Exam Questions NSE4-5.4

Fortinet Network Security Expert - FortiOS 5.4

https://www.2passeasy.com/dumps/NSE4-5.4/

NEW QUESTION 1
A FortiGate interface is configured with the following commands:

What statements about the configuration are correct? (Choose two.)

A. IPv6 clients connected to port1 can use SLAAC to generate their IPv6 addresses.
B. FortiGate can provide DNS settings to IPv6 clients.
C. FortiGate can send IPv6 router advertisements (RAs.)
D. FortiGate can provide IPv6 addresses to DHCPv6 client.

Answer: AC

NEW QUESTION 2
Which of the following Fortinet hardware accelerators can be used to offload flow-based antivirus inspection? (Choose two.)

A. SP3
B. CP8
C. NP4
D. NP6

Answer: AB

NEW QUESTION 3
What methods can be used to deliver the token code to a user who is configured to use two-factor authentication? (Choose three.)

A. Code blocks
B. SMS phone message
C. FortiToken
D. Browser pop-up window
E. Email

Answer: BCE

NEW QUESTION 4
View the exhibit.

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

A. This is a redundant IPsec setup.

B. The TunnelB route is the primary one for searching the remote sit
C. The TunnelA route is used only if the TunnelB VPN is down.
D. This setup requires at least two firewall policies with action set to IPsec.
E. Dead peer detection must be disabled to support this type of IPsec setup.

Answer: AB

NEW QUESTION 5
An administrator needs to offload logging to FortiAnalyzer from a FortiGate with an internal hard drive. Which statements are true? (Choose two.)

A. Logs must be stored on FortiGate first, before transmitting to FortiAnalyzer
B. FortiGate uses port 8080 for log transmission
C. Log messages are transmitted as plain text in LZ4 compressed format (store-and-upload method).
D. FortiGate can encrypt communications using SSL encrypted OFTP traffic.

Answer: AC

NEW QUESTION 6
An administrator observes that the port1 interface cannot be configured with an IP address. What can be the reasons for that? (Choose three.)

A. The interface has been configured for one-arm sniffer.
B. The interface is a member of a virtual wire pair.
C. The operation mode is transparent.
D. The interface is a member of a zone.
E. Captive portal is enabled in the interface.

Answer: ABC

NEW QUESTION 7
When browsing to an internal web server using a web-mode SSL VPN bookmark, which IP address is used as the source of the HTTP request?

A. The FortiGate unit’s public IP address
B. The FortiGate unit’s internal IP address
C. The remote user’s virtual IP address
D. The remote user’s public IP address

Answer: B

NEW QUESTION 8
What is FortiGate’s behavior when local disk logging is disabled?

A. Only real-time logs appear on the FortiGate dashboard.
B. No logs are generated.
C. Alert emails are disabled.
D. Remote logging is automatically enabled.

Answer: A

NEW QUESTION 9
What traffic and attacks can be blocked by a web application firewall (WAF) profile? (Choose three.)

A. Traffic to inappropriate web sites
B. SQL injection attacks
C. Server information disclosure attacks
D. Credit card data leaks
E. Traffic to botnet command and control (C&C) servers

Answer: BCE

NEW QUESTION 10
Which statements about One-to-One IP pool are true? (Choose two.)

A. It allows configuration of ARP replies.
B. It allows fixed mapping of an internal address range to an external address range.
C. It is used for destination NAT.
D. It does not use port address translation.

Answer: BD

NEW QUESTION 10
What step is required to configure an SSL VPN to access to an internal server using port forward mode?

A. Configure the virtual IP addresses to be assigned to the SSL VPN users.
B. Install FortiClient SSL VPN client

C. Create a SSL VPN realm reserved for clients using port forward mode.
D. Configure the client application to forward IP traffic to a Java applet proxy.

Answer: D

NEW QUESTION 14
View the exhibit.

This is a sniffer output of a telnet connection request from 172.20.120.186 to the port1 interface of FGT1.

In this scenario. FGT1 has the following routing table:

Assuming telnet service is enabled for port1, which of the following statements correctly describes
why FGT1 is not responding?

A. The port1 cable is disconnected.
B. The connection is dropped due to reverse path forwarding check.
C. The connection is denied due to forward policy check.
D. FGT1's port1 interface is administratively down.

Answer: B

NEW QUESTION 18
An administrator needs to be able to view logs for application usage on your network. What configurations are required to ensure that FortiGate generates logs for application usage activity? (Choose two.)

A. Enable a web filtering profile on the firewall policy.
B. Create an application control policy.
C. Enable logging on the firewall policy.
D. Enable an application control security profile on the firewall policy.

Answer: CD

Explanation: By default the fortigate have one app control to monitor and for that not need create other app control and it necessary active logs in the policy to monitoring.

NEW QUESTION 20
Examine the routing database.

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

A. The port3 default route has the lowest metric, making it the best route.
B. There will be eight routes active in the routing table.
C. The port3 default has a higher distance than the port1 and port2 default routes.
D. Both port1 and port2 default routers are active in the routing table.

Answer: CD

NEW QUESTION 22
Which statement is true regarding the policy ID numbers of firewall policies?

A. Change when firewall policies are re-ordered.
B. Defines the order in which rules are processed.
C. Are required to modify a firewall policy from the CLI.
D. Represent the number of objects used in the firewall policy.

Answer: C

Explanation: The ID no change when re-ordered and the rules are processed to top to bottom not by ID.

NEW QUESTION 23
An administrator needs to inspect all web traffic (including Internet web traffic) coming from users connecting to SSL VPN. How can this be achieved?

A. Disabling split tunneling
B. Configuring web bookmarks
C. Assigning public IP addresses to SSL VPN clients
D. Using web-only mode

Answer: A

NEW QUESTION 27
Which traffic inspection features can be executed by a security processor (SP)? (Choose three.)

A. TCP SYN proxy
B. SIP session helper
C. Proxy-based antivirus
D. Attack signature matching
E. Flow-based web filtering

Answer: CDE
Explanation:

NEW QUESTION 32
An administrator has configured two VLAN interfaces:

A DHCP server is connected to the VLAN10 interface. A DHCP client is connected to the VLAN5 interface. However, the DHCP client cannot get a dynamic IP address from the DHCP server. What is the cause of the problem?

A. Both interfaces must be in different VDOMs
B. Both interfaces must have the same VLAN ID.
C. The role of the VLAN10 interface must be set to server.
D. Both interfaces must belong to the same forward domain.

Answer: D

Explanation:

NEW QUESTION 35
What are the purposes of NAT traversal in IPsec? (Choose two.)

A. To detect intermediary NAT devices in the tunnel path.
B. To encapsulate ESP packets in UDP packets using port 4500.
C. To force a new DH exchange with each phase 2 re-key
D. To dynamically change phase 1 negotiation mode to Aggressive.

Answer: AB

NEW QUESTION 36
View the exhibit.

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

What should be done next to troubleshoot the problem?

A. Execute another sniffer in the FortiGate, this time with the filter “host 10.0.1.10”.
B. Run a sniffer in the web server.
C. Capture the traffic using an external sniffer connected to port1.
D. Execute a debug flow.

Answer: B

NEW QUESTION 41
Which statements best describe auto discovery VPN (ADVPN). (Choose two.)

A. It requires the use of dynamic routing protocols so that spokes can learn the routes to other spokes.
B. ADVPN is only supported with IKEv2.
C. Tunnels are negotiated dynamically between spokes.
D. Every spoke requires a static tunnel to be configured to other spokes so that phase 1 and phase 2 proposals are defined in advance.

Answer: AC

NEW QUESTION 44

Which statement about the firewall policy authentication timeout is true?

A. It is a hard timeou
B. The FortiGate removes the temporary policy for a user’s source IP address after this times expires.
C. It is a hard timeou
D. The FortiGate removes the temporary policy for a user’s source MAC address after this times expires.
E. It is an idle timeou
F. The FortiGate considers a user to be idle if it does not see any packets coming from the user’s source MAC address.
G. It is an idle timeou
H. The FortiGate considers a user to be idle if it does not see any packets coming from the user’s source IP.

Answer: D

NEW QUESTION 47
How can a browser trust a web-server certificate signed by a third party CA?

A. The browser must have the CA certificate that signed the web-server certificate installed.
B. The browser must have the web-server certificate installed.
C. The browser must have the private key of CA certificate that signed the web-browser certificate installed.
D. The browser must have the public key of the web-server certificate installed.

Answer: A

NEW QUESTION 51
Examine this output from the diagnose sys top command:

Which statements about the output are true? (Choose two.)

A. sshd is the process consuming most memory
B. sshd is the process consuming most CPU
C. All the processes listed are in sleeping state
D. The sshd process is using 123 pages of memory

Answer: BC

NEW QUESTION 55
An administrator wants to configure a FortiGate as a DNS server. The FortiGate must use its DNS database first, and then relay all irresolvable queries to an external DNS server. Which of the following DNS method must you use?

