NSE4_FGT-6.4 Q&As

Fortinet NSE 4 - FortiOS 6.4

Pass Fortinet NSE4_FGT-6.4 Exam with 100% Guarantee

QUESTION 1

Which two settings can be separately configured per VDOM on a FortiGate device? (Choose two.)

A. System time

B. FortiGuaid update servers

C. Operating mode

D. NGFW mode

Correct Answer: CD

C: "Operating mode is per-VDOM setting. You can combine transparent mode VDOM\\'s with NAT mode VDOMs on the same physical Fortigate.

D: "Inspection-mode selection has moved from VDOM to firewall policy, and the default inspection-mode is flow, so NGFW Mode can be changed from Profile-base (Default) to Policy-base directly in System > Settings from the VDOM" Page 125 of FortiGate_Infrastructure_6.4_Study_Guide

QUESTION 2

Which statements about the firmware upgrade process on an active-active HA cluster are true? (Choose two.)

A. The firmware image must be manually uploaded to each FortiGate.

B. Only secondary FortiGate devices are rebooted.

C. Uninterruptable upgrade is enabled by default.

D. Traffic load balancing is temporally disabled while upgrading the firmware.

Correct Answer: CD

QUESTION 3

How does FortiGate act when using SSL VPN in web mode?

A. FortiGate acts as an FDS server.

B. FortiGate acts as an HTTP reverse proxy.

C. FortiGate acts as DNS server.

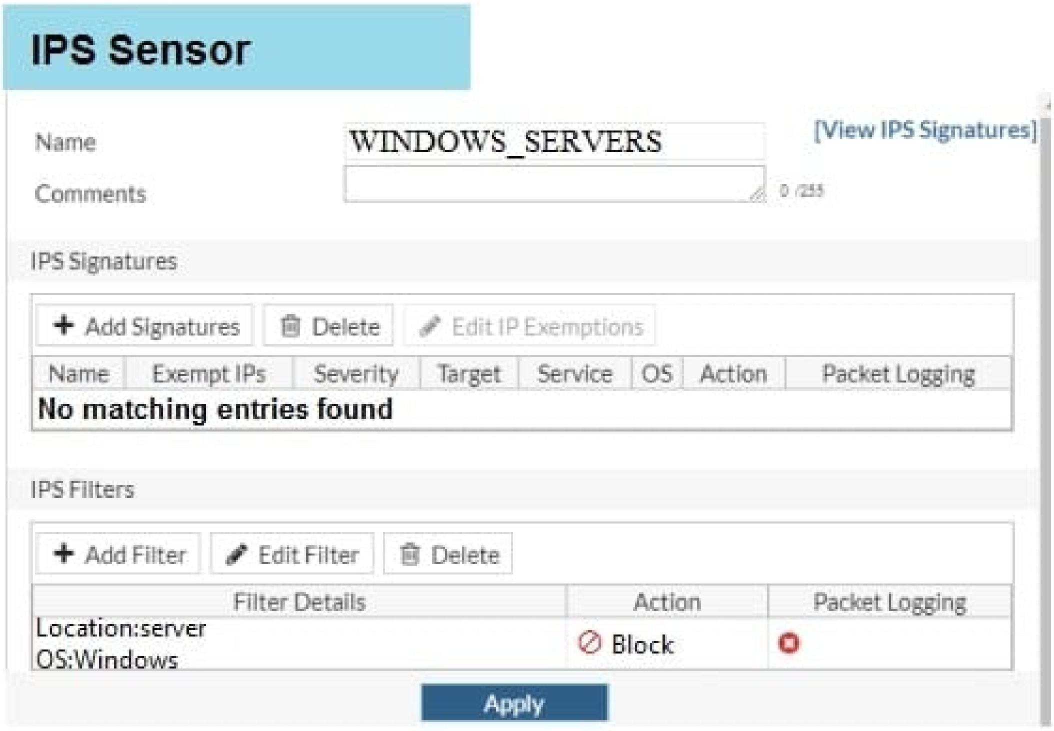
D. FortiGate acts as router.

Correct Answer: B

Reference: https://pub.kb.fortinet.com/ksmcontent/Fortinet-Public/current/Fortigate_v4.0MR3/fortigatesslvpn-40-mr3.pdf

QUESTION 4

Examine the IPS sensor configuration shown in the exhibit, and then answer the question below.



