NSE4^Q&As

Fortinet Network Security Expert 4 Written Exam (400)

Pass Fortinet NSE4 Exam with 100% Guarantee

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

https://www.pass4itsure.com/nse4.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

Which IPsec configuration mode can be used for implementing GRE-over-IPsec VPNs?

A. Policy-based only.

B. Route-based only.

C. Either policy-based or route-based VPN.

D. GRE-based only.

Correct Answer: B

QUESTION 2

What functions can the IPv6 Neighbor Discovery Protocol accomplish? (Choose two.)

A. Negotiate the encryption parameters to use.

B. Auto-adjust the MTU setting.

C. Autoconfigure addresses and prefixes.

D. Determine other nodes reachability.

Correct Answer: CD

QUESTION 3

Which of the following statements is true regarding a FortiGate device operating in transparent mode? (Choose three.)

A. It acts as a layer 2 bridge

B. It acts as a layer 3 router

C. It forwards frames using the destination MAC address.

D. It forwards packets using the destination IP address.

E. It can perform content inspection (antivirus, web filtering, etc)

Correct Answer: ACE

QUESTION 4

If you enable the option "Generate Logs when Session Starts", what effect does this have on the number of traffic log messages generated for each session?

A. No traffic log message is generated.

B. One traffic log message is generated.

C. Two traffic log messages are generated.

D. A log message is only generated if there is a security event.

Correct Answer: C

QUESTION 5

FSSO provides a single sign on solution to authenticate users transparently to a FortiGate unit using credentials stored in Windows active directory.

Which of the following statements are correct regarding FSSO in a Windows domain environment when DC-agent mode is used? (Choose two.)

A. An FSSO collector agent must be installed on every domain controller.

B. An FSSO domain controller agent must be installed on every domain controller.

C. The FSSO domain controller agent will regularly update user logon information on the FortiGate unit.

D. The FSSO collector agent will receive user logon information from the domain controller agent and will send it to the FortiGate unit.

Correct Answer: BD

QUESTION 6

Which is true of FortiGate\\'s session table?

A. NAT/PAT is shown in the central NAT table, not the session table.

B. It shows TCP connection states.

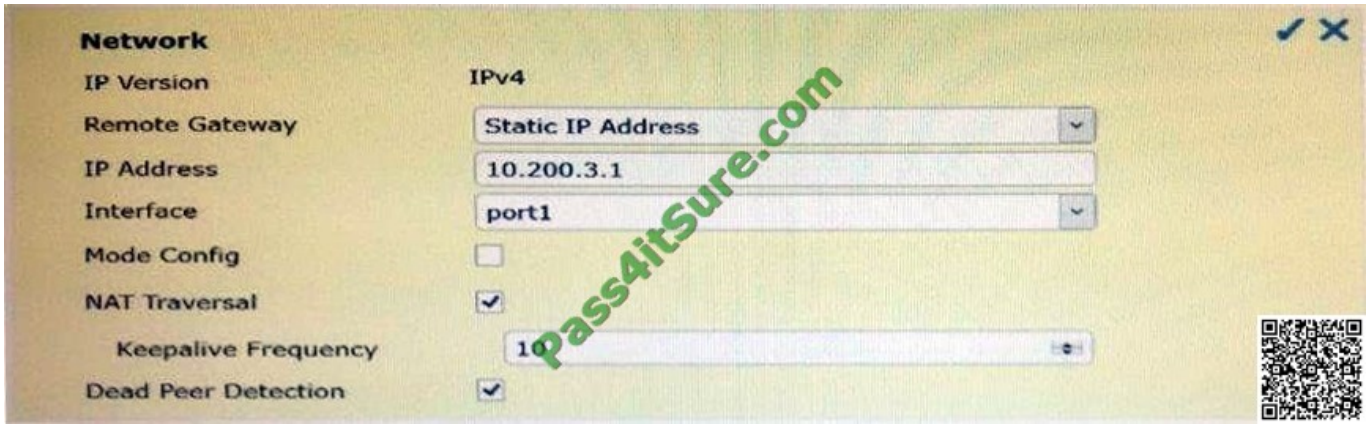
C. It shows IP, SSL, and HTTP sessions.