A. Non-recursive
B. Recursive
C. Forward to primary and secondary DNS
D. Forward to system DNS

Answer: B

NEW QUESTION 60
Which statements about high availability (HA) for FortiGates are true? (Choose two.)

A. Virtual clustering can be configured between two FortiGate devices with multiple VDOM.
B. Heartbeat interfaces are not required on the primary device.
C. HA management interface settings are synchronized between cluster members.
D. Sessions handled by UTM proxy cannot be synchronized.

Answer: AC

NEW QUESTION 62
Which of the following statements about central NAT are true? (Choose two.)

A. IP tool references must be removed from existing firewall policies before enabling central NAT.
B. Central NAT can be enabled or disabled from the CLI only.
C. Source NAT, using central NAT, requires at least one central SNAT policy.
D. Destination NAT, using central NAT, requires a VIP object as the destination address in a firewallpolicy.

Answer: AB

NEW QUESTION 66
Which statement about the FortiGuard services for the FortiGate is true?

A. Antivirus signatures are downloaded locally on the FortiGate.
B. FortiGate downloads IPS updates using UDP port 53 or 8888.
C. FortiAnalyzer can be configured as a local FDN to provide antivirus and IPS updates.
D. The web filtering database is downloaded locally on the FortiGate.

Answer: A

Explanation:

NEW QUESTION 71
Which statements about antivirus scanning using flow-based full scan are true? (Choose two.)

A. The antivirus engine starts scanning a file after the last packet arrives.
B. It does not support FortiSandbox inspection.
C. FortiGate can insert the block replacement page during the first connection attempt only if a virus is detected at the start of the TCP stream.
D. It uses the compact antivirus database.

Answer: AC

NEW QUESTION 74
What information is flushed when the chunk-size value is changed in the config dlp settings?

A. The database for DLP document fingerprinting
B. The supported file types in the DLP filters
C. The archived files and messages
D. The file name patterns in the DLP filters

Answer: A

NEW QUESTION 75
How does FortiGate select the central SNAT policy that is applied to a TCP session?

A. It selects the SNAT policy specified in the configuration of the outgoing interface.
B. It selects the first matching central-SNAT policy from top to bottom.
C. It selects the central-SNAT policy with the lowest priority.
D. It selects the SNAT policy specified in the configuration of the firewall policy that matches the traffic.

Answer: B

NEW QUESTION 76
An administrator is using the FortiGate built-in sniffer to capture HTTP traffic between a client and a server, however, the sniffer output shows only the packets

related with TCP session setups and disconnections. Why?

A. The administrator is running the sniffer on the internal interface only.
B. The filter used in the sniffer matches the traffic only in one direction.
C. The FortiGate is doing content inspection.
D. TCP traffic is being offloaded to an NP6.

Answer: D

NEW QUESTION 78
Which of the following statements about advanced AD access mode for FSSO collector agent are true? (Choose two.)

A. It is only supported if DC agents are deployed.
B. FortiGate can act as an LDAP client configure the group filters.
C. It supports monitoring of nested groups.
D. It uses the Windows convention for naming, that is, Domain\Username.

Answer: BC

NEW QUESTION 82
Which configuration objects can be selected for the Source filed of a firewall policy? (Choose two.)

A. FQDN address
B. IP pool
C. User or user group
D. Firewall service

Answer: AC

Explanation:

NEW QUESTION 85
Examine the exhibit, which contains a virtual IP and a firewall policy configuration.

The WAN(port1) interface has the IP address 10.200.1.1/24. The LAN(port2) interface has the IP address 10.0.1.254/24.
The top firewall policy has NAT enabled using outgoing interface address. The second firewall policy configured with a virtual IP (VIP) as the destination address.
Which IP address will be used to source NAT the Internet traffic coming from a workstation with the IP address 10.0.1.10/24?

A. 10.200.1.1
B. 10.0.1.254
C. Any available IP address in the WAN(port1) subnet 10.200.1.0/24
D. 10.200.1.10

Answer: D

NEW QUESTION 89
Which statement about data leak prevention (DLP) on a FortiGate is true?

A. Traffic shaping can be applied to DLP sensors.
B. It can be applied to a firewall policy in a flow-based VDOM.
C. Files can be sent to FortiSandbox for detecting DLP threats.
D. It can archive files and messages.

Answer: D

NEW QUESTION 94
Which statements about an IPv6-over-IPv4 IPsec configuration are correct? (Choose two.)

A. The remote gateway IP must be an IPv6 address.
B. The source quick mode selector must be an IPv4 address.
C. The local gateway IP must an IPv4 address.
D. The destination quick mode selector must be an IPv6 address.

Answer: CD

NEW QUESTION 99
How can you format the FortiGate flash disk?

A. Load the hardware test (HQIP) image.
B. Execute the CLI command execute formatlogdisk.
C. Load a debug FortiOS image.
D. Select the format boot device option from the BIOS menu.

Answer: D

NEW QUESTION 102
View the exhibit.

Based on this output, which statements are correct? (Choose two.)

A. FortiGate generated an event log for system conserve mode.
B. FortiGate has entered in to system conserve mode.
C. By default, the FortiGate blocks new sessions.
D. FortiGate changed the global av-failopen settings to idledrop.

Answer: BC

NEW QUESTION 103
An administrator has blocked Netflix login in a cloud access security inspection (CASI) profile. The administrator has also applied the CASI profile to a firewall policy.
What else is required for the CASI profile to work properly?

A. You must enable logging for security events on the firewall policy.
B. You must activate a FortiCloud account.
C. You must apply an application control profile to the firewall policy.
D. You must enable SSL inspection on the firewall policy.

Answer: D

NEW QUESTION 107
How do you configure a FortiGate to do traffic shaping of P2P traffic, such as BitTorrent?

A. Apply an application control profile allowing BitTorrent to a firewall policy and configure a traffic shaping policy.
B. Enable the shape option in a firewall policy with service set to BitTorrent.
C. Apply a traffic shaper to a BitTorrent entry in the SSL/SSH inspection profile.
D. Apply a traffic shaper to a protocol options profile.

Answer: A

NEW QUESTION 109
An administrator has configured a dialup IPsec VPN with XAuth. Which method statement best
describes this scenario?

A. Only digital certificates will be accepted as an authentication method in phase 1.
B. Dialup clients must provide a username and password for authentication.
C. Phase 1 negotiations will skip pre-shared key exchange.

D. Dialup clients must provide their local ID during phase 2 negotiations.

Answer: B

NEW QUESTION 112
What does the command diagnose debug fsso-polling refresh-user do?

A. It refreshes user group information form any servers connected to the FortiGate using a collector agent.
B. It refreshes all users learned through agentless polling.
C. It displays status information and some statistics related with the polls done by FortiGate on each DC.
D. It enables agentless polling mode real-time debug.

Answer: B

NEW QUESTION 116
An administrator has configured the following settings:

What does the configuration do? (Choose two.)

A. Reduces the amount of logs generated by denied traffic.
B. Enforces device detection on all interfaces for 30 minutes.
C. Blocks denied users for 30 minutes.
D. Creates a session for traffic being denied.

Answer: AD

NEW QUESTION 120
Which of the following statements are true when using Web Proxy Auto-discovery Protocol (WPAD) with the DHCP discovery method? (Choose two.)

A. The browser sends a DHCPINFORM request to the DHCP server.
B. The browser will need to be preconfigured with the DHCP server's IP address.
C. The DHCP server provides the PAC file for download.
D. If the DHCP method fails, browsers will try the DNS method.

Answer: AD

NEW QUESTION 123
What inspections are executed by the IPS engine? (Choose three.)

A. Application control
B. Flow-based data leak prevention
C. Proxy-based antispam
D. Flow-based web filtering
E. Proxy-based antivirus

Answer: ABD

NEW QUESTION 127
An administrator wants to create a policy-based IPsec VPN tunnel between two FortiGate devices.
Which configuration steps must be performed on both units to support this scenario? (Choose three.)

A. Define the phase 2 parameters.
B. Set the phase 2 encapsulation method to transport mode.
C. Define at least one firewall policy, with the action set to IPsec.
D. Define a route to the remote network over the IPsec tunnel.

E. Define the phase 1 parameters, without enabling IPsec interface mode.

Answer: ACE

NEW QUESTION 132
Which of the following statements about web caching are true? (Choose two.)

A. Web caching slows down web browsing due to constant read-write cycles from FortiGate memory.
B. When a client makes a web request, the proxy checks if the requested URL is already in memory.
C. Only heavy content is cached, for example, videos, images, audio and so on.
D. Web caching is supported in both explicit and implicit proxy.

Answer: BD

NEW QUESTION 134
View the exhibit.

