Cisco CCNP Security SNCF 300-710 PassFast

Securing Networks with Cisco Firepower (300-710 SNCF)

Todd Lammle
CCNP Security Expert Trainer

TL TODD LAMMLE

CCNP Security SNCF PassFast Securing Networks with Cisco Firepower (300-710)

Book Update Version 1.0

This book will dive into the latest practice questions you need before you take the Cisco Firepower SNCF exam 300-710

Table of Contents

Chapter 1: Deployment

The objectives covered in this chapter:

30% 1.0 Deployment

1.1 Implement NGFW modes

1.1.a Routed mode

1.1.b Transparent mode

1.2 Implement NGIPS modes

1.2.a Passive

1.2.b Inline

1.3 Implement high availability options

1.3.a Link redundancy

1.3.b Active/standby failover

1.3.c Multi-instance

1.4 Describe IRB configurations

1. Which of the following is the command issued from the CLI when logged into an FTD unit used to determine whether the unit is managed locally or remotely?
A. show managers
B. show configuration session
C. system generate-troubleshoot
D. show running-config | include manager

2. Which protocol listed establishes network redundancy in a switched Firepower device deployment?
A. STP
B. VRRP
C. ICMP
D. GLBP

3. Which of the following is a behavior of a Cisco FMC database purge?
A. The appropriate process is restarted.
B. User login and history data are removed from the database if the User Activity check box is chosen.
C. Data can be recovered from the device.
D. The specified data is removed from the Cisco FMC and archived for two weeks.

4. What is the result of enabling Cisco Firepower Threat Defense clustering?
A. For the dynamic routing feature, if the master unit fails, the newly elected master 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.

5. The following two functions are available on a Cisco FTD: Inline tap and Inline. What is the difference between the two?
A. Inline mode can drop malicious traffic.
B. Inline mode cannot do SSL decryption.
C. Inline tap mode does full packet capture.
D. Inline tap mode can send a copy to the traffic to another device.

6. What are two ways access control policies operate on a Cisco Firepower system? (Choose two).
A. They can block traffic based on Security Intelligence data.
B. The system performs intrusion prevention followed by file inspection.
C. File policies use an associated variable set to perform intrusion prevention.
D. The system performs a preliminary inspection based on trusted traffic to validate it matches trusted parameters.
E. Traffic inspection can be interrupted temporarily when configuration changes are deployed.

7. Which two object types are reusable and supported by the Cisco FMC? (Choose two).
A. Reputation-based objects that represent Security Intelligence feeds and lists, application filters based on category and reputation, and file lists.
B. Reputation-based objects, such as URL categories.
C. Network-based objects that represent IP addresses and networks, ports and/or protocols, VLAN tags, security zones, and origin/destination country.
D. Network-based objects that represent FQDN mappings and networks, port and/or protocol pairs, VXLAN tags, security zones, and origin/destination country.
E. Dynamic key mapping objects that help link HTTP and HTTPs GET requests to layer 7 protocols.

8. When deploying a network-monitoring tool to manage and monitor networking devices, you realize you need to manually upload a MIB for the Cisco FMC. Which folder from would you upload the MIB file into?
A. system/etc/DCEALERT.MIB
B. /etc/sf/DCEALERT.MIB
C. /sf/etc/DCEALERT.MIB

D. /etc/sf/DCMIB.ALERT

9. What is the disadvantage of setting up site-to-site VPN in a clustered-units environment?
A. VPN connections can be re-established only if the failed master unit recovers.
B. VPN connections must be re-established when a new master unit is elected.
C. Only established VPN connections are maintained when a new master unit is elected.
D. Smart License is required to maintain VPN connections simultaneously across all cluster units.

10. Which Firepower feature allows users to configure bridges in routed mode and enables devices to perform Layer 2 lookups?
A. IRB
B. BDI
C. SGT
D. FlexConfig

11. Which policy rule is included in the deployment of a local DMZ during a Cisco NGFW initial deployment using the Cisco Firepower Management Console GUI?
A. deny ip any any
B. permit ip any
C. no policy rule is included
D. a default DMZ policy rule for which only a user can change the IP address

12. Which two of the following are application layer preprocessors? (Choose two).
A. CIFS
B. SSL
C. ICMP
D. IMAP
E. DNP3

13. Which two statements about deleting and re-adding a device to the Cisco FMC are true? (Choose two).
A. Before re-adding the device in the FMC, you must add the manager back

in the device.
B. No option to re-apply NAT and VPN policies during registrations is available so user need to re-apply the configuration before the registration is completed.
C. An option to re-apply NAT and VPN policies during registrations is available so users do not need to re- apply the configuration before the registration is completed.
D. No option to delete and re-add a device is available in the Cisco FMC web interface.
The Cisco FMC web interface prompts users to re-apply access control policies.

14. What is the maximum number of report templates the Cisco Firepower Management Center supports?
A. 5
B. 10
C. 64
D. Unlimited

15. What is the functionality of port objects in the Cisco FMC?
A. To represent all protocols in the same way
B. To represent protocols other than TCP, UDP, and ICMP
C To add any protocol other than TCP or UDP for source port conditions in access control rules
D. To mix transport protocols when setting both source and destination port conditions in a rule

16. Which of the following is a report template field format available in the Cisco FMC?
A. Box level chart
B. Benchmark chart
C. Arrow chart
D. Bar chart

17. Which of the following represent the minimum requirements to deploy a managed device inline?
A. Inline interface, MTU, and mode.
B. Passive interface, security zone, MTU, and zone.
C. Inline interfaces, security zones, MTU, and mode.

D. Passive interface, MTU, and mode.

18. Which two of the following are deployment types that support HA (high availability)?
A. Routed
B. Transparent
C. Clustered
D. Intra-chassis multi-instance pretense
E. Virtual appliance in a public cloud

19. Which policy is used to capture host information on the Cisco Next Generation Intrusion Prevention System?
A. Network discovery
B. Correlation
C. Intrusion
D. Access control

20. Which two routing options are valid with Cisco Firepower threat Defense version 6.0? (Choose two).
A. ECMP with up to three equal cost paths across multiple interfaces
B. BGPv6
C. BGPv4 with nonstop forwarding
D. BGPv4 unicast address family
E. ECMP with up to four equal cost paths

21. Which three access control actions permit traffic to pass through the device when using Cisco Firepower? (Choose three).
A. Pass
B. Trust
C. Monitor
D. Allow
E. Permit
F. Inspect

22. Which SSL traffic decryption feature is used when decrypting traffic from an external host to a server on your network?
A. Decrypt by stripping the server certificate.
B. Decrypt by resigning the server certificate
C. Decrypt with a known private key

D. Decrypt with a known public key

23. Which option lists the minimum requirements to deploy a managed device inline?
A. Passive interface, security zone, MTU, and link mode.
B. Passive interface, MTU, MDI/MDIX, and link mode.
C. Inline interfaces, MTU, MDI/MDIX, and link mode.
D. Inline interfaces, security zones, MTU, and link mode.

24. When deploying Cisco Firepower appliances, which option must you configure to enable VLAN rewriting?
A. Hybrid interfaces
B. Virtual switch
C. Virtual router
D. Inline set

25. Which Cisco AMP file disposition is valid?
A. Pristine
B. Malware
C. Dirty
D. Nonmalicious
E. Mostly Clean

Chapter 1: Answers

1. Which of the following is the command issued from the CLI when logged into an FTD unit used to determine whether the unit is managed locally or remotely?

