S 2230966104:223096       6104(0) win
64240 <3133 1390,sac      kOK,timestamp 1425336509 O.ncp.wscale 7> >
16: 209.165.202.143       209.165.201.66 irmp: host 209.165.202.143 unre
admin prohibited fi
```

Refer to the exhibit. Users attempt to connect to numerous external resources on various TCP ports. If the users mistype the port, their connection closes immediately, and it takes more than one minute before the connection is torn down. An engineer manages to capture both types of connections as shown in the exhibit. What must the engineer configure to lower the timeout values for the second group of connections and resolve the user issues?

A. outbound access rule that allows the entire ICMP protocol suite B. inbound access rule that allows ICMP Type 3 from outside C. inbound access rule that allows TCP reset packets from outside D. outbound access rule with the Block with reset action

Answer: D

Question: 358

A network administrator is configuring a transparent Cisco Secure Firewall Threat Defense registered to a Cisco Secure Firewall Management Center. The administrator wants to configure the Secure Firewall Threat Defense to allow ARP traffic to pass between two interfaces of a bridge group. What must be configured?

A. Use the default configuration on the devices.

B. An access policy must allow MAC address FFFF.FFFF.FFFF.
C. ARP inspection must be disabled.
D. An access policy must allow MAC address 0100.0CCC.CCCD.

Answer: A

Question: 359

Refer to the exhibit.

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

A. Disable Option 82 in the DHCP relay configuration properties using Secure Firewall Management Center.
B. Add access rules that allow DHCP traffic by using Cisco Secure Firewall Management Center.
C. Add another DHCP pool on Server_A with DHCP relay on Secure Firewall Threat Defense.
D. Disable all the DHCP Snort rules by using Secure Firewall Device Manager.

Answer: B

Question: 360

A network administrator manages a network with multiple firewalls in a datacenter using Cisco Secure Firepower Management Center. The administrator must change a next-generation firewall from routed to transparent mode. Which action must the administrator take next to meet the requirement?

A. Deregister the firewall in Cisco Secure Firewall Management Center.
B. Enter the configure transparent firewall command from the CLI.

C. Create one or more bridge groups from the CLI.

D. Manually delete the interface configuration from the CLI.

Answer: A

Question: 361

DRAG DROP

```
ASA# show interface | include ",|MAC|Member
Interface GigabitEthernet1/1 "inside", is up, line protocol is up
        MAC address e4aa.5ae4.612e, MTU 1500
Interface GigabitEthernet1/2 "outside", is up, line protocol is up
        MAC address e4aa.5ae4.612f, MTU 1500
Interface GigabitEthernet1/3 "", is up, line protocol is up
        MAC address 500f.8000.bbb5, MTU 1500
Interface GigabitEthernet1/4 "", is up, line protocol is up
        MAC address 500f.8000.bbb6, MTU 1500
Interface GigabitEthernet1/5 "", is up, line protocol is up
        MAC address 500f.8000.bbb7, MTU 1500
Interface GigabitEthernet1/6 "", is up, line protocol is up
        MAC address 500f.8000.bbb8, MTU 1500
Interface GigabitEthernet1/7 "", is up, line protocol is up
        MAC address 500f.8000.bbb9, MTU 1500
Interface GigabitEthernet1/8 "", is up, line protocol is up
        MAC address 500f.8000.bbba, MTU 1500
Interface Management1/1 "", is up, line protocol is up
        MAC address 500f.8000.bbb2, MTU 1500
Interface Redundant1 "Redundant1", is up, line protocol is up
        MAC address 500f.8000.bbb7, MTU 1500
        Member GigabitEthernet1/5(Active), GigabitEthernet1/4
```

Refer to the exhibit. An engineer must configure a connection on a Cisco ASA Firewall with a Cisco Secure Firewall Services Module to ensure that the secondary interface takes over all the functions of the primary interface if the primary interface fails. Drag and drop the code snippets from the bottom onto the boxes in the CLI commands to configure the failover. Not all options are used.

```
ASA(config)#interface Redundant1
ASA(config-if)# GigabitEthernet1/5
ASA(config-if)# member-interface GigabitEthernet1/4
ASA(config-if)# nameif Redundant1
ASA(config-if)# security-level 20
ASA(config-if)# ip address 172.16.47.1
ASA(config-if)# end