In this scenario, FGT1 has the following routing table: S*0. 0. 0. 0/0 [10/0] via 10. 40. 72. 2, port1
C172. 16. 32. 0/24 is directly connected, port2 C10. 40. 72. 0/30 is directly connected, port1
A user at 192.168.32.15 is trying to access the web server at 172.16.32.254. Which of the following statements best describe how the FortiGate will perform reverse path forwarding checks on this traffic? (Choose two.)

A. Strict RPF check will deny the traffic.
B. Strict RPF check will allow the traffic.
C. Loose RPF check will allow the traffic.
D. Loose RPF check will deny the traffic.

Answer: BD

NEW QUESTION 138
View the exhibit.

What does this exhibit represent?

A. SSL handshake
B. Interchanging digital certificates
C. Certificate signing request (CSR)
D. Inline SSL inspection

Answer: A

NEW QUESTION 141
View the exhibit.

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

A. next-hop IP address is not required when configuring a static route that uses the wan-load balance interface.
B. Sessions will be load-balanced based on source and destination IP addresses.
C. Each member interface requires its own firewall policy to allow traffic.
D. The wan-load-balance interface must be manually created.

Answer: AB

NEW QUESTION 143
Examine the following web filtering log.

Which statement about the log message is true?

A. The action for the category Games is set to block.
B. The usage quota for the IP address 10.0.1.10 has expired.
C. The name of the applied web filter profile is default.
D. The web site miniclip.com matches a static URL filter whose action is set to Warning.

Answer: D

NEW QUESTION 146
Examine this output from a debug flow:

Which statements about the output are correct? (Choose two.)

A. The packet was allowed by the firewall policy with the ID 00007fc0.
B. FortiGate routed the packet through port3.
C. FortiGate received a TCP SYN/ACK packet.
D. The source IP address of the packet was translated to 10.0.1.10.

Answer: BD

NEW QUESTION 150
An administrator needs to create a tunnel mode SSLVPN to access an internal web server from the
Internet. The web server is connected to port1. The Internet is connected to port2. Both interfaces belong to the VDOM named Corporation. What interface must be used as the source for the firewall policy that will allow this traffic?

A. ssl.root
B. ssl.Corporation
C. port2
D. port1

Answer: C

NEW QUESTION 151
View the exhibit.

Why is the administrator getting the error shown in the exhibit?

A. The administrator admin does not have the privileges required to configure global settings.
B. The global settings cannot be configured from the root VDOM context.
C. The command config system global does not exist in FortiGate.
D. The administrator must first enter the command edit global.

Answer: A

NEW QUESTION 152
Which statements about the firmware upgrade process on an active-active high availability (HA) cluster are true? (Choose two.)

A. The firmware image must be manually uploaded to each FortiGate.
B. Only secondary FortiGate devices are rebooted.
C. Uninterruptable upgrade is enabled by default.
D. Traffic load balancing is temporally disabled while upgrading the firmware.

Answer: BD

NEW QUESTION 155
Examine the exhibit, which shows the output of a web filtering real time debug.

Why is the site www.bing.com being blocked?

A. The web server IP address 204.79.197.200 is categorized by FortiGuard as Malicious Websites.
B. The rating for the web site www.bing.com has been locally overridden to a category that is being blocked.
C. The web site www.bing.com is categorized by FortiGuard as Malicious Websites.
D. The user has not authenticated with the FortiGate yet.

Answer: A

NEW QUESTION 156
What IPv6 extension header can be used to provide encryption and data confidentiality?

A. Mobility
B. ESP
C. Authentication
D. Destination options

Answer: C

NEW QUESTION 158
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 160
A user logs into a SSL VPN portal and activates the tunnel mode.
The administrator has enabled split tunneling. The exhibit shows the firewall policy configuration:

Which static route is automatically added to the client's routing table when the tunnel mode is activated?

A. A route to a destination subnet matching the Internal_Servers address object.
B. A route to the destination subnet configured in the tunnel mode widget.

C. A default route.
D. A route to the destination subnet configured in the SSL VPN global settings.

Answer: A

NEW QUESTION 162
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 167
DLP archiving gives the ability to store session transaction data on a FortiAnalyzer unit for which of the following types of network traffic? (Select all that apply.)

A. SNMP
B. IPSec
C. SMTP
D. POP3
E. HTTP

Answer: CDE

NEW QUESTION 168
Which statements regarding banned words are correct? (Choose two.)

A. Content is automatically blocked if a single instance of a banned word appears.
B. The FortiGate updates banned words on a periodic basis.
C. The FortiGate can scan web pages and email messages for instances of banned words.
D. Banned words can be expressed as simple text, wildcards and regular expressions.

Answer: CD

NEW QUESTION 170
Examine the following FortiGate web proxy configuration; then answer the question below:

Assuming that the FortiGate proxy IP address is 10.10.1.1, which URL must an Internet browser use to download the PAC file?

A. https://10.10.1.1:8080
B. https://10.10.1.1:8080/wpad.dat
C. http://10.10.1.1:8080/
D. http://10.10.1.1:8080/wpad.dat

Answer: D

NEW QUESTION 172
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 auto configuration

Answer: AC

NEW QUESTION 173
What is a 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 176
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 177
Which web filtering inspection mode inspects DNS traffic?

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

Answer: A

NEW QUESTION 180
Which of the following regular expression patterns make the terms "confidential data" case insensitive?

A. [confidential data]
B. /confidential data/i
C. i/confidential data/
D. "confidential data"

Answer: B

NEW QUESTION 185
How do you configure a FortiGate to apply traffic shaping to P2P traffic, such as BitTorrent?

A. Apply a traffic shaper to a BitTorrent entry in an application control list, which is then applied to a firewall policy.
B. Enable the shape option in a firewall policy with service set to BitTorrent.
C. Define a DLP rule to match against BitTorrent traffic and include the rule in a DLP sensor with traffic shaping enabled.
D. Apply a traffic shaper to a protocol options profile.

Answer: A

NEW QUESTION 188
When does a FortiGate load-share traffic between two static routes to the same destination subnet?

A. When they have the same cost and distance.
B. When they have the same distance and the same weight.
C. When they have the same distance and different priority.
D. When they have the same distance and same priority.

Answer: D

NEW QUESTION 190
In the case of TCP traffic, which of the following correctly describes the routing table lookups performed by a FortiGate operating 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 192
Examine the exhibit below; then answer the question following it.

In this scenario, the FortiGate unit in Ottawa has the following routing table:

Sniffer tests show that packets sent from the source IP address 172.20.168.2 to the destination IP address 172.20.169.2 are being dropped by the FortiGate located in Ottaw

A. Which of the following correctly describes the cause for the dropped packets?
B. The forward policy check.
C. The reverse path forwarding check.
D. The subnet 172.20.169.0/24 is NOT in the Ottawa FortiGate's routing table.
E. The destination workstation 172.20.169.2 does NOT have the subnet 172.20.168.0/24 in its routing table.

Answer: B

NEW QUESTION 197

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:

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 201
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.

Answer: D

NEW QUESTION 205
Which statements are correct regarding virtual domains (VDOMs)? (Choose two.)

A. VDOMs divide a single FortiGate unit into two or more virtual units that each have dedicated memory and CPUs.
B. A management VDOM handles SNMP, logging, alert email, and FDN-based updates.
C. VDOMs share firmware versions, as well as antivirus and IPS databases.
D. Different time zones can be configured in each VDOM.

Answer: BC

NEW QUESTION 207
A FortiGate unit is configured with three Virtual Domains (VDOMs) as illustrated in the exhibit.

Which of the following statements are true if the network administrator wants to route traffic between all the VDOMs? (Choose three.)

A. The administrator can configure inter-VDOM links to avoid using external interfaces and routers.
B. As with all FortiGate unit interfaces, firewall policies must be in place for traffic to be allowed to pass through any interface, including inter-VDOM links.
C. This configuration requires a router to be positioned between the FortiGate unit and the Internet for proper routing.
D. Inter-VDOM routing is automatically provided if all the subnets that need to be routed are locally attached.
E. As each VDOM has an independent routing table, routing rules need to be set (for example, static routing, OSPF) in each VDOM to route traffic between VDOMs.

Answer: ABE

NEW QUESTION 210
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 213
In transparent mode, forward-domain is an CLI setting associate with .

A. static route
B. a firewall policy
C. an interface
D. a virtual domain

Answer: C

NEW QUESTION 216
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 221
Review the IPsec diagnostics output of the command diagnose vpn tunnel list shown in the exhibit.

Which of the following statements is correct regarding this output? (Select one answer).

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

Answer: C

NEW QUESTION 222
Review the IPsec phase 2 configuration shown in the exhibit; then answer the question below.

