NSE4-5.4^{Q&As}

Fortinet Network Security Expert 4 Written Exam - FortiOS 5.4

Pass Fortinet NSE4-5.4 Exam with 100% Guarantee

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

https://www.passapply.com/nse4-5-4.html

100% Passing Guarantee
100% Money Back Assurance

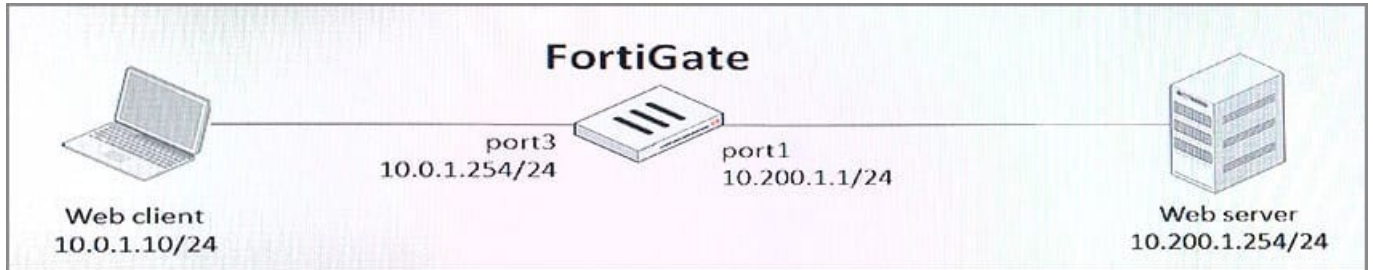Following Questions and Answers are all new published by Fortinet
Official Exam Center

⚙ **Instant Download** After Purchase

⚙ **100% Money Back** Guarantee

⚙ **365 Days** Free Update

⚙ **800,000+** Satisfied Customers

QUESTION 1

View the exhibit.

The client cannot connect to the HTTP web server. The administrator run the FortiGate built-in sniffer and got the following output:

```
FortiGate # diagnose sniffer packet any "port 80" 4
interfaces=[any]
filters=[port 80]
11.510058 port3 in 10.0.1.10.49255 -> 10.200.1.254.80: syn 697263124
11.760531 port3 in 10.0.1.10.49255 -> 10.200.1.254.80: syn 868017830
14.505371 port3 in 10.0.1.10.49255 -> 10.200.1.254.80: syn 697263124
14.755510 port3 in 10.0.1.10.49255 -> 10.200.1.254.80: syn 868017830
```

What should be done next to troubleshoot the problem?

A. Execute another sniffer in the FortiGate, this time with the filter "host 10.0.1.10".

B. Run a sniffer in the web server.

C. Capture the traffic using an external sniffer connected to port1.

D. Execute a debug flow.

Correct Answer: B

QUESTION 2

Which statement describes how traffic flows in sessions handled by a slave unit in an active- active HA cluster?

A. Packet are sent directly to the slave unit using the slave physical MAC address.

B. Packets are sent directly to the slave unit using the HA virtual MAC address.

C. Packets arrived at both units simultaneously, but only the salve unit forwards the session.

D. Packets are first sent to the master unit, which then forwards the packets to the slave unit.

Correct Answer: D

QUESTION 3

Which of the following statements are correct concerning IPsec dialup VPN configurations for FortiGate devices? (Choose two)

A. Main mode mist be used when there is no more than one IPsec dialup VPN configured on the same FortiGate device.

B. A FortiGate device with an IPsec VPN configured as dialup can initiate the tunnel connection to any remote IP address.

C. Peer ID must be used when there is more than one aggressive-mode IPsec dialup VPN on the same FortiGate device.

D. The FortiGate will automatically add a static route to the source quick mode selector address received from each remote peer.

Correct Answer: CD

QUESTION 4

The eicar test virus is put into a zip archive, which is given the password of "Fortinet" in order to open the archive. Review the configuration in the exhibits shown below; then answer the question that follows. Exhibit A - Antivirus Profile:

Inspection Mode	○ Proxy	⦿ Flow-based

☐ Block Connections to Botnet Servers

Protocol	Virus Scan and Removal
Web	
HTTP	☑
Email	
SMTP	☐
POP3	☐
IMAP	☐
MAPI	☐
File Transfer	
FTP	☐
SMB	☐
IM	
ICQ, Yahoo, MSN Messenger	☐

Exhibit B - Non-default UTM Proxy Options Profile:

Protocol Port Mapping

Enable	Protocol	Inspection Port(s)		
✓	HTTP	○ Any	◉ Specify	8080
✓	SMTP	○ Any	◉ Specify	25
✓	POP3	○ Any	◉ Specify	110
✓	IMAP	○ Any	◉ Specify	143
✓	FTP	○ Any	◉ Specify	21
✓	NNTP	○ Any	◉ Specify	119
✓	MAPI	135		
✓	DNS	53		

Exhibit C - DLP Profile: Which of one the following profiles could be enabled in order to prevent the file from passing through the FortiGate device over HTTP on the standard port for that protocol?

⊕ Create New	✎ Edit Filter	⬚ Delete		
Seq #	Type	Action	Services	Archive
1	Encrypted	Block	POP3, HTTP	Disable

Apply

A. Only Exhibit A

B. Only Exhibit B

C. Only Exhibit C with default UTM Proxy settings.

D. All of the Exhibits (A, B and C)

E. Only Exhibit C with non-default UTM Proxy settings (Exhibit B).

Correct Answer: C

QUESTION 5

Which of the following Fortinet hardware accelerators can be used to offload flow-based antivirus inspection? (Choose two.)

A. SP3

B. CP8

C. NP4

D. NP6

Correct Answer: AB