ASA# show version | include Gigabit.*address is
  1: Ext: GigabitEthernet1/1  : address is 500f.8000.bbb3, irq 255
  2: Ext: GigabitEthernet1/2  : address is 500f.8000.bbb4, irq 255
  3: Ext: GigabitEthernet1/3  : address is 500f.8000.bbb5, irq 255
  4: Ext: GigabitEthernet1/4  : address is 500f.8000.bbb6, irq 255
  5: Ext: GigabitEthernet1/5  : address is 500f.8000.bbb7, irq 255
  6: Ext: GigabitEthernet1/6  : address is 500f.8000.bbb8, irq 255
  7: Ext: GigabitEthernet1/7  : address is 500f.8000.bbb9, irq 255
  8: Ext: GigabitEthernet1/8  : address is 500f.8000.bbba, irq 255
```

member-interface GigabitEthernet1/5	member-interface GigabitEthernet1/4
GigabitEthernet1/5	backup interface GigabitEthernet1/4
Redundant1	reactivation mode timed
failover link Redundant1 GigabitEthernet1/4	

Answer:

Explanation:
ASA (config)# interface (Reduntant 1),ASA(config-if) #(GigabitEthernet 1/5), ASA(config-if) #(member-interface GigabitEthernet ¼)

Question: 362

An engineer must configure an inline set on a Cisco Secure IPS by using the Cisco Secure Firewall Management Center. The inline set must make a copy of each packet before analyzing the packet and block any connections that do not complete the three-way handshake. These configurations have been performed already:

Select and enable the interfaces that will be added to the inline set.

Configure the speed and duplex.

Configure the inline set and add the interfaces to the inline set.

Which action completes the task?

A. Set Tap Mode to Inline.
B. Configure Snort Fail Open.
C. Configure Link State Propagation.
D. Implement Strict TCP Enforcement.

Answer: D

Question: 363

An engineer must perform a packet capture on a Cisco Secure Firewall Threat Defense device to confirm the MAC

address of the host using IP address 192.168.100.100 while troubleshooting an ARP issue. What is the correct tcpdump command syntax to ensure that the MAC address appears in the packet capture output?

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

B. -nm src 192.168.100.100

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

D. -ne src 192.168.100.100

Answer: D

Question: 364

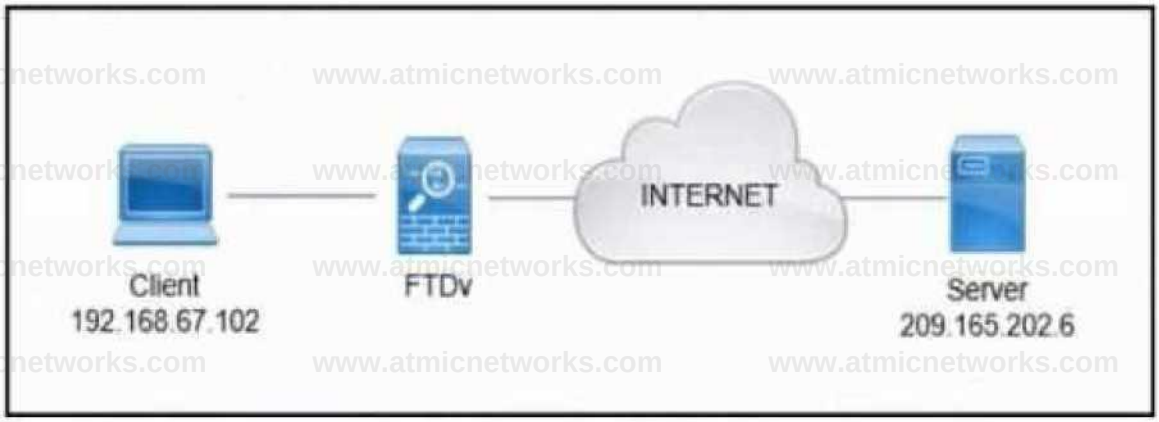
Refer to the exhibit.

```
HC: System > Monitor > IFTEVJ > Advanced TrsuhleshMting > racket Tracer

Interface: iMin> lack** type: TCf» source: 192.146.4*.102, Source Sort; P3$l« lestiMtlcn: 229.1(5.202.4, JesttMtiM fort: 40
(redacts outoutl

- Shoe: 1
Type: XiroT-M30IS*10CKV>, Subtype: Active Egress Interface. Result: ALLCW found next-hop 209.145.301.3 or tn? egress if:
public(vrfid:3)
Him: 2
Type: ACCHS-UST, Subtype: leg, Result: ALLOW
Config: access-list OK TW ATL^ teaair rule-id 2m3U5i: SSX8: AUflWjmfd . Phase: 3
Type: COBW-SETTINM. Result: ALLOW fnase: <
Type: MAT. Result: ALLOW
Conffgr
object networc SETS"
Mt (inside,public] CYMRIC IH?
- Additional Lnliicaticn: Lynamic translate 3$2.1cl.ft.lG2'dU to 192.If!.<".<*' • SUSI
Phase: S - 10
Result: ALLOW
. Share: 11
Type; ABJAOBKE-WOWP. subtype: Resolve ftxtbop If suite:: to NBC. Result:
> ALUN
Additional Infaraation: Found adjacency entry for Mat-hop 209.143.201.2 on
* Interface public
Adjacency tActive, MAT address C34c.29fc.41c3 bits $524 reference J

