Fortinet

Exam Questions NSE4-5.4

Fortinet Network Security Expert - FortiOS 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
Under what circumstance would you enable LEARN as the Action on a firewall policy?

A. You want FortiGate to compile security feature activity from various security-related logs, such as virus and attack logs.
B. You want FortiGate to monitor a specific security profile in a firewall policy, and provide recommendations for that profile.
C. You want to capture data across all traffic and security vectors, and receive learning logs and a report with recommendations.
D. You want FortiGate to automatically modify your firewall policies as it learns your networking behavior.

Answer: C

NEW QUESTION 4
Which statements about DNS filter profiles are true? (Choose two.)

A. They can inspect HTTP traffic.
B. They must be applied in firewall policies with SSL inspection enabled.
C. They can block DNS request to known botnet command and control servers.
D. They can redirect blocked requests to a specific portal.

Answer: CD

NEW QUESTION 5
Which of the following statements describe WMI polling mode for FSSO collector agent? (Choose two.)

A. The collector agent does not need to search any security event logs.
B. WMI polling can increase bandwidth usage with large networks.
C. The NetSessionEnum function is used to track user logoffs.
D. The collector agent uses a Windows API to query DCs for user logins.

Answer: BD

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
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 8
Which statements correctly describe transparent mode operation? (Choose three.)

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

Answer: CDE

NEW QUESTION 9
View the exhibit.

What is the effect of the Disconnect Cluster Member operation as shown in the exhibit? (Choose two.)

A. The HA mode changes to standalone.
B. The firewall policies are deleted on the disconnected member.
C. The system hostname is set to the FortiGate serial number.
D. The port3 is configured with an IP address for management access.

Answer: AD

NEW QUESTION 10
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 10
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 14
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 15
View the exhibit.

When Role is set to Undefined, which statement is true?

A. The GUI provides all the configuration options available for the port1 interface.
B. You cannot configure a static IP address for the port1 interface because it allows only DHCP addressing mode.
C. Firewall policies can be created from only the port1 interface to any interface.
D. The port1 interface is reserved for management only.

Answer: A

NEW QUESTION 17
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 22
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

NEW QUESTION 26
View the exhibit.

A user behind the FortiGate is trying to go to http://www.addictinggames.com (Addicting.Games).
Based on this configuration, which statement is true?

A. Addicting.Games is allowed based on the Application Overrides configuration.
B. Addicting.Games is blocked based on the Filter Overrides configuration.
C. Addicting.Games can be allowed only if the Filter Overrides actions is set to Exempt.
D. Addicting.Games is allowed based on the Categories configuration.

Answer: A

NEW QUESTION 27
Which of the following statements about NTLM authentication are correct? (Choose two.)

A. It is useful when users log in to DCs that are not monitored by a collector agent.
B. It takes over as the primary authentication method when configured alongside FSSO.
C. Multi-domain environments require DC agents on every domain controller.
D. NTLM-enabled web browsers are required.

Answer: AD

NEW QUESTION 29
View the exhibit.

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

A. port1-VLAN10 and port2-VLAN10 can be assigned to different VDOMs.
B. port1-VLAN1 is the native VLAN for the port1 physical interface.
C. Traffic between port1-VLAN1 and port2-VLAN1 is allowed by default.
D. Broadcast traffic received in port1-VLAN10 will not be forwarded to port2-VLAN10.

Answer: AD

NEW QUESTION 30
An administrator has enabled proxy-based antivirus scanning and configured the following settings:

Which statement about the above configuration is true?

A. Files bigger than 10 MB are not scanned for viruses and will be blocked.
B. FortiGate scans only the first 10 MB of any file.
C. Files bigger than 10 MB are sent to the heuristics engine for scanning.
D. FortiGate scans the files in chunks of 10 MB.

Answer: A

NEW QUESTION 35
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 40
An administrator has created a custom IPS signature. Where does the custom IPS signature have to be applied?

A. In an IPS sensor
B. In an interface.
C. In a DoS policy.
D. In an application control profile.

Answer: A

Explanation: I create a custom signature then I try to add and appear only in IPS sensor.

