



NSE4_FGT-7.2^{Q&As}

Fortinet NSE 4 - FortiOS 7.2

Pass Fortinet NSE4_FGT-7.2 Exam with 100% Guarantee

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

https://www.geekcert.com/nse4_fgt-7-2.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

Which two statements are correct about a software switch on FortiGate? (Choose two.)

- A. It can be configured only when FortiGate is operating in NAT mode
- B. Can act as a Layer 2 switch as well as a Layer 3 router
- C. All interfaces in the software switch share the same IP address
- D. It can group only physical interfaces

Correct Answer: AC

QUESTION 2

Which two statements about FortiGate FSSO agentless polling mode are true? (Choose two.)

- A. FortiGate uses the AD server as the collector agent.
- B. FortiGate uses the SMB protocol to read the event viewer logs from the DCs.
- C. FortiGate does not support workstation check .
- D. FortiGate directs the collector agent to use a remote LDAP server.

Correct Answer: BC

You can deploy FSSO w/o installing an agent. FG polls the DCs directly, instead of receiving logon info indirectly from a collector agent.

Because FG collects all of the data itself, agentless polling mode requires greater system resources, and it doesn't scale as easily.

Agentless polling mode operates in a similar way to WinSecLog, but with only two event IDs: 4768 and 4769. Because there's no collector agent, FG uses the SMB protocol to read the event viewer logs from the DCs.

FG acts as a collector. It's responsible for polling on top of its normal FSSO tasks but does not have all the extra features, such as workstation checks, that are available with the external collector agent.

Reference: <https://kb.fortinet.com/kb/documentLink.do?externalID=FD47732> <https://community.fortinet.com/t5/FortiGate/Troubleshooting-Tip-How-to-troubleshoot-FSSO-agentless-polling/ta-p/214349>

QUESTION 3

A network administrator has enabled full SSL inspection and web filtering on FortiGate. When visiting any HTTPS websites, the browser reports certificate warning errors. When visiting HTTP websites, the browser does not report errors.

What is the reason for the certificate warning errors?



- A. The matching firewall policy is set to proxy inspection mode.
- B. The certificate used by FortiGate for SSL inspection does not contain the required certificate extensions.
- C. The full SSL inspection feature does not have a valid license.
- D. The browser does not trust the certificate used by FortiGate for SSL inspection.

Correct Answer: D

FortiGate Security 7.2 Study Guide (p.235): "If FortiGate receives a trusted SSL certificate, then it generates a temporary certificate signed by the built-in Fortinet_CA_SSL certificate and sends it to the browser. If the browser trusts the Fortinet_CA_SSL certificate, the browser completes the SSL handshake. Otherwise, the browser also presents a warning message informing the user that the site is untrusted. In other words, for this function to work as intended, you must import the Fortinet_CA_SSL certificate into the trusted root CA certificate store of your browser."

QUESTION 4

Refer to the exhibit.

Name	Severity	Target	OS	Action
IPS Signature 1				
FTP.Login.Failed	5	Server	All	Pass

Review the Intrusion Prevention System (IPS) profile signature settings. Which statement is correct in adding the FTP.Login.Failed signature to the IPS sensor profile?

- A. The signature setting uses a custom rating threshold.
- B. The signature setting includes a group of other signatures.
- C. Traffic matching the signature will be allowed and logged.
- D. Traffic matching the signature will be silently dropped and logged.



Correct Answer: D

Select Block to silently drop traffic matching any of the signatures included in the entry. So, while the default action would be \\Pass\\ for this signature the administrator is specifically overriding that to set the Block action. To use the default action the setting would have to be \\Default\\.

Action is drop, signature default action is listed only in the signature, it would only match if action was set to default.

QUESTION 5

Refer to the exhibits.

Exhibit A shows a network diagram. Exhibit B shows the firewall policy configuration and a VIP object 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.



