

Fortinet

Exam Questions NSE4

Fortinet Network Security Expert 4 Written Exam (400)



NEW QUESTION 1

Examine the two static routes to the same destination subnet 172.20.168.0/24 as shown below; then answer the question following it.

```
config router static
edit 1
set dst 172.20.168.0 255.255.255.0
set distance 20
set priority 10
set device port1
next
edit 2
set dst 172.20.168.0 255.255.255.0
set distance 20
set priority 20
set device port2
next
end
```

Which of the following statements correctly describes the static routing configuration provided above?

- A. The FortiGate evenly shares the traffic to 172.20.168.0/24 through both routes.
- B. The FortiGate shares the traffic to 172.20.168.0/24 through both routes, but the port2 route will carry approximately twice as much of the traffic.
- C. The FortiGate sends all the traffic to 172.20.168.0/24 through port1.
- D. Only the route that is using port1 will show up in the routing table.

Answer: C

NEW QUESTION 2

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 compliant switches.

Answer: B

NEW QUESTION 3

Review the exhibit of an explicit proxy policy configuration.

<div> Create New Edit Delete Expand All Collapse All Search </div>								
Seq.#	To	Source	Destination	Users	Schedule	Action	AV	
web (1 - 2)								
1	port1	10.0.1.0/24	all			✓ ACCEPT		
1.1				Student	always			
2	port1	10.0.0.0/8	all		always	✓ ACCEPT		

If there is a proxy connection attempt coming from the IP address 10.0.1.5, and from a user that has not authenticated yet, what action does the FortiGate proxy take?

- A. User is prompted to authenticat
- B. Traffic from the user Student will be allowed by the policy #1. Traffic from any other user will be allowed by the policy #2.
- C. User is not prompted to authenticat
- D. The connection is allowed by the proxy policy #2.
- E. User is not prompted to authenticat
- F. The connection will be allowed by the proxy policy #1.
- G. User is prompted to authenticat
- H. Only traffic from the user Student will be allowe
- I. Traffic from any other user will be blocked.

Answer: D

NEW QUESTION 4

How is traffic routed onto an SSL VPN tunnel from the FortiGate unit side?

- A. A static route must be configured by the administrator using the ssl.root interface as the outgoing interface.
- B. Assignment of an IP address to the client causes a host route to be added to the FortiGate unit's kernel routing table.
- C. A route back to the SSLVPN IP pool is automatically created on the FortiGate unit.

D. The FortiGate unit adds a route based upon the destination address in the SSL VPN firewall policy.

Answer: B

NEW QUESTION 5

Which protocols can you use for secure administrative access to a FortiGate? (Choose two)

- A. SSH
- B. Telnet
- C. NTLM
- D. HTTPS

Answer: AD

NEW QUESTION 6

A FortiGate administrator with the super_admin profile configures a virtual domain (VDM) for a new customer. After creating the VDM, the administrator is unable to reassign the dmz interface to the new VDM as the option is greyed out in the GUI in the management VDM. What would be a possible cause for this problem?

- A. The administrator does not have the proper permissions the dmz interface.
- B. The dmz interface is referenced in the configuration of another VDM.
- C. Non-management VDMs cannot reference physical interfaces
- D. The dmz interface is in PPPoE or DHCP mode.

Answer: B

NEW QUESTION 7

Examine the exhibit; then answer the question below.



The Vancouver FortiGate initially had the following information in its routing table:

S 172.20.0.0/16 [10/0] via 172.21.1.2, port2
 C 172.21.0.0/16 is directly connected, port2
 C 172.11.11.0/24 is directly connected, port1

Afterwards, the following static route was added:

```

config router static edit 6
set dst 172.20.1.0 255.255.255.0
set priority 0
set device port1
set gateway 172.11.12.1 next
  
```

Since this change, the new static route is NOT showing up in the routing table. Given the information provided, which of the following describes the cause of this problem?

- A. The subnet 172.20.1.0/24 is overlapped with the subnet of one static route that is already in the routing table (172.20.0.0/16), so, we need to enable allow-subnet-overlap first.
- B. The 'gateway' IP address is NOT in the same subnet as the IP address of port1.
- C. The priority is 0, which means that the route will remain inactive.
- D. The static route configuration is missing the distance setting.

Answer: B

NEW QUESTION 8

What are examples of correct syntax for the session table diagnostics command? (Choose two.)

- A. diagnose sys session filter clear
- B. diagnose sys session src 10.0.1.254
- C. diagnose sys session filter
- D. diagnose sys session filter list dst.

Answer: AC

NEW QUESTION 9

Your Linux email server runs on a non-standard port number, port 2525. Which statement is true?

- A. IPS cannot scan that traffic for SMTP anomalies because of the non-standard port number
- B. You must reconfigure the server to run on port 25.
- C. To apply IPS to traffic to that server, you must configure FortiGate SMTP proxy to listen on port 2525
- D. IPS will apply all SMTP signatures, regardless of whether they apply to clients or servers.
- E. Protocol decoders automatically detect SMTP and scan for matches with appropriate IPS signature.

Answer: B

NEW QUESTION 10

Review to the network topology in the exhibit.



The workstation, 172.16.1.1/24, connects to port2 of the FortiGate device, and the ISP router, 172.16.1.2, connects to port1. Without changing IP addressing, which configuration changes are required to properly forward users traffic to the Internet? (Choose two)

- A. At least one firewall policy from port2 to port1 to allow outgoing traffic.
- B. A default route configured in the FortiGuard devices pointing to the ISP's router.
- C. Static or dynamic IP addresses in both FortiGate interfaces port1 and port2.
- D. The FortiGate devices configured in transparent mode.

Answer: AD

NEW QUESTION 10

Which best describes the authentication timeout?

- A. How long FortiGate waits for the user to enter his or her credentials.
- B. How long a user is allowed to send and receive traffic before he or she must authenticate again.
- C. How long an authenticated user can be idle (without sending traffic) before they must authenticate again.
- D. How long a user-authenticated session can exist without having to authenticate again.

Answer: C

NEW QUESTION 13

Files reported as "suspicious" were subject to which Antivirus check?"

- A. Grayware
- B. Virus
- C. Sandbox
- D. Heuristic

Answer: D

NEW QUESTION 15

Which statements are correct for port pairing and forwarding domains? (Choose two.)

- A. They both create separate broadcast domains.
- B. Port Pairing works only for physical interfaces.
- C. Forwarding Domain only applies to virtual interfaces
- D. They may contain physical and/or virtual interfaces.

Answer: AD

NEW QUESTION 19

Which profile could IPS engine use on an interface that is in sniffer mode? (Choose three)

- A. Antivirus (flow based)
- B. Web filtering (PROXY BASED)
- C. Intrusion Protection
- D. Application Control
- E. Endpoint control

Answer: ABD

NEW QUESTION 24

A FortiGate is configured with the 1.1.1.1/24 address on the wan2 interface and HTTPS Administrative Access, using the default tcp port, is enabled for that interface. Given the SSL VPN settings in the exhibit.

Listen on Interface(s)

wan2

X

+

This is generally your external interface (i.e. wan1)

Listen on Port

443

▲

▼

URL Path	Virtual Host	Max Concurrent U
Training		0
students		0

Which of the following SSL VPN login portal URLs are valid? (Choose two.)

- A. http://1.1.1.1:443/Training
- B. https://1.1.1.1:443/STUDENTS
- C. https://1.1.1.1/login
- D. https://1.1.1.1/

Answer: BD

NEW QUESTION 29

Review the configuration for FortiClient IPsec shown in the exhibit.

Network

IP Version

IPv4

Incoming Interface

port1

Client Address Range

172.20.1.1-172.20.1.5

Subnet Mask

255.255.255.255

Use System DNS

☒

Enable IPv4 Split Tunnel

☒

Accessible Networks

student_internal

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.

Answer: A

NEW QUESTION 34

Which of the following statements is true regarding the use of a PAC file to configure the web proxy settings in an Internet browser? (Choose two.)

- A. More than one proxy is supported.
- B. Can contain a list of destinations that will be exempt from the use of any proxy.
- C. Can contain a list of URLs that will be exempted from the FortiGate web filtering inspection.
- D. Can contain a list of users that will be exempted from the use of any proxy.

Answer: BC

NEW QUESTION 38

What is the maximum number of different virus databases a FortiGate can have?