D. It does not show UDP or ICMP connection state codes, because those protocols are connectionless.

Correct Answer: B

QUESTION 7

Review the IPsec phase 1 configuration in the exhibit; then answer the question below.



Which statements are correct regarding this configuration? (Choose two.)

A. The remote gateway address is 10.200.3.1

B. The local IPsec interface address is 10.200.3.1

C. The local gateway IP is the address assigned to port1

D. The local gateway IP is 10.200.3.1

Correct Answer: AC

QUESTION 8

Which statements are true regarding local user authentication? (Choose two.)

A. Two-factor authentication can be enabled on a per user basis.

B. Local users are for administration accounts only and cannot be used to authenticate network users.

C. Administrators can create the user accounts in a remote server and store the user passwords locally in the FortiGate.

D. Both the usernames and passwords can be stored locally on the FortiGate.

Correct Answer: AD

QUESTION 9

Which best describe the mechanism of a TCP SYN flood?

A. The attacker keeps open many connections with slow data transmission so that other clients cannot start new connections.

B. The attacker sends a packet designed to "sync" with the FortiGate.

C. The attacker sends a specially crafted malformed packet, intended to crash the target by exploiting its parser.

D. The attacker starts many connections, but never acknowledges to fully form them.

Correct Answer: D

QUESTION 10

Which statement is correct regarding virus scanning on a FortiGate unit?

A. Virus scanning is enabled by default.

B. Fortinet customer support enables virus scanning remotely for you.

C. Virus scanning must be enabled in a security profile, which must be applied to a firewall policy.

D. Enabling virus scanning in a UTM security profile enables virus scanning for all traffic flowing through the FortiGate device.

Correct Answer: C

QUESTION 11

Which UTM feature sends a UDP query to FortiGuard servers each time FortiGate scans a packet (unless the response is locally cached)?

A. Antivirus

B. VPN

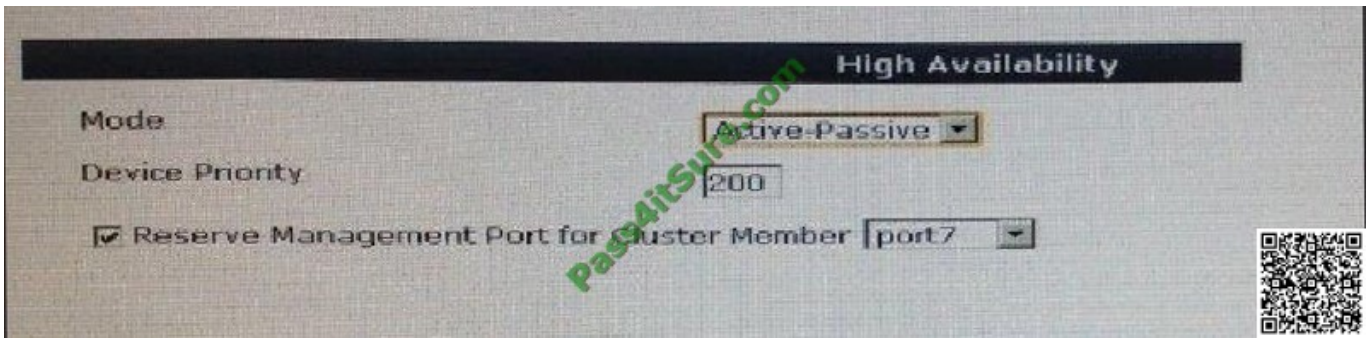
C. IPS

D. Web Filtering

Correct Answer: D

QUESTION 12

In HA, the option Reserve Management Port for Cluster Member is selected as shown in the exhibit below.



Which statements are correct regarding this setting? (Choose two.)

