VCE & PDF
https://www.pass4itsure.com/nse4_fgt-7-0.html
Pass4itSure.com

NSE4_FGT-7.0^{Q&As}

Fortinet NSE 4 - FortiOS 7.0

Pass Fortinet NSE4_FGT-7.0 Exam with 100% Guarantee

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

https://www.pass4itsure.com/nse4_fgt-7-0.html

100% Passing Guarantee
100% Money Back Assurance

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

⚙ **Instant Download** After Purchase

⚙ **100% Money Back** Guarantee

⚙ **365 Days** Free Update

⚙ **800,000+** Satisfied Customers

QUESTION 1

Why does FortiGate Keep TCP sessions in the session table for several seconds, even after both sides (client and server) have terminated the session?

A. To allow for out-of-order packets that could arrive after the FIN/ACK packets

B. To finish any inspection operations

C. To remove the NAT operation

D. To generate logs

Correct Answer: A

TCP provides the ability for one end of a connection to terminate its output while still receiving data from the other end. This is called a half-close. FortiGate unit implements a specific timer before removing an

entry in the firewall session table.

QUESTION 2

An administrator is configuring an Ipsec between site A and siteB. The Remotes Gateway setting in both sites has been configured as Static IP Address. For site A, the local quick mode selector is 192.16.1.0/24 and the remote quick mode selector is 192.16.2.0/24. How must the administrator configure the local quick mode selector for site B?

A. 192.168.3.0/24

B. 192.168.2.0/24

C. 192.168.1.0/24

D. 192.168.0.0/8

Correct Answer: B

QUESTION 3

Refer to the exhibit.

Name	SLA_1	
Protocol	Ping HTTP DNS	
Servers	4.2.2.2	✗
	4.2.2.1	✗
Participants	All SD-WAN Members Specify	
	🔌 port1	✗
	🔌 port2	✗
	+	
Enable probe packets	◯	

Which contains a Performance SLA configuration.

An administrator has configured a performance SLA on FortiGate. Which failed to generate any traffic. Why is FortiGate not generating any traffic for the performance SLA?

A. Participants configured are not SD-WAN members.

B. There may not be a static route to route the performance SLA traffic.

C. The Ping protocol is not supported for the public servers that are configured.

D. You need to turn on the Enable probe packets switch.

Correct Answer: D

Reference:https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/478384/performance-slalinkmonitoring

QUESTION 4

Which two statements about antivirus scanning mode are true? (Choose two.)

A. In proxy-based inspection mode, files bigger than the buffer size are scanned.

B. In flow-based inspection mode, FortiGate buffers the file, but also simultaneously transmits it to the client.

C. In proxy-based inspection mode, antivirus scanning buffers the whole file for scanning, before sending it to the client.