A. show managers

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

A. STP

3. Which of the following is a behavior of a Cisco FMC database purge?

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

You can use the database purge page to purge discovery, identity, connection, and Security Intelligence data files from the FMC databases. Note that when you purge a database, the appropriate process is restarted. Purging a database removes the data you specify from the Firepower Management Center. After the data is deleted, it cannot be recovered. Check the Network Discovery Events check box to remove all network discovery events from the database. Check the Hosts check box to remove all hosts and Host Indications of Compromise flags from the database. Check the User Activity check box to remove all user activity events from the database. Check the User Identities check box to remove all user login and user history data from the database as well as User Indications of Compromise flags.

4. What is the result of enabling Cisco Firepower Threat Defense clustering?

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

VPN functionality is limited to the master unit and does not take advantage of the cluster high availability capabilities. If the master unit fails, all existing VPN connections are lost, and VPN users will see a disruption in service. The routing process only runs on the master unit, and routes are learned through the master unit and replicated to secondaries. If there is a master unit switchover, the neighboring router will detect a restart; the switchover is not transparent. Clustering is only supported for the FTD device on the Firepower 9300 and the Firepower 4100 series. These features cannot be configured with clustering enabled, and the commands will be rejected.

5. The following two functions are available on a Cisco FTD: Inline tap and Inline. What is the difference between the two?

A. Inline mode can drop malicious traffic.

An inline deployment can prevent intrusion and block malicious traffic in real time (but not in passive or a tap implementation). In an inline deployment, the Firepower System processes the TLS/SSL handshake, potentially modifying the ClientHello message and acting as a TCP proxy server for the session. Inline tap mode "can" do full packet capture but does not do full packet capture by default (i.e. that's not the purpose of "inline tap mode"). Inline tap mode does not send traffic to another device, it passively monitors traffic passing across the interface pairs.

6. What are two ways access control policies operate on a Cisco Firepower system? (Choose two).

A. They can block traffic based on Security Intelligence data.

Traffic inspection can be interrupted temporarily when configuration changes are deployed. Intrusion policies are paired with variable sets, which allow you to use named values to accurately reflect your network environment. Changing the total number of intrusion policies used by an access control policy restarts the Snort process when you deploy configuration changes, temporarily interrupting traffic inspection.

7. Which two object types are reusable and supported by the Cisco FMC? (Choose two).

A. Reputation-based objects that represent Security Intelligence feeds and lists, application filters based on category and reputation, and file lists.
C. Network-based objects that represent IP addresses and networks, ports and/or protocols, VLAN tags, security zones, and origin/destination country.

The following partial table lists reusable object types supported by FMC supported with the FMC REST API.
Network – Yes
Port - Yes Protocol – Yes
VLAN – Yes
Security Zones – Yes
Geolocation – Yes
Security Intelligence – Yes
Application Filters – Yes
File Lists - Yes

8. When deploying a network-monitoring tool to manage and monitor networking devices, you realize you need to manually upload a MIB for the Cisco FMC. Which folder from would you upload the MIB file into?

B. /etc/sf/DCEALERT.MIB

If your network management system requires a management information base file (MIB), you can obtain it from the Firepower Management Center at /etc/sf/DCEALERT.MIB.

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

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

For centralized features, if the master unit fails, all connections are dropped, and you have to re-establish the connections on the new master unit.

10. Which Firepower feature allows users to configure bridges in routed mode and enables devices to perform Layer 2 lookups?

A. IRB

IRB - Integrated Routing and Bridging. Allows users to configure bridges in routed mode and enables devices to perform L2 switching between interfaces (including subinterfaces).
BDI - Bridge Domain Interface - Firepower interfaces to connect to the Cisco UCS E-Series Blade.
SGT - Security Group Tag - Use ISE to define and use security group tags (SGT) for classifying traffic in a Cisco TrustSec network.
FlexConfig - Flex Config gives a firewall administrator access to configure the underlying ASA engine (LINA in the Firepower vernacular) when there is no GUI object for the configuration change that you

wish to make

11. Which policy rule is included in the deployment of a local DMZ during a Cisco NGFW initial deployment using the Cisco Firepower Management Console GUI?

C. no policy rule is included

The ACP (Access Control Prefilter) which is set for all interfaces contains only the default rule which is set to have an 'action' of Block All Traffic. This is the 'Action' for the default 'policy', which has no policy rules defined (or included).

12. Which two of the following are application layer preprocessors? (Choose two).

B. SSL
D. IMAP

The following are application layer preprocessors: DCE/RPC, DNS, FTP, Sun, RPC, SIP, GTP, IMAP, POP, SMTP, SSH, SSL.

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

B. No option to re-apply NAT and VPN policies during registrations is available so user need to re-apply the configuration before the registration is completed.
E. The Cisco FMC web interface prompts users to re-apply access control policies.

When a device is deleted and then re-added, the Firepower Management Center web interface prompts you to re-apply your access control policies. However, there is no option to re-apply the NAT and VPN policies during registration. Any previously applied NAT or VPN configuration will be removed during registration and must be re-applied after registration is complete.

14. What is the maximum number of report templates the Cisco Firepower Management Center supports?

D. Unlimited

The Firepower System provides a flexible reporting system that allows you to quickly and easily generate multi- section reports with the event views or dashboards that appear on your Firepower Management Center. You can also design your own custom reports from scratch. You can build as many report templates as you need.

15. What is the functionality of port objects in the Cisco FMC?

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

A port object can represent other protocols that do not use ports.

16. Which of the following is a report template field format available in the Cisco FMC?

D. Bar chart

The following are report template fields:
Format - Bar / Pie / Line chart / Table View / Detail View
Table
Preset

Search or Filter
X-axis
Y-axis
and more...

17. Which of the following represent the minimum requirements to deploy a managed device inline?

C. Inline interfaces, security zones, MTU, and mode.

The minimum set of requirements to deploy a device inline is to set the interfaces to inline, set the security zone, verify the MTU and set the mode (to none, which makes it inline).

18. Which two of the following are deployment types that support HA (high availability)?

A. Routed
B. Transparent

You determine how to configure device high availability depending on your Firepower System deployment: passive, inline, routed, or switched (transparent).

19. Which policy is used to capture host information on the Cisco Next Generation Intrusion Prevention System?

A. Network discovery

20. Which two routing options are valid with Cisco Firepower threat Defense version 6.0? (Choose two).

A. ECMP with up to three equal cost paths across multiple interfaces
D. BGPv4 unicast address family

21. Which three access control actions permit traffic to pass through the device when using Cisco Firepower? (Choose three).

B. Trust
C. Monitor
D. Allow

22. Which SSL traffic decryption feature is used when decrypting traffic from an external host to a server on your network?

B. Decrypt by resigning the server certificate

23. Which option lists the minimum requirements to deploy a managed device inline?

D. Inline interfaces, security zones, MTU, and link mode.

24. When deploying Cisco Firepower appliances, which option must you configure to enable VLAN rewriting?

B. Virtual switch

25. Which Cisco AMP file disposition is valid?

D. Nonmalicious

Chapter 2: Configuration

The objectives covered in this chapter:

30% 2.0 Configuration

2.1 Configure system settings in Cisco Firepower Management Center

2.2 Configure these policies in Cisco Firepower Management Center

2.2.a Access control

2.2.b Intrusion

2.2.c Malware and file

2.2.d DNS

2.2.e Identity

2.2.f SSL

2.2.g Prefilter

2.3 Configure these features using Cisco Firepower Management Center

2.3.a Network discovery

2.3.b Application detectors (Open AppID)

2.3.c Correlation

2.3.d Actions

2.4 Configure objects using Firepower Management Center

2.4.a Object Management

2.4.b Intrusion Rules

2.5 Configure devices using Firepower Management

Center

2.5.a Device Management

2.5.b NAT

2.5.c VPN

2.5.d QoS

2.5.e Platform Settings

2.5.f Certificates

1. Which interface type allows packets to be dropped?
An inline set acts like a bump on the wire and binds two interfaces together to slot into an existing network. Inline interfaces receive all traffic unconditionally, but all traffic received on these interfaces is retransmitted out of an inline set unless explicitly dropped.
A. TAP
B. Inline
C. Passive
D. ERSPAN

2. Which of the following Cisco Firepower rule actions will display an HTTP warning page?
A. Interactive Block
B. Block
C. Monitor
D. Allow with Warning

3. Which of the following commands are executed on the primary FTD CLI to temporarily stop running HA (high- availability)?
A. Configure high-availability continue.
B. Configure high-availability disable.
C. Configure high-availability suspend.
D. System support network-options.