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

A. The Phase 2 will re-key even if there is no traffic.
B. There will be a DH exchange for each re-key.
C. The sequence number of ESP packets received from the peer will not be checked.
D. Quick mode selectors will default to those used in the firewall policy.

Answer: AB

NEW QUESTION 226
Review the IKE debug output for IPsec shown in the exhibit below.

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 227
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.

Answer: A

NEW QUESTION 231
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 233
Examine the following log message for IPS and identify the valid responses below. (Select all that apply.)

A. The target is 192.168.3.168.
B. The target is 192.168.3.170.
C. The attack was detected and blocked.
D. The attack was detected only.
E. The attack was TCP based.

Answer: BD

NEW QUESTION 235
Which is the following statement are true regarding application control? (choose two)

A. Application control is based on TCP destination port numbers.
B. Application control is proxy based.
C. Encrypted traffic can be identified by application control.
D. Traffic Shaping can be applied to the detected application traffic.

Answer: CD

NEW QUESTION 237
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 238
When the SSL proxy is NOT doing man-in-the-middle interception of SSL traffic, which certificate field can be used to determine the rating of a website?

A. Organizational Unit.
B. Common Name.
C. Serial Number.
D. Validity.

Answer: B

NEW QUESTION 243
Which tasks fall under the responsibility of the SSL proxy in a typical HTTPS connection? (Choose two.)

A. The web client SSL handshake.
B. The web server SSL handshake.
C. File buffering.
D. Communication with the URL filter process.

Answer: AB

NEW QUESTION 248
Bob wants to send Alice a file that is encrypted using public key cryptography.
Which of the following statements is correct regarding the use of public key cryptography in this scenario?

A. Bob will use his private key to encrypt the file and Alice will use her private key to decrypt the file.
B. Bob will use his public key to encrypt the file and Alice will use Bob's private key to decrypt the file
C. Bob will use Alice's public key to encrypt the file and Alice will use her private key to decrypt the file.
D. Bob will use his public key to encrypt the file and Alice will use her private key to decrypt the file.

Answer: C

NEW QUESTION 252
Which Fortinet products & features could be considered part of a comprehensive solution to monitor and prevent the leakage of sensitive data? (Select all that apply.)

A. Archive non-compliant outgoing e-mails using FortiMail.
B. Restrict unofficial methods of transferring files such as P2P using Application Control lists on a FortiGate.
C. Monitor database activity using FortiAnalyzer.
D. Apply a DLP sensor to a firewall policy.
E. Configure FortiClient to prevent files flagged as sensitive from being copied to a USB disk.

Answer: ABD

NEW QUESTION 256
For data leak prevention, which statement describes the difference between the block and quarantine actions?

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

Answer: A

NEW QUESTION 257
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 259
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. Both the phase 1 and phases 2 must use encryption algorithms supported by the NP6.
D. IPsec traffic must not be inspected by any FortiGate session helper.

Answer: C

NEW QUESTION 264
Which IP packets can be hardware-accelerated by a NP6 processor? (Choose two.)

A. Fragmented packet.
B. Multicast packet.
C. SCTP packet
D. GRE packet.

Answer: BC

NEW QUESTION 265
What are valid options for handling DNS requests sent directly to a FortiGates interface IP? (Choose three.)

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

Answer: BCE

NEW QUESTION 269
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 274
What methods can be used to access the FortiGate CLI? (Choose two.)

A. Using SNMP.
B. A direct connection to the serial console port.
C. Using the CLI console widget in the GUI.
D. Using RCP.

Answer: BC

NEW QUESTION 278
What capabilities can a FortiGate provide? (Choose three.)

A. Mail relay.
B. Email filtering.
C. Firewall.
D. VPN gateway.
E. Mail server.

Answer: BCD

NEW QUESTION 283
Which network protocols are supported for administrative access to a FortiGate unit? (Choose three.)

A. SNMP
B. WINS
C. HTTP
D. Telnet
E. SSH

Answer: CDE

NEW QUESTION 287
What logging options are supported on a FortiGate unit? (Choose two.)

A. LDAP
B. Syslog
C. FortiAnalyzer
D. SNMP

Answer: BC

NEW QUESTION 290
Which header field can be used in a firewall policy for traffic matching?

A. ICMP type and code.
B. DSCP.
C. TCP window size.
D. TCP sequence number.

Answer: A

NEW QUESTION 292
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 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 297
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 is 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

Answer: AD

NEW QUESTION 299
Examine the following spanning tree configuration on a FortiGate in transparent mode:

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 302
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 307
In a high availability cluster operating in active-active mode, which of the following correctly describes the path taken by the SYN packet of an HTTP session that is offloaded to a slave unit?

A. Request: internal host; slave FortiGate; master FortiGate; Internet; web server.
B. Request: internal host; slave FortiGate; Internet; web server.
C. Request: internal host; slave FortiGate; master FortiGate; Internet; web server.
D. Request: internal host; master FortiGate; slave FortiGate; Internet; web server.

Answer: D

NEW QUESTION 311
Two FortiGate devices fail to form an HA cluster, the device hostnames are STUDENT and REMOTE.
Exhibit A shows the command output of show system ha for the STUDENT device. Exhibit B shows the command output of show system ha for the REMOTE device.
Exhibit A:

Exhibit B

Which one of the following is the most likely reason that the cluster fails to form?

A. Password
B. HA mode
C. Heartbeat
D. Override

Answer: B

NEW QUESTION 316
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 317
You are the administrator in charge of a FortiGate acting as an IPsec VPN gateway using route- based
mode. Users from either side must be able to initiate new sessions. There is only 1 subnet at either end and the FortiGate already has a default route.
Which two configuration steps are required to achieve these objectives? (Choose two.)

A. Create one firewall policy.
B. Create two firewall policies.
C. Add a route to the remote subnet.
D. Add two IPsec phases 2.

Answer: BC

NEW QUESTION 318
An administrator wants to create an IPsec VPN tunnel between two FortiGate devices. Which three configuration steps must be performed on both units to support this scenario? (Choose three.)

A. Create firewall policies to allow and control traffic between the source and destination IP addresses.

B. Configure the appropriate user groups to allow users access to the tunnel.
C. Set the operating mode to IPsec VPN mode.
D. Define the phase 2 parameters.
E. Define the Phase 1 parameters.

Answer: ADE

NEW QUESTION 322
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 325
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 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 330
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 security profile enables virus protection for all traffic flowing through the FortiGate.

Answer: C

NEW QUESTION 335
Examine the exhibit; then answer the question below.

Which statement describes the green status indicators that appear next to the different FortiGuard Distribution Network services as illustrated in the exhibit?

A. They indicate that the FortiGate has the latest updates available from the FortiGuard Distribution Network.
B. They indicate that updates are available and should be downloaded from the FortiGuard Distribution Network to the FortiGate unit.
C. They indicate that the FortiGate is in the process of downloading updates from the FortiGuard Distribution Network.
D. They indicate that the FortiGate is able to connect to the FortiGuard Distribution Network.

Answer: D

NEW QUESTION 337
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 342
Which two statements are true regarding firewall policy disclaimers? (Choose two.)

A. They cannot be used in combination with user authentication.
B. They can only be applied to wireless interfaces.
C. Users must accept the disclaimer to continue.
D. The disclaimer page is customizable.

Answer: CD

NEW QUESTION 344
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 347
A client can create a secure connection to a FortiGate device using SSL VPN in web-only mode. Which one of the following statements is correct regarding the use of web-only mode SSL VPN?

A. Web-only mode supports SSL version 3 only.
B. A Fortinet-supplied plug-in is required on the web client to use web-only mode SSL VPN.
C. Web-only mode requires the user to have a web browser that supports 64-bit cipher length.
D. The JAVA run-time environment must be installed on the client to be able to connect to a web- only mode SSL VPN.

Answer: C

NEW QUESTION 348
A FortiGate AntiVirus profile can be configured to scan for viruses on SMTP, FTP, POP3, and SMB
protocols using which inspection mode?

A. Proxy
B. DNS
C. Flow-based
D. Man-in-the-middle

Answer: C

NEW QUESTION 352
Which of the following is true regarding Switch Port Mode?

A. Allows all internal ports to share the same subnet.
B. Provides separate routable interfaces for each internal port.
C. An administrator can select ports to be used as a switch.
D. Configures ports to be part of the same broadcast domain.

Answer: A

NEW QUESTION 357
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? (Select all that apply.)

A. 192.168.11.100
B. 192.168.11.251
C. 192.168.10.100
D. 192.168.10.251

Answer: AB

NEW QUESTION 362
Which of the following statements are correct regarding logging to memory on a FortiGate unit?
(Select all that apply.)

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.

Answer: BC

NEW QUESTION 365
Examine the exhibit shown below; then answer the question following it.

Which of the following statements best describes the green status indicators that appear next to the different FortiGuard Distribution Network services as illustrated in the exhibit?