NEW QUESTION 41
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 43
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 48

An administrator has configured a route-based IPsec VPN between two FortiGates. Which statement about this IPsec VPN configuration is true?

A. A phase 2 configuration is not required.
B. This VPN cannot be used as part of a hub and spoke topology.
C. The IPsec firewall policies must be placed at the top of the list.
D. A virtual IPsec interface is automatically created after the phase 1 configuration is completed.

Answer: D

NEW QUESTION 51
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

Explanation:

NEW QUESTION 52
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 57
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 59
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

NEW QUESTION 60
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 61
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 66
How does FortiGate look for a matching firewall policy to process traffic?

A. From top to bottom, based on the sequence numbers.
B. Based on best match.
C. From top to bottom, based on the policy ID numbers.
D. From lower to higher, based on the priority value.

Answer: A

NEW QUESTION 69
Which file names will match the *.tiff file name pattern configured in a data leak prevention filter?
(Choose two.)

A. tiff.tiff
B. tiff.png
C. tiff.jpeg
D. gif.tiff

Answer: AD

NEW QUESTION 71
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 73
Which component of FortiOS performs application control inspection?

A. Kernel
B. Antivirus engine
C. IPS engine
D. Application control engine

Answer: C

NEW QUESTION 76
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 81
A FortiGate is operating in NAT/Route mode and configured with two virtual LAN (VLAN) sub-interfaces added to the same physical interface.
Which statement about the VLAN IDs in this scenario is true?

A. The two VLAN sub-interfaces can have the same VLAN ID only if they belong to different VDOMs.
B. The two VLAN sub-interfaces must have different VLAN IDs.
C. The two VLAN sub-interfaces can have the same VLAN ID only if they have IP addresses in the same subnet.
D. The two VLAN sub-interfaces can have the same VLAN ID only if they have IP addresses in different subnets.

Answer: B

NEW QUESTION 84
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 86
View the Exhibit.

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

A. The global configuration is synchronized between the primary and secondary FortiGate.
B. The all VDOM is not synchronized between the primary and secondary FortiGate.
C. The root VDOM is not synchronized between the primary and secondary FortiGate.
D. The FortiGates have three VDOMs.

Answer: AC

NEW QUESTION 89
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 94
Which condition must be met to offload the encryption and decryption of IPsec traffic to an NP6 processor?

A. Phase 2 must use an encryption algorithm supported by the NP6.
B. Anti-replay must be disabled.
C. IPsec traffic must not be inspected by a session helper.
D. No content inspection can be applied to traffic that is going to be encrypted.

Answer: A

NEW QUESTION 98
View the exhibit.

Which users and user groups are allowed access to the network through captive portal?

A. Only individual users–not groups–defined in the captive portal configuration.
B. Groups defined in the captive portal configuration
C. All users
D. Users and groups defined in the firewall policy.

Answer: A

NEW QUESTION 99
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 101
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 102
What FortiGate feature can be used to block a ping sweep scan from an attacker?

A. Web application firewall (WAF)
B. Rate based IPS signatures
C. One-arm sniffer
D. DoS policies

Answer: B

NEW QUESTION 105
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 109
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 111
Which statements are true regarding the use of a PAC file to configure the web proxy settings in an

Internet browser? (Choose two.)

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

Answer: CD

NEW QUESTION 112
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 115
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 116
Which statements are correct regarding URL filtering on a FortiGate unit? (Choose two.)

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

Answer: AC

NEW QUESTION 121
Which statements are correct regarding application control? (Choose two.)

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

Answer: AC

NEW QUESTION 122
Which statements are true regarding traffic shaping that is applied in an application sensor, and associated with a firewall policy? (Choose two.)

A. Shared traffic shaping cannot be used.
B. Only traffic matching the application control signature is shaped.
C. Can limit the bandwidth usage of heavy traffic applications.
D. Per-IP traffic shaping cannot be used.