A. Interface settings on port7 will not be synchronized with other cluster members.

B. The IP address assigned to this interface must not overlap with the IP address subnet assigned to another interface.

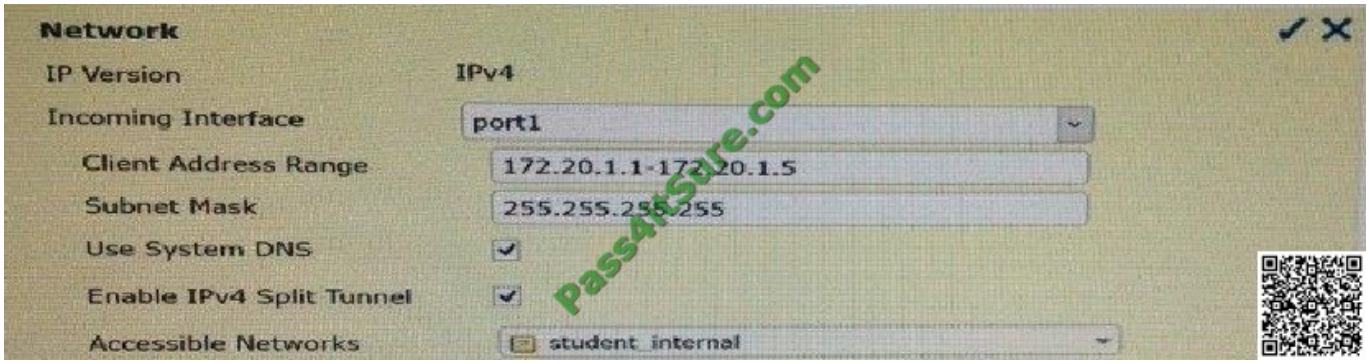
C. When connecting to port7 you always connect to the master device.

D. A gateway address may be configured for port7.

Correct Answer: AD

QUESTION 13

Review the configuration for FortiClient IPsec shown in the exhibit.



Which statement is correct regarding this configuration?

A. The connecting VPN client will install a route to a destination corresponding to the student internal address object.

B. The connecting VPN client will install a default route.

C. The connecting VPN client will install a route to the 172.20.1.[1-5] address range.

D. The connecting VPN client will connect in web portal mode and no route will be installed.

Correct Answer: A

QUESTION 14

What actions are possible with Application Control? (Choose three.)

A. Warn

B. Allow

C. Block

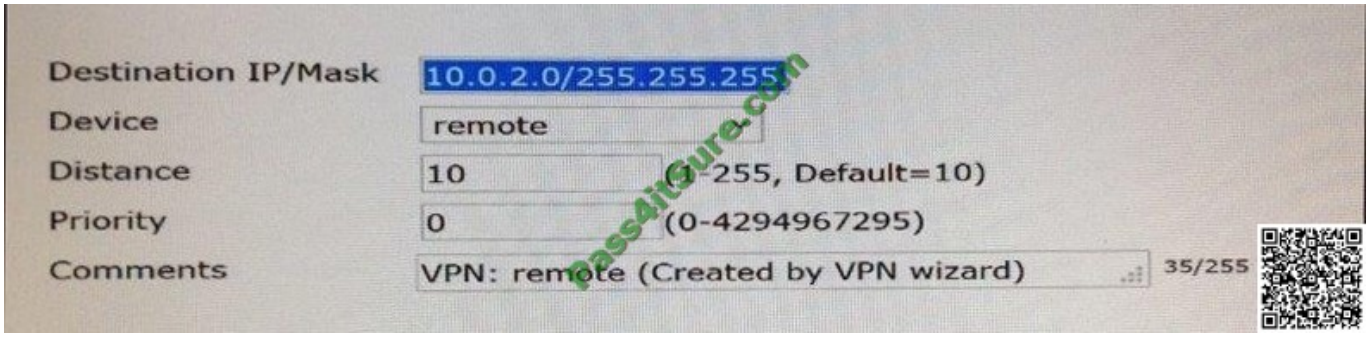
D. Traffic Shaping

E. Quarantine

Correct Answer: BCD

QUESTION 15

Review the static route configuration for IPsec shown in the exhibit; then answer the question below.



Which statements are correct regarding this configuration? (Choose two.)

