Cisco

Exam Questions 300-710

Securing Networks with Cisco Firepower (SNCF)

NEW QUESTION 1
- (Exam Topic 5)
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

NEW QUESTION 2
- (Exam Topic 5)
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

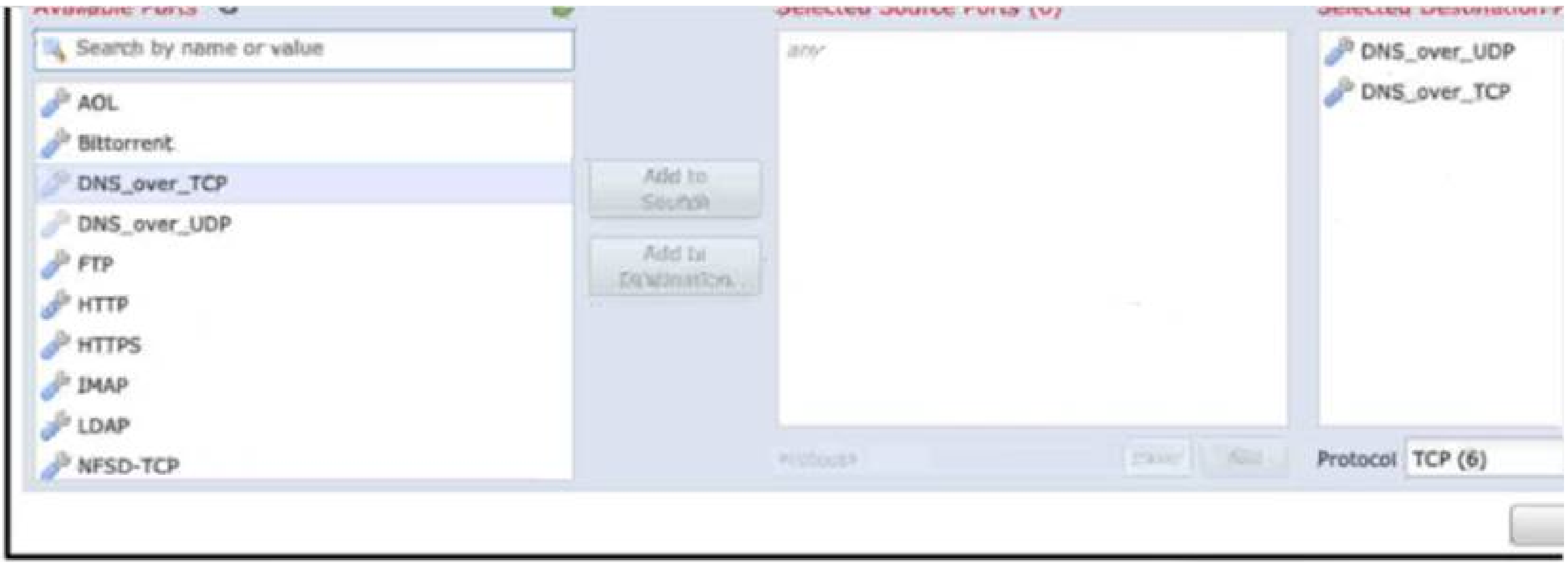
Answer: D

NEW QUESTION 3
- (Exam Topic 5)
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

NEW QUESTION 4
- (Exam Topic 5)
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

NEW QUESTION 5
- (Exam Topic 5)
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

NEW QUESTION 6
- (Exam Topic 5)
Due to an Increase in malicious events, a security engineer must generate a threat report to include intrusion events, malware events, and security intelligence events. How Is this information collected in a single report?

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

Answer: D

NEW QUESTION 7
- (Exam Topic 5)
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

NEW QUESTION 8
- (Exam Topic 5)
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

NEW QUESTION 9
- (Exam Topic 5)
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 CiscoFTD.
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

NEW QUESTION 10
- (Exam Topic 5)
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

NEW QUESTION 10
- (Exam Topic 5)
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

NEW QUESTION 11
- (Exam Topic 5)
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

NEW QUESTION 13
- (Exam Topic 5)
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

NEW QUESTION 18
- (Exam Topic 5)
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

NEW QUESTION 22
- (Exam Topic 5)
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.

