300-710 Q&As

Securing Networks with Cisco Firepower (SNCF)

Pass Cisco 300-710 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.leads4pass.com/300-710.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Cisco Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

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

A. routed mode

B. Cisco Firepower Threat Defense mode

C. transparent mode

D. integrated routing and bridging

Correct Answer: C

QUESTION 2

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

HIGH BANDWIDTH APPLICATIONS

Some applications use a substantial amount of network bandwidth. This bandwidth usage can be costly to your organization and can negatively impact overall network performance. You may want to restrict the usage of these applications to particular networks: for instance, a wireless network may not be well suited for video streaming. Or, you can shut down these applications entirely or simply get visibility into how your bandwidth is being used.

Application	Times Accessed	Application Risk	Productivity Rating	Data Transferred (MB)
YouTube	525	High	Very Low	76.7262
Pandora Audio	5	Medium	Very Low	8.4889
Spotify	44	Medium	Very Low	6.7747
Microsoft Update	122	Medium	Low	2.5577
Flash Video	240	Low	Low	2.4371

ENCRYPTED APPLICATIONS

Some applications encrypt data they process, causing security administrators to be bind to attacks and usage patterns. With SSL decryption, administrators can look inside these applications and observe they use. An SSL decryption appliance, such as a Cisco SSL Appliance, can decrypt SSL traffic inbound and outbound: inbound by storing the certificates of private web servers, and outbound by acting as an intermediary in browsers' connections to the Internet. It is important to use SSL decryption to obtain visibility into encrypted applications to help mitigate this potential attack vector.

Application	Times Accessed	Application Risk	Productivity Rating	Data Transferred (MB)
Chrome	24,658	Medium	Medium	799.6732
Internet Explorer	11,030	Medium	Medium	375.1055
Firefox	2,702	Medium	Medium	88.5616
Safari	1,866	Medium	Medium	43.1158
Kerberos	1,756	Very Low	High	4.9429

EVASIVE APPLICATIONS

Evasive applications ty 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)
BitTorrent	0	Very High	Very Low	1.7281
TOR	5	Medium	Low	0.0006
SSL client	10,100	Medium	Medium	48.4102
Skype	644	Medium	Medium	10.3545
cURL	280	Medium	Medium	0.4840

A. YouTube

B. TOR

C. Chrome

D. Kerberos

Correct Answer: A

QUESTION 3

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 this task?

A. Modify the device\\'s settings using the device management feature within Cisco FMC to force only secure protocols.

B. Use the Cisco FTD platform policy to change the minimum SSL version on the device to TLS 1.2.

C. Enable the UCAPL/CC compliance on the device to support only the most secure protocols available.

D. Configure a FlexConfig object to disable any insecure TLS protocols on the Cisco FTD device.

Correct Answer: B

QUESTION 4

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

Correct Answer: AC

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

QUESTION 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.

Correct Answer: A