- A. 5
- B. 2
- C. 3
- D. 4

Answer: B

NEW QUESTION 42

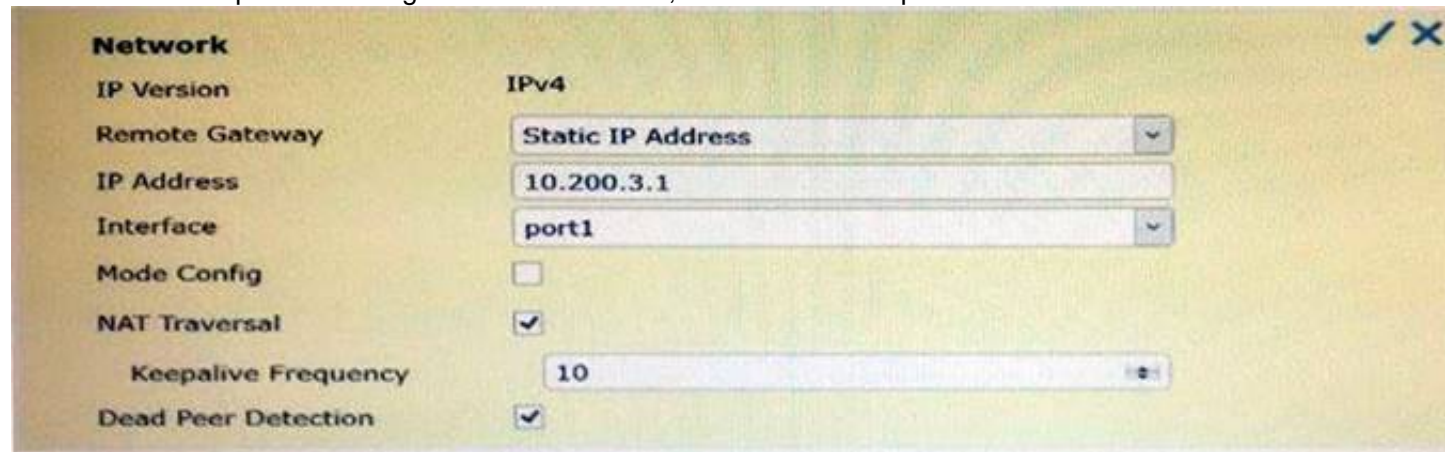
Which are valid replies from a RADIUS server to an ACCESS-REQUEST packet from a FortiGate? (Choose two.)

- A. ACCESS-CHALLENGE
- B. ACCESS-RESTRICT
- C. ACCESS-PENDING
- D. ACCESS-REJECT

Answer: AD

NEW QUESTION 45

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

Answer: AC

NEW QUESTION 46

For data leak prevention, which statement describes the difference between the block and quarantine actions?

- A. A block action prevents the transactio
- B. A quarantine action blocks all future transactions, regardless of the protocol.
- C. A block action prevents the transactio
- D. A quarantine action archives the data.
- E. A block action has a finite duratio
- F. A quarantine action must be removed by an administrator.
- G. A block action is used for known user
- H. A quarantine action is used for unknown users.

Answer: A

NEW QUESTION 49

Examine the output below from the diagnose sys top command:

```
# diagnose sys top 1
Run time: 11 days, 3 hours and 29 minutes
OU,  ON,  1S,  99I;  971T,  528F,  160 KF
sshd      123      S      1.9    1.2
ipsendjine 61      S<     0.0    5.2
miglogd   45      S      0.0    4.9
pyfcgid   75      S      0.0    4.5
pyfcgid   73      S      0.0    3.9
```

Which statements are true regarding the output above (Choose two.)

- A. The sshd process is the one consuming most CPU.
- B. The sshd process is using 123 pages of memory.
- C. The command diagnose sys kill miglogd will restart the miglogd process.
- D. All the processes listed are in sleeping state.

Answer: AD

NEW QUESTION 52

Which of the following authentication methods can be used for SSL VPN authentication? (Choose three.)

- A. Remote Password Authentication (RADIUS, LDAP)
- B. Two-Factor Authentication
- C. Local Password Authentication
- D. FSSO
- E. RSSO

Answer: ABC

NEW QUESTION 56

Which antivirus inspection mode must be used to scan SMTP, FTP, POP3 and SMB protocols?

- A. Proxy-based.
- B. DNS-based.

- C. Flow-based.
- D. Man-in-the-middle.

Answer: C

NEW QUESTION 61

Where are most of the security events logged?

- A. Security log
- B. Forward Traffic log
- C. Event log
- D. Alert log
- E. Alert Monitoring Console

Answer: C

NEW QUESTION 64

Which commands are appropriate for investigating high CPU? (Choose two.)

- A. diag sys top
- B. diag hardware sysinfo mem
- C. diag debug flow
- D. get system performance status

Answer: AD

NEW QUESTION 67

Review the IPsec diagnostics output of the command diagnose vpn tunnel list shown in the exhibit below.

```
STUDENT # diagnose vpn tunnel list
list all ipsec tunnel in vd 0
-----
name=FCClient_0 ver=1 serial=3 10.200.1.1:4500->10.200.3.1:64916 lgwy=static tun=intf mode=dial_inst bound_if=2
parent=FCClient index=0
proxyid_num=1 child_num=0 refcnt=8 ilast=2 olast=2
stat: rxp=59 txp=0 rxb=15192 txb=0
dpd: mode=active on=1 idle=5000ms retry=3 count=0 seqno=10
natt: mode=keepalive draft=32 interval=10 remote_port=64916
proxyid=FCClient proto=0 sa=1 ref=2 auto_negotiate=0 serial=1
  src: 0:0.0.0.0-255.255.255.255:0
  dst: 0:172.20.1.1-172.20.1.1:0
  SA: ref=3 options=00000006 type=00 soft=0 mtu=1280 expire=1717 replaywin=1024 seqno=1
  life: type=01 bytes=0/0 timeout=1791/1800
  dec: spi=a29046e9 esp=3des key=24 0525830c6fd67ca37e9d6dad174d175e24f97c3b87f428fa
      ah=sha1 key=20 982f8ba194f3f797773efc605c8321b728dabf1d
  enc: spi=19be4052 esp=3des key=24 da597cb7fec913528f8598d1aa7ecd17156a2a7a4afeeb4c
      ah=sha1 key=20 9e2c5d0fc055fa0149bc66024732e9a85bbe8016
-----
```

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

- A. The connecting client has been allocated address 172.20.1.1.
- B. In the Phase 1 settings, dead peer detection is enabled.
- C. The tunnel is idle.
- D. The connecting client has been allocated address 10.200.3.1.

Answer: AB

NEW QUESTION 68

Which statements are true regarding the use of a PAC file to configure the web proxy settings in an Internet browser? (Choose two.)

- A. Only one proxy is supported.
- B. Can be manually imported to the browser.
- C. The browser can automatically download it from a web server.
- D. Can include a list of destination IP subnets where the browser can connect directly to without using a proxy.

Answer: CD

NEW QUESTION 70

What is not true of configuring disclaimers on the FortiGate?

- A. Disclaimers can be used in conjunction with captive portal.
- B. Disclaimers appear before users authenticate.
- C. Disclaimers can be bypassed through security exemption lists.
- D. Disclaimers must be accepted in order to continue to the authentication login or originally intended destination.

Answer: C

NEW QUESTION 74

Which is one of the conditions that must be met for offloading the encryption and decryption of IPsec traffic to an NP6 processor?

- A. no protection profile can be applied over the IPsec traffic.
- B. Phase-2 anti-replay must be disabled.
- C. Phase 2 must have an encryption algorithm supported by the NP6.
- D. IPsec traffic must not be inspected by any FortiGate session helper.

Answer: C

NEW QUESTION 77

Regarding the header and body sections in raw log messages, which statement is correct?

- A. The header and body section layouts change depending on the log type.
- B. The header section layout is always the same regardless of the log type
- C. The body section layout changes depending on the log type.
- D. Some log types include multiple body sections.
- E. Some log types do not include a body section.

Answer: B

NEW QUESTION 81

Which two methods are supported by the web proxy auto-discovery protocol (WPAD) to automatically learn the URL where a PAC file is located? (Choose two.)

- A. DHCP
- B. BOOTP
- C. DNS
- D. IPv6 autoconfiguration.

Answer: AC

NEW QUESTION 86

When an administrator attempts to manage FortiGate from an IP address that is not a trusted host, what happens?

