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.leads4pass.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

Examine this FortiGate configuration:

```
config authentication setting
      set active-auth-scheme SCHEME1
end
config authentication rule
      edit WebProxyRule
         set srcaddr 10.0.1.0/24
         set active-auth-method SCHEME2
      next
end
```

How does the FortiGate handle web proxy traffic coming from the IP address 10.2.1.200 that requires authorization?

A. It always authorizes the traffic without requiring authentication.

B. It drops the traffic.

C. It authenticates the traffic using the authentication scheme SCHEME2.

D. It authenticates the traffic using the authentication scheme SCHEME1.

Correct Answer: D

"What happens to traffic that requires authorization, but does not match any authentication rule? The active and passive SSO schemes to use for those cases is defined under config authentication setting"

QUESTION 2

Which statements are true regarding firewall policy NAT using the outgoing interface IP address with fixed port disabled? (Choose two.)

A. This is known as many-to-one NAT.

B. Source IP is translated to the outgoing interface IP.

C. Connections are tracked using source port and source MAC address.

D. Port address translation is not used.

Correct Answer: BD

QUESTION 3

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 4

Refer to the exhibit.

Network Diagram
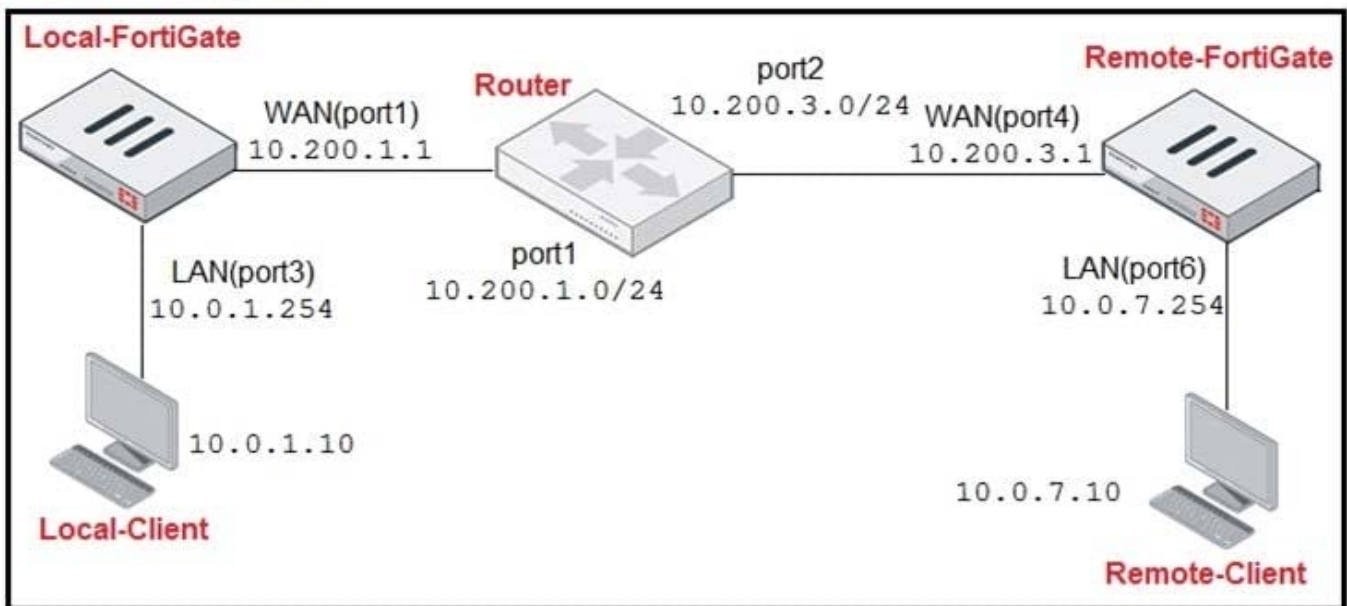
Central SNAT Policies Local-FortiGate

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	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

QUESTION 5

You have enabled logging on your FortiGate device for Event logs and all Security logs, and you have set up logging to use the FortiGate local disk.

What is the default behavior when the local disk is full?

A. Logs are overwritten and the only warning is issued when log disk usage reaches the threshold of 95%.

B. No new log is recorded until you manually clear logs from the local disk.

C. Logs are overwritten and the first warning is issued when log disk usage reaches the threshold of 75%.

D. No new log is recorded after the warning is issued when log disk usage reaches the threshold of 95%.

Correct Answer: C

Reference: https://docs.fortinet.com/document/fortigate/6.4.0/cli-reference/462620/log-disk-setting

Latest NSE4_FGT-7.0 Dumps   NSE4_FGT-7.0 PDF Dumps   NSE4_FGT-7.0 Study Guide Dumps