4. Which of the following FTD commands is used to associate the unit with an FMC manager located at 10.0.0.40 and has the registration key FTD1212?
A. configure manager add FTD1212 10.0.0.40
B. configure manager local FTD1212 10.0.0.40

C. configure manager add 10.0.0.40 FTD1212
D. configure manager local 10 0.0 40 FTD1212

5. Which of the following allows an interface to emulate a passive interface located on the advanced tab under inline set properties?
A. TAP mode
B. Strict TCP enforcement
C. Propagate link state
D. Transparent inline mode

6. What connector is used to integrate Cisco ISE with the Cisco FMC for Rapid Threat Containment?
A. FMC RTC
B. pxGrid
C. ISEGridlock
D. FTD RTC

7. Which object type supports object overrides?
A. DNS server group
B. Time range
C. Network object
D. Security group tag

8. A network engineer is configuring URL Filtering on Cisco FTD. Which of the following two port requirements on the Firepower Management Console must be available to allow communication with a CSP (cloud service provider)? (Choose two).
A. Inbound port TCP/80
B. Outbound port TCP/80
C. Inbound port TCP/443
D. Outbound port TCP/443
E. Outbound port TCP/8080

9. Which two packet captures does the FTD LINA engine support? (Choose two).
A. dynamic firewall importing
B. application ID service
C. Layer 7 network ID
D. protocol

E. source IP

10. Which of the following dynamic routing protocols are supported by the Cisco FTD without using FlexConfig? (Choose two).
A. IS-IS
B. Static routing
C. OSPF
D. BGP
E. EIGRP

11. Which action should be taken after editing an object that is used inside and access control policy?
A. Delete the existing object in use.
B. Redeploy the updated configuration.
C. Create another rule using a different object name.
D. Refresh the Cisco FMC GUI or CLI for the access control policy.

12. Where does a user add/modify widgets in the Cisco FMC (Firepower Management Center)?
A. Context explorer
B. Summary process
C. Dashboard
D. Reporting

13. On a Cisco FTD, which of the following two statements are true about bridge-group interfaces? (Choose two).
A. The BVI IP address must be in a separate subnet from the connected network.
B. Each directly connected network must be on the same subnet.
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. Bridge groups are supported in both transparent and routed firewall modalities.

14. Which two OSPF routing features are configured in the Cisco FMC and propagated to the Cisco FTD? (Choose two).
A. SHA authentication to OSPF packets
B. MD5 authentication to OSPF packets

C. Virtual links
D. OSPFv2 with IPv6 capabilities
E. Area border router type 1 LSA filtering

15. What CLI command is used to control special handling of ClientHello messages?
A. system support ssl-client-hello-display
B. system support ssl-client-hello-force-reset
C. system support ssl-client-hello-tuning
D. system support ssl-client-hello-reset

16. Where can threshold settings be configured? (Choose two).
A. On each IPS rule
B. Globally, per intrusion policy
C. On each access control rule
D. Per processor, within the network analysis policy
E. Globally, within the network analysis policy

17. What is the maximum size a Cisco FMC supports for its HTTPs certificates?
A. 1024
B. 2048
C. 4096
D. 8192

18. When creating an SSL policy on Cisco Firepower, which three options do you have?
A. do not decrypt
B. trust
C. allow
D. block with reset
E. block
F. encrypt

19. With Cisco Firepower Threat Defense software, which interface mode do you configure to passively receive traffic that passes the appliance?
A. Transparent
B. Routed

C. Passive
D. Inline set
E. Inline tap

20. Which Cisco Firepower setting is used to reduce the number of events received in a period of time and avoid being overwhelmed?
A. Thresholding
B. Rate-limiting
C. Limiting
D. Correlation

21. An engineer must architect an AMP private cloud deployment. What is the benefit of running in air-gaped mode?
A. Internet connection is not required for disposition.
B. Database sync time is reduced.
C. Disposition queries are done on AMP appliances.
D. A dedicated server is needed to run amp-sync.

22. With Cisco AMP for Endpoints on Windows, which three engines are available in the connector? (Choose three).
A. Ethos
B. Tetra
C. Annos
D. Spero
E. Talos
F. ClamAV

23. In Cisco Firepower 5.x and 6.0, which type of traffic causes a web page to be displayed by the appliance when Block or Interactive Block is selected as an access control action?
A. FTP
B. Decrypted HTTP
C. Encrypted HTTP
D. Unencrypted HHTP

24. Which Cisco Firepower rule action displays a HTTP warning page and resets the connection of HTTP traffic specified in the access control rule?
A. Interactive Block with Reset
B. Block
C. Allow with Warning

D. Interactive Block

25. Which CLI command is used to register a Cisco Firepower sensor to Firepower Management Center?
A. configure system add <host> <key>
B. configure manager <key> add host
C. configure manager delete
D. configure manger add <host> <key>

26. Which type of interface do you configure to receive traffic from a switch or tap, promiscuously, on a Cisco Firepower device?
A. Inline set
B. Transparent
C. Routed
D. Passive

27. Which object can be used on a Cisco Firepower appliance, but not in an access control policy rule on Cisco Firepower services running on a Cisco ASA?
A. URL
B. Security intelligence
C. VLAN
D. Geolocation

28. Which two appliances support logical routed interfaces? (Choose two).
A. FirePOWER services for ASA-5500-X
B. FP-4100-series
C. FP-8000-series
D. FP-7000-series
E. FP-9300-series

29. Which protocols can be specified in a Snort rule header for analysis?
A. TCP, UDP, ICMP, and IP
B. TCP, UDP, and IP
C. TCP, UDP, and ICMP
D. TCP, UDP, ICMP, IP, and ESP
E. TCP and UDP

30. Which two types of software can be installed on a cisco ASA-5545-X appliance? (Choose two).
A. Cisco ASAv
B. Cisco FirePOWER Appliance
C. Cisco FirePOWER services
D. Cisco ASA
E. Cisco FirePOWER management Center

31. What CLI command configures IP-based access to restrict GUI and CLI access to a Cisco Email Security appliance's administrative interface?
A. adminaccessconfig
B. sshconfig
C. sslconfig
D. ipaccessconfig

32. Which Cisco IPS CLI command shows the most fired signature?
A. show statistics virtual-sensor
B. show event alert
C. show alert
D. show version

33. Refer to the exhibit. What Cisco ESA CLI command generated the output?

Status as of: Wed May 22 16:05:13 2013 GMT
Hosts marked with '*' were down as of last delivery attempt.