- A. FortiGate will still subject that person's traffic to firewall policies; it will not bypass them.
- B. FortiGate will drop the packets and not respond.
- C. FortiGate responds with a block message, indicating that it will not allow that person to log in.
- D. FortiGate responds only if the administrator uses a secure protocol
- E. Otherwise, it does not respond

Answer: B

NEW QUESTION 90

Which statement is not correct regarding SSL VPN Tunnel mode?

- A. IP traffic is encapsulated over HTTPS.
- B. The standalone FortiClient SSL VPN client can be used to establish a Tunnel mode SSL VPN.
- C. A limited amount of IP applications are supported.
- D. The FortiGate device will dynamically assign an IP address to the SSL VPN network adapter.

Answer: C

NEW QUESTION 92

Which of the following statements best describes what a Public Certificate Authority (CA) is?

- A. A service that provides a digital certificate each time a user is authenticating
- B. An entity that certifies that the information contained in a digital certificate is valid and true.
- C. The FortiGate process in charge of generating digital certificates on the fly for SSL inspection purposes
- D. A service that validates digital certificates for certificate-based authentication purposes

Answer: D

NEW QUESTION 93

Which of the following statement correct describes the use of the "diagnose sys ha reset- uptime" command?

- A. To force an HA failover when the HA override setting is disabled.
- B. To force an HA failover when the HA override setting is enabled.
- C. To clear the HA counters.
- D. To restart a FortiGate unit that is part of an HA cluster.

Answer: A

NEW QUESTION 94

Which of the following web filtering modes can inspect the full URL? (Choose two.)

- A. Proxy based
- B. DNS based
- C. Policy based

D. Flow based

Answer: AD

NEW QUESTION 98

In a Crash log, what does a status of 0 indicate?

- A. Abnormal termination of a process
- B. A process closed for any reason
- C. Scanunitd process crashed
- D. Normal shutdown with no abnormalities
- E. DHCP process crashed

Answer: D

NEW QUESTION 100

Regarding tunnel-mode SSL VPN, which three statements are correct? (Choose three.)

- A. Split tunneling is supported.
- B. It requires the installation of a VPN client.
- C. It requires the use of an Internet browser.
- D. It does not support traffic from third-party network applications.
- E. An SSL VPN IP address is dynamically assigned to the client by the FortiGate unit.

Answer: ABE

NEW QUESTION 103

Which is not a FortiGate feature?

- A. Database auditing
- B. Intrusion prevention
- C. Web filtering
- D. Application control

Answer: A

NEW QUESTION 107

Which of the following are possible actions for FortiGuard web category filtering? (Choose three.)

- A. Allow
- B. Block
- C. Exempt
- D. Warning
- E. Shape

Answer: ABD

NEW QUESTION 111

Examine the following spanning tree configuration on a FortiGate in transparent mode:

```
config system interface edit <interface name> set stp-forward enable end
```

Which statement is correct for the above configuration?

- A. The FortiGate participates in spanning tree.
- B. The FortiGate device forwards received spanning tree messages.
- C. Ethernet layer-2 loops are likely to occur.
- D. The FortiGate generates spanning tree BPDU frames.

Answer: B

NEW QUESTION 115

Which best describes the mechanism of a TCP SYN flood?

- A. The attackers keeps open many connections with slow data transmission so that other clients cannot start new connections.
- B. The attackers sends a packets 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.

Answer: D

NEW QUESTION 120

A FortiGate is operating in NAT/Route mode and configured with two virtual LAN (VLAN) sub-interfaces added to the same physical interface.

Which one of the following statements is correct regarding the VLAN IDs in this scenario?

- A. The two VLAN sub-interfaces can have the same VLAN ID 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 the same VLAN ID only if they belong to different VDOMs.
- D. The two VLAN sub-interfaces can have the same VLAN ID if they are connected to different L2 IEEE 802.1Q compliant switches.

Answer: B

NEW QUESTION 121

Which of the following actions can be used to back up the keys and digital certificates in a FortiGate device? (Choose two.)

- A. Taking a full backup of the FortiGate configuration
- B. Uploading a PKCS#10 file to a USB drive
- C. Manually uploading the certificate information to a Certificate authority (CA)
- D. Uploading a PKCS#12 file to a TFTP server

Answer: AD

NEW QUESTION 126

What action does an IPsec Gateway take with the user traffic routed to an IPsec VPN when it does not match any phase 2 quick mode selector?

- A. Traffic is dropped
- B. Traffic is routed across the default phase 2.
- C. Traffic is routed to the next available route in the routing table.
- D. Traffic is routed unencrypted to the interface where the IPsec VPN is terminating.

Answer: A

NEW QUESTION 128

A backup file begins with this line:

```
#config-version=FGVM64-5.02-FW-build589-140613:opmode=0:vdom=0:user=admin
```

```
#conf_file_ver=3881503152630288414 #buildno=0589 #global_vdom=1
```

Can you restore it to a FortiWiFi 60D?

- A. Yes
- B. Yes, but only if you replace the "#conf_file_ver" line so that it contains the serial number of that specific FortiWiFi 60D.
- C. Yes, but only if it is running the same version of FortiOS, or a newer compatible version.
- D. No

Answer: D

NEW QUESTION 130

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

- A. Allow
- B. Block
- C. Exempt
- D. Warning
- E. Shape

Answer: ABC

NEW QUESTION 134

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.

Answer: B

NEW QUESTION 137

A FortiGate is configured to receive push updates from the FortiGuard Distribution Network, however, they are not being received. Which is one reason for this problem?

- A. The FortiGate is connected to multiple ISPs.
- B. FortiGuard scheduled updates are enabled in the FortiGate configuration.
- C. The FortiGate is in Transparent mode.
- D. The external facing interface of the FortiGate is configured to get the IP address from a DHCP server.

Answer: D

NEW QUESTION 139

Which traffic can match a firewall policy's "Services" setting? (Choose three.)

- A. HTTP

- B. SSL
- C. DNS
- D. RSS
- E. HTTPS

Answer: ACE

NEW QUESTION 144

Acme Web Hosting is replacing one of their firewalls with a FortiGate. It must be able to apply port forwarding to their back-end web servers while blocking virus uploads and TCP SYN floods from attackers. Which operation mode is the best choice for these requirements?

- A. NAT/route
- B. NAT mode with an interface in one-arm sniffer mode
- C. Transparent mode
- D. No appropriate operation mode exists

Answer: A

NEW QUESTION 146

Which of the following statements are true about the SSL Proxy certificate that must be used for SSL Content Inspection? (Choose two.)

- A. It cannot be signed by a private CA
- B. It must have either the field "CA=True" or the field "Key Usage=KeyCertSign"
- C. It must be installed in the FortiGate device
- D. The subject field must contain either the FQDN, or the IP address of the FortiGate device

Answer: CD

NEW QUESTION 149

An administrator has configured a route-based site-to-site IPsec VPN. Which statement is correct regarding this IPsec VPN configuration?

- A. The IPsec firewall policies must be placed at the top of the list.
- B. This VPN cannot be used as a part of a hub and spoke topology.
- C. Routes are automatically created based on the quick mode selectors.
- D. A virtual IPsec interface is automatically created after the Phase 1 configuration is completed.

Answer: D

NEW QUESTION 150

An Internet browser is using the WPAD DNS method to discover the PAC file's URL. The DNS server replies to the browser's request with the IP address 10.100.1.10. Which URL will the browser use to download the PAC file?

- A. http://10.100.1.10/proxy.pac
- B. https://10.100.1.10/
- C. http://10.100.1.10/wpad.dat
- D. https://10.100.1.10/proxy.pac

Answer: C

NEW QUESTION 155

Which two statements are true about IPsec VPNs and SSL VPNs? (Choose two.)

- A. SSL VPN creates a HTTPS connectio
- B. IPsec does not.
- C. Both SSL VPNs and IPsec VPNs are standard protocols.
- D. Either a SSL VPN or an IPsec VPN can be established between two FortiGate devices.
- E. Either a SSL VPN or an IPsec VPN can be established between an end-user workstation and a FortiGate device.

Answer: AD

NEW QUESTION 157

Which statement is correct concerning creating a custom signature?

- A. It must start with the name
- B. It must indicate whether the traffic flow is from the client or the server.
- C. It must specify the protoco
- D. Otherwise, it could accidentally match lower-layer protocols.
- E. It is not supported by Fortinet Technical Support.

Answer: A

NEW QUESTION 162

Which statement regarding the firewall policy authentication timeout is true?