Result:
input-interface: inside (vrfid:0)
input-status: up
input-line-status: up
output-interface: publicivrfid:0• - output-status: up
3 output-line-status: up
```



Refer to the exhibit. A client that has IP address 192.168.67.102 reports issues when connecting to a remote server. Based on the topology and output of packet tracer tool, which action resolves the connectivity issue?

A. Add the route to the destination.

B. Unblock the access rule on FTDv.

C. Restart the client-side application.
D. Reconfigure NAT on FTDv.

Answer: D

Question: 365

An engineer is integrating Cisco Secure Endpoint with Cisco Secure Firewall Management Center in high availability mode. Malware events detected by Secure Endpoint must also be received by Secure Firewall Management Center and public cloud services are used. Which two configurations must be selected on both high availability peers independently? (Choose two.)

A. internet connection
B. Smart Software Manager Satellite
C. Cisco Success Network
D. security group tag
E. Secure Endpoint Cloud Connection

Answer: A, E

Question: 366

What is the role of realms in the Cisco ISE and Cisco Secure Firewall Management Center integration?

A. TACACS+ database
B. AD definition
C. Cisco Secure Firewall VDC
D. Cisco ISE context
E. (Option not provided – please confirm or provide)

Answer: C

Question: 367

An engineer must investigate a connectivity issue by using Cisco Secure Firewall Management Center to access the Packet Capture feature on a Cisco Secure Firewall Threat Defense device. The engineer must see a real packet going through the Secure Firewall Threat Defense device and the Snort detection actions. While reviewing the packet capture, the engineer discovers that the Snort detection actions are missing. Which action must the engineer take to resolve the issue?

A. Specify the packet size.
B. Specify the buffer size.
C. Enable the Continuous Capture option.
D. Enable the Trace option.

Answer: D

Question: 368

An engineer is setting up a new Cisco Secure Firewall Threat Defense appliance to replace the current firewall. The company requests that inline sets be used and that when one interface in an inline set goes down, the second interface in the inline set goes down. What must the engineer configure to meet the deployment requirements?

A. strict TCP enforcement
B. propagate link state
C. Snort fail open
D. inline tap mode

Answer: C

Question: 369

Which feature sets up multiple interfaces on a Cisco Secure Firewall Threat Defense to be on the same subnet?

A. EtherChannel
B. SVI
C. BVI
D. security levels

Answer: C

Question: 370

Refer to the exhibit.

Refer to the exhibit. An engineer is configuring a high-availability solution that has the hardware devices and software versions:

two Cisco Secure Firewall 9300 Security Appliances with FXOS SW 2.0(1.23)

software Cisco Secure Firewall Threat Defense 6.0.1.1 (build 1023) on both appliances one Cisco Secure Firewall Management Center with SW 6.0.1.1 (build 1023)

Which condition must be met to complete the high-availability configuration?

A. DHCP must be configured on at least one firewall interface.
B. The version numbers must have the same patch number.
C. Both firewalls must have the same number of interfaces.
D. Both firewalls must be in transparent mode.

Answer: C

Question: 371

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

A. Custom
B. View
C. System

D. None

Answer: D

Question: 372

A VPN administrator converted an instance of Cisco Secure Firewall Threat Defense, which is managed by Cisco Secure Firewall Management Center, from using LDAP to LDAPS for remote access VPN authentication. Which certificate must be added to allow for remote users to authenticate over the VPN?

A. LDAPS server certificate must be added to Secure Firewall Management Center realms.
B. Secure Firewall Management Center certificate must be added to the LDAPS server.
C. LDAPS server certificate must be added to Secure Firewall Threat Defense.
D. Secure Firewall Threat Defense certificate must be added to the LDAPS server.

Answer: C

Question: 373

An engineer must integrate a third-party security intelligence feed with Cisco Secure Firewall Management Center. Secure Firewall Management Center is running Version 6.2.3 and has 8

GB of memory. Which two actions must be taken to implement Threat Intelligence Director? (Choose two.)

A. Enable REST API access.
B. Add a TAXII server.
C. Add the URL of the TAXII server.
D. Upgrade to version 6.6.
E. Add 7 GB of memory.

Answer: A, E

Question: 374

An engineer must permit SSH on the inside interface of a Cisco Secure Firewall Threat Defense device. SSH is currently permitted only on the management interface. Which type of policy must the engineer configure?

A. platform policy
B. access control policy
C. NAT policy
D. intrusion policy

Answer: A

Question: 375

After a network security breach, an engineer must strengthen the security of the corporate network. Upper management must be regularly updated with a high-level overview of any occurring network threats. Which access must the engineer provide upper management to view the required data from Cisco Secure Firewall Management Center?

A. Analysis > Status with a sliding time window of one day
B. Events by priority and classification and set a sliding time window of one day
C. Reports with a daily recurring task that generates based on the network risk report template
D. Security Intelligence Statistics dashboard set to Show the Last option to one day

Answer: C

Question: 376

DRAG DROP

An engineer must configure high availability on two Cisco Secure Firewall Threat Defense appliances.

Drag and drop the configuration steps from the left into the sequence on the right.

Configure the primary unit for high availability.	step 1
Configure failover criteria for health monitoring.	step 2
Configure the two units for high availability.	step 3
Configure the secondary unit for high availability.	step 4

Answer:

Explanation:

Step 1(Configure the primary unit for high availability), Step 2(Configure the secondary unit for high availability), Step 3(Configure the two units for high availability), Step 4(Configure failover criteria for health monitoring)