Answer: BC

NEW QUESTION 127
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 131
Examine the two static routes to the same destination subnet 172.20.168.0/24 as shown below; then
answer the question following it.

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

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

Answer: C

NEW QUESTION 135
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 138
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 142
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 144
Review the static route configuration for IPsec shown in the exhibit; then answer the question below.

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

A. Interface remote is an IPsec interface.
B. A gateway address is not required because the interface is a point-to-point connection.
C. A gateway address is not required because the default route is used.
D. Interface remote is a zone.

Answer: AB

NEW QUESTION 148
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 149
Review the IPsec diagnostics output of the command diagnose vpn tunnel list shown in the exhibit below.

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

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

Answer: AB

NEW QUESTION 152
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 157
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 160
Identify the statement which correctly describes the output of the following command: diagnose ips anomaly list

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

Answer: B

NEW QUESTION 163
Review the IPS sensor filter configuration shown in the exhibit

Based on the information in the exhibit, which statements are correct regarding the filter? (Choose two.)

A. It does not log attacks targeting Linux servers.
B. It matches all traffic to Linux servers.
C. Its action will block traffic matching these signatures.
D. It only takes effect when the sensor is applied to a policy.

Answer: CD

NEW QUESTION 166
Which statement describes what the CLI command diagnose debug authd fsso list is used for

A. Monitors communications between the FSSO collector agent and FortiGate unit.
B. Displays which users are currently logged on using FSSO.
C. Displays a listing of all connected FSSO collector agents.
D. Lists all DC Agents installed on all domain controllers.

Answer: B

NEW QUESTION 168
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 171
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 175
Examine the following output from the diagnose sys session list command:

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

A. Session Time-To-Live (TTL) was configured to 9 seconds.
B. FortiGate is doing NAT of both the source and destination IP addresses on all packets coming fromthe 192.168.1.110 address.
C. The IP address 192.168.1.110 is being translated to 172.17.87.16.
D. The FortiGate is not translating the TCP port numbers of the packets in this session.

Answer: CD

NEW QUESTION 178
How is the FortiGate password recovery process?

A. Interrupt boot sequence, modify the boot registry and reboo
B. After changing the password, resetthe boot registry.
C. Log in through the console port using the "maintainer" account within several seconds of physically power cycling the FortiGate.
D. Hold down the CTRL + Esc (Escape) keys during reboot, then reset the admin password.
E. Interrupt the boot sequence and restore a configuration file for which the password has been modified.

Answer: B

NEW QUESTION 182
When creating FortiGate administrative users, which configuration objects specify the account rights?

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

Answer: C

NEW QUESTION 185
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 190
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 191
Which is an advantage of using SNMP v3 instead of SNMP v1/v2 when querying a FortiGate unit?

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

Answer: C

NEW QUESTION 196
What logging options are supported on a FortiGate unit? (Choose two.)

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

Answer: BC

NEW QUESTION 200
In HA, the option Reserve Management Port for Cluster Member is selected as shown in the exhibit below.

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

A. Interface settings on port7 will not be synchronized with other cluster members.
B. The IP address assigned to this interface must not overlap with the IP address subnet assigned to another interface.
C. When connecting to port7 you always connect to the master device.
D. A gateway address may be configured for port7.

Answer: AD

NEW QUESTION 201
The exhibit shows the Disconnect Cluster Member command in a FortiGate unit that is part of a HA cluster with two HA members.

What is the effect of the Disconnect Cluster Member command as given in the exhibit. (Choose two.)

A. Port3 is configured with an IP address for management access.
B. The firewall rules are purged on the disconnected unit.
C. The HA mode changes to standalone.
D. The system hostname is set to the unit serial number.

Answer: AC

NEW QUESTION 202
In which order are firewall policies processed on a FortiGate unit?

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

Answer: A

NEW QUESTION 205
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 208

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 209
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 210
Which antivirus inspection mode must be used to scan SMTP, FTP, POP3 and SMB protocols?