- A. It is an idle timeou

- B. The FortiGate considers a user to be “idle” if it does not see any packets coming from the user's source IP.
- C. It is a hard timeout
- D. The FortiGate removes the temporary policy for a user's source IP address after this timer has expired.
- E. It is an idle timeout
- F. The FortiGate considers a user to be “idle” if it does not see any packets coming from the user's source MAC.
- G. It is a hard timeout
- H. The FortiGate removes the temporary policy for a user's source MAC address after this timer has expired.

Answer: A

NEW QUESTION 164

Which of the following statements are correct concerning the FortiGate session life support protocol? (Choose two)

- A. By default, UDP sessions are not synchronized.
- B. Up to four FortiGate devices in standalone mode are supported.
- C. only the master unit handles the traffic.
- D. Allows per-VDOM session synchronization.

Answer: AD

NEW QUESTION 167

Examine the static route configuration shown below; then answer the question following it.

```
config router static edit 1
set dst 172.20.1.0 255.255.255.0
set device port1
set gateway 172.11.12.1
set distance 10
set weight 5 next
edit 2
set dst 172.20.1.0 255.255.255.0
set blackhole enable set distance 5
set weight 10 next
end
```

Which of the following statements correctly describes the static routing configuration provided? (Choose two.)

- A. All traffic to 172.20.1.0/24 is dropped by the FortiGate.
- B. As long as port1 is up, all traffic to 172.20.1.0/24 is routed by the static route number 1. if the interface port1 is down, the traffic is routed using the blackhole route.
- C. The FortiGate unit does NOT create a session entry in the session table when the traffic is being routed by the blackhole route.
- D. The FortiGate unit creates a session entry in the session table when the traffic is being routed by the blackhole route.

Answer: AC

NEW QUESTION 168

Which FSSO agents are required for a FSSO agent-based polling mode solution?

- A. Collector agent and DC agents
- B. Polling agent only
- C. Collector agent only
- D. DC agents only

Answer: A

NEW QUESTION 170

What are the requirements for a HA cluster to maintain TCP connections after device or link failover? (Choose two.)

- A. Enable session pick-up.
- B. Enable override.
- C. Connections must be UDP or ICMP.
- D. Connections must not be handled by a proxy.

Answer: AD

NEW QUESTION 173

There are eight (8) log severity levels that indicate the importance of an event. Not including Debug, which is only needed to log diagnostic data, what are both the lowest AND highest severity levels?

- A. Notification, Emergency
- B. Information, Critical
- C. Error, Critical
- D. Information, Emergency
- E. Information, Alert

Answer: D

NEW QUESTION 178

Which of the following statements best describe the main requirements for a traffic session to be offload eligible to an NP6 processor? (Choose three.)

- A. Session packets do NOT have an 802.1Q VLAN tag.
- B. It is NOT multicast traffic.
- C. It does NOT require proxy-based inspection.
- D. Layer 4 protocol must be UDP, TCP, SCTP or ICMP.
- E. It does NOT require flow-based inspection.

Answer: CDE

NEW QUESTION 181

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

- A. Main mode must 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.

Answer: CD

NEW QUESTION 184

Which two web filtering inspection modes inspect the full URL? (Choose two.)

- A. DNS-based
- B. Proxy-based
- C. Flow-based
- D. URL-based

Answer: BC

NEW QUESTION 187

Which network protocols are supported for administrative access to a FortiGate unit? (Choose three.)

- A. SMTP
- B. WINS
- C. HTTP
- D. Telnet
- E. SSH

Answer: CDE

NEW QUESTION 192

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.

Answer: B

NEW QUESTION 194

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.

Answer: AB

NEW QUESTION 199

If there are no changes in the routing table and in the case of TCP traffic, which of the following correctly describes the routing table lookups performed by a FortiGate in NAT /Route mode, when searching for a suitable gateway?

- A. A lookup is done only when the first packet coming from the client (SYN) arrives.
- B. A lookup is done when the first packet coming from the client (SYN) arrives, and a second one is performed when the first packet coming from the server (SYN/ACK) arrives.
- C. Three lookups are done during the TCP 3-way handshake (SYN, SYN/ACK, ACK).
- D. A lookup is always done each time a packet arrives, from either the server or the client side.

Answer: B

NEW QUESTION 204

For FortiGate devices equipped with Network Processor (NP) chips, which are true? (Choose three.)

- A. For each new IP session, the first packet always goes to the CPU.
- B. The kernel does not need to program the NP
- C. When the NPU sees the traffic, it determines by itself whether it can process the traffic
- D. Once offloaded, unless there are errors, the NP forwards all subsequent packet
- E. The CPU does not process them.
- F. When the last packet is sent or received, such as a TCP FIN or TCP RST signal, the NP returns this session to the CPU for tear down.
- G. Sessions for policies that have a security profile enabled can be NP offloaded.

Answer: ACD

NEW QUESTION 206

In a FSSO agent mode solution, how does the FSSO collector agent learn each IP address?

- A. The DC agents get each user IP address from the event logs and forward that information to the collector agent
- B. The collector agent does not know, and does not need, each user IP address
- C. Only workstation names are known by the collector agent.
- D. The collector agent frequently polls the AD domain controllers to get each user IP address.
- E. The DC agent learns the workstation name from the event logs and DNS is then used to translate those names to the respective IP addresses.

Answer: D

NEW QUESTION 210

Which of the following statements are true regarding WAN Link Load Balancing? (Choose two).

- A. There can be only one virtual WAN Link per VDOM.
- B. FortiGate can measure the quality of each link based on latency, jitter, or packets percentage.
- C. Link health checks can be performed over each link member if the virtual WAN interface.
- D. Distance and priority values are configured in each link member if the virtual WAN interface.

Answer: AC

NEW QUESTION 212

Which of the following statements best describes what the Document Fingerprinting feature is for?

- A. Protects sensitive documents from leakage
- B. Appends a fingerprint signature to all documents sent by users
- C. Appends a fingerprint signature to all the emails sent by users
- D. Validates the fingerprint signature in users' emails

Answer: A

NEW QUESTION 214

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. Pull updates from the FortiGate device
- C. Push updates from the FortiGuard Distribution Network.
- D. execute fortiguard-AV-AS command from the CLI.

Answer: ABC

NEW QUESTION 219

Which firewall objects can be included in the Destination Address field of a firewall policy? (Choose three.)

- A. IP address pool.
- B. Virtual IP address.
- C. IP address.
- D. IP address group.
- E. MAC address.

Answer: BCD

NEW QUESTION 222

Which of the following statements is correct concerning multiple vdoms configured in a FortiGate device?

- A. FortiGate devices, from the FGT/FWF 60D and above, all support VDOMS.
- B. All FortiGate devices scale to 250 VDOMS.
- C. Each VDOM requires its own FortiGuard license.
- D. FortiGate devices support more NAT/route VDOMs than Transparent Mode VDOMs.

Answer: A

NEW QUESTION 223

A static route is configured for a FortiGate unit from the CLI using the following commands:
config router static edit 1

```
set device "wan1" set distance 20
set gateway 192.168.100.1 next
end
```

Which of the following conditions are required for this static default route to be displayed in the FortiGate unit's routing table? (Choose two.)

- A. The administrative status of the wan1 interface is displayed as down.
- B. The link status of the wan1 interface is displayed as up.
- C. All other default routers should have a lower distance.
- D. The wan1 interface address and gateway address are on the same subnet.

Answer: BD

NEW QUESTION 228

A FortiGate devices is configured with four VDOMs: 'root' and 'vdom1' are in NAT/route mode; 'vdom2' and 'vdom2' are in transparent mode. The management VDOM is 'root'. Which of the following statements are true? (Choose two.)

- A. An inter-VDOM link between 'root' and 'vdom1' can be created.
- B. An inter-VDOM link between 'vdom1' and vdom2' can created.
- C. An inter-VDOM link between 'vdom2' and vdom3' can created.
- D. Inter-VDOM link links must be manually configured for FortiGuard traffic.

Answer: AB

NEW QUESTION 231

Alert emails enable the FortiGate unit to send email notifications to an email address upon detection of a pre-defined event type. Which of the following are some of the available event types in Web Config?

- A. Intrusion detected.
- B. Successful firewall authentication.
- C. Oversized file detected.
- D. DHCP address assigned.
- E. FortiGuard Web Filtering rating error detected.