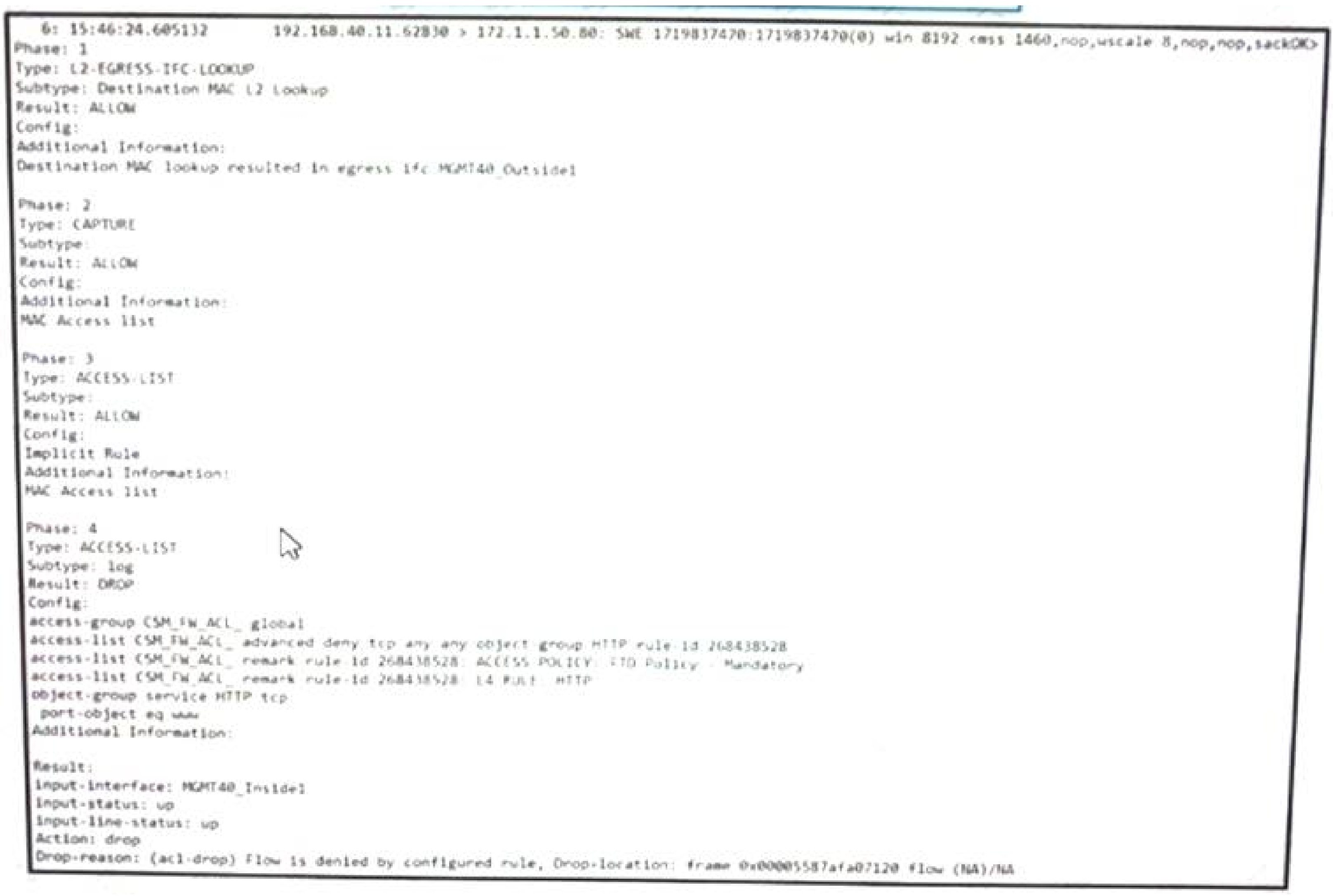
Answer: A

NEW QUESTION 26
- (Exam Topic 5)
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

NEW QUESTION 31
- (Exam Topic 5)
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

NEW QUESTION 36
- (Exam Topic 5)
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

NEW QUESTION 39
- (Exam Topic 5)
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.