A. Interface remote is an IPsec interface.

B. A gateway address is not required because the interface is a point-to-point connection.

C. A gateway address is not required because the default route is used.

D. Interface remote is a zone.

Correct Answer: AB

QUESTION 16

Which of the following statements are correct concerning IKE mode config? (Choose two)

A. It can dynamically assign IP addresses to IPsec VPN clients.

B. It can dynamically assign DNS settings to IPsec VPN clients.

C. It uses the ESP protocol.

D. It can be enabled in the phase 2 configuration.

Correct Answer: AB

QUESTION 17

Which statements are true about offloading antivirus inspection to a Security Processor (SP)? (Choose two.)

A. Both proxy-based and flow-based inspection are supported.

B. A replacement message cannot be presented to users when a virus has been detected.

C. It saves CPU resources.

D. The ingress and egress interfaces can be in different SPs.

Correct Answer: BC

QUESTION 18

Which of the following statements are true regarding DLP File Type Filtering? (Choose two.)

A. Filters based on file extension

B. Filters based on fingerprints

C. Filters based on file content

D. File types are hard coded in the FortiOS

Correct Answer: BC

QUESTION 19

A firewall policy has been configured for the internal email server to receive email from external parties through SMTP. Exhibits A and B show the antivirus and email filter profiles applied to this policy.

Exhibit A

Exhibit B:

What is the correct behavior when the email attachment is detected as a virus by the FortiGate antivirus engine?

A. The FortiGate unit will remove the infected file and deliver the email with a replacement message to alert the recipient that the original attachment was infected.

B. The FortiGate unit will reject the infected email and the sender will receive a failed delivery message.

C. The FortiGate unit will remove the infected file and add a replacement message. Both sender and recipient are notified that the infected file has been removed.

D. The FortiGate unit will reject the infected email and notify the sender.

Correct Answer: B

QUESTION 20

Which antivirus and attack definition update options are supported by FortiGate units? (Choose two.)

A. Manual update by downloading the signatures from the support site.

B. FortiGuard pull updates.

C. Push updates from a FortiAnalyzer.

D. execute fortiguard-AV-AS command from the CLI.

Correct Answer: AB

QUESTION 21

A FortiGate is configured with three virtual domains (VDOMs). Which of the following statements is correct regarding multiple VDOMs?

A. The FortiGate must be a model 1000 or above to support multiple VDOMs.

B. A license has to be purchased and applied to the FortiGate before VDOM mode could be enabled.

C. Changing the operational mode of a VDOM requires a reboot of the FortiGate.

D. The FortiGate supports any combination of VDOMs in NAT/Route and transparent modes.

Correct Answer: D

QUESTION 22

Which statement best describes what SSL VPN Client Integrity Check does?

A. Blocks SSL VPN connection attempts from users that has been blacklisted.

B. Detects the Windows client security applications running in the SSL VPN client\\'s PCs.

C. Validates the SSL VPN user credential.

D. Verifies which SSL VPN portal must be presented to each SSL VPN user.

E. Verifies that the latest SSL VPN client is installed in the client\\'s PC.

Correct Answer: B

QUESTION 23

Which of the following statements are correct regarding logging to memory on a FortiGate unit?

A. When the system has reached its capacity for log messages, the FortiGate unit will stop logging to memory.

B. When the system has reached its capacity for log messages, the FortiGate unit overwrites the oldest messages.

C. If the FortiGate unit is reset or loses power, log entries captured to memory will be lost.

D. None of the above.

Correct Answer: BC

QUESTION 24

Review the output of the command get router info routing-table database shown in the exhibit below; then answer the question following it.

```
STUDENT # get router info routing-table database
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       > - selected route, * - FIB route, p - stale info

S     *> 0.0.0.0/0 [10/0] via 10.200.1.254, port1
      *>           [10/0] via 10.200.2.254, port2, [5/0]
C     *> 10.0.1.0/24 is directly connected, port3
S       10.0.2.0/24 [20/0] is directly connected, Remote_2
S     *> 10.0.2.0/24 [10/0] is directly connected, Remote_1
C     *> 10.200.1.0/24 is directly connected, port1
C     *> 10.200.2.0/24 is directly connected, port2
```

Which two statements are correct regarding this output? (Choose two.)