#	Recipient Host	Active Recip.	Conn. Out	Deliv. Recip.	Soft Bounced	Hard Bounced
1	example.com	1	11	10078	0	1
2	acme.com	0	3	34021	0	0
3	biology.acme.com	0	9	64026	0	0
4	*chemistry.acme.com	0	2	94091	0	0
5	pluto.acme.com	0	6	75021	0	0
6	*venus.acme.com	1000	0	0	0	0
7	the.encryption.com	0	0	90649	0	0
8	the.euq.queue	0	0	1	0	0
9	the.euq.release.queue	0	0	4531	0	0

A. smtproutes
B. tophosts
C. hoststatus
D. workqueuestatus

Chapter 2: Answers

1. Which interface type allows packets to be dropped?

B. Inline

An inline set acts like a bump on the wire and binds two interfaces together to slot into an existing network. Inline interfaces receive all traffic unconditionally, but all traffic received on these interfaces is retransmitted out of an inline set unless explicitly dropped.

2. Which of the following Cisco Firepower rule actions will display an HTTP warning page?

A. Interactive Block

As part of access control, you can configure an HTTP response page to display when the system blocks web requests, using either access control rules or the access control policy default action. The response page displayed depends on how you block the session:
Block Response Page: Overrides the default browser or server page that explains that the connection was denied. Interactive Block Response Page: Warns users, but also allows them to click a button (or refresh the page) to load the originally requested site. Users may have to refresh after bypassing the response page to load page elements that did not load.

3. Which of the following commands are executed on the primary FTD CLI to temporarily stop running HA (high- availability)?

C. Configure high-availability suspend.

To suspend the HA from the FTD CLI: On the Primary FTD, run the following command and confirm configure high-availability suspend.

4. Which of the following FTD commands is used to associate the unit with an FMC manager located at 10.0.0.40 and has the registration key FTD1212?

C. configure manager add 10.0.0.40 FTD1212

Add a manager (Firepower Management Center). Use the configure manager add <IP Address> <registration key> command. The registration key is a unique key that you need to enter on both the firewall and FMC. This can be anything at all that you make up but must match on both sides.

5. Which of the following allows an interface to emulate a passive interface located on the advanced tab under inline set properties?

A. TAP mode

Inline Set advanced options include:
Tap Mode—Set to inline tap mode.
Propagate Link State—Configure link state propagation. Link state propagation automatically brings down the second interface in the inline interface pair when one of the interfaces in an inline set goes down.
Strict TCP Enforcement—To maximize TCP security, you can enable strict enforcement, which blocks connections where the three-way handshake was not completed.
Snort Fail Open—Enable or disable either or both of the Busy and Down options if you want new and existing traffic to pass without inspection (enabled) or drop (disabled) when the Snort process is busy or down.

6. What connector is used to integrate Cisco ISE with the Cisco FMC for Rapid Threat Containment?

B. pxGrid

pxGrid is used to share context collected by ISE with other products including FMC.

7. Which object type supports object overrides?

C. Network object

An object override allows you to define an alternate value for an object, which the system uses for the devices you specify. You can use object overrides with the following object types only: Network, Port, VLAN tag, and URL

8. A network engineer is configuring URL Filtering on Cisco FTD. Which of the following two port requirements on the Firepower Management Console

must be available to allow communication with a CSP (cloud service provider)? (Choose two).

B. Outbound port TCP/80
D. Outbound port TCP/443

FireSIGHT Systems use TCP ports 443/HTTPS and 80/HTTP in order to communicate with the cloud service. Confirm that the Management Center is able to perform a successful connectivity to port 80 and port 443.

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

D. protocol
E. source IP

FTD LINA Engine Capture options: Source IP, Destination IP, Protocol, Interface.

10. Which of the following dynamic routing protocols are supported by the Cisco FTD without using FlexConfig? (Choose two).

C. OSPF
D. BGP

The Firepower Threat Defense device supports several Internet protocols for routing. Open Shortest Path First (OSPF). Routing Information Protocol (RIP) Border Gateway Protocol (BGP).

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

B. Redeploy the updated configuration.

When you edit an object group used in a policy (for example, a network object group used in an access control policy), you must re-deploy the changed configuration for your changes to take effect.

12. Where does a user add/modify widgets in the Cisco FMC (Firepower Management Center)?

C. Dashboard

When adding a widget to a dashboard, you choose the tab to which you want to add the widget. Each tab can display one or more widgets in a three-column layout. After you add widgets, you can move them to any location on the tab. You cannot, however, move widgets from tab to tab.

13. On a Cisco FTD, which of the following two statements are true about bridge-group interfaces? (Choose two).

B. Each directly connected network must be on the same subnet.
C. Bridge groups are supported only in transparent firewall mode.

A bridge group is a group of interfaces that the Firepower Threat Defense device bridges instead of routes. Bridge groups are only supported in Transparent Firewall Mode. The BVI IP address must be on the same subnet as the bridge group member interfaces.

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

B. MD5 authentication to OSPF packets
C. Virtual links

Authentication - Choose the OSPF authentication: None—(Default) Disables OSPF area authentication.
Password—Provides a clear text password for area authentication, which is not recommended where security is a concern.
MD5—Allows MD5 authentication.
Virtual Link - Configure the following options for each OSPF process: Peer Router, Hello Interval, Transmit Delay, Retransmit Interval, Dead Interval, Authentication.

15. What CLI command is used to control special handling of ClientHello messages?

C. system support ssl-client-hello-tuning

The ssl-client-hello-tuning command allows you to refine how the managed device modifies ClientHello messages during SSL handshakes. This command tunes the default lists of cipher suites, elliptic curves, and

extensions that the system allows in ClientHello messages

16. Where can threshold settings be configured? (Choose two).

B. Globally, per intrusion policy
C. On each access control rule

You can set a threshold for one or more specific rules in an intrusion policy. You can set a single threshold for each. You can also modify the global threshold that applies by default to all rules and preprocessor-generated events associated with the intrusion policy.

17. What is the maximum size a Cisco FMC supports for its HTTPs certificates?

B. 2048

The FMC supports 2048-bit HTTPS certificates. If the certificate used by the FMC was generated using a public server key larger than 2048 bits, you will not be able to log in to the FMC web interface.

18. When creating an SSL policy on Cisco Firepower, which three options do you have?

A. do not decrypt
D. block with reset
E. block

19. With Cisco Firepower Threat Defense software, which interface mode do you configure to passively receive traffic that passes the appliance?

C. Passive

20. Which Cisco Firepower setting is used to reduce the number of events received in a period of time and avoid being overwhelmed?

A. Thresholding

21. An engineer must architect an AMP private cloud deployment. What is the benefit of running in air-gaped mode?

D. A dedicated server is needed to run amp-sync.

22. With Cisco AMP for Endpoints on Windows, which three engines are available in the connector? (Choose three).

A. Ethos
B. Tetra
D. Spero

23. In Cisco Firepower 5.x and 6.0, which type of traffic causes a web page to be displayed by the appliance when Block or Interactive Block is selected as an access control action?

D. Unencrypted HTTP

24. Which Cisco Firepower rule action displays a HTTP warning page and resets the connection of HTTP traffic specified in the access control rule?

A. Interactive Block with Reset

25. Which CLI command is used to register a Cisco Firepower sensor to Firepower Management Center?

D. configure manger add <host> <key>

26. Which type of interface do you configure to receive traffic from a switch or tap, promiscuously, on a Cisco Firepower device?

D. Passive

27. Which object can be used on a Cisco Firepower appliance, but not in an access control policy rule on Cisco Firepower services running on a Cisco ASA?

C. VLAN

28. Which two appliances support logical routed interfaces? (Choose two).

C. FP-8000-series
D. FP-7000-series

29. Which protocols can be specified in a Snort rule header for analysis?

A. TCP, UDP, ICMP, and IP

30. Which two types of software can be installed on a cisco ASA-5545-X appliance? (Choose two).

C. Cisco FirePOWER services
D. Cisco ASA

31. What CLI command configures IP-based access to restrict GUI and CLI access to a Cisco Email Security appliance's administrative interface?