Answer: A

NEW QUESTION 236

Examine the following log message for IPS:

```
2012-07-01 09:54:28 oid=2 log_id=18433 type=ips subtype=anomaly pri=alert vd=root severity="critical" src="192.168.3.168" dst="192.168.3.170" src_int="port2"
serial=0 status="detected" proto=1 service="icmp" count=1 attack_name="icmp_flood"
icmp_id="0xa8a4"
icmp_type="0x08" icmp_code="0x00" attack_id=16777316 sensor="1" ref="http://www.fortinet.com/ids/VID16777316" msg="anomaly: icmp_flood, 51 > threshold
50"
```

Which statement is correct about the above log? (Choose two.)

- A. The target is 192.168.3.168.
- B. The target is 192.168.3.170.
- C. The attack was NOT blocked.
- D. The attack was blocked.

Answer: BD

NEW QUESTION 240

Which statements are correct regarding application control? (Choose two.)

- A. It is based on the IPS engine.
- B. It is based on the AV engine.
- C. It can be applied to SSL encrypted traffic.
- D. It cannot be applied to SSL encrypted traffic.

Answer: AC

NEW QUESTION 241

You have created a new administrator account, and assign it the prof_admin profile. Which is false about that account's permissions?

- A. It cannot upgrade or downgrade firmware.
- B. It can create and assign administrator accounts to parts of its own VDOM.
- C. It can reset forgotten passwords for other administrator accounts such as "admin".
- D. It has a smaller permissions scope than accounts with the "super_admin" profile.

Answer: A

NEW QUESTION 243

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.

Answer: AD

NEW QUESTION 246

Which of the following statements best describes how the collector agent learns that a user has logged off from the network?

- A. The workstation fails to reply to the polls frequently done by the collector agent.
- B. The DC agent captures the log off event from the event logs, which it forwards to the collector agent.
- C. The work station notifies the DC agent that the user has logged off.
- D. The collector agent gets the logoff events when polling the respective domain controller.

Answer: D

NEW QUESTION 248

Which define device identification? (Choose two.)

- A. Device identification is enabled by default on all interfaces.
- B. Enabling a source device in a firewall policy enables device identification on the source interfaces of that policy.
- C. You cannot combine source user and source device in the same firewall policy.
- D. FortiClient can be used as an agent based device identification technique.
- E. Only agentless device identification techniques are supported.

Answer: BD

NEW QUESTION 251

Which of the following items is NOT a packet characteristic matched by a firewall service object?

- A. ICMP type and code
- B. TCP/UDP source and destination ports
- C. IP protocol number
- D. TCP sequence number

Answer: D

NEW QUESTION 253

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.

Answer: BC

NEW QUESTION 254

Which statements are true regarding the factory default configuration? (Choose three.)

- A. The default web filtering profile is applied to the first firewall policy.
- B. The 'Port1' or 'Internal' interface has the IP address 192.168.1.99.
- C. The implicit firewall policy action is ACCEPT.
- D. The 'Port1' or 'Internal' interface has a DHCP server set up and enabled (on device models that support DHCP servers).
- E. Default login uses the username: admin (all lowercase) and no password.

Answer: BDE

NEW QUESTION 256

What types of troubleshooting can you do when uploading firmware? (Choose two.)

- A. Investigate corrupted firmware
- B. Investigate current runtime state
- C. Investigate damaged hardware
- D. Investigate configuration history

Answer: AD

NEW QUESTION 259

Which of the following FSSO modes must be used for Novell eDirectory networks?

- A. Agentless polling
- B. LDAP agent
- C. eDirectory agent
- D. DC agent

Answer: C

NEW QUESTION 264

Examine the following log message attributes and select two correct statements from the list below. (Choose two.)

hostname=www.youtube.com profiletype="Webfilter_Profile" profile="default" status="passthrough" msg="URL belongs to a category with warnings enabled"

- A. The traffic was blocked.
- B. The user failed authentication.
- C. The category action was set to warning.
- D. The website was allowed

Answer: CD

NEW QUESTION 266

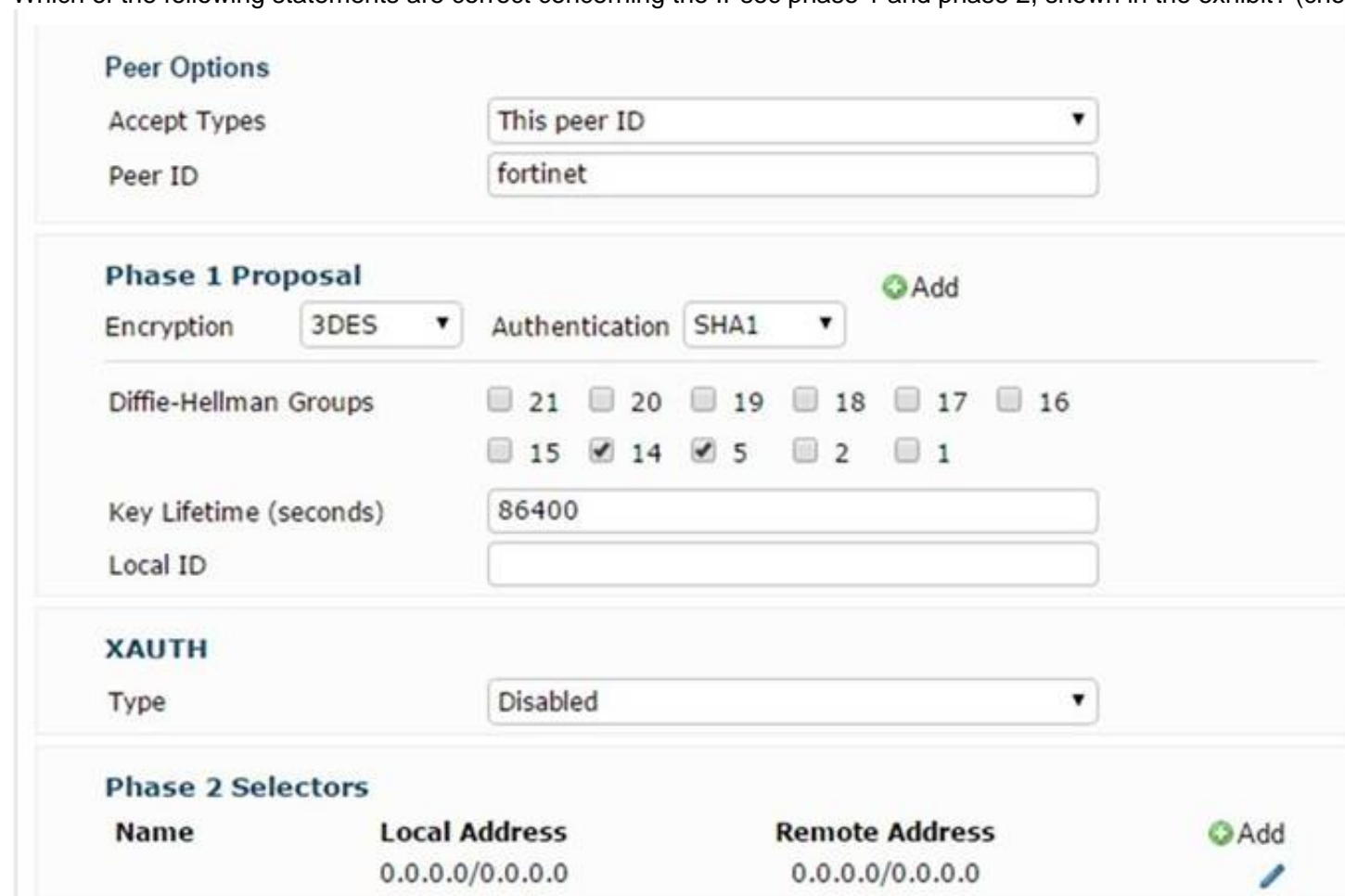
What are valid options for handling DNS requests sent directly to a FortiGate's interface IP? (Choose three.)

- A. Conditional-forward.
- B. Forward-only.
- C. Non-recursive.
- D. Iterative.
- E. Recursive.

Answer: BCE

NEW QUESTION 267

Which of the following statements are correct concerning the IPsec phase 1 and phase 2, shown in the exhibit? (choose two)



The screenshot shows the FortiGate configuration interface for IPsec. It is divided into four main sections:

- Peer Options:** Contains 'Accept Types' set to 'This peer ID' and 'Peer ID' set to 'fortinet'.
- Phase 1 Proposal:** Contains 'Encryption' set to '3DES' and 'Authentication' set to 'SHA1'. Below these are 'Diffie-Hellman Groups' with checkboxes for 21, 20, 19, 18, 17, 16, 15, 14 (checked), 5 (checked), 2, and 1. 'Key Lifetime (seconds)' is set to '86400' and 'Local ID' is empty.
- XAUTH:** Contains 'Type' set to 'Disabled'.
- Phase 2 Selectors:** A table with columns 'Name', 'Local Address', and 'Remote Address'. The 'Local Address' is '0.0.0.0/0.0.0.0' and the 'Remote Address' is '0.0.0.0/0.0.0.0'. There is an 'Add' button and a pencil icon.