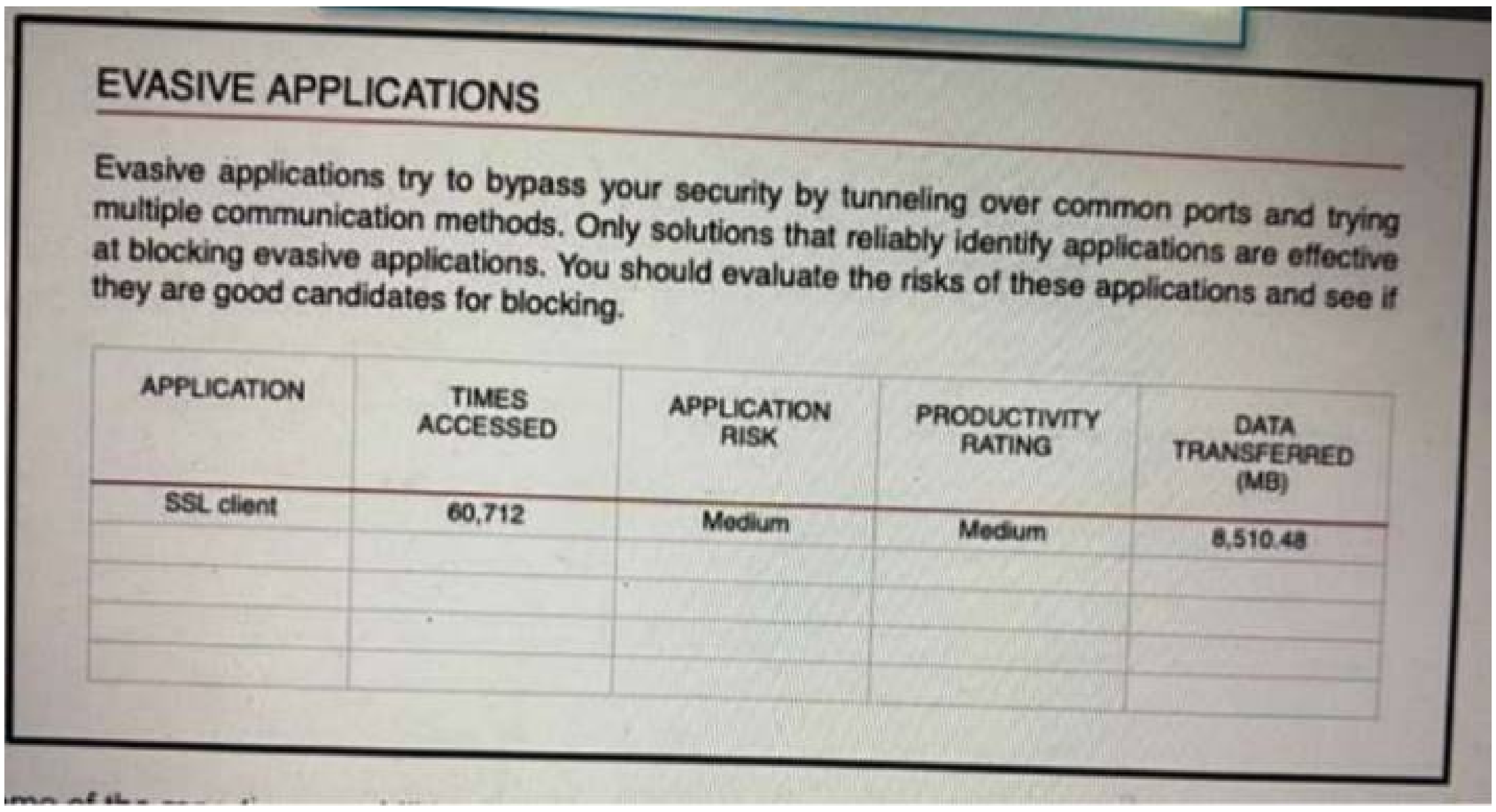
Answer: D

NEW QUESTION 41
- (Exam Topic 5)
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

NEW QUESTION 43
- (Exam Topic 5)
Refer to the exhibit.