A. They indicate that the FortiGate unit is able to connect to the FortiGuard Distribution Network.
B. They indicate that the FortiGate unit has the latest updates that are available from the FortiGuard Distribution Network.
C. They indicate that updates are available and should be downloaded from the FortiGuard Distribution Network to the FortiGate unit.
D. They indicate that the FortiGate unit is in the process of downloading updates from the FortiGuard Distribution Network.

Answer: A

NEW QUESTION 366
A FortiGate unit is configured to receive push updates from the FortiGuard Distribution Network,

however, updates are not being received.
Which of the following statements are possible reasons for this? (Select all that apply.)

A. The external facing interface of the FortiGate unit is configured to use DHCP.
B. The FortiGate unit has not been registered.
C. There is a NAT device between the FortiGate unit and the FortiGuard Distribution Network and no override push IP is configured.
D. The FortiGate unit is in Transparent mode which does not support push updates.

Answer: ABC

NEW QUESTION 369
What are the valid sub-types for a Firewall type policy? (Select all that apply)

A. Device Identity
B. Address
C. User Identity
D. Schedule
E. SSL VPN

Answer: ABC

NEW QUESTION 373
In NAT/Route mode when there is no matching firewall policy for traffic to be forwarded by the Firewall, which of the following statements describes the action taken on traffic?

A. The traffic is blocked.
B. The traffic is passed.
C. The traffic is passed and logged.
D. The traffic is blocked and logged.

Answer: A

NEW QUESTION 375
The ordering of firewall policies is very important. Policies can be re-ordered within the FortiGate unit's GUI and also using the CLI. The command used in the CLI to perform this function is ______.

A. set order
B. edit policy
C. reorder
D. move

Answer: D

NEW QUESTION 380
You wish to create a firewall policy that applies only to traffic intended for your web server. The web server has an IP address of 192.168.2.2 and a /24 subnet mask. When defining the firewall address for use in this policy, which one of the following addresses is correct?

A. 192.168.2.0 / 255.255.255.0
B. 192.168.2.2 / 255.255.255.0
C. 192.168.2.0 / 255.255.255.255
D. 192.168.2.2 / 255.255.255.255

Answer: D

NEW QUESTION 384
Which of the following statements is correct regarding a FortiGate unit operating in NAT/Route mode?

A. The FortiGate unit applies NAT to all traffic.
B. The FortiGate unit functions as a Layer 3 device.
C. The FortiGate unit functions as a Layer 2 device.
D. The FortiGate unit functions as a router and the firewall function is disabled.

Answer: B

NEW QUESTION 386
A FortiGate unit can provide which of the following capabilities? (Select all that apply.)

A. Email filtering
B. Firewall
C. VPN gateway
D. Mail relay
E. Mail server

Answer: ABC

NEW QUESTION 391
CORRECT TEXT
The ______ CLI command is used on the FortiGate unit to run static commands such as ping or to reset the FortiGate unit to factory defaults.

Answer:

Explanation: execute

NEW QUESTION 395
When creating administrative users which of the following configuration objects determines access rights on the FortiGate unit.

A. profile
B. allowaccess interface settings
C. operation mode
D. local-in policy

Answer: A

NEW QUESTION 396
Which of the following options can you use to update the virus definitions on a FortiGate unit? (Select all that apply.)

A. Push update.
B. Scheduled update
C. Manual update
D. FTP update

Answer: ABC

NEW QUESTION 401
Which of the following statements are true of the FortiGate unit's factory default configuration?

A. `Port1' or `Internal' interface will have an IP of 192.168.1.99.
B. `Port1' or `Internal' interface will have a DHCP server set up and enabled (on devices that support DHCP Servers).
C. Default login will always be the username: admin (all lowercase) and no password.
D. The implicit firewall action is ACCEPT.

Answer: ABC

NEW QUESTION 402
Under the System Information widget on the dashboard, which of the following actions are available for the system configuration? (Select all that apply.)

A. Backup
B. Restore
C. Revisions
D. Export

Answer: ABC

NEW QUESTION 403
The FortiGate unit's GUI provides a link to update the firmware. Clicking this link will perform which of the following actions?

A. It will connect to the Fortinet Support site where the appropriate firmware version can be selected.
B. It will send a request to the FortiGuard Distribution Network so that the appropriate firmware version can be pushed down to the FortiGate unit.
C. It will present a prompt to allow browsing to the location of the firmware file.
D. It will automatically connect to the Fortinet Support site to download the most recent firmware version for the FortiGate unit.

Answer: C

NEW QUESTION 404
Which of the following products provides dedicated hardware to analyze log data from multiple FortiGate devices?

A. FortiGate device
B. FortiAnalyzer device
C. FortiClient device
D. FortiManager device
E. FortiMail device
F. FortiBridge device

Answer: B

NEW QUESTION 405
Which of the following logging options are supported on a FortiGate unit? (Select all that apply.)

A. LDAP
B. Syslog
C. FortiAnalyzer
D. Local disk and/or memory

Answer: BCD

NEW QUESTION 408
In order to match an identity-based policy, the FortiGate unit checks the IP information. Once inside the policy, the following logic is followed:

A. First, a check is performed to determine if the user's login credentials are vali
B. Next, the user is checked to determine if they belong to any of the groups defined for that polic
C. Finally, user restrictions are determined and port, time, and UTM profiles are applied.
D. First, user restrictions are determined and port, time, and UTM profiles are applie
E. Next, a check is performed to determine if the user's login credentials are vali
F. Finally, the user is checked to determine if they belong to any of the groups defined for that policy.
G. First, the user is checked to determine if they belong to any of the groups defined for that polic
H. Next, user restrictions are determined and port, time, and UTM profiles are applie
I. Finally, a check is performed to determine if the user's login credentials are valid.

Answer: A

NEW QUESTION 412
Which of the following statements regarding the firewall policy authentication timeout is true?

A. The authentication timeout is an idle timeout.This means that the FortiGate unit will consider a user to be "idle" if it does not see any packets coming from the user's source IP.
B. The authentication timeout is a hard timeout.This means that the FortiGate unit will remove the temporary policy for this user's source IP after this timer has expired.
C. The authentication timeout is an idle timeout.This means that the FortiGate unit will consider a user to be "idle" if it does not see any packets coming from the user's source MAC.
D. The authentication timeout is a hard timeout.This means that the FortiGate unit will remove the temporary policy for this user's source MAC after this timer has expired.

Answer: A

NEW QUESTION 417
Examine the firewall configuration shown below; then answer the question following it.

Which of the following statements are correct based on the firewall configuration illustrated in the exhibit? (Select all that apply.)

A. A user can access the Internet using only the protocols that are supported by user authentication.
B. A user can access the Internet using any protocol except HTTP, HTTPS, Telnet, and FT
C. These require authentication before the user will be allowed access.
D. A user must authenticate using the HTTP, HTTPS, SSH, FTP, or Telnet protocol before they can access any services.
E. A user cannot access the Internet using any protocols unless the user has passed firewall authentication.

Answer: AD

NEW QUESTION 418
An issue could potentially occur when clicking Connect to start tunnel mode SSL VPN. The tunnel will start up for a few seconds, then shut down.
Which of the following statements best describes how to resolve this issue?

A. This user does not have permission to enable tunnel mode.Make sure that the tunnel mode widget has been added to that user's web portal.
B. This FortiGate unit may have multiple Internet connections.To avoid this problem, use the appropriate CLI command to bind the SSL VPN connection to the original incoming interface.
C. Check the SSL adaptor on the host machine.If necessary, uninstall and reinstall the adaptor from the tunnel mode portal.
D. Make sure that only Internet Explorer is use
E. All other browsers are unsupported.

Answer: B

NEW QUESTION 422
You are the administrator in charge of a FortiGate unit which acts as a VPN gateway.
You have chosen to use Interface Mode when configuring the VPN tunnel and you want users from either side to be able to initiate new sessions.
There is only 1 subnet at either end and the FortiGate unit already has a default route.
Which of the following configuration steps are required to achieve these objectives? (Select all that apply.)

A. Create one firewall policy.
B. Create two firewall policies.
C. Add a route for the remote subnet.
D. Add a route for incoming traffic.
E. Create a phase 1 definition.
F. Create a phase 2 definition.

Answer: BCEF

NEW QUESTION 425
Which one of the following statements is correct about raw log messages?

A. Logs have a header and a body section.The header will have the same layout for every log message.The body section will change layout from one type of log message to another.
B. Logs have a header and a body section.The header and body will change layout from one type of log message to another.
C. Logs have a header and a body section.The header and body will have the same layout for every log message.

Answer: A

NEW QUESTION 430
Which of the following is an advantage of using SNMP v3 instead of SNMP v1/v2 when querying the FortiGate unit?