- A. The quick mode selector in the remote site must also be 0.0.0.0/0 for the source and destination addresses.
- B. Only remote peers with the peer ID 'fortinet' will be able to establish a VPN.
- C. The FortiGate device will automatically add a static route to the source quick mode selector address received from each remote VPN peer.
- D. The configuration will work only to establish FortiClient-to-FortiGate tunnel
- E. A FortiGate tunnel requires a different configuration.

Answer: CD

NEW QUESTION 269

What information is synchronized between two FortiGate units that belong to the same HA cluster? (Choose three)

- A. IP addresses assigned to DHCP enabled interface.
- B. The master devices hostname.
- C. Routing configured and state.
- D. Reserved HA management interface IP configuration.
- E. Firewall policies and objects.

Answer: ACE

NEW QUESTION 273

Which action is taken by the FortiGate device when a file matches more than one rule in a Data Leak Prevention sensor?

- A. The actions specified by the rule that most specifically matched the file
- B. The actions specified in the first rule from top to bottom

- C. All actions specified by all the matched rules.
- D. The actions specified in the rule with the higher priority number

Answer: D

NEW QUESTION 278

Review the IPsec diagnostics output of the command diagnose vpn tunnel list shown in the exhibit.

```
STUDENT # diagnose vpn tunnel list
list all ipsec tunnel in vd 0
-----
name=Remote_1 ver=1 serial=1 10.200.1.1:0->10.200.3.1:0 lgwy=static tun=intf mode=auto bound_if=2
proxyid_num=1 child_num=0 refcnt=6 ilast=2 olast=2
stat: rxp=8 txp=8 rxb=960 txb=480
dpd: mode=active on=1 idle=5000ms retry=3 count=0 seqno=128
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=P2_Remote_1 proto=0 sa=1 ref=2 auto_negotiate=0 serial=1
src: 0:0.0.0.0/0.0.0.0:0
dst: 0:0.0.0.0/0.0.0.0:0
SA: ref=3 options=0000000f type=00 soft=0 mtu=1412 expire=1486 replaywin=1024 seqno=1
life: type=01 bytes=0/0 timeout=1753/1800
dec: spi=b95a77fe esp=aes key=32 84ed410c1bb9f61e635a49563c4e7646e9e110628b79b0ac03482d05e3b6a0e6
ah=sha1 key=20 6bddbfad7161237daa46c19725dd0292b062dda5
enc: spi=9293e7d4 esp=aes key=32 951be1d87860cdb59b98b170a17dcb75f77bd541bdc3a1847e54c78c0d43aa13
ah=sha1 key=20 8a5bedd6a0ce0f8daf7593601acfe2c618a0d4e2
-----
name=Remote_2 ver=1 serial=2 10.200.2.1:0->10.200.4.1:0 lgwy=static tun=intf mode=auto bound_if=3
proxyid_num=1 child_num=0 refcnt=6 ilast=0 olast=0
stat: rxp=0 txp=0 rxb=0 txb=0
dpd: mode=active on=1 idle=5000ms retry=3 count=0 seqno=0
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=P2_Remote_2 proto=0 sa=1 ref=2 auto_negotiate=0 serial=1
src: 0:0.0.0.0/0.0.0.0:0
dst: 0:0.0.0.0/0.0.0.0:0
SA: ref=3 options=0000000f type=00 soft=0 mtu=1280 expire=1732 replaywin=1024 seqno=1
life: type=01 bytes=0/0 timeout=1749/1800
dec: spi=b95a77ff esp=aes key=32 582af59d71635b835c9208878e0e3f3fe31ba1dfdf88ff83ca9bab1ed66ac325e
ah=sha1 key=20 0d951e62a1bcb63232df6d0fb86df49ab714f53b
enc: spi=9293e7d5 esp=aes key=32 eeeecac3a58161f3390fa612b794c776654c86aef51fbc7542906223d56ebb3
ah=sha1 key=20 09eaa3085bc30a59091f182eb3d11550385b8304
```

Which statements is correct regarding this output?

- A. One tunnel is rekeying.
- B. Two tunnels are rekeying.
- C. Two tunnels are up.
- D. One tunnel is up.

Answer: C

NEW QUESTION 279

Which of the following statements are correct concerning layer 2 broadcast domains in transparent mode VDOMs?(Choose two)

- A. The whole VDOM is a single broadcast domain even when multiple VLAN are used.
- B. Each VLAN is a separate broadcast domain.
- C. Interfaces configured with the same VLAN ID can belong to different broadcast domains.
- D. All the interfaces in the same broadcast domain must use the same VLAN ID.

Answer: BC

NEW QUESTION 281

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.

Answer: C

NEW QUESTION 286

Which of the following actions that can be taken by the Data Leak Prevention scanning? (Choose three.)

- A. Block
- B. Reject
- C. Tag
- D. Log only
- E. Quarantine IP address

Answer: ADE

NEW QUESTION 289

What configuration objects are automatically added when using the FortiGate's FortiClient VPN Configurations Wizard?(Choose two)

- A. Static route
- B. Phase 1
- C. Users group
- D. Phase 2

Answer: BD

NEW QUESTION 294

Examine the following CLI configuration:
config system session -ttl set default 1800
end

What statement is true about the effect of the above configuration line?

- A. Sessions can be idle for no more than 1800 seconds.
- B. The maximum length of time a session can be open is 1800 seconds.
- C. After 1800 seconds, the end user must re-authenticate.
- D. after a session has been open for 1800 seconds, the FortiGate sends a keepalive packet to both client and server.

Answer: A

NEW QUESTION 298

What is required in a FortiGate configuration to have more than one dialup IPsec VPN using aggressive mode?

- A. All the aggressive mode dialup VPNs MUST accept connections from the same peer ID.
- B. Each peer ID MUST match the FQDN of each remote peer.
- C. Each aggressive mode dialup MUST accept connections from different peer ID.
- D. The peer ID setting must NOT be used.

Answer: C

NEW QUESTION 299

Which of the following statements are correct about the HA command diagnose sys ha reset-uptime? (Choose two.)

- A. The device this command is executed on is likely to switch from master to slave status if override is disabled.
- B. The device this command executed on is likely to switch from master to slave status if override is enabled.
- C. The command has no impact on the HA algorithm.
- D. This commands resets the uptime variable used in the HA algorithm so it may cause a new master to become elected.

Answer: AD

NEW QUESTION 301

Which statement correctly describes the output of the command diagnose ips anomaly list?

- A. Lists the configured DoS policy.
- B. List the real-time counters for the configured DoS policy.
- C. Lists the errors captured when compiling the DoS policy.
- D. Lists the IPS signature matches.

Answer: B

NEW QUESTION 303

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

Answer: D

NEW QUESTION 305

Which is NOT true about the settings for an IP pool type port block allocation?

- A. A Block Size defines the number of connections.
- B. Blocks Per User defines the number of connection blocks for each user.
- C. An Internal IP Range defines the IP addresses permitted to use the pool.
- D. An External IP Range defines the IP addresses in the pool.

Answer: B

NEW QUESTION 307

Which of the following network protocols can be inspected by the Data Leak Prevention scanning? (Choose three.)

- A. SMTP
- B. HTTP-POST

- C. AIM
- D. MAPI
- E. ICQ

Answer: ABD

NEW QUESTION 312

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.

Answer: B

NEW QUESTION 315

A FortiGate is configured with multiple VDOMs. An administrative account on the device has been assigned a Scope value of VDOM:root. Which of the following settings will this administrator be able to configure? (Choose two.)

- A. Firewall addresses
- B. DHCP servers
- C. FortiGuard Distribution Network configuration.
- D. System hostname.

Answer: AB

NEW QUESTION 316

Which statement best describes what SSL.root is?

- A. The name of the virtual network adapter required in each user's PC for SSL VPN Tunnel mode.
- B. The name of a virtual interface in the root VDOM where all the SSL VPN user traffic comes from.
- C. A Firewall Address object that contains the IP addresses assigned to SSL VPN users.
- D. The virtual interface in the root VDOM that the remote SSL VPN tunnels connect to.