IPS Sensor

Name: WINDOWS_SERVERS [View IPS Signatures]

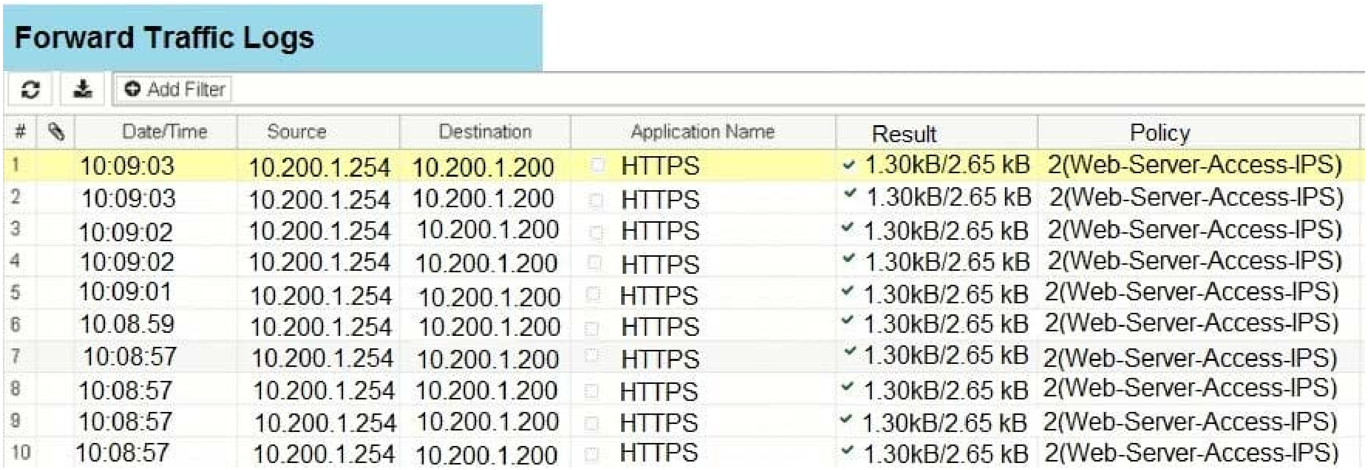
Comments: 0 /255

IPS Signatures

Name	Exempt IPs	Severity	Target	Service	OS	Action	Packet Logging
No matching entries found							

IPS Filters

Filter Details	Action	Packet Logging
Location:server OS:Windows	⊘ Block	●



Forward Traffic Logs

#		Date/Time	Source	Destination	Application Name	Result	Policy
1		10:09:03	10.200.1.254	10.200.1.200	HTTPS	✓ 1.30kB/2.65 kB	2(Web-Server-Access-IPS)
2		10:09:03	10.200.1.254	10.200.1.200	HTTPS	✓ 1.30kB/2.65 kB	2(Web-Server-Access-IPS)
3		10:09:02	10.200.1.254	10.200.1.200	HTTPS	✓ 1.30kB/2.65 kB	2(Web-Server-Access-IPS)
4		10:09:02	10.200.1.254	10.200.1.200	HTTPS	✓ 1.30kB/2.65 kB	2(Web-Server-Access-IPS)
5		10:09:01	10.200.1.254	10.200.1.200	HTTPS	✓ 1.30kB/2.65 kB	2(Web-Server-Access-IPS)
6		10.08.59	10.200.1.254	10.200.1.200	HTTPS	✓ 1.30kB/2.65 kB	2(Web-Server-Access-IPS)
7		10:08:57	10.200.1.254	10.200.1.200	HTTPS	✓ 1.30kB/2.65 kB	2(Web-Server-Access-IPS)
8		10:08:57	10.200.1.254	10.200.1.200	HTTPS	✓ 1.30kB/2.65 kB	2(Web-Server-Access-IPS)
9		10:08:57	10.200.1.254	10.200.1.200	HTTPS	✓ 1.30kB/2.65 kB	2(Web-Server-Access-IPS)
10		10:08:57	10.200.1.254	10.200.1.200	HTTPS	✓ 1.30kB/2.65 kB	2(Web-Server-Access-IPS)

An administrator has configured the WINDOWS_SERVERS IPS sensor in an attempt to determine whether the influx of HTTPS traffic is an attack attempt or not. After applying the IPS sensor, FortiGate is still not generating any IPS logs for the HTTPS traffic.

What is a possible reason for this?

A. The IPS filter is missing the Protocol: HTTPS option.

B. The HTTPS signatures have not been added to the sensor.

C. A DoS policy should be used, instead of an IPS sensor.

D. A DoS policy should be used, instead of an IPS sensor.

E. The firewall policy is not using a full SSL inspection profile.

Correct Answer: E

QUESTION 5

A network administrator wants to set up redundant IPsec VPN tunnels on FortiGate by using two IPsec VPN tunnels and static routes.

*

All traffic must be routed through the primary tunnel when both tunnels are up

*

The secondary tunnel must be used only if the primary tunnel goes down

*

In addition, FortiGate should be able to detect a dead tunnel to speed up tunnel failover

Which two key configuration changes are needed on FortiGate to meet the design requirements? (Choose two,)

A. Configure a high distance on the static route for the primary tunnel, and a lower distance on the static route for the secondary tunnel.

B. Enable Dead Peer Detection.

C. Configure a lower distance on the static route for the primary tunnel, and a higher distance on the static route for the secondary tunnel.

D. Enable Auto-negotiate and Autokey Keep Alive on the phase 2 configuration of both tunnels.

Correct Answer: BC