A. Packet encryption
B. MIB-based report uploads
C. SNMP access limits through access lists
D. Running SNMP service on a non-standard port is possible

Answer: A

NEW QUESTION 432
Users may require access to a web site that is blocked by a policy. Administrators can give users the ability to override the block.
Which of the following statements regarding overrides are correct? (Select all that apply.)

A. A protection profile may have only one user group defined as an override group.
B. A firewall user group can be used to provide override privileges for FortiGuard Web Filtering.
C. Authentication to allow the override is based on a user's membership in a user group.
D. Overrides can be allowed by the administrator for a specific period of time.

Answer: BCD

NEW QUESTION 433
Users may require access to a web site that is blocked by a policy. Administrators can give users the ability to override the block.
Which of the following statements regarding overrides is NOT correct?

A. A web filter profile may only have one user group defined as an override group.
B. A firewall user group can be used to provide override privileges for FortiGuard Web Filtering.
C. When requesting an override, the matched user must belong to a user group for which the override capability has been enabled.
D. Overrides can be allowed by the administrator for a specific period of time.

Answer: A

NEW QUESTION 438
An administrator has configured a FortiGate unit so that end users must authenticate against the firewall using digital certificates before browsing the Internet.
What must the user have for a successful authentication? (Select all that apply.)

A. An entry in a supported LDAP Directory.
B. A digital certificate issued by any CA server.
C. A valid username and password.
D. A digital certificate issued by the FortiGate unit.
E. Membership in a firewall user group.

Answer: BE

NEW QUESTION 443
A FortiGate unit can create a secure connection to a client using SSL VPN in tunnel mode. Which of the following statements are correct regarding the use of tunnel mode SSL VPN? (Select all that apply.)

A. Split tunneling can be enabled when using tunnel mode SSL VPN.
B. Software must be downloaded to the web client to be able to use a tunnel mode SSL VPN.
C. Users attempting to create a tunnel mode SSL VPN connection must be members of a configured user group on the FortiGate unit.
D. Tunnel mode SSL VPN requires the FortiClient software to be installed on the user's computer.
E. The source IP address used by the client for the tunnel mode SSL VPN is assigned by the FortiGate unit.

Answer: ABCE

NEW QUESTION 447
Which of the following antivirus and attack definition update features are supported by FortiGate units? (Select all that apply.)

A. Manual, user-initiated updates from the FortiGuard Distribution Network.
B. Hourly, daily, or weekly scheduled antivirus and attack definition and antivirus engine updates from the FortiGuard Distribution Network.
C. Push updates from the FortiGuard Distribution Network.
D. Update status including version numbers, expiry dates, and most recent update dates and times.

Answer: ABCD

NEW QUESTION 451
A FortiGate unit can scan for viruses on which types of network traffic? (Select all that apply.)

A. POP3
B. FTP
C. SMTP
D. SNMP
E. NetBios

Answer: ABC

NEW QUESTION 455
Which of the following statements is correct regarding URL Filtering on the FortiGate unit?

A. The available actions for URL Filtering are Allow and Block.
B. Multiple URL Filter lists can be added to a single Web filter profile.
C. A FortiGuard Web Filtering Override match will override a block action in the URL filter list.
D. The available actions for URL Filtering are Allow, Block and Exempt.

Answer: D

NEW QUESTION 457
Which of the following Regular Expression patterns will make the term "bad language" case insensitive?

A. [bad language]
B. /bad language/i
C. i/bad language/
D. "bad language"
E. /bad language/c

Answer: B

NEW QUESTION 458
Which of the following statements describes the method of creating a policy to block access to an FTP site?

A. Enable Web Filter URL blocking and add the URL of the FTP site to the URL Block list.
B. Create a firewall policy with destination address set to the IP address of the FTP site, the Service set to FTP, and the Action set to Deny.
C. Create a firewall policy with a protection profile containing the Block FTP option enabled.
D. None of the above.

Answer: B

NEW QUESTION 463
Each UTM feature has configurable UTM objects such as sensors, profiles or lists that define how the feature will function. How are UTM features applied to traffic?

A. One or more UTM features are enabled in a firewall policy.
B. In the system configuration for that UTM feature, you can identify the policies to which the feature is to be applied.
C. Enable the appropriate UTM objects and identify one of them as the default.
D. For each UTM object, identify which policy will use it.

Answer: A

NEW QUESTION 466
Which of the following network protocols can be used to access a FortiGate unit as an administrator?

A. HTTPS, HTTP, SSH, TELNET, PING, SNMP
B. FTP, HTTPS, NNTP, TCP, WINS
C. HTTP, NNTP, SMTP, DHCP
D. Telnet, FTP, RLOGIN, HTTP, HTTPS, DDNS
E. Telnet, UDP, NNTP, SMTP

Answer: A

NEW QUESTION 469
If a FortiGate unit has a dmz interface IP address of 210.192.168.2 with a subnet mask of 255.255.255.0, what is a valid dmz DHCP addressing range?

A. 172.168.0.1 - 172.168.0.10

B. 210.192.168.3 - 210.192.168.10
C. 210.192.168.1 - 210.192.168.4
D. All of the above.

Answer: B

NEW QUESTION 472
A FortiGate unit can act as which of the following? (Select all that apply.)

A. Antispam filter
B. Firewall
C. VPN gateway
D. Mail relay
E. Mail server

Answer: ABC

NEW QUESTION 474
CORRECT TEXT
When creating administrative users, the assigned ______ determines user rights on the FortiGate unit.

Answer:

Explanation: access profile

NEW QUESTION 477
Which of the following items represent the minimum configuration steps an administrator must
perform to enable Data Leak Prevention for traffic flowing through the FortiGate unit? (Select all that apply.)

A. Assign a DLP sensor in a firewall policy.
B. Apply one or more DLP rules to a firewall policy.
C. Enable DLP globally using the config sys dlp command in the CLI.
D. Define one or more DLP rules.
E. Define a DLP sensor.
F. Apply a DLP sensor to a DoS sensor policy.

Answer: ADE

NEW QUESTION 482
Because changing the operational mode to Transparent resets device (or vdom) to all defaults, which precautions should an Administrator take prior to performing this? (Select all that apply.)

A. Backup the configuration.
B. Disconnect redundant cables to ensure the topology will not contain layer 2 loops.
C. Set the unit to factory defaults.
D. Update IPS and AV files.

Answer: AB

NEW QUESTION 486
Which part of an email message exchange is NOT inspected by the POP3 and IMAP proxies?

A. TCP connection
B. File attachments
C. Message headers
D. Message body

Answer: A

NEW QUESTION 489
Which of the following statements correctly describes how a push update from the FortiGuard
Distribution Network (FDN) works?

A. The FDN sends push updates only once.
B. The FDN sends package updates automatically to the FortiGate unit without requiring an update request.
C. The FDN continues to send push updates until the FortiGate unit sends an acknowledgement.
D. The FDN sends a message to the FortiGate unit that there is an update available and that the FortiGate unit should download the update.

Answer: D

NEW QUESTION 491
CORRECT TEXT
In addition to AntiVirus services, the FortiGuard Subscription Services provide IPS, Web Filtering, and _______ services.

Answer:

Explanation: antispam

NEW QUESTION 496
Examine the exhibit shown below then answer the question that follows it.

Within the UTM Proxy Options, the CA certificate Fortinet_CA_SSLProxy defines which of the following:

A. FortiGate unit's encryption certificate used by the SSL proxy.
B. FortiGate unit's signing certificate used by the SSL proxy.
C. FortiGuard's signing certificate used by the SSL proxy.
D. FortiGuard's encryption certificate used by the SSL proxy.

Answer: A

NEW QUESTION 500
Which of the following statements are correct regarding virtual domains (VDOMs)? (Select all that apply.)

A. VDOMs divide a single FortiGate unit into two or more virtual units that function as multiple, independent units.
B. A management VDOM handles SNMP, logging, alert email, and FDN-based updates.
C. VDOMs share firmware versions, as well as antivirus and IPS databases.
D. Only administrative users with a 'super_admin' profile will be able to enter multiple VDOMs to make configuration changes.

Answer: ABC

NEW QUESTION 504
Examine the Exhibits shown below, then answer the question that follows. Review the following DLP
Sensor (Exhibit 1):

Review the following File Filter list for rule #1 (Exhibit 2):

Review the following File Filter list for rule #2 (Exhibit 3):

Review the following File Filter list for rule #3 (Exhibit 4):

An MP3 file is renamed to `workbook.exe' and put into a ZIP archive. It is then sent through the FortiGate device over HTTP. It is intercepted and processed by the configuration shown in the above Exhibits 1-4.
Assuming the file is not too large for the File scanning threshold, what action will the FortiGate unit take?

A. The file will be detected by rule #1 as an `Audio (mp3)', a log entry will be created and it will be allowed to pass through.
B. The file will be detected by rule #2 as a "*.exe", a log entry will be created and the interface that received the traffic will be brought down.
C. The file will be detected by rule #3 as an Archive(zip), blocked, and a log entry will be created.
D. Nothing, the file will go undetected.