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

Answer: C

NEW QUESTION 215
The FortiGate port1 is connected to the Internet. The FortiGate port2 is connected to the internal network. Examine the firewall configuration shown in the exhibit; then answer the question below.

Based on the firewall configuration illustrated in the exhibit, which statement is correct?

A. A user that has not authenticated can access the Internet using any protocol that does not trigger an authentication challenge.
B. A user that has not authenticated can access the Internet using any protocol except HTTP, HTTPS, Telnet, and FTP.
C. A user must authenticate using the HTTP, HTTPS, SSH, FTP, or Telnet protocol before they can access all Internet services.
D. DNS Internet access is always allowed, even for users that has not authenticated.

Answer: D

NEW QUESTION 219
Which statement regarding the firewall policy authentication timeout is true?

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

Answer: A

NEW QUESTION 220
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 223
When firewall policy authentication is enabled, only traffic on supported protocols will trigger an authentication challenge.
Select all supported protocols from the following:

A. SMTP
B. SSH
C. HTTP

D. FTP
E. SCP

Answer: CD

NEW QUESTION 227
In an IPSec gateway-to-gateway configuration, two FortiGate units create a VPN tunnel between two separate private networks.
Which of the following configuration steps must be performed on both FortiGate units to support this configuration? (Select all that apply.)

A. Create firewall policies to control traffic between the IP source and destination address.
B. Configure the appropriate user groups on the FortiGate units to allow users access to the IPSec VPN connection.
C. Set the operating mode of the FortiGate unit to IPSec VPN mode.
D. Define the Phase 2 parameters that the FortiGate unit needs to create a VPN tunnel with the remote peer.
E. Define the Phase 1 parameters that the FortiGate unit needs to authenticate the remote peers.

Answer: ADE

NEW QUESTION 231
An end user logs into the full-access SSL VPN portal and selects the Tunnel Mode option by clicking on the "Connect" button. The administrator has enabled split tunneling.

Given that the user authenticates against the SSL VPN policy shown in the image below, which statement below identifies the route that is added to the client's routing table.

A. A route to destination matching the `WIN2K3' address object.
B. A route to the destination matching the `all' address object.
C. A default route.
D. No route is added.

Answer: A

NEW QUESTION 234
Which of the following antivirus and attack definition update options are supported by FortiGate units? (Select all that apply.)

A. Manual update by downloading the signatures from the support site.
B. Pull updates from the FortiGate device
C. Push updates from the FortiGuard Distribution Network.
D. "update-AV/AS" command from the CLI

Answer: ABC

NEW QUESTION 236
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 240
Which of the following items does NOT support the Logging feature?

A. File Filter
B. Application control
C. Session timeouts
D. Administrator activities
E. Web URL filtering

Answer: C

NEW QUESTION 244
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 247
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 251
A firewall policy has been configured for the internal email server to receive email from external parties through SMTP. Exhibits A and B show the antivirus and email filter profiles applied to this policy.
Exhibit A:

Exhibit B:

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

A. The FortiGate unit will remove the infected file and deliver the email with a replacement message to alert the recipient that the original attachment was infected.
B. The FortiGate unit will reject the infected email and the sender will receive a failed delivery message.
C. The FortiGate unit will remove the infected file and add a replacement messag
D. Both sender and recipient are notified that the infected file has been removed.
E. The FortiGate unit will reject the infected email and notify the sender.

Answer: A

NEW QUESTION 253
Caching improves performance by reducing FortiGate unit requests to the FortiGuard server. Which of the following statements are correct regarding the caching of FortiGuard responses? (Select all that apply.)

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

Answer: BCD

NEW QUESTION 256
In which order are firewall policies processed on the FortiGate unit?

A. They are processed from the top down according to their sequence number.
B. They are processed based on the policy ID number shown in the left hand column of the policy window.
C. They are processed on best match.
D. They are processed based on a priority value assigned through the priority column in the policy window.

Answer: A

NEW QUESTION 257
Which of the following pieces of information can be included in the Destination Address field of a firewall policy? (Select all that apply.)