A. adminaccessconfig

32. Which Cisco IPS CLI command shows the most fired signature?

A. show statistics virtual-sensor

33. Refer to the exhibit. What Cisco ESA CLI command generated the output?

Status as of: Wed May 22 16:05:13 2013 GMT
Hosts marked with '*' were down as of last delivery attempt.

#	Recipient Host	Active Recip.	Conn. Out	Deliv. Recip.	Soft Bounced	Hard Bounced
1	example.com	1	11	10078	0	1
2	acme.com	0	3	34021	0	0
3	biology.acme.com	0	9	64026	0	0
4	*chemistry.acme.com	0	2	94091	0	0
5	pluto.acme.com	0	6	75021	0	0
6	*venus.acme.com	1000	0	0	0	0
7	the.encryption.com	0	0	90649	0	0
8	the.euq.queue	0	0	1	0	0
9	the.euq.release.queue	0	0	4531	0	0

B. tophosts

Chapter 3: Management and Troubleshooting

The objectives covered in this chapter:

25% 3.0 Management and Troubleshooting

3.1 Troubleshoot with FMC CLI and GUI

3.2 Configure dashboards and reporting in FMC

3.3 Troubleshoot using packet capture procedures

3.4 Analyze risk and standard reports

1. In a Cisco Firepower Threat Defense access control policy rule, which of the following two actions are valid?
A. Monitor
B. Block
C. Discover
D. Stipulate
E. Block with reset

2. What are the two remediation options available when the Cisco Firepower Management Console is integrated into the Cisco ISE? (Choose two).
A. Dynamic null route configured
B. Port shutdown
C. Host shutdown
D. DHCP pool distribution
E. Quarantine

3. When creating a report template, how are you able to limit the results to only show the activity of a specific subnet?
A. Add a Table View section to the report with the Search field defined as the CIDR format network value.
B. Add an Input Parameter in the Advanced Settings of the report.
C. Select the IP Address as the X-axis for each section of the report.
D. Create a custom search in the FMC and select the search in each section of the report.

4. What is the maximum SHA level the Threat Intelligence Director supports?
A. SHA-256
B. SHA-512
C. SHA-1024
D. SHA-2048

5. Which Cisco AMP for Endpoints policy is used to only monitor endpoint

activity?
A. Windows domain controller
B. Protection
C. Triage
D. Audit

6. What is the result of specifying a QoS rule having a rate limit that is more than the maximum available on the interface?
A. Matching traffic is not rate limited.
B. The system repeatedly generates warning messages.
C. The rate-limiting rule is disabled.
D. The policy rate limits all traffic exiting any virtual interface.

7. Using Cisco AMP for Endpoints, what is meant by simple custom detection?
A. It is a rule for identifying a file that should be blacklisted by Cisco AMP.
B. It is a method for identifying and quarantining a specify file by its SHA-256 hash.
C. It is a feature for configuring a personal firewall.
D. It is a method for identifying and quarantining a set of filters by regular expression language.

8. Which of the following is Cisco AMP file disposition?
A. Non-malicious
B. Known
C. Malware
D. Pristine

9. Which of the following is a command-line mode supported by the Cisco FMC CLI?
A. User
B. Privileged
C. Configuration
D. Admin

10. Which one of the following commands can be used to generate Cisco Firepower sensor debug messages?
A. system support ssl-debug
B. system support platform

C. system support firewall-engine-debug
D. system support dump-table

11. What is the appropriate action to take when the Cisco Threat Response notifies you AMP has identified a malicious file?
A. Send a snapshot to Cisco for technical support.
B. Wait for the Cisco Threat Response to automatically block the malicious file.
C. Add the malicious file to the block list.
D. Forward the results of the investigation to an external threat analysis engine.

12. Which Cisco group does the Threat Response Team use for threat analysis and research?
A. Cisco Talos
B. Cisco Deep Analytics
C. Cisco Network Response
D. The OpenDNS Group

13. Given the Cisco Firepower Threat Defense CLI, which command would be issued to capture all traffic destined to hit a specific interface?
A. Configure coredump packet-engine enable
B. Capture WORD
C. Capture-traffic
D. Capture

14. Which Cisco Firepower feature is used to reduce the number of events received in a period of time?
A. Prepending
B. Rate-limiting
C. Thresholding
D. Correlation

15. The benefit of selecting the 'trace' option for packet capture is:
A. The option captures details of each packet.
B. The option indicates whether the destination host responds through an alternate path.
C. The option limits the number of packets captured.
D. The option indicates whether the packet was dropped or whether the

packet was successful.

16. Which command can be entered to generate a troubleshooting file in the Cisco FMC?
A. sudo sf_troubleshoot.pl
B. system support diagnostic-cli
C. show tech-support chassis
D. show running-config

17. When troubleshooting using packet-capture, the file-size command would need to be used for the following:
A. When captured packets exceed 32MB.
B. When captured packets exceed 10GB.
C. When captured packets are less than 16MB.
D. When captured packets are restricted from the secondary memory.

18. Which disposition is returned in a Cisco AMP for Networks implementation when the cloud cannot be reached?
A. Unknown
B. Unavailable
C. Clean
D. Disconnected

19. Of the following commands, which is used to generate troubleshooting files on an FTD?
A. show tech-support
B. sudo sf_troubleshoot.pl
C. system generate-troubleshoot all
D. system support view-files

20. When using Cisco AMP for Networks, which feature copies a file to the Cisco AMP cloud for analysis?
A. Spero analysis
B. Dynamic analysis
C. Sandbox analysis
D. Malware analysis

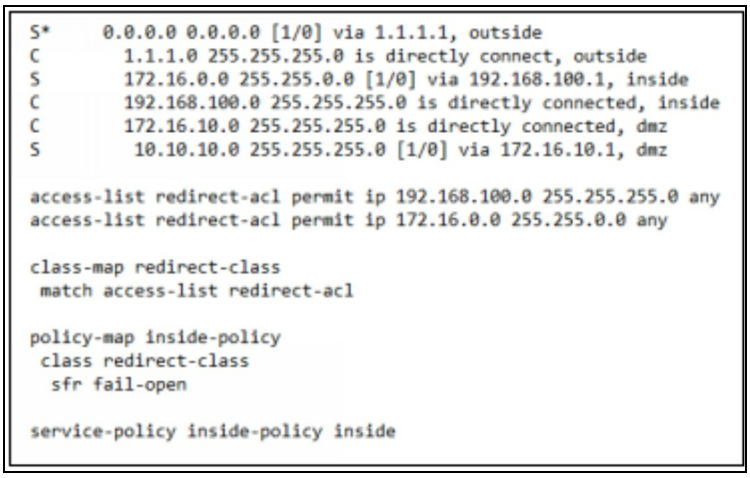
21. Which interface type allows packets to be dropped?
A. Passive

B. Inline
C. TAP
D. Either passive or inline, provided that the intrusion policy has the Drop When Inline check box selected.

22. Which Cisco AMP for Endpoints, what, is meant by simple custom detection?
A. It is a rule for identifying a file that should be whitelisted by Cisco AMP.
B. It is a method for identifying and quarantining a specific file by its SHA-256 hash.
C. It is a feature for configuring a personal firewall.
D. It is a method for identifying and quarantining a set of files by regular expression language.