A. There will be six routes in the routing table.

B. There will be seven routes in the routing table.

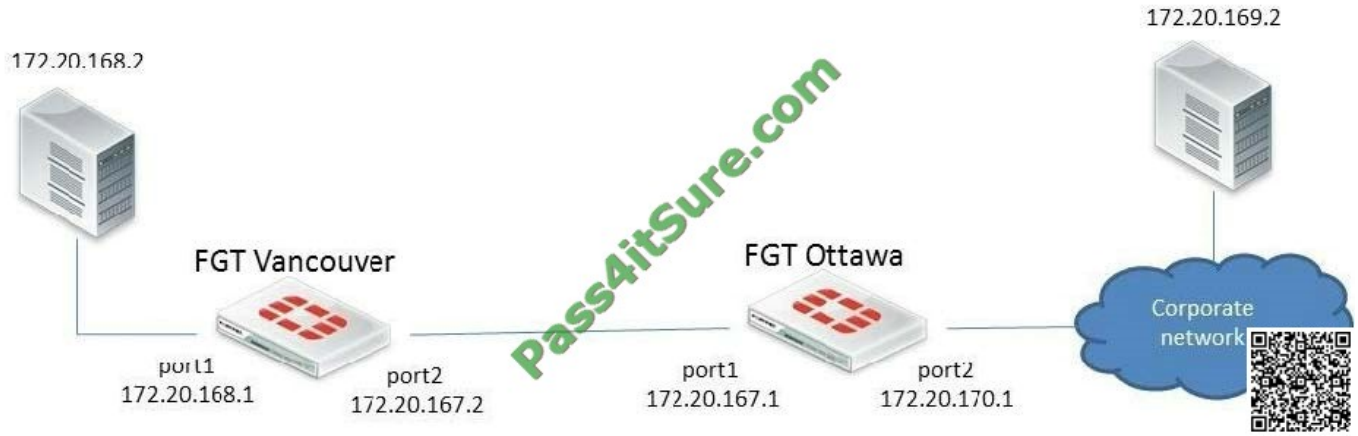
C. There will be two default routes in the routing table.

D. There will be two routes for the 10.0.2.0/24 subnet in the routing table.

Correct Answer: AC

QUESTION 25

Examine the exhibit below; then answer the question following it.



In this scenario. The FortiGate unit in Ottawa has the following routing table: s*0.0.0.0/0 [10/0] via 172.20.170.254, port2 c172.20.167.0/24 is directly connected, port1 c172.20.170.0/24 is directly connected, port2 Sniffer tests show that packets sent from the source IP address 170.20.168.2 to the destination IP address 172.20.169.2 are being dropped by the FortiGate located in Ottawa. Which of the following correctly describes the cause for the

dropped packets?

A. The forward policy check.

B. The reserve path forwarding check.

C. The subnet 172.20.169.0/24 is NOT in the Ottawa FortiGate\\'s routing table.

D. The destination workstation 172.20.169.2 does NOT have the subnet 172.20.168.0/24 in its routing table.

Correct Answer: B

QUESTION 26

Which type of conserve mode writes a log message immediately, rather than when the device exits conserve mode?

A. Kernel

B. Proxy

C. System

D. Device

Correct Answer: B

QUESTION 27

Which of the following statements are true regarding traffic accelerated by an NP processor? (Choose two.)

A. TCP SYN packets are always handled by the NP Processor

B. The initial packets go to the NP Processor, where a decision is taken on if the session can be offloaded or not.

C. Packets for a session termination are always handled by the CPU.

D. The initial packets go to the CPU, where a decision is taken on if the session can be offloaded or not.

Correct Answer: AD

QUESTION 28

Which of the following statements best describe what a FortiGate does when packets match a black hole route?

A. Packets are dropped.

B. Packets are routed based on the information in the policy-based routing table.

C. An ICMP error message is sent back to the originator.

D. Packet are routed back to the originator.

Correct Answer: A

QUESTION 29

Which of the following are possible actions for static URL filtering? (Choose three.)