A. An IP address pool.
B. A virtual IP address.
C. An actual IP address or an IP address group.
D. An FQDN or Geographic value(s).

Answer: BCD

NEW QUESTION 258
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 262
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 264
A FortiAnalyzer device could use which security method to secure the transfer of log data from FortiGate devices?

A. SSL
B. IPSec
C. direct serial connection
D. S/MIME

Answer: B

NEW QUESTION 266
Which of the following network protocols are supported for administrative access to a FortiGate unit?

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 267
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 268
When backing up the configuration file on a FortiGate unit, the contents can be encrypted by enabling the encrypt option and supplying a password. If the password is forgotten, the configuration file can still be restored using which of the following methods?

A. Selecting the recover password option during the restore process.
B. Having the password emailed to the administrative user by selecting the Forgot Password option.
C. Sending the configuration file to Fortinet Support for decryption.
D. If the password is forgotten, there is no way to use the file.

Answer: D

NEW QUESTION 271
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 272
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 274
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 275
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 279
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 280
By default, the Intrusion Protection System (IPS) on a FortiGate unit is set to perform which action?

A. Block all network attacks.
B. Block the most common network attacks.
C. Allows all traffic
D. Allow and log all traffic

Answer: C

NEW QUESTION 285
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 286
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 291
Which of the following statements is correct regarding URL Filtering on the FortiGate unit?

A. The FortiGate unit can filter URLs based on patterns using text and regular expressions.
B. The available actions for URL Filtering are Allow and Block.
C. Multiple URL Filter lists can be added to a single Web filter profile.
D. A FortiGuard Web Filtering Override match will override a block action in the URL filter list.

Answer: A

NEW QUESTION 292
SSL content inspection is enabled on the FortiGate unit. Which of the following steps is required to prevent a user from being presented with a web browser warning when accessing an SSL- encrypted website?

A. The root certificate of the FortiGate SSL proxy must be imported into the local certificate store on the user's workstation.
B. Disable the strict server certificate check in the web browser under Internet Options.
C. Enable transparent proxy mode on the FortiGate unit.
D. Enable NTLM authentication on the FortiGate uni
E. NTLM authentication suppresses the certificate warning messages in the web browser.

Answer: A

NEW QUESTION 293
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 298
UTM features can be applied to which of the following items?

A. Firewall policies
B. User groups
C. Policy routes
D. Address groups

Answer: A

NEW QUESTION 302
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 305
If no firewall policy is specified between two FortiGate interfaces and zones are not used, which of the following statements describes the action taken on traffic flowing between these interfaces?

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 310
Which of the following products can be installed on a computer running Windows XP to provide personal firewall protection, antivirus protection, web and mail filtering, spam filtering, and VPN functionality?

A. FortiGate
B. FortiAnalyzer
C. FortiClient
D. FortiManager
E. FortiReporter

Answer: C

NEW QUESTION 311
File blocking rules are applied before which of the following?

A. Firewall policy processing
B. Virus scanning
C. Web URL filtering
D. White/Black list filtering

Answer: B

NEW QUESTION 313
FortiGate units are preconfigured with four default protection profiles. These protection profiles are used to control the type of content inspection to be performed.
What action must be taken for one of these profiles to become active?

A. The protection profile must be assigned to a firewall policy.
B. The "Use Protection Profile" option must be selected in the Web Config tool under the sections for AntiVirus, IPS, WebFilter, and AntiSpam.
C. The protection profile must be set as the Active Protection Profile.
D. All of the above.

Answer: A

NEW QUESTION 317
Which of the following statements is correct regarding a FortiGate unit operating in NAT/Route mode?

A. The FortiGate unit requires only a single IP address for receiving updates and configuring from a management computer.
B. The FortiGate unit must use public IP addresses on both the internal and external networks.
C. The FortiGate unit commonly uses private IP addresses on the internal network but hides them using network address translation.
D. The FortiGate unit uses only DHCP-assigned IP addresses on the internal network.

Answer: C

NEW QUESTION 319
The Idle Timeout setting on a FortiGate unit applies to which of the following?