23. Which detection method is also known as machine learning on Network-based Cisco Advanced Malware Protection?
A. Custom file detection
B. Hashing
C. Spero engine
D. Dynamic analysis

24. When using Cisco Firepower Services for ASA, how is traffic directed from based Cisco ASA to the Firepower Services?
A. SPAN port on a Cisco Catalyst switch.
B. WCCP on the ASA.
C. Inline interface pair on the Cisco FirePOWER module.
D. Service policy on the ASA.
25. Refer to the exhibit. Which option is a result of this configuration?



```
S*     0.0.0.0 0.0.0.0 [1/0] via 1.1.1.1, outside
C        1.1.1.0 255.255.255.0 is directly connect, outside
S        172.16.0.0 255.255.0.0 [1/0] via 192.168.100.1, inside
C        192.168.100.0 255.255.255.0 is directly connected, inside
C        172.16.10.0 255.255.255.0 is directly connected, dmz
S         10.10.10.0 255.255.255.0 [1/0] via 172.16.10.1, dmz

access-list redirect-acl permit ip 192.168.100.0 255.255.255.0 any
access-list redirect-acl permit ip 172.16.0.0 255.255.0.0 any

class-map redirect-class
 match access-list redirect-acl

policy-map inside-policy
 class redirect-class
  sfr fail-open

service-policy inside-policy inside
```

A. All ingress traffic on the inside interface that matches the access list is redirected.
B. All egress traffic on the outside interface that matches the access list is redirected.
C. All TCP traffic that arrives on the inside interface is redirected.
D. All ingress and egress traffic is redirected to the Cisco FirePOWER module.

26. Which two TCP ports can allow the Cisco Firepower Management Center to communication with FireAMP cloud for file disposition information? (Choose two).
A. 8080
B. 22
C. 8305
D. 32137
E. 443

27. Which three operating systems are supported with Cisco AMP for Endpoints? (Choose three).
A. Windows
B. AWS
C. Android
D. Cisco IOS
E. OS X
F. ChromeOS
28. Which feature requires the network discovery policy for it to work on the

Cisco Next Generation Intrusion Prevention System?
A. Impact flags
B. URL filtering
C. Security intelligence
D. Health monitoring

29. Which CLI command is used to generate firewall debug messages on a Cisco Firepower sensor?
A. system support ssl-debug
B. system support firewall-engine-debug
C. system support capture-traffic
D. system support platform

30. With Cisco AMP for Endpoints, which option shows a list of all files that have been executed in your environment?
A. Vulnerable software
B. File analysis
C. Detections
D. Prevalence
E. Threat root cause

31. Which type of policy is used to define the scope for applications that are running on hosts?
A. Access control policy.
B. Application awareness policy.
C. Application detector policy.
D. Network discovery policy.

32. Which type of policy do you configure if you want to look for a combination of events using Boolean logic?
A. Correlation
B. Application detector
C. Traffic profile
D. Access control
E. Intrusion

33. Which two tasks can the network discovery feature perform? (Choose two).
A. Host discovery

B. Block traffic
C. User discovery
D. Reset connection
E. Route traffic

34. In which two places can thresholding settings be configured? (Choose two).
A. Globally, per intrusion policy.
B. Globally, within the network analysis policy.
C. On each access control rule.
D. On each IPS rule.
E. Per preprocessor, within the network analysis policy.

35. Which two Cisco IPS events will generate an IP log? (Choose two).
A. A signature had an event action that was configured to log packets.
B. A statically configured IP or IP network criterion was matched.
C. A dynamically configured IP address or IP network was matched.
D. An attack produced a response action.

36. Which three functions can Cisco Application Visibility and Control perform? (Choose three).
A. Validation of malicious traffic.
B. Traffic control.
C. Extending Web Security to all computing devices.
D. Application-level classification.
E. Monitoring.
F. Signature tuning.

Chapter 3: Answers

1. In a Cisco Firepower Threat Defense access control policy rule, which of the following two actions are valid?

B. Block
E. Block with reset

Within an access control policy, access control rules provide a granular method of handling network traffic across multiple managed devices. Traffic is evaluated as follows:
Rule 1: Monitor - no Actions for monitor, only for logging.
Rule 2: Trust - Actions: Traffic Allowed, File Inspection, Intrusion Inspection, and Discovery.
Rule 3: Block - Actions: Block and Block with Reset.
Rule 4: Allow - Action is to allow matching traffic to pass

2. What are the two remediation options available when the Cisco Firepower Management Console is integrated into the Cisco ISE? (Choose two).

B. Port shutdown
E. Quarantine

ISE remediations run the following Mitigation Actions on the source or destination host involved in a correlation policy violation:
quarantine—Limits or denies an endpoint's access the network.
unquarantine—Reverses an endpoint's quarantine status and allows full access to the network shutdown—Deactivates an endpoint's network attached system (NAS) port to disconnect it from the network

3. When creating a report template, how are you able to limit the results to only show the activity of a specific subnet?

B. Add an Input Parameter in the Advanced Settings of the report.

From the Advanced tab, you use input parameters to expand the usefulness of your searches. There are several user-defined parameter types including

Network/IP, Application, Event Message, Device, Username, Number, or String.

4. What is the maximum SHA level the Threat Intelligence Director supports?

A. SHA-256

The Threat Intelligence Director supports additional traffic filtering based on IP address, URL, and (if DNS policy is enabled) domain name. The TID also supports filtering adding support for filtering on SHA-256 hash values.

5. Which Cisco AMP for Endpoints policy is used to only monitor endpoint activity?

D. Audit

Audit policies provide a means of deploying an AMP for Endpoints connector while ensuring limited interference on an endpoint. Default Audit policies will not quarantine files or block network connections and as such, they are useful for gathering data for connector tuning during initial deployment and troubleshooting. The converse are protect policies which provide a higher degree of endpoint protection. Connectors utilizing these protect policies will quarantine known malicious files, block C2 network traffic, and perform other protective actions.

6. What is the result of specifying a QoS rule having a rate limit that is more than the maximum available on the interface?

A. Matching traffic is not rate limited.

If you specify a limit greater than the maximum throughput of an interface, the system does not rate limit matching traffic.

7. Using Cisco AMP for Endpoints, what is meant by simple custom detection?

B. It is a method for identifying and quarantining a specify file by its SHA-256 hash.

A Simple Custom Detection list is used to detect, block and quarantine specific files to prevent the files to be allowed on devices that have installed the Advanced Malware Protection (AMP) for Endpoints connectors; this can be done using the SHA-256 digest.

8. Which of the following is Cisco AMP file disposition?

C. Malware

Dispositions returned from an AMP cloud query are:
Clean
Unknown
Malware

9. Which of the following is a command-line mode supported by the Cisco FMC CLI?

C. Configuration

The CLI encompasses four modes. The default mode, CLI Management, includes commands for navigating within the CLI itself. The remaining modes contain commands addressing three different areas of Firepower Management Center functionality; the commands within these modes begin with the mode name: system, show, or configure.

10. Which one of the following commands can be used to generate Cisco Firepower sensor debug messages?

C. system support firewall-engine-debug

The system support ssl-debug debug_policy_all command can be run to generate debugging information for every flow specific to the SSL Policy. The system support platform simply refers to the system support command set. The system support firewall-engine-debug command is used in order to send general debug traffic that hits your FMC policy rules. The system support dump-table command can dump a specified database table to a common file repository.

11. What is the appropriate action to take when the Cisco Threat Response notifies you AMP has identified a malicious file?

C. Add the malicious file to the block list.

Threat Response is an application that automates and aggregates threat intelligence sources and data from multiple security technologies - Cisco and third-party - into a central interface. Threat Response direct remediation lets

you take corrective action directly from its interface. You can block suspicious files, domains, and more without having to log in to another product.