A. Allow

B. Block

C. Exempt

D. Warning

E. Shape

Correct Answer: ABC

QUESTION 30

What protocol cannot be used with the active authentication type?

A. Local

B. RADIUS

C. LDAP

D. RSSO

Correct Answer: D

QUESTION 31

What are required to be the same for two FortiGate units to form an HA cluster? (Choose two)

A. Firmware.

B. Model.

C. Hostname.

D. System time zone.

Correct Answer: AB

QUESTION 32

An administrator configures a FortiGate unit in Transparent mode on the 192.168.11.0 subnet. Automatic Discovery is

enabled to detect any available FortiAnalyzers on the network. Which of the following FortiAnalyzers will be detected?

A. 192.168.11.100

B. 192.168.11.251

C. 192.168.10.100

D. 192.168.10.251

Correct Answer: AB

QUESTION 33

A FortiGate unit operating in NAT/route mode and configured with two sub-interface on the same physical interface. Which of the following statement is correct regarding the VLAN IDs in this scenario?

A. The two VLAN sub-interfaces can have the same VLAN IDs only if they have IP addresses in different subnets.

B. The two VLAN sub-interfaces must have different VLAN IDs.

C. The two VLAN sub-interfaces can have VLAN ID only if they belong to different VDOMs.

D. The two VLAN sub-interfaces can have the same VLAN if they are connected to different L2 IEEE 802.1Q complaint switches.

Correct Answer: B

QUESTION 34

On your FortiGate 60D, you\\'ve configured firewall policies. They port forward traffic to your Linux Apache web server. Select the best way to protect your web server by using the IPS engine.

A. Enable IPS signatures for Linux servers with HTTP, TCP and SSL protocols and Apache applications. Configured DLP to block HTTP GET request with credit card numbers.

B. Enable IPS signatures for Linux servers with HTTP, TCP and SSL protocols and Apache applications. Configure DLP to block HTTP GET with credit card numbers. Also configure a DoS policy to prevent TCP SYn floods and port scans.

C. None. FortiGate 60D is a desktop model, which does not support IPS.

D. Enable IPS signatures for Linux and windows servers with FTP, HTTP, TCP, and SSL protocols and Apache and PHP applications.

Correct Answer: D

QUESTION 35

Which of the following settings can be configured per VDOM? (Choose three)

A. Operating mode (NAT/route or transparent)

B. Static routes

C. Hostname

D. System time

E. Firewall Policies

Correct Answer: ABE

QUESTION 36

How many packets are interchanged between both IPSec ends during the negotiation of a main-mode phase 1?

A. 5

B. 3

C. 2

D. 6

Correct Answer: D

QUESTION 37

Which of the following statements best describes what a Certificate Signing Request (CSR) is?

A. A message sent by the Certificate Authority (CA) that contains a signed digital certificate.

B. An enquiry submitted to a Certificate Authority (CA) to request a root CA certificate

C. An enquiry submitted to a Certificate Authority (CA) to request a signed digital certificate

D. An enquiry submitted to a Certificate Authority (CA) to request a Certificate Revocation List (CRL)

Correct Answer: B

QUESTION 38

Which action does the FortiGate take when link health monitor times out?

A. All routes to the destination subnet configured in the link health monitor are removed from the routing table.

B. The distance values of all routes using interface configured in the link health monitor are increased.

C. The priority values of all routes using configured in the link health monitor are increased.

D. All routes using the next-hop gateway configured in the link health monitor are removed from the routing table.

Correct Answer: D

QUESTION 39

The exhibit shoes three static routes.

Which routes will be used to route the packets to the destination IP address 172.20.168.1?

A. The route with the ID number 2 and 3.

B. Only the route with the ID number 3.

C. Only the route with the ID number 2.

D. Only the route with the ID number 1.

Correct Answer: D

QUESTION 40

Which of the following IPsec configuration modes can be used when the FortiGate is running in NAT mode?

A. Policy-based VPN only

B. Both policy-based and route-based VPN.

C. Route-based VPN only.

D. IPSec VPNs are not supported when the FortiGate is running in NAT mode.

Correct Answer: B