Answer: A

NEW QUESTION 505
What are the requirements for a cluster to maintain TCP connections after device or link failover?
(Select all that apply.)

A. Enable session pick-up.
B. Only applies to connections handled by a proxy.
C. Only applies to UDP and ICMP connections.
D. Connections must not be handled by a proxy.

Answer: AD

NEW QUESTION 506
With FSSO, a domain user could authenticate either against the domain controller running the
Collector Agent and Domain Controller Agent, or a domain controller running only the Domain Controller Agent.
If you attempt to authenticate with the Secondary Domain Controller running only the Domain Controller Agent, which of the following statements are correct?
(Select all that apply.)

A. The login event is sent to the Collector Agent.
B. The FortiGate unit receives the user information from the Domain Controller Agent of the Secondary Controller.
C. The Collector Agent performs the DNS lookup for the authenticated client's IP address.
D. The user cannot be authenticated with the FortiGate device in this manner because each DomainController Agent requires a dedicated Collector Agent.

Answer: AC

NEW QUESTION 511
In Transparent Mode, forward-domain is an attribute of .

A. an interface
B. a firewall policy
C. a static route
D. a virtual domain

Answer: A

NEW QUESTION 515
Which of the following statements is correct regarding the antivirus scanning function on the FortiGate unit?

A. Antivirus scanning provides end-to-end virus protection for client workstations.
B. Antivirus scanning provides virus protection for the HTTP, Telnet, SMTP, and FTP protocols.
C. Antivirus scanning supports banned word checking.
D. Antivirus scanning supports grayware protection.

Answer: D

NEW QUESTION 516
Both the FortiGate and FortiAnalyzer units can notify administrators when certain alert conditions are met.
Considering this, which of the following statements is NOT correct?

A. On a FortiGate device, the alert condition is based either on the severity level or on the log type, but not on a combination of the two.
B. On a FortiAnalyzer device, the alert condition is based either on the severity level or on the log type, but not on a combination of the two.
C. Only a FortiAnalyzer device can send the alert notification in the form of a syslog message.
D. Both the FortiGate and FortiAnalyzer devices can send alert notifications in the form of an email alert.

Answer: B

NEW QUESTION 520
Which of the following statements is correct about how the FortiGate unit verifies username and
password during user authentication?

A. If a remote server is included in a user group, it will be checked before local accounts.
B. An administrator can define a local account for which the password must be verified by querying a remote server.
C. If authentication fails with a local password, the FortiGate unit will query the authentication server if the local user is configured with both a local password and an authentication server.
D. The FortiGate unit will only attempt to authenticate against Active Directory if Fortinet Server Authentication Extensions are installed and configured.

Answer: B

NEW QUESTION 523
Which of the following cannot be used in conjunction with the endpoint compliance check?

A. HTTP Challenge Redirect to a Secure Channel (HTTPS) in the Authentication Settings.
B. Any form of firewall policy authentication.
C. WAN optimization.
D. Traffic shaping.

Answer:

A

NEW QUESTION 527
An administrator configures a VPN and selects the Enable IPSec Interface Mode option in the phase 1 settings.
Which of the following statements are correct regarding the IPSec VPN configuration?

A. To complete the VPN configuration, the administrator must manually create a virtual IPSec interface in Web Config under System > Network.
B. The virtual IPSec interface is automatically created after the phase1 configuration.
C. The IPSec policies must be placed at the top of the list.
D. This VPN cannot be used as part of a hub and spoke topology.
E. Routes were automatically created based on the address objects in the firewall policies.

Answer: B

NEW QUESTION 530
When configuring a server load balanced virtual IP, which of the following is the best distribution algorithm to be used in applications where the same physical destination server must be maintained between sessions?

A. Static
B. Round robin
C. Weighted round robin
D. Least connected

Answer: A

NEW QUESTION 533
If Routing Information Protocol (RIP) version 1 or version 2 has already been configured on a FortiGate unit, which of the following statements is correct if the routes learned through RIP need to be advertised into Open Shortest Path First (OSPF)?

A. The FortiGate unit will automatically announce all routes learned through RIP v1 or v2 to its OSPF neighbors.
B. The FortiGate unit will automatically announce all routes learned only through RIP v2 to its OSPF neighbors.
C. At a minimum, the network administrator needs to enable Redistribute RIP in the OSPF Advanced Options.
D. The network administrator needs to configure a RIP to OSPF announce policy as part of the RIP settings.
E. At a minimum, the network administrator needs to enable Redistribute Default in the OSPF Advanced Options.

Answer: C

NEW QUESTION 537
Which of the following report templates must be used when scheduling report generation?

A. Layout Template
B. Data Filter Template
C. Output Template
D. Chart Template

Answer: A

NEW QUESTION 542
Which of the following statements is not correct regarding virtual domains (VDOMs)?

A. VDOMs divide a single FortiGate unit into two or more virtual units that function as multiple, independent units.
B. A management VDOM handles SNMP, logging, alert email, and FDN-based updates.
C. A backup management VDOM will synchronize the configuration from an active management VDOM.
D. VDOMs share firmware versions, as well as antivirus and IPS databases.
E. Only administrative users with a super_admin profile will be able to enter all VDOMs to make configuration changes.

Answer: C

NEW QUESTION 547
Which of the following must be configured on a FortiGate unit to redirect content requests to remote web cache servers?

A. WCCP must be enabled on the interface facing the Web cache.
B. You must enabled explicit Web-proxy on the incoming interface.
C. WCCP must be enabled as a global setting on the FortiGate unit.
D. WCCP must be enabled on all interfaces on the FortiGate unit through which HTTP traffic is passing.

Answer: A

NEW QUESTION 551
Which of the following statements is correct based on the firewall configuration illustrated in the exhibit?

A. A user can access the Internet using only the protocols that are supported by user authentication.
B. A user can access the Internet using any protocol except HTTP, HTTPS, Telnet, and FT
C. These require authentication before the user will be allowed access.
D. A user must authenticate using the HTTP, HTTPS, SSH, FTP, or Telnet protocol before they can access any services.
E. A user cannot access the Internet using any protocols unless the user has passed firewall authentication.

Answer: D

NEW QUESTION 552
Which of the following statements is correct regarding the NAC Quarantine feature?

A. With NAC quarantine, files can be quarantined not only as a result of antivirus scanning, but also for other forms of content inspection such as IPS and DLP.
B. NAC quarantine does a client check on workstations before they are permitted to have administrative access to FortiGate.
C. NAC quarantine allows administrators to isolate clients whose network activity poses a security risk.
D. If you chose the quarantine action, you must decide whether the quarantine type is NAC quarantine or File quarantine.

Answer: C

NEW QUESTION 554
What advantages are there in using a fully Meshed IPSec VPN configuration instead of a hub and spoke set of IPSec tunnels?

A. Using a hub and spoke topology is required to achieve full redundancy.
B. Using a full mesh topology simplifies configuration.
C. Using a full mesh topology provides stronger encryption.
D. Full mesh topology is the most fault-tolerant configuration.

Answer: D

NEW QUESTION 556
In a High Availability configuration operating in Active-Active mode, which of the following correctly describes the path taken by a load-balanced HTTP session?

A. Request: Internal Host -> Master FG -> Slave FG -> Internet -> Web Server
B. Request: Internal Host -> Master FG -> Slave FG -> Master FG -> Internet -> Web Server
C. Request: Internal Host -> Slave FG -> Internet -> Web Server
D. Request: Internal Host -> Slave FG -> Master FG -> Internet -> Web Server

Answer: A

NEW QUESTION 559
The following diagnostic output is displayed in the CLI:

Based on this output, which of the following statements is correct?

A. Firewall policy 9 has endpoint compliance enabled but not firewall authentication.
B. The client check that is part of an SSL VPN connection attempt failed.
C. This user has been associated with a guest profile as evidenced by the group id of 0.
D. An auth-keepalive value has been enabled.

Answer: A

NEW QUESTION 562
Which of the following statements are correct regarding URL Filtering on the FortiGate unit? (Select all that apply.)

A. The allowed actions for URL Filtering include Allow, Block and Exempt.
B. The allowed actions for URL Filtering are Allow and Block.
C. The FortiGate unit can filter URLs based on patterns using text and regular expressions.
D. Any URL accessible by a web browser can be blocked using URL Filtering.
E. Multiple URL Filter lists can be added to a single protection profile.

Answer: AC

NEW QUESTION 567
An administrator sets up a new FTP server on TCP port 2121. A FortiGate unit is located between the FTP clients and the server. The administrator has created a policy for TCP port 2121.
Users have been complaining that when downloading data they receive a 200 Port command successful message followed by a 425 Cannot build data connection message.
Which of the following statements represents the best solution to this problem?

