KillTest

质量更高　服务更好

学习资料

http://www.killtest.cn

半年免费更新服务

Exam : **300-710**

Title : Securing Networks with Cisco Firepower (SNCF)

Version : DEMO

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

2.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: B,E
Explanation:
https://www.cisco.com/c/en/us/support/docs/security/firepower-management-center/212699-configure-ftd-high-availability-on-firep.html
Conditions
In order to create an HA between 2 FTD devices, these conditions must be met:
Same model
Same version (this applies to FXOS and to FTD -(major (first number), minor (second number), and maintenance (third number) must be equal)) Same number of interfaces
Same type of interfaces
Both devices as part of same group/domain in FMC
Have identical Network Time Protocol (NTP) configuration
Be fully deployed on the FMC without uncommitted changes
Be in the same firewall mode: routed or transparent.
Note that this must be checked on both FTD devices and FMC GUI since there have been cases where the FTDs had the same mode, but FMC does not reflect this.
Does not have DHCP/Point-to-Point Protocol over Ethernet (PPPoE) configured in any of the interface
Different hostname (Fully Qualified Domain Name (FQDN)) for both chassis. In order to check the chassis hostname navigate to FTD CLI and run this command

3.An organization has a Cisco FTD that uses bridge groups to pass traffic from the inside interfaces to the outside interfaces. They are unable to gather information about neighbouring Cisco devices or use multicast in their environment.
What must be done to resolve this issue?
A. Create a firewall rule to allow CDP traffic.
B. Create a bridge group with the firewall interfaces.
C. Change the firewall mode to transparent.
D. Change the firewall mode to routed.
Answer: C
Explanation:
"In routed firewall mode, broadcast and multicast traffic is blocked even if you allow it in an access rule..."
"The bridge group does not pass CDP packets packets..."
https://www.cisco.com/c/en/us/td/docs/security/asa/asa913/configuration/general/asa-913-general-config/intro-fw.html
Passing Traffic Not Allowed in Routed Mode
In routed mode, some types of traffic cannot pass through the ASA even if you allow it in an access rule. The bridge group, however, can allow almost any traffic through using either an access rule (for IP traffic) or an EtherType rule (for non-IP traffic):
IP traffic—In routed firewall mode, broadcast and "multicast traffic is blocked even if you allow it in an access rule," including unsupported dynamic routing protocols and DHCP (unless you configure DHCP relay). Within a bridge group, you can allow this traffic with an access rule (using an extended ACL).
Non-IP traffic—AppleTalk, IPX, BPDUs, and MPLS, for example, can be configured to go through using an EtherType rule.
Note
"The bridge group does not pass CDP packets packets, or any packets that do not have a valid EtherType greater than or equal to 0x600. An exception is made for BPDUs and IS-IS, which are supported. "

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

5.Which firewall design allows a firewall to forward traffic at layer 2 and layer 3 for the same subnet?
A. Cisco Firepower Threat Defense mode
B. transparent mode
C. routed mode

D. integrated routing and bridging
Answer: B