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.geekcert.com/300-710.html

100% Passing Guarantee
100% Money Back Assurance

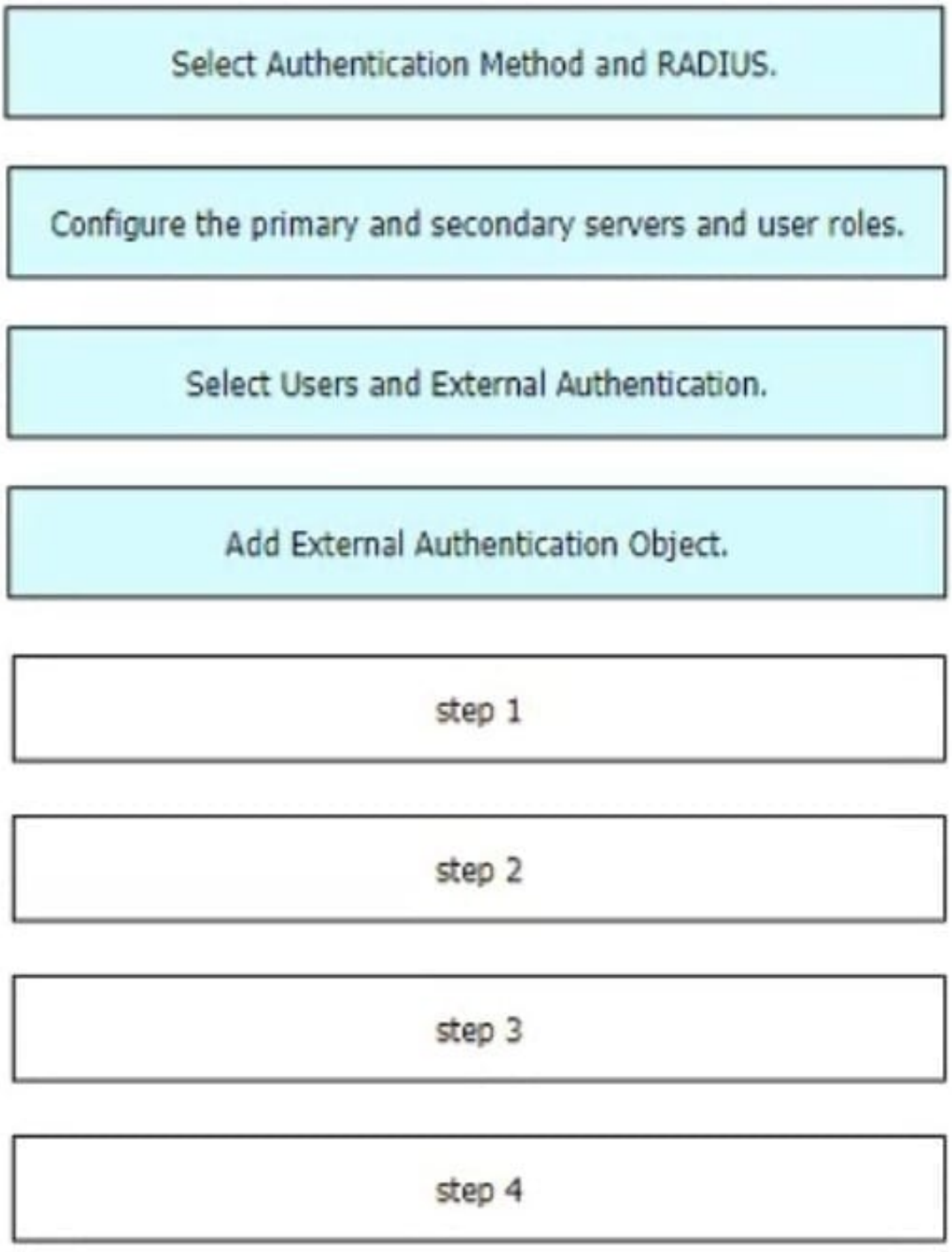
Following Questions and Answers are all new published by Cisco Official Exam Center

QUESTION 1

DRAG DROP

Drag and drop the configuration steps from the left into the sequence on the right to enable external authentication on Cisco FMC to a RADIUS server.

Select and Place:



Correct Answer:

QUESTION 2

A network engineer sets up a secondary Cisco FMC that is integrated with Cisco Security Packet Analyzer. What occurs when the secondary Cisco FMC synchronizes with the primary Cisco FMC?

A. The existing configuration for integration of the secondary Cisco FMC the Cisco Security Packet Analyzer is overwritten.

B. The synchronization between the primary and secondary Cisco FMC fails.

C. The existing integration configuration is replicated to the primary Cisco FMC.

D. The secondary Cisco FMC must be reintegrated with the Cisco Security Packet Analyzer after the synchronization.

Correct Answer: A

QUESTION 3

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

Correct Answer: BE

"static routing" is wrong, OSPF and BGP are the right choice, both can be configured with Smart CLI without FlexConfig
Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/660/fdm/fptd-fdm-config-guide-660/fptd-fdm-routing.html

QUESTION 4

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 5

An engineer has been tasked with using Cisco FMC to determine if files being sent through the network are malware. Which two configuration tasks must be performed to achieve this file lookup? (Choose two.)

A. The Cisco FMC needs to include a SSL decryption policy.

B. The Cisco FMC needs to connect to the Cisco AMP for Endpoints service.

C. The Cisco FMC needs to connect to the Cisco ThreatGrid service directly for sandboxing.

D. The Cisco FMC needs to connect with the FireAMP Cloud.

E. The Cisco FMC needs to include a file inspection policy for malware lookup.

Correct Answer: BE

Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Reference_a_wrapper_Chapter_topic_here.html#ID-2193-00000296