A. Web browsing
B. FTP connections
C. User authentication
D. Administrator access
E. Web filtering overrides

Answer: D

NEW QUESTION 324
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 325
Which of the following methods can be used to access the CLI? (Select all that apply.)

A. By using a direct connection to a serial console.
B. By using the CLI console window in Web Config.
C. By using an SSH connection.
D. By using a Telnet connection.

Answer: ABCD

NEW QUESTION 328
The command structure of the FortiGate CLI consists of commands, objects, branches, tables, and parameters.
Which of the following items describes user?

A. A command
B. An object
C. A table
D. A parameter.

Answer: B

NEW QUESTION 332
The command structure of the CLI on a FortiGate unit consists of commands, objects, branches, tables and parameters. Which of the following items describes port1?

A. A command
B. An object
C. A table
D. A parameter

Answer: C

NEW QUESTION 333
Each UTM feature has configurable UTM objects such as sensors, profiles or lists that define how the feature will function.
An administrator must assign a set of UTM features to a group of users. Which of the following is the correct method for doing this?

A. Enable a set of unique UTM features under "Edit User Group".
B. The administrator must enable the UTM features in an identify-based policy applicable to the user group.
C. When defining the UTM objects, the administrator must list the user groups which will use the UTM object.
D. The administrator must apply the UTM features directly to a user object.

Answer: B

NEW QUESTION 336
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 341
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 346
Data Leak Prevention archiving gives the ability to store files and message data onto 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 349
Which of the following statements are correct regarding Application Control?

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

Answer: AC

NEW QUESTION 354
CORRECT TEXT
In addition to AntiVirus services, the FortiGuard Subscription Services provide IPS, Web Filtering, and _____ services.

Answer:

Explanation: antispam

NEW QUESTION 358
Shown below is a section of output from the debug command diag ip arp list.

In the output provided, which of the following best describes the IP address 172.20.187.150?

A. It is the primary IP address of the port1 interface.
B. It is one of the secondary IP addresses of the port1 interface.
C. It is the IP address of another network device located in the same LAN segment as the FortiGate unit's port1 interface.

Answer: C

NEW QUESTION 360
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 363
What advantages are there in using a hub-and-spoke IPSec VPN configuration instead of a fully-meshed set of IPSec tunnels? (Select all that apply.)

A. Using a hub and spoke topology is required to achieve full redundancy.
B. Using a hub and spoke topology simplifies configuration because fewer tunnels are required.
C. Using a hub and spoke topology provides stronger encryption.
D. The routing at a spoke is simpler, compared to a meshed node.

Answer: BD

NEW QUESTION 364
The eicar test virus is put into a zip archive, which is given the password of "Fortinet" in order to open the archive. Review the configuration in the exhibits shown below; then answer the question that follows.
Exhibit A - Antivirus Profile:

Exhibit B - Non-default UTM Proxy Options Profile:

Exhibit C - DLP Profile:

Which of one the following profiles could be enabled in order to prevent the file from passing through the FortiGate device over HTTP on the standard port for that protocol?

A. Only Exhibit A
B. Only Exhibit B
C. Only Exhibit C with default UTM Proxy settings.
D. All of the Exhibits (A, B and C)
E. Only Exhibit C with non-default UTM Proxy settings (Exhibit B).

Answer: C

NEW QUESTION 366
Review the CLI configuration below for an IPS sensor and identify the correct statements regarding this configuration from the choices below. (Select all that apply.)

A. The sensor will log all server attacks for all operating systems.
B. The sensor will include a PCAP file with a trace of the matching packets in the log message of any matched signature.
C. The sensor will match all traffic from the address object `LINUX_SERVER'.
D. The sensor will reset all connections that match these signatures.
E. The sensor only filters which IPS signatures to apply to the selected firewall policy.

Answer: BE

NEW QUESTION 369
An administrator is examining the attack logs and notices the following entry:

Based on the information displayed in this entry, which of the following statements are correct? (Select all that apply.)