EVASIVE APPLICATIONS

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

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

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

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

Answer: A

NEW QUESTION 45
- (Exam Topic 5)
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

NEW QUESTION 50
- (Exam Topic 5)
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

NEW QUESTION 51
- (Exam Topic 5)
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

NEW QUESTION 56
- (Exam Topic 5)
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 onlysecure 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

NEW QUESTION 57
- (Exam Topic 5)
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

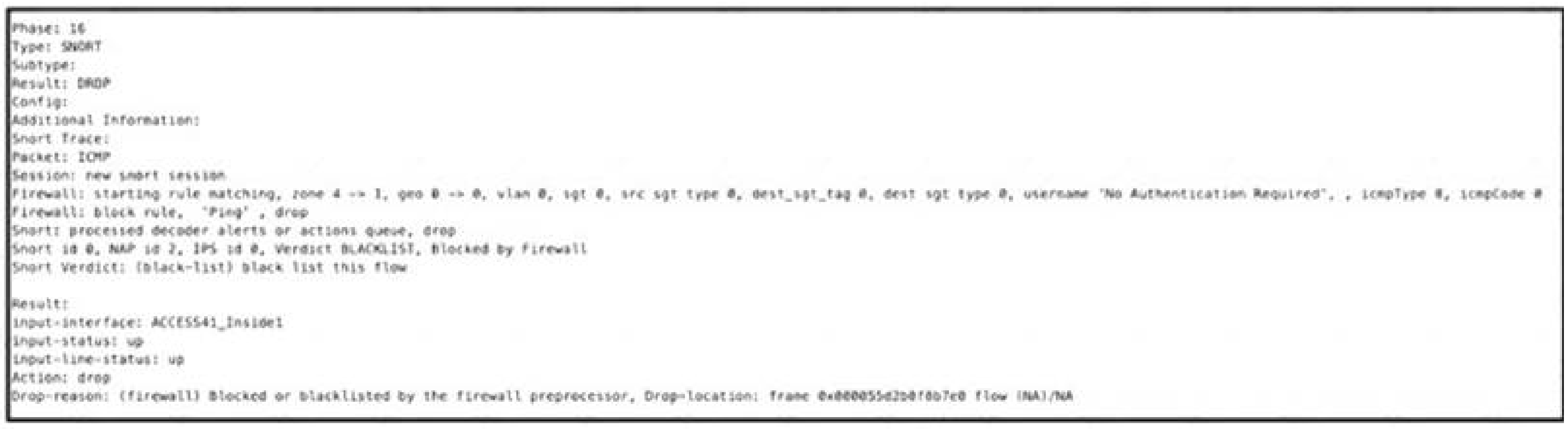
Answer: B

NEW QUESTION 58
- (Exam Topic 5)
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

NEW QUESTION 62
- (Exam Topic 5)
Refer to the exhibit.



```
Phase: 16
Type: SNORT
Subtype:
Result: DROP
Config:
Additional Information:
Snort Trace:
Packet: ICMP
Session: new snort session
Firewall: starting rule matching, zone 4 -> 1, geo 0 -> 0, vlan 0, sgt 0, src sgt type 0, dest_sgt_tag 0, dest sgt type 0, username 'No Authentication Required', , icmpType 0, icmpCode 0
Firewall: block rule,  'Ping' , drop
Snort: processed decoder alerts or actions queue, drop
Snort id 0, NAP id 2, IPS id 0, Verdict BLACKLIST, Blocked by Firewall
Snort Verdict: (black-list) black list this flow

Result:
input-interface: ACCESS41_Inside1
input-status: up
input-line-status: up
Action: drop
Drop-reason: (firewall) Blocked or blacklisted by the firewall preprocessor, Drop-location: frame 0x000055d2b0f0b7e0 flow (NA)/NA
```