12. Which Cisco group does the Threat Response Team use for threat analysis and research?

A. Cisco Talos

Cisco Threat Response can simplify complex threat investigations in order to improve incident response in these ways including coordination of activities among Firepower, Umbrella, AMP, Email Security, Threat Grid, and Talos to improve threat hunting efficiency.

13. Given the Cisco Firepower Threat Defense CLI, which command would be issued to capture all traffic destined to hit a specific interface?

D. Capture

To capture traffic from a Firepower LINA engine, enable captures from the console using the capture command specifying match parameters including interface. To capture traffic from a Firepower SNORT engine, log in to the FTD CLI run the capture-traffic command on the shell; When the system prompts you to choose a domain, select the Router domain to capture traffic from the data interfaces. To enable or disable packet-engine coredump generation, use the configure coredump packet- engine command. A coredump is a snapshot of the running program when the program has terminated abnormally, or crashed, not traffic hitting an interface. The capture WORD command along with show command (show capture <word>)will show the captured file with the name <word>.

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

C. Thresholding

You can control the number of events that are generated per rule over time by setting the threshold options in the packet view of an intrusion event.

15. The benefit of selecting the 'trace' option for packet capture is:

D. The option indicates whether the packet was dropped or whether the packet was successful.

In order to identify issues such as misconfiguration, capacity overload, or even the ordinary software bug while troubleshooting, it is necessary to understand what happens to a packet within a system. The Cisco Packet Trace feature addresses this need.

16. Which command can be entered to generate a troubleshooting file in the Cisco FMC?

A. sudo sf_troubleshoot.pl

Enter this command on the Firepower Management Center in order to generate a troubleshoot file: sudo sf_troubleshoot.pl

17. When troubleshooting using packet-capture, the file-size command would need to be used for the following:

A. When captured packets exceed 32MB.

You can increase the size of the capture buffer on the FTD (Firepower Threat Defense) to a value up 32MB (with the buffer option)(default is 500Kbytes). From FTD version 6.3 on, the file-size command allows you to configure a capture file up to 10GBytes.

18. Which disposition is returned in a Cisco AMP for Networks implementation when the cloud cannot be reached?

B. Unavailable

Malware Event Generation Scenarios: When the system detects a file and queries the AMP cloud but cannot establish a connection or the cloud is otherwise unavailable.
Disposition: Unavailable

19. Of the following commands, which is used to generate troubleshooting files on an FTD?

C. system generate-troubleshoot all

Enter this command on Firepower devices/modules and virtual managed devices in order to generate a troubleshoot file: system generate-troubleshoot all.

20. When using Cisco AMP for Networks, which feature copies a file to the Cisco AMP cloud for analysis?

B. Dynamic analysis

21. Which interface type allows packets to be dropped?

D. Either passive or inline, provided that the intrusion policy has the Drop When Inline check box selected.

22. Which Cisco AMP for Endpoints, what, is meant by simple custom detection?

B. It is a method for identifying and quarantining a specific file by its SHA-256 hash.

23. Which detection method is also known as machine learning on Network-based Cisco Advanced Malware Protection?

D. Dynamic analysis

24. When using Cisco Firepower Services for ASA, how is traffic directed from based Cisco ASA to the Firepower Services?

D. Service policy on the ASA.

25. Refer to the exhibit. Which option is a result of this configuration?

```
S*     0.0.0.0 0.0.0.0 [1/0] via 1.1.1.1, outside
C        1.1.1.0 255.255.255.0 is directly connect, outside
S        172.16.0.0 255.255.0.0 [1/0] via 192.168.100.1, inside
C        192.168.100.0 255.255.255.0 is directly connected, inside
C        172.16.10.0 255.255.255.0 is directly connected, dmz
S         10.10.10.0 255.255.255.0 [1/0] via 172.16.10.1, dmz

access-list redirect-acl permit ip 192.168.100.0 255.255.255.0 any
access-list redirect-acl permit ip 172.16.0.0 255.255.0.0 any

class-map redirect-class
 match access-list redirect-acl

policy-map inside-policy
 class redirect-class
  sfr fail-open

service-policy inside-policy inside
```

C. All TCP traffic that arrives on the inside interface is redirected.

26. Which two TCP ports can allow the Cisco Firepower Management Center to communication with FireAMP cloud for file disposition information? (Choose two).

D. 32137
E. 443

27. Which three operating systems are supported with Cisco AMP for Endpoints? (Choose three).

A. Windows
C. Android
E. OS X

28. Which feature requires the network discovery policy for it to work on the Cisco Next Generation Intrusion Prevention System?

A. Impact flags

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

B. system support firewall-engine-debug

30. With Cisco AMP for Endpoints, which option shows a list of all files that

have been executed in your environment?

C. Detections

31. Which type of policy is used to define the scope for applications that are running on hosts?

C. Application detector policy.

32. Which type of policy do you configure if you want to look for a combination of events using Boolean logic?

A. Correlation

33. Which two tasks can the network discovery feature perform? (Choose two).

A. Host discovery
C. User discovery

34. In which two places can thresholding settings be configured? (Choose two).

A. Globally, per intrusion policy.
D. On each IPS rule.

35. Which two Cisco IPS events will generate an IP log? (Choose two).

A. A signature had an event action that was configured to log packets.
B. A statically configured IP or IP network criterion was matched.

36. Which three functions can Cisco Application Visibility and Control perform? (Choose three).

B. Traffic control.
D. Application-level classification.
E. Monitoring.

Chapter 4: Integration

The objectives covered in this chapter:

15% 4.0 Integration

- ***4.1 Configure Cisco AMP for Networks in Firepower Management Center***
- ***4.2 Configure Cisco AMP for Endpoints in Firepower Management Center***
- ***4.3 Implement Threat Intelligence Director for third-party security intelligence feeds***
- ***4.4 Describe using Cisco Threat Response for security investigations***
- ***4.5 Describe Cisco FMC PxGrid Integration with Cisco Identify Services Engine (ISE)***
- ***4.6 Describe Rapid Threat Containment (RTC) functionality within Firepower Management Center***

1. Which limitation applies to Cisco Firepower Management Center dashboards in a multidomain environment?
A. Child domains cannot view dashboards that originate from an ancestor domain.
B. Child domains have access to a limited set of widgets from ancestor domains.
C. Only the domain administrator can view all ancestor dashboards.
D. Child domains can view but not edit dashboards that originate from an ancestor domain.

2. Which of the following are two routing options that are valid for the Cisco Firepower Threat Defense? (Choose two).
A. BGPv4 with non-stop forwarding.
B. BGPv4 in transparent firewall mode.
C. BGPv6 supporting IPv6 networks.
D. ECMP with up to 3 equal cost paths on a single interface.
E. ECMP with up to 3 equal cost paths on multiple interfaces.

3. Using Cisco Firepower Threat Defense software, which interface mode must be configured to passively receive traffic from a network device?
A. Inline tap
B. Inline set
C. Passive
D. Routed

4. Which of the two following conditions are required for HA (high availability) to function between two Firepower Threat Defense systems? (Choose two).
A. The units must be the same model.
B. The units must be the same version.
C. The units must be configured only for routed mode.
D. Both systems can be part of a different group but must be in the same domain when configured from the FMC.
E. The units must be different models if they are part of the same series.