A. This is an HTTP server attack.
B. The attack was detected and blocked by the FortiGate unit.
C. The attack was against a FortiGate unit at the 192.168.1.100 IP address.
D. The attack was detected and passed by the FortiGate unit.

Answer: CD

NEW QUESTION 374
An administrator wishes to generate a report showing Top Traffic by service type. They notice
that web traffic overwhelms the pie chart and want to exclude the web traffic from the report. Which of the following statements best describes how to do this?

A. In the Service field of the Data Filter, type 80/tcp and select the NOT checkbox.
B. Add the following entry to the Generic Field section of the Data Filter: service="!web".
C. When editing the chart, uncheck wlog to indicate that Web Filtering data is being excluded when generating the chart.
D. When editing the chart, enter 'http' in the Exclude Service field.

Answer: A

NEW QUESTION 379
Which of the following methods does the FortiGate unit use to determine the availability of a web
cache using Web Cache Communication Protocol (WCCP)?

A. The FortiGate unit receives periodic "Here I am" messages from the web cache.
B. The FortiGate unit polls all globally-defined web cache servers at a regular intervals.
C. The FortiGate using uses the health check monitor to verify the availability of a web cache server.
D. The web cache sends an "I see you" message which is captured by the FortiGate unit.

Answer: C

NEW QUESTION 384
A FortiGate unit is configured with multiple VDOMs. An administrative account on the device has
been assigned a Scope value of VDOM:root.
Which of the following items would an administrator logging in using this account NOT be able to configure?

A. Firewall addresses
B. DHCP servers
C. FortiGuard Distribution Network configuration
D. PPTP VPN configuration

Answer: C

NEW QUESTION 389

WAN optimization is configured in Active/Passive mode. When will the remote peer accept an attempt to initiate a tunnel?

A. The attempt will be accepted when the request comes from a known peer and there is a matching WAN optimization passive rule.
B. The attempt will be accepted when there is a matching WAN optimization passive rule.
C. The attempt will be accepted when the request comes from a known peer.
D. The attempt will be accepted when a user on the remote peer accepts the connection request.

Answer: A

NEW QUESTION 394
An administrator logs into a FortiGate unit using an account which has been assigned a super_admin profile. Which of the following operations can this administrator perform?

A. They can delete logged-in users who are also assigned the super_admin access profile.
B. They can make changes to the super_admin profile.
C. They can delete the admin account if the default admin user is not logged in.
D. They can view all the system configuration settings but can not make changes.
E. They can access configuration options for only the VDOMs to which they have been assigned.

Answer: C

NEW QUESTION 395
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 400
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 404
A FortiGate administrator configures a Virtual Domain (VDOM) for a new customer. After creating the VDOM, the administrator is unable to reassign the dmz interface to the new VDOM as the option is greyed out in Web Config in the management VDOM.
What would be a possible cause for this problem?

A. The dmz interface is referenced in the configuration of another VDOM.
B. The administrator does not have the proper permissions to reassign the dmz interface.
C. Non-management VDOMs can not reference physical interfaces.
D. The dmz interface is in PPPoE or DHCP mode.
E. Reassigning an interface to a different VDOM can only be done through the CLI.

Answer: A

NEW QUESTION 408
If Open Shortest Path First (OSPF) has already been configured on a FortiGate unit, which of the following statements is correct if the routes learned through OSPF need to be announced by Border Gateway Protocol (BGP)?

A. The FortiGate unit will automatically announce all routes learned through OSPF to its BGP peers if the FortiGate unit is configured as an OSPF Autonomous System Boundary Router (ASBR).
B. The FortiGate unit will automatically announce all routes learned through OSPF to its BGP peers if the FortiGate unit is configured as an OSPF Area Border Router (ABR).
C. At a minimum, the network administrator needs to enable Redistribute OSPF in the BGP settings.
D. The BGP local AS number must be the same as the OSPF area number of the routes learned that need to be redistributed into BGP.
E. By design, BGP cannot redistribute routes learned through OSPF.