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

NEW QUESTION 67
- (Exam Topic 5)
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

NEW QUESTION 69
- (Exam Topic 5)
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 us
B. so QoS cannot be added
C. The network segments that the interfaces are on do not have contiguous IP space
D. QoS is available only on routed interfaces, and this device is in transparent mode.
E. A conflict exists between the destination interface types that is preventing QoS from being added

Answer: C

NEW QUESTION 74
- (Exam Topic 5)
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

NEW QUESTION 77
- (Exam Topic 5)
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

NEW QUESTION 78
- (Exam Topic 5)
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

NEW QUESTION 80
- (Exam Topic 5)
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

NEW QUESTION 82
- (Exam Topic 5)
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

NEW QUESTION 87
- (Exam Topic 5)
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 FM
C. configure cluster members in Cisco FMC, create cluster in Cisco FM
D. and configure cluster members in Cisco FMC.
E. Configure the Cisco FTD interfaces and cluster members, add members to Cisco FM
F. and create the cluster in Cisco FMC.
G. 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

NEW QUESTION 88
- (Exam Topic 5)
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

NEW QUESTION 92
- (Exam Topic 5)
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

NEW QUESTION 97
- (Exam Topic 5)
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

NEW QUESTION 99
- (Exam Topic 5)
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

NEW QUESTION 101
- (Exam Topic 5)
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-M

NEW QUESTION 102
- (Exam Topic 5)
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

NEW QUESTION 104
- (Exam Topic 5)
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

NEW QUESTION 105
- (Exam Topic 5)
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

NEW QUESTION 110
- (Exam Topic 5)
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

NEW QUESTION 113
- (Exam Topic 4)
Which two remediation options are available when Cisco FMC is integrated with Cisco ISE? (Choose two.)

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

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

NEW QUESTION 117
- (Exam Topic 4)
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

NEW QUESTION 121
- (Exam Topic 3)

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

NEW QUESTION 123
- (Exam Topic 3)
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

NEW QUESTION 126
- (Exam Topic 2)
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

NEW QUESTION 127
- (Exam Topic 3)
Which two statements about deleting and re-adding a device to Cisco FMC are true? (Choose two.)

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

Answer: 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

NEW QUESTION 129
- (Exam Topic 2)
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

NEW QUESTION 133
- (Exam Topic 2)
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

NEW QUESTION 135
- (Exam Topic 2)
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-verif

NEW QUESTION 140
- (Exam Topic 2)
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

NEW QUESTION 141
- (Exam Topic 2)
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

NEW QUESTION 144
- (Exam Topic 2)
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

NEW QUESTION 146
- (Exam Topic 2)
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

NEW QUESTION 148
- (Exam Topic 2)
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

NEW QUESTION 152
- (Exam Topic 1)
A Cisco FTD has two physical interfaces assigned to a BVI. Each interface is connected to a different VLAN on the same switch. Which firewall mode is the Cisco FTD set up to support?

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

Answer: B

NEW QUESTION 157
- (Exam Topic 1)
When deploying a Cisco ASA Firepower module, an organization wants to evaluate the contents of the traffic without affecting the network. It is currently configured to have more than one instance of the same device on the physical appliance Which deployment mode meets the needs of the organization?

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

Answer: A

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

NEW QUESTION 162
- (Exam Topic 1)
A network engineer implements a new Cisco Firepower device on the network to take advantage of its intrusion detection functionality. There is a requirement to analyze the traffic going across the device, alert on any malicious traffic, and appear as a bump in the wire How should this be implemented?

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

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.

NEW QUESTION 164
- (Exam Topic 1)
Which two deployment types support high availability? (Choose two.)

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

E. virtual appliance in public cloud

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

NEW QUESTION 167
......