5. Which two features of Cisco Advanced Malware Protection for Endpoints allows for an uploaded file to be blocked? (Choose two).
A. Application whitelisting
B. Application blocking
C. Simple custom detection
D. File repository
E. Exclusions

6. Which two interface settings are required when configuring a routed interface with Cisco Firepower Threat Defense? (Choose two).
A. Speed
B. Duplex
C. Media mode
D. Etherchannel
E. Redundant Interface

7. What are two requirements for configuring a hybrid interface in FirePOWER? (Choose two).
A. Virtual network
B. Virtual router
C. Virtual appliance
D. Virtual switch

E. Virtual context

8. In cisco Firepower 6.0, which policy contains the button that allows you to access the network analysis policy?
A. Network discovery policy
B. Intrusion Policy
C. Access control policy
D. File policy

9. An engineer must deploy AMP with cloud protection. Which machine learning engine uses active heuristics?
A. Spero
B. IOCs
C. 1to1
D. Ethos

10. Which cloud-based malware detection engine uses machine-learning detection techniques in the Cisco Advanced Malware Protection cloud?
A. Third-party detections
B. Spero
C. Ethos
D. Memcache

11. Which two options are the basic parts of a Snort rule? (Choose two).
A. Rule policy
B. Rule header
C. Rule assignment and ports
D. Rule options
E. Rule footer

12. Which two statement about Cisco Firepower file and intrusion inspection under control policies are true? (Choose two).
A. File inspection occurs before intrusion prevention.
B. Intrusion Inspection occurs after traffic is blocked by file type.
C. File and intrusion drop the same packet.
D. Blocking by file type takes precedence over malware inspection and blocking.
E. File inspection occurs after file discovery.

13. With Firepower Threat Defense, which two interface settings are required when configuring a routed interface? (Choose two).
A. Speed
B. Duplex
C. Media Type
D. Redundant Interface
E. EtherChannel

14. Which policy must you edit to make changes to the Snort preprocessors?
A. Access control policy
B. Network discovery policy
C. Intrusion policy
D. File policy
E. Network analysis policy

15. On Cisco Firepower Management Center, which policy is used to collect health modules alerts from managed devices?
A. Health policy
B. System policy
C. Correlation policy
D. Access control policy
E. health awareness policy

16. With Cisco Firepower Threat Defense software, which interface mode do you configure for an IPS deployment, where traffic passes through the appliance but does not require VLAN rewriting?
A. Inline set
B. Passive
C. Inline tap
D. Routed
E. Transparent

17. In a Cisco Firepower intrusion policy, which two event actions can be configured on a rule? (Choose two).
A. Drop packet
B. Drop and generate
C. Drop connection
D. Capture trigger packet
E. Generate events

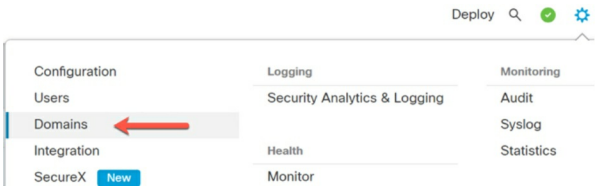
18. Which Cisco Advanced Malware protection for Endpoints deployment architecture is designed to keep data within a network perimeter?
A. Cloud web services
B. Network AMP
C. Private cloud
D. Public cloud

Chapter 4: Answers

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

A. Child domains cannot view dashboards that originate from an ancestor domain.

Cisco Firepower domains are not an objective so does this question even count?



In a multidomain deployment, you cannot view dashboards from ancestor domains; however, you can create new dashboards that are copies of the higher-level dashboards. The dashboard widgets that you can view depend on the type of appliance you are using, your user role, and your current domain (in a multidomain deployment). In a multidomain deployment, you should see a widget that you expect to see, if not, switch to the Global domain.
Reference: CCIE/CCNP Security SNCF 300-710 Study Guide chapter 20

2. Which of the following are two routing options that are valid for the Cisco Firepower Threat Defense? (Choose two).

A. BGPv4 with non-stop forwarding.

D. ECMP with up to 3 equal cost paths on a single interface.

Looking at the Cisco FMC routing tab, it doesn't appear to support any of the options listed, so where is the "none of the above" option?
But if we look closer we can see that we can possibly find the answer. Kinda. The Firepower Threat Defense device supports several Internet protocols for routing. Open Shortest Path First (OSPF). Routing Information Protocol (RIP) Border Gateway Protocol (BGPv4) with non-stop routing, but this is only listed in the documentation. The Firepower Threat Defense device supports Equal-Cost Multi-Path (ECMP) routing. You can have up to 3 equal cost static or dynamic routes per interface, but you can only find this in the documentation, not in the FMC. Transparent Firewall is a bridged implementation (layer 2), not routing
Reference: CCIE/CCNP Security SNCF 300-710 Study Guide chapter x

3. Using Cisco Firepower Threat Defense software, which interface mode must be configured to passively receive traffic from a network device?

C. Passive

An interface in Passive Mode can only detect intrusion attempts. ERSPAN mirrors all the packets it receives and sends a copy of each packet to the FTD device but won't drop anything either. Only an inline interface can be in prevention mode and drop traffic

4. Which of the two following conditions are required for HA (high availability) to function between two Firepower Threat Defense systems? (Choose two).

A. The units must be the same model.
B. The units must be the same version.

High Availability System Requirements:
Hardware Requirements: The two units in a High Availability configuration must: Be the same model. Have the same number and types of interfaces. Software Requirements: The two units in a High Availability configuration must: Be in the same firewall mode (routed or transparent). Have the same software version. Be in the same domain and/or group on the Firepower Management Center. Have the same NTP configuration. Be fully deployed

on the Firepower Management Center with no uncommitted changes. Devices cannot have DHCP or PPPoE configured on any of their interfaces.
Reference: CCIE/CCNP Security SNCF 300-710 Study Guide chapter 20

5. Which two features of Cisco Advanced Malware Protection for Endpoints allows for an uploaded file to be blocked? (Choose two).

C. Simple custom detection
D. File repository

You can create a Simple Custom Detection list to detect, block and quarantine specific files to prevent the files to be allowed on devices that have installed the Advanced Malware Protection (AMP) for Endpoints connectors. The File Repository allows you to download files you have requested from your AMP for Endpoints Connectors. This feature is useful for performing analysis on suspicious and malicious files observed by your Connectors.
Reference: CCIE/CCNP Security SNCF 300-710 Study Guide chapter 20

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

A. Speed
B. Duplex

Enable the physical interface. By default, physical interfaces are disabled (with the exception of the Diagnostic interface). Set a specific speed and duplex. By default, speed and duplex are set to Auto.

7. What are two requirements for configuring a hybrid interface in FirePOWER? (Choose two).

B. Virtual router
D. Virtual switch

8. In cisco Firepower 6.0, which policy contains the button that allows you to access the network analysis policy?

C. Access control policy

9. An engineer must deploy AMP with cloud protection. Which machine

learning engine uses active heuristics?

A. Spero

10. Which cloud-based malware detection engine uses machine-learning detection techniques in the Cisco Advanced Malware Protection cloud?

B. Spero

11. Which two options are the basic parts of a Snort rule? (Choose two).

B. Rule header
D. Rule options

12. Which two statement about Cisco Firepower file and intrusion inspection under control policies are true? (Choose two).

A. File inspection occurs before intrusion prevention.
E. File inspection occurs after file discovery.

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

A. Speed
B. Duplex

14. Which policy must you edit to make changes to the Snort preprocessors?

E. Network analysis policy

15. On Cisco Firepower Management Center, which policy is used to collect health modules alerts from managed devices?

A. Health policy

16. With Cisco Firepower Threat Defense software, which interface mode do you configure for an IPS deployment, where traffic passes through the appliance but does not require VLAN rewriting?

E. Transparent

17. In a Cisco Firepower intrusion policy, which two event actions can be configured on a rule? (Choose two)

B. Drop and generate
E. Generate events

18. Which Cisco Advanced Malware protection for Endpoints deployment architecture is designed to keep data within a network perimeter?

C. Private cloud