| | |
|---|---|
| **Exam** | **300-710** |
| **Title** | **Securing Networks with Cisco Firepower (300-710 SNCF) Exam** |
| **Version** | **18.0** |
| **Product Type** | **260 Q&A with explanations** |

**QUESTION** 1
What is a result of enabling Cisco FTD clustering?

A. For the dynamic routing feature, if the master unit fails, the newly elected master unit maintains all existing connections.
B. Integrated Routing and Bridging is supported on the master unit.
C. Site-to-site VPN functionality is limited to the master unit, and all VPN connections are dropped if the master unit fails.
D. All Firepower appliances can support Cisco FTD clustering.

Answer: C

Explanation:
Reference:
https://www.cisco.com/c/en/us/td/docs/security/firepower0/configuration/guide/fpmc-configguide-v64/clustering_for_the_firepower_threat_defense.html

---

**QUESTION** 2
Which two conditions are necessary for high availability to function between two Cisco FTD devices? (Choose two.)

A. The units must be the same version
B. Both devices can be part of a different group that must be in the same domain when configured within the FMC.
C. The units must be different models if they are part of the same series.
D. The units must be configured only for firewall routed mode.
E. The units must be the same model.

Answer: AE

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

---

**QUESTION** 3
On the advanced tab under inline set properties, which allows interfaces to emulate a passive interface?

A. transparent inline mode
B. TAP mode
C. strict TCP enforcement
D. propagate link state

Answer: D

Explanation:

Reference:
https://www.cisco.com/c/en/us/td/docs/security/firepower0/configuration/guide/fpmc-configguide-v64/inline_sets_and_passive_interfaces_for_firepower_threat_defense.html

**QUESTION** 4
What are the minimum requirements to deploy a managed device inline?

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

Answer: C

Explanation:
Reference:
https://www.cisco.com/c/en/us/td/docs/security/firepower0/configuration/guide/fpmc-configguide-v65/ips_device_deployments_and_configuration.html

**QUESTION** 5
What is the difference between inline and inline tap on Cisco Firepower?

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

Answer: A

Explanation:

**QUESTION** 6
With Cisco Firepower Threat Defense software, which interface mode must be configured to passively receive traffic that passes through the appliance?

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

Answer: B

Explanation:
Reference:
https://www.cisco.com/c/en/us/td/docs/security/firepower0/configuration/guide/fpmc-configguide-v64/interface_overview_for_firepower_threat_defense.html

**QUESTION** 7
Which two deployment types support high availability? (Choose two.)

A. transparent
B. routed
C. clustered
D. intra-chassis multi-instance
E. virtual appliance in public cloud

Answer: AB

Explanation:
Reference:
https://www.cisco.com/c/en/us/td/docs/security/firepower0/configuration/guide/fpmc-configguide-v61/firepower_threat_defense_high_availability.html

---

**QUESTION** 8
Which protocol establishes network redundancy in a switched Firepower device deployment?

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

Answer: A

Explanation:
Reference:
https://www.cisco.com/c/en/us/td/docs/security/firepower0/configuration/guide/fpmc-configguide-v62/firepower_threat_defense_high_availability.html

---

**QUESTION** 9
Which interface type allows packets to be dropped?

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

Answer: B

Explanation:
Reference: https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw908-configuring-firepower- threat-defense-int.html

---

**QUESTION** 10
Which Cisco Firepower Threat Defense, which two interface settings are required when configuring a

routed interface? (Choose two.)

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

Answer: CE

Explanation:
https://www.cisco.com/c/en/us/td/docs/security/firepower0/fdm/fptd-fdm-config-guide-610/fptd-fdm- interfaces.html

---

**QUESTION** 11
Which two dynamic routing protocols are supported in Firepower Threat Defense without using FlexConfig? (Choose two.)

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

Answer: BE

Explanation:
Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower0/fdm/fptd-fdm-configguide-660/fptd- fdm-routing.html

---

**QUESTION** 12
Which policy rule is included in the deployment of a local DMZ during the initial deployment of a Cisco NGFW through the Cisco FMC GUI?

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

Answer: C

Explanation:

---

**QUESTION** 13
What are two application layer preprocessors? (Choose two.)

A. CIFS

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

Answer: BC

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

---

**QUESTION** 14
An engineer is tasked with deploying an internal perimeter firewall that will support multiple DMZs Each DMZ has a unique private IP subnet range. How is this requirement satisfied?

A. Deploy the firewall in transparent mode with access control policies.
B. Deploy the firewall in routed mode with access control policies.
C. Deploy the firewall in routed mode with NAT configured.
D. Deploy the firewall in transparent mode with NAT configured.