Answer: B

NEW QUESTION 318

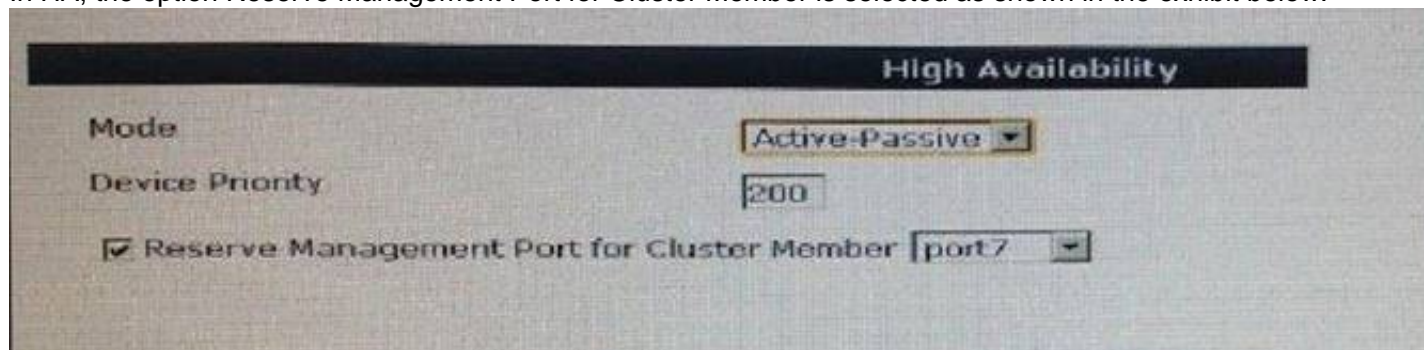
Which of the following statements are correct differences between NAT/route and transparent mode? (Choose two.)

- A. In transparent mode, interfaces do not have IP addresses.
- B. Firewall policies are only used in NAT/ route mode.
- C. Static routers are only used in NAT/route mode.
- D. Only transparent mode permits inline traffic inspection at layer 2.

Answer: AC

NEW QUESTION 320

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.

Answer: AD

NEW QUESTION 325

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

Answer: B

NEW QUESTION 326

Which of the following IKE modes is the one used during the IPsec phase 2 negotiation?

- A. Aggressive mode
- B. Quick mode
- C. Main mode
- D. Fast mode

Answer: B

NEW QUESTION 330

Which user group types does FortiGate support for firewall authentication? (Choose three.)

- A. RSSO
- B. Firewall
- C. LDAP
- D. NTLM
- E. FSSO

Answer: ABE

NEW QUESTION 331

Which authentication scheme is not supported by the RADIUS implementation on FortiGate?

- A. CHAP
- B. MSCHAP2
- C. PAP
- D. FSSO

Answer: D

NEW QUESTION 335

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.

Answer: CD

NEW QUESTION 336

Of the following information, what can be recorded by a Data Leak Prevention sensor configured to do a summary archiving? (Choose three.)

- A. Visited URL (for the case of HTTP traffic)
- B. Sender email address (for the case of SMTP traffic)
- C. Recipient email address (for the case of SMTP traffic)
- D. Attached file (for the case of SMTP traffic)
- E. Email body (for the case of SMTP traffic)

Answer: BCE

NEW QUESTION 341

The exhibit shows a FortiGate routing table.

```
# get router info routing-table all
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       E1 - OSPF external type 1, E2 - OSPF external type 2
       * - candidate default
O*E2  0.0.0.0/0 [110/10] via 192.168.11.254, wan1, 01:29:24
C      172.16.78.0/24 is directly connected, wan2
O      192.168.1.0/24 [110/200] via 192.168.11.59, internal, 01:30:28
C      192.168.3.0/24 is directly connected, dmz
C      192.168.11.0/24 is directly connected, internal
```

Which of the following statements are correct?(Choose two)

- A. There is only one active default route.
- B. The distance values for the route to 192.168.1.0/24 is 200
- C. An IP address in the subnet 172.16.78.0/24 has been assigned to the dmz interface.

D. The FortiGate will route the traffic to 172.17.1.2 to next hop with the IP address 192.168.11.254

Answer: AD

NEW QUESTION 344

Which statements correctly describe transparent mode operation? (Choose three.)

- A. The FortiGate acts as transparent bridge and forwards traffic at Layer-2.
- B. Ethernet packets are forwarded based on destination MAC addresses, NOT IP addresses.
- C. The transparent FortiGate is clearly visible to network hosts in an IP trace route.
- D. Permits inline traffic inspection and firewalling without changing the IP scheme of the network.
- E. All interfaces of the transparent mode FortiGate device must be on different IP subnets.

Answer: ABD

NEW QUESTION 349

Which IPSec mode includes the peer id information in the first packet?

- A. Main mode.
- B. Quick mode.
- C. Aggressive mode.
- D. IKEv2 mode.

Answer: C

NEW QUESTION 350

Which of the following statements are correct regarding SSL VPN Web-only mode? (Choose two.)

- A. It can only be used to connect to web services.
- B. IP traffic is encapsulated over HTTPS.
- C. Access to internal network resources is possible from the SSL VPN portal.
- D. The standalone FortiClient SSL VPN client CANNOT be used to establish a Web-only SSL VPN.
- E. It is not possible to connect to SSH servers through the VPN.

Answer: BC

NEW QUESTION 351

Examine this log entry.

What does the log indicate? (Choose three.)

date=2013-12-04 time=09:30:18 logid=0100032001 type=event subtype=system level=information vd="root" user="admin" ui=http(192.168.1.112) action=login status=success reason=none profile="super_admin" msg="Administrator admin logged in successfully from http(192.168.1.112)"

- A. In the GUI, the log entry was located under "Log & Report > Event Log > User".
- B. In the GUI, the log entry was located under "Log & Report > Event Log > System".
- C. In the GUI, the log entry was located under "Log & Report > Traffic Log > Local Traffic".
- D. The connection was encrypted.
- E. The connection was unencrypted.
- F. The IP of the FortiGate interface that "admin" connected to was 192.168.1.112.
- G. The IP of the computer that "admin" connected from was 192.168.1.112.

Answer: BEG

NEW QUESTION 355

Which statement is one disadvantage of using FSSO NetAPI polling mode over FSSO Security Event Log (WinSecLog) polling mode?

- A. It requires a DC agent installed in some of the Windows DC.
- B. It runs slower.
- C. It might miss some logon events.
- D. It requires access to a DNS server for workstation name resolution.

Answer: C

NEW QUESTION 356

Which of the following statements are correct about NTLM authentication? (Choose three)

- A. NTLM negotiation starts between the FortiGate device and the user's browser.
- B. It must be supported by the user's browser.
- C. It must be supported by the domain controllers.
- D. It does not require a collector agent.
- E. It does not require DC agents.

Answer: ABC

NEW QUESTION 361

Which of the following statements are true about IPsec VPNs? (Choose three.)

- A. IPsec increases overhead and bandwidth.
- B. IPsec operates at the layer 2 of the OSI model.
- C. End-user's network applications must be properly pre-configured to send traffic across the IPsec VPN.
- D. IPsec protects upper layer protocols.
- E. IPsec operates at the layer 3 of the OSI model.

Answer: ADE

NEW QUESTION 362

Review the IKE debug output for IPsec shown in the exhibit below.

```
STUDENT # ike 0: comes 10.200.3.1:500->10.200.1.1:500, ifindex=2....
ike 0: IKEv1 exchange=Informational id=9e2606ac7ae83d7a/612da78d3ab3f945:15b10705 len=92
ike 0: in SE2606AC7AE83D7A612DA78D3AB3F9450810050115B107050000005C26E2A7EC8461AC15E98B9C705B6C1F667A41957AED11F37003C07A1
07B0934D938E1A2C74348ED08FD6B39146C618525C6EC51E2F26385B63B8E035F52B4
ike 0:Remote_1:10: dec 9E2606AC7AE83D7A612DA78D3AB3F9450810050115B107050000005C08000018E281874EECF170EB5222B6A4E3A027C714
C0000C02000000001011089289E2606AC7AE83D7A612DA78D3AB3F9450C00009C17511ED6EE549507
ike 0:Remote_1:10: notify msg received: R-U-THERE
ike 0:Remote_1:10: enc 9E2606AC7AE83D7A612DA78D3AB3F94508100501734C5CDF000000540B0000181C047F014CEEF1B0EC8DA915F3B18AEB20
A0000C02000000001011089299E2606AC7AE83D7A612DA78D3AB3F9450C00009C
ike 0:Remote_1:10: out 9E2606AC7AE83D7A612DA78D3AB3F94508100501734C5CDF0000005CB3CC431065A1737144B02F1AAE79C1BE712B84255
EB84E5FA7A9677E99C7B731057FF33728B842AA983E79C919DA9B64EBC087EFOA02666C1FBD2C62F
ike 0:Remote_1:10: sent IKE msg (R-U-THERE-ACK): 10.200.1.1:500->10.200.3.1:500, len=92, id=9e2606ac7ae83d7a/612da78d3ab3
734c5cdf
ike 0:Remote_1: link is idle 2 10.200.1.1->10.200.3.1:500 dpd=1 seqno=34
```

Which statements is correct regarding this output?