D. In flow-based inspection mode, files bigger than the buffer size are scanned.

Correct Answer: BC

An antivirus profile in full scan mode buffers up to your specified file size limit. The default is 10 MB. That is large enough for most files, except video files. If your FortiGate model has more RAM, you may be able to increase this threshold. Without a limit, very large files could exhaust the scan memory. So, this threshold balances risk and performance. Is this tradeoff unique to FortiGate, or to a specific model? No. Regardless of vendor or model, you must make a choice. This is because of the difference between scans in theory, that have no limits, and scans on real-world devices, that have finite RAM. In order to detect 100% of malware regardless of file size, a firewall would need infinitely
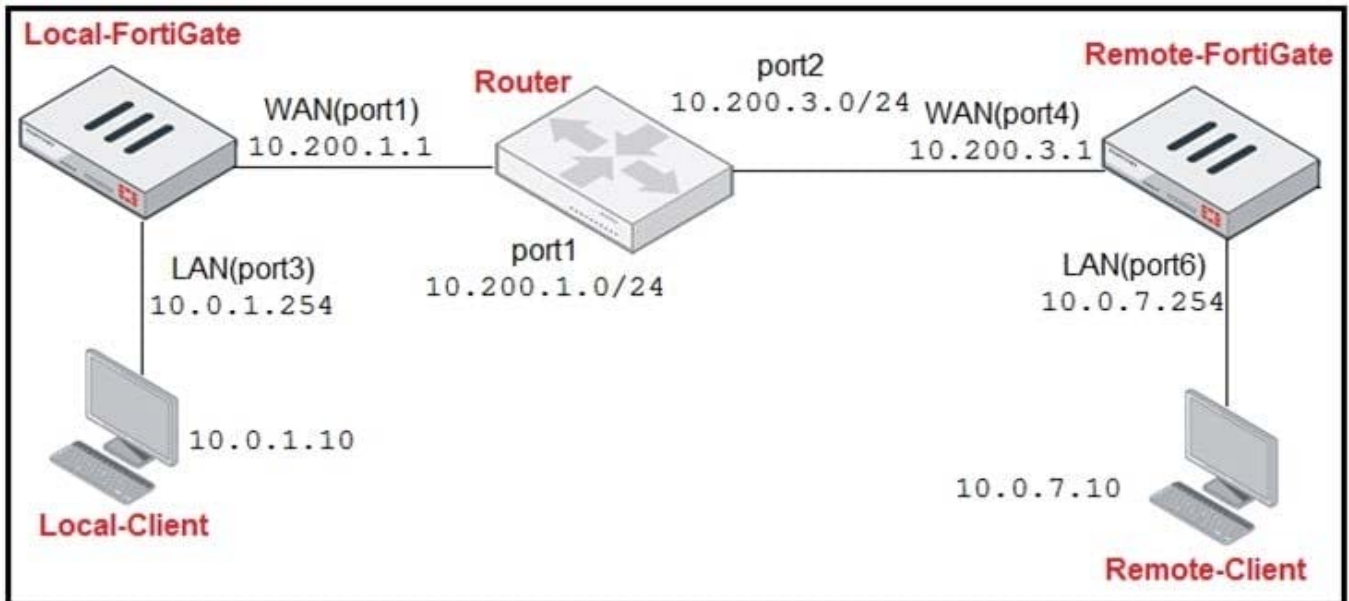
large RAM--something that no device has in the real world. Most viruses are very small. This table shows a typical tradeoff. You can see that with the default 10 MB threshold, only 0.01% of viruses pass through.

QUESTION 5

Refer to the exhibit.

Network Diagram

Central SNAT Policies Local-FortiGate

ID	From	To	Source Address	Protocol Number	Destination Address	Translated Address
□	●					
2	LAN(port3)	WAN(port1)	all	6	REMOTE_FORTIGATE	SNAT-Pool
1	LAN(port3)	WAN(port1)	all	1	all	SNAT-Remote1
3	LAN(port3)	WAN(port1)	all	2	all	SNAT-Remote

IP Pool Local-FortiGate

Name ⇕	External IP Range ⇕	Type ⇕	ARP Reply ⇕
SNAT-Pool	10.200.1.49-10.200.1.49	Overload	✔ Enabled
SNAT-Remote	10.200.1.149-10.200.1.149	Overload	✔ Enabled
SNAT-Remote1	10.200.1.99-10.200.1.99	Overload	✔ Enabled

Protocol Number Table

Protocol Number Table	
Protocol	Protocol Number
TCP	6
ICMP	1
IGMP	2

The exhibit contains a network diagram, central SNAT policy, and IP pool configuration.

The WAN (port1) interface has the IP address 10.200.1.1/24.

The LAN (port3) interface has the IP address 10.0.1.254/24.

A firewall policy is configured to allow to destinations from LAN (port3) to WAN (port1).

Central NAT is enabled, so NAT settings from matching Central SNAT policies will be applied.

Which IP address will be used to source NAT the traffic, if the user on Local-Client (10.0.1.10) pings the IP

address of Remote-FortiGate (10.200.3.1)?

A. 10.200.1.149

B. 10.200.1.1

C. 10.200.1.49

D. 10.200.1.99

Correct Answer: D

NSE4_FGT-7.0 PDF Dumps   NSE4_FGT-7.0 VCE Dumps   NSE4_FGT-7.0 Practice
                                                        Test