Answer: C

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

---

**QUESTION** 15
An engineer must configure high availability for the Cisco Firepower devices. The current network topology does not allow for two devices to pass traffic concurrently. How must the devices be implemented in this environment?

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

Answer: C

Explanation:

---

**QUESTION** 16
When deploying a Cisco ASA Firepower module, an organization wants to evaluate the contents of the traffic without affecting the network. It is currently configured to have more than one instance of the same device on the physical appliance Which deployment mode meets the needs of the organization?

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

Answer: A

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

---

**QUESTION** 17
An organization has a Cisco FTD that uses bridge groups to pass traffic from the inside interfaces to the outside interfaces. They are unable to gather information about neighbouring Cisco devices or use multicast in their environment. What must be done to resolve this issue?

A. Create a firewall rule to allow CDP traffic.
B. Create a bridge group with the firewall interfaces.
C. Change the firewall mode to transparent.
D. Change the firewall mode to routed.

Answer: C

Explanation:
"In routed firewall mode, broadcast and multicast traffic is blocked even if you allow it in an access rule..." "The bridge group does not pass CDP packets packets..."
https://www.cisco.com/c/en/us/td/docs/security/asa/asa913/configuration/general/asa-913-general-config/intro-fw.html
Passing Traffic Not Allowed in Routed Mode
In routed mode, some types of traffic cannot pass through the ASA even if you allow it in an access rule. The bridge group, however, can allow almost any traffic through using either an access rule (for IP traffic) or an EtherType rule (for non-IP traffic):
IP trafficâ€”In routed firewall mode, broadcast and "multicast traffic is blocked even if you allow it in an access rule," including unsupported dynamic routing protocols and DHCP (unless you configure DHCP relay). Within a bridge group, you can allow this traffic with an access rule (using an extended ACL).
Non-IP trafficâ€”AppleTalk, IPX, BPDUs, and MPLS, for example, can be configured to go through using an EtherType rule.
Note
"The bridge group does not pass CDP packets packets, or any packets that do not have a valid

EtherType greater than or equal to 0x600. An exception is made for BPDUs and IS-IS, which are supported. "

**QUESTION** 18
A network engineer implements a new Cisco Firepower device on the network to take advantage of its intrusion detection functionality. There is a requirement to analyze the traffic going across the device, alert on any malicious traffic, and appear as a bump in the wire How should this be implemented?

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

**QUESTION** 19
Which two conditions must be met to enable high availability between two Cisco FTD devices? (Choose two.)

A. same flash memory size
B. same NTP configuration
C. same DHCP/PPoE configuration
D. same host name
E. same number of interfaces

Answer: BE

Explanation:
https://www.cisco.com/c/en/us/support/docs/security/firepower-management-center699-configure-ftd-high-availability-on-firep.html
Conditions
In order to create an HA between 2 FTD devices, these conditions must be met:
Same model

Same version (this applies to FXOS and to FTD - (major (first number), minor (second number), and maintenance (third number) must be equal))
Same number of interfaces
Same type of interfaces
Both devices as part of same group/domain in FMC
Have identical Network Time Protocol (NTP) configuration
Be fully deployed on the FMC without uncommitted changes
Be in the same firewall mode: routed or transparent.
Note that this must be checked on both FTD devices and FMC GUI since there have been cases where the FTDs had the same mode, but FMC does not reflect this.
Does not have DHCP/Point-to-Point Protocol over Ethernet (PPPoE) configured in any of the interface
Different hostname (Fully Qualified Domain Name (FQDN)) for both chassis. In order to check the chassis hostname navigate to FTD CLI and run this command

---

**QUESTION** 20
An engineer is building a new access control policy using Cisco FMC. The policy must inspect a unique IPS policy as well as log rule matching. Which action must be taken to meet these requirements?

A. Configure an IPS policy and enable per-rule logging.
B. Disable the default IPS policy and enable global logging.
C. Configure an IPS policy and enable global logging.
D. Disable the default IPS policy and enable per-rule logging.

Answer: C

Explanation:

---

**QUESTION** 21
Within an organization's high availability environment where both firewalls are passing traffic, traffic must be segmented based on which department it is destined for. Each department is situated on a different LAN. What must be configured to meet these requirements?

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

Answer: D

Explanation:

---

**QUESTION** 22
An engineer is configuring a Cisco IPS to protect the network and wants to test a policy before deploying it. A copy of each incoming packet needs to be monitored while traffic flow remains constant. Which IPS mode should be implemented to meet these requirements?