- A. The output is a phase 1 negotiation.
- B. The output is a phase 2 negotiation.
- C. The output captures the dead peer detection messages.
- D. The output captures the dead gateway detection packets.

Answer: C

NEW QUESTION 363

A FortiGate devices has two VDOMs in NAT/route mode. Which of the following solutions can be implemented by a network administrator to route traffic between the two VDOMs.(Choose two)

- A. Use the inter-VDOMs links automatically created between all VDOMS.
- B. Manually create and configured an inter-VDOM link between yours.
- C. Interconnect and configure an external physical interface in one VDOM to another physical interface in the second VDOM.
- D. Configure both VDOMs to share the same table.

Answer: BC

NEW QUESTION 367

The exhibit shoes three static routes.

```
config router static
  edit 1
    set dst 172.20.168.0 255.255.255.0
    set distance 10
    set priority 10
    set device port1
  next
  edit 2
    set dst 172.20.0.0 255.255.0.0
    set distance 5
    set priority 20
    set device port2
  next
  edit 3
    set dst 172.20.0.0 255.255.0.0
    set distance 5
    set priority 20
    set device port3
  next
end
```

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.

Answer: D

NEW QUESTION 368

In which order are firewall policies processed on a FortiGate unit?

- A. From top to bottom, according with their sequence number.
- B. From top to bottom, according with their policy ID number.
- C. Based on best match.
- D. Based on the priority value.

Answer: A

NEW QUESTION 373

Which of the following statements must be true for a digital certificate to be valid? (Choose two.)

- A. It must be signed by a “trusted” CA
- B. It must be listed as valid in a Certificate Revocation List (CRL)
- C. The CA field must be “TRUE”
- D. It must be still within its validity period

Answer: AD

NEW QUESTION 374

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

- A. Warn
- B. Allow
- C. Block
- D. Traffic Shaping
- E. Quarantine

Answer: BCD

NEW QUESTION 378

Two FortiGate units with NP6 processors form an active-active cluster. The cluster is doing security profile (UTM) inspection over all the user traffic. What statements are true regarding the sessions that the master unit is offloading to the slave unit for inspection? (Choose two.)

- A. They are offloaded to the NP6 in the master unit.
- B. They are not offloaded to the NP6 in the master unit.
- C. They are offloaded to the NP6 in the slave unit.
- D. They are not offloaded to the NP6 in the slave unit.

Answer: BC

NEW QUESTION 380

Which answer best describes what an "Unknown Application" is?

- A. All traffic that matches the internal signature for unknown applications.
- B. Traffic that does not match the RFC pattern for its protocol.
- C. Any traffic that does not match an application control signature
- D. A packet that fails the CRC check.

Answer: C

NEW QUESTION 381

Caching improves performance by reducing FortiGate unit requests to the FortiGuard server. Which of the following statements are correct regarding the caching of FortiGuard responses?

- A. Caching is available for web filtering, antispam, and IPS requests.
- B. The cache uses a small portion of the FortiGate system memory.
- C. When the cache is full, the least recently used IP address or URL is deleted from the cache.
- D. An administrator can configure the number of seconds to store information in the cache before the FortiGate unit contacts the FortiGuard server again.
- E. The size of the cache will increase to accommodate any number of cached queries.

Answer: BCD

NEW QUESTION 386

Which of the following statements are true about Man-in-the-middle SSL Content Inspection? (Choose three.)

- A. The FortiGate device “re-signs” all the certificates coming from the HTTPS servers
- B. The FortiGate device acts as a sub-CA
- C. The local service certificate of the web server must be installed in the FortiGate device
- D. The FortiGate device does man-in-the-middle inspection.

E. The required SSL Proxy certificate must first be requested to a public certificate authority (CA).

Answer: BCE

NEW QUESTION 387

What are the advantages of FSSO DC mode over polling mode?

- A. Redundancy in the collector agent.
- B. Allows transparent authentication.
- C. DC agents are not required in the AD domain controllers.
- D. Scalability

Answer: C

NEW QUESTION 392

When creating FortiGate administrative users, which configuration objects specify the account rights?

- A. Remote access profiles.
- B. User groups.
- C. Administrator profiles.
- D. Local-in policies.

Answer: C

NEW QUESTION 395

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.

Answer: C

NEW QUESTION 397

An administrator has formed a high availability cluster involving two FortiGate units.

[Multiple upstream Layer 2 switches] – [FortiGate HA Cluster] – [Multiple downstream Layer 2 Switches]

The administrator wishes to ensure that a single link failure will have minimal impact upon the overall throughput of traffic through this cluster.

Which of the following options describes the best step the administrator can take? The administrator should

- A. Increase the number of FortiGate units in the cluster and configure HA in active-active mode.
- B. Enable monitoring of all active interfaces.
- C. Set up a full-mesh design which uses redundant interfaces.
- D. Configure the HA ping server feature to allow for HA failover in the event that a path is disrupted.

Answer: C

NEW QUESTION 399

When firewall policy authentication is enabled, which protocols can trigger an authentication challenge? (Choose two.)

- A. SMTP
- B. POP3
- C. HTTP
- D. FTP

Answer: CD

NEW QUESTION 403

Which of the following options best defines what Diffie-Hellman is?

- A. A symmetric encryption algorithm.
- B. A "key-agreement" protocol.
- C. A "Security-association-agreement" protocol.
- D. An authentication algorithm.

Answer: B

NEW QUESTION 406

Which statements are correct regarding URL filtering on a FortiGate unit? (Choose two.)

- A. The allowed actions for URL filtering include allow, block, monitor and exempt.
- B. The allow actions for URL filtering and Allow and Block only.
- C. URL filters may be based on patterns using simple text, wildcards and regular expressions.
- D. URL filters are based on simple text only and require an exact match.

Answer: AC

NEW QUESTION 408

What is IPsec Perfect Forwarding Secrecy (PFS)?

- A. A phase-1 setting that allows the use of symmetric encryption.
- B. A phase-2 setting that allows the recalculation of a new common secret key each time the session key expires.
- C. A 'key-agreement' protocol.
- D. A 'security-association- agreement' protocol.

Answer: B

NEW QUESTION 409

What are the ways FortiGate can monitor logs? (Choose three.)

- A. MIB
- B. SMS
- C. Alert Emails
- D. SNMP
- E. FortiAnalyzer
- F. Alert Message Console

Answer: CDF

NEW QUESTION 413

What is valid reason for using session based authentication instead of IP based authentication in a FortiGate web proxy solution?

- A. Users are required to manually enter their credentials each time they connect to a different web site.
- B. Proxy users are authenticated via FSSO.
- C. There are multiple users sharing the same IP address.
- D. Proxy users are authenticated via RADIUS.

Answer: C

NEW QUESTION 416

Which of the following statements are true about PKI users created in a FortiGate device? (Choose two.)

- A. Can be used for token-based authentication
- B. Can be used for two-factor authentication
- C. Are used for certificate-based authentication
- D. Cannot be members of user groups

Answer: AB

NEW QUESTION 419

What is longest length of time allowed on a FortiGate device for the virus scan to complete?

- A. 20 seconds
- B. 30 seconds
- C. 45 seconds
- D. 10 seconds

Answer: B

NEW QUESTION 421

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

NSE4 Practice Exam Features:

- * NSE4 Questions and Answers Updated Frequently
- * NSE4 Practice Questions Verified by Expert Senior Certified Staff
- * NSE4 Most Realistic Questions that Guarantee you a Pass on Your First Try
- * NSE4 Practice Test Questions in Multiple Choice Formats and Updates for 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The NSE4 Practice Test Here](#)