Exhibit A Exhibit B

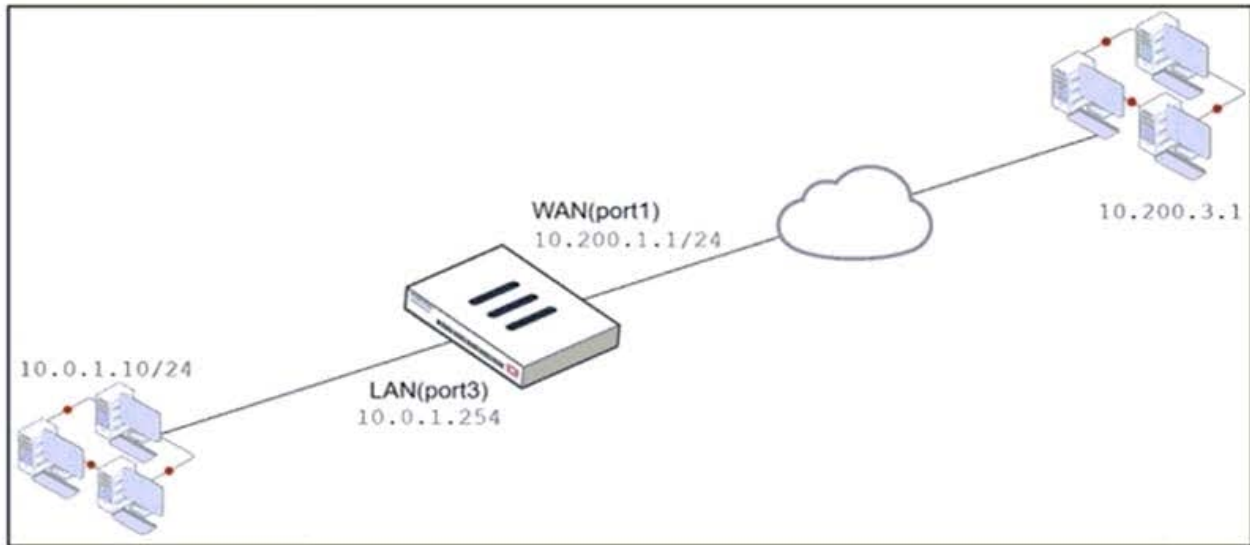


Exhibit A Exhibit B

Name	From	To	Source	Destination	Schedule	Service	Action	NAT
WebServer	WAN (port1)	LAN (port3)	all	VIP	always	ALL	ACCEPT	Enabled

Edit Virtual IP

VIP type: IPv4
 Name: VIP
 Comments: Write a comment... 0/255
 Color: Change

Network

Interface: WAN (port1)
 Type: Static NAT
 External IP address/range: 10.200.1.10
 Map to:
 IPv4 address/range: 10.0.1.10

Optional Filters

Port Forwarding

Protocol: **TCP** | UDP | SCTP | ICMP
 Port Mapping Type: **One to one** | Many to many
 External service port: 10443
 Map to IPv4 port: 443

If the host 10.200.3.1 sends a TCP SYN packet on port 10443 to 10.200.1.10, what will the source address, destination



address, and destination port of the packet be, after FortiGate forwards the packet to the destination?

- A. 10.0.1.254, 10.0.1.10, and 443, respectively
- B. 10.0.1.254, 10.200.1.10, and 443, respectively
- C. 10.200.3.1, 10.0.1.10, and 443, respectively
- D. 10.0.1.254, 10.0.1.10, and 10443, respectively

Correct Answer: A

Translations:

10.200.3.1 --> 10.0.1.254 because NAT enable in firewall policy

10.200.1.10 --> 10.0.1.10 because VIP as Destination 10443 --> 443 because Port Forwarding enabled on VIP

Reference and download study guide: <https://ebin.pub/fortinet-fortigate-security-study-guide-for-fortios-72.html>

[Latest NSE4_FGT-7.2 Dumps](#)

[NSE4_FGT-7.2 Study Guide](#)

[NSE4_FGT-7.2 Exam Questions](#)