A. Create a new session helper for the FTP service monitoring port 2121.
B. Enable the ANY service in the firewall policies for both incoming and outgoing traffic.
C. Place the client and server interface in the same zone and enable intra-zone traffic.
D. Disable any protection profiles being applied to FTP traffic.

Answer: A

NEW QUESTION 571
A network administrator connects his PC to the INTERNAL interface on a FortiGate unit.
The administrator attempts to make an HTTPS connection to the FortiGate unit on the VLAN1 interface at the IP address of 10.0.1.1, but gets no connectivity.
The following troubleshooting commands are executed from the CLI:

Based on the output from these commands, which of the following is a possible cause of the problem?

A. The FortiGate unit has no route back to the PC.
B. The PC has an IP address in the wrong subnet.
C. The PC is using an incorrect default gateway IP address.
D. There is no firewall policy allowing traffic from INTERNAL -> VLAN1.

Answer: D

NEW QUESTION 576
Which of the following features could be used by an administrator to block FTP uploads while still
allowing FTP downloads?

A. Anti-Virus File-Type Blocking
B. Data Leak Prevention
C. Network Admission Control
D. FortiClient Check

Answer: B

NEW QUESTION 577
Based on the web filtering configuration illustrated in the exhibit,

which one of the following statements is not a reasonable conclusion?

A. Users can access both the www.google.com site and the www.fortinet.com site.
B. When a user attempts to access the www.google.com site, the FortiGate unit will not perform web filtering on the content of that site.
C. When a user attempts to access the www.fortinet.com site, any remaining web filtering will be bypassed.
D. Downloaded content from www.google.com will be scanned for viruses if antivirus is enabled.

Answer: B

NEW QUESTION 581
The transfer of encrypted files or the use of encrypted protocols between users and servers on the
internet can frustrate the efforts of administrators attempting to monitor traffic passing through the FortiGate unit and ensuring user compliance to corporate rules.
Which of the following items will allow the administrator to control the transfer of encrypted data through the FortiGate unit? (Select all that apply.)

A. Encrypted protocols can be scanned through the use of the SSL proxy.

B. DLP rules can be used to block the transmission of encrypted files.
C. Firewall authentication can be enabled in the firewall policy, preventing the use of encrypted communications channels.
D. Application control can be used to monitor the use of encrypted protocols; alerts can be sent to the administrator through email when the use of encrypted protocols is attempted.

Answer: ABD

NEW QUESTION 582
Which of the following statements correctly describes the deepscan option for HTTPS?

A. When deepscan is disabled, only the web server certificate is inspected; no decryption of content occurs.
B. Enabling deepscan will perform further checks on the server certificate.
C. Deepscan is only applicable to mail protocols, where all IP addresses in the header are checked.
D. With deepscan enabled, archived files will be decompressed before scanning for a more comprehensive file inspection.

Answer: A

NEW QUESTION 584
What protocol cannot be used with the active authentication type?

A. Local
B. RADIUS
C. LDAP
D. RSSO

Answer: D

NEW QUESTION 589
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 591
Which statement best describes the objective of the SYN proxy feature available in SP processors?

A. Accelerate the TCP 3-way handshake
B. Collect statistics regarding traffic sessions
C. Analyze the SYN packet to decide if the new session can be offloaded to the SP processor
D. Protect against SYN flood attacks.

Answer: D

NEW QUESTION 592
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 597
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.

Answer: D

NEW QUESTION 598
Which of the following statements describe some of the differences between symmetric and asymmetric cryptography? (Choose two.)

A. In symmetric cryptography, the keys are publicly availabl
B. In asymmetric cryptography, the keys must be kept secret.
C. Asymmetric cryptography can encrypt data faster than symmetric cryptography
D. Symmetric cryptography uses one pre-shared ke

E. Asymmetric cryptography uses a pair or keys
F. Asymmetric keys can be sent to the remote peer via digital certificate
G. Symmetric keys cannot

Answer: CD

NEW QUESTION 600
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 602
Which of the following statements best describes the role of a DC agents in an FSSO DC?

A. Captures the login events and forward them to the collector agent.
B. Captures the user IP address and workstation name and forward that information to the FortiGate devices.
C. Captures the login and logoff events and forward them to the collector agent.
D. Captures the login events and forward them to the FortiGate devices.

Answer: C

NEW QUESTION 605
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 610
Which operating system vulnerability can you protect when selecting signatures to include in an IPS sensor? (Choose three)

A. Irix
B. QNIX
C. Linux
D. Mac OS
E. BSD

Answer: CDE

NEW QUESTION 611
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 615
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 616
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 621
Which of the following statements are correct concerning IPsec dialup VPN configurations for FortiGate devices? (Choose two)

A. Main mode mist be used when there is no more than one IPsec dialup VPN configured on the same FortiGate device.
B. A FortiGate device with an IPsec VPN configured as dialup can initiate the tunnel connection to any remote IP address.
C. Peer ID must be used when there is more than one aggressive-mode IPsec dialup VPN on the same FortiGate device.
D. The FortiGate will automatically add a static route to the source quick mode selector address received from each remote peer.

Answer: CD

NEW QUESTION 623
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 624
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 627
Which statement describes how traffic flows in sessions handled by a slave unit in an active- active HA cluster?

A. Packet are sent directly to the slave unit using the slave physical MAC address.
B. Packets are sent directly to the slave unit using the HA virtual MAC address.
C. Packets arrived at both units simultaneously, but only the salve unit forwards the session.
D. Packets are first sent to the master unit, which then forwards the packets to the slave unit.

Answer: D

NEW QUESTION 629
Files that are larger than the oversized limit are subjected to which Antivirus check?

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

Answer: C

NEW QUESTION 632
Which of the following traffic shaping functions can be offloaded to a NP processor? (Choose two.)

A. Que prioritization
B. Traffic cap (bandwidth limit)
C. Differentiated services field rewriting
D. Guarantee bandwidth

Answer: CD

NEW QUESTION 634
Which statement best describes what a Fortinet System on a Chip (SoC) is?

A. Low-power chip that provides general purpose processing power
B. Chip that combines general purpose processing power with Fortinet's custom ASIC technology
C. Light-version chip (with fewer features) of an SP processor

D. Light-version chip (with fewer features) of a CP processor

Answer: B

NEW QUESTION 637
A static route is configured for a FortiGate unit from the CLI using the following commands:

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 639
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 641
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 646
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 647
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 652
A FortiGate device is configured with two VDOMs. The management VDOM is 'root', and is configured in transparent mode,'vdom1' is configured as NAT/route mode. Which traffic is generated only by 'root' and not 'vdom1'? (Choose three.)

A. SNMP traps
B. FortiGaurd
C. ARP
D. NTP
E. ICMP redirect

Answer: ABD

NEW QUESTION 654
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 656
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 659
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 660
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 664
In a FSSO agentless polling mode solution, where must the collector agent be?

A. In any Windows server

B. In any of the AD domain controllers
C. In the master AD domain controller
D. The FortiGate device polls the AD domain controllers

Answer: D

NEW QUESTION 667
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 668
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 670
You have configured the DHCP server on a FortiGate's port1 interface (or internal, depending on the model) to offer IPs in a range of 192.168.1.65-192.168.1.253.
When the first host sends a DHCP request, what IP will the DHCP offer?

A. 192.168.1.99
B. 192.168.1.253
C. 192.168.1.65
D. 192.168.1.66

Answer: C

NEW QUESTION 671
Regarding the use of web-only mode SSL VPN, which statement is correct?

A. It support SSL version 3 only.
B. It requires a Fortinet-supplied plug-in on the web client.
C. It requires the user to have a web browser that suppports 64-bit cipher length.
D. The JAVA run-time environment must be installed on the client.

Answer: C

NEW QUESTION 675
The exhibit shows a part output of the diagnostic command 'diagnose debug application ike 255',
taken during establishment of a VPN. Which of the following statement are correct concerning this output? (Choose two)

A. The quick mode selectors negotiated between both IPsec VPN peers is 0.0.0.0/32 for both source and destination addresses.
B. The output corresponds to a phase 2 negotiation
C. NAT-T enabled and there is third device in the path performing NAT of the traffic between both IPsec VPN peers.
D. The IP address of the remote IPsec VPN peer is 172.20.187.114

Answer: BD

NEW QUESTION 676
Which statement concerning IPS is false?

A. IPS packages contain an engine and signatures used by both IPS and other flow-based scans.
B. One-arm topology with sniffer mode improves performance of IPS blocking.
C. IPS can detect zero-day attacks.
D. The status of the last service update attempt from FortiGuard IPS is shown on System>Config>FortiGuard and in output from 'diag autoupdate version'

Answer: D

NEW QUESTION 677
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 polices 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 680
......