Answer: C

NEW QUESTION 410
When the SSL proxy inspects the server certificate for Web Filtering only in SSL Handshake mode, which certificate field is being used to determine the site rating?

A. Common Name
B. Organization

C. Organizational Unit
D. Serial Number
E. Validity

Answer: A

NEW QUESTION 413
Which of the following Session TTL values will take precedence?

A. Session TTL specified at the system level for that port number
B. Session TTL specified in the matching firewall policy
C. Session TTL dictated by the application control list associated with the matching firewall policy
D. The default session TTL specified at the system level

Answer: C

NEW QUESTION 414
In the Tunnel Mode widget of the web portal, the administrator has configured an IP Pool and
enabled split tunneling.
Which of the following statements is true about the IP address used by the SSL VPN client?

A. The IP pool specified in the SSL-VPN Tunnel Mode Widget Options will override the IP address range defined in the SSL-VPN Settings.
B. Because split tunneling is enabled, no IP address needs to be assigned for the SSL VPN tunnel to be established.
C. The IP address range specified in SSL-VPN Settings will override the IP address range in the SSL- VPN Tunnel Mode Widget Options.

Answer: A

NEW QUESTION 415
The Host Check feature can be enabled on the FortiGate unit for SSL VPN connections. When this
feature is enabled, the FortiGate unit probes the remote host computer to verify that it is "safe" before access is granted.
Which of the following items is NOT an option as part of the Host Check feature?

A. FortiClient Antivirus software
B. Microsoft Windows Firewall software
C. FortiClient Firewall software
D. Third-party Antivirus software

Answer: B

NEW QUESTION 418
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 422
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 425
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 430
An administrator is examining the attack logs and notices the following entry:

Based solely upon this log message, which of the following statements is correct?

A. This attack was blocked by the HTTP protocol decoder.
B. This attack was caught by the DoS sensor "protect-servers".
C. This attack was launched against the FortiGate unit itself rather than a host behind the FortiGate unit.
D. The number of concurrent connections to destination IP address 64.64.64.64 has exceeded the configured threshold.

Answer: B

NEW QUESTION 435
An administrator is configuring a DLP rule for FTP traffic. When adding the rule to a DLP sensor,

the administrator notes that the Ban Sender action is not available (greyed-out), as shown in the exhibit.
Which of the following is the best explanation for the Ban Sender action NOT being available?

A. The Ban Sender action is never available for FTP traffic.
B. The Ban Sender action needs to be enabled globally for FTP traffic on the FortiGate unit before configuring the sensor.
C. Firewall policy authentication is required before the Ban Sender action becomes available.
D. The Ban Sender action is only available for known domain
E. No domains have yet been added to the domain list.

Answer: A

NEW QUESTION 440
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 443
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 448
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 449
A portion of the device listing for a FortiAnalyzer unit is displayed in the exhibit.

Which of the following statements best describes the reason why the FortiGate 60B unit is unable to archive data to the FortiAnalyzer unit?

A. The FortiGate unit is considered an unregistered device.
B. The FortiGate unit has been blocked from sending archive data to the FortiAnalyzer device by the administrator.
C. The FortiGate unit has insufficient privilege
D. The administrator should edit the device entry in the FortiAnalyzer and modify the privileges.
E. The FortiGate unit is being treated as a syslog device and is only permitted to send log data.

Answer: A

NEW QUESTION 453
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 456
A FortiClient fails to establish a VPN tunnel with a FortiGate unit. The following information is displayed in the FortiGate unit logs:

Which of the following statements is a possible cause for the failure to establish the VPN tunnel?

A. An IPSec DHCP server is not enabled on the external interface of the FortiGate unit.
B. There is no IPSec firewall policy configured for the policy-based VPN.
C. There is a mismatch between the FortiGate unit and the FortiClient IP addresses in the phase 2 settings.
D. The phase 1 configuration on the FortiGate unit uses Aggressive mode while FortiClient uses Main mode.

Answer: A

NEW QUESTION 460
The diag sys session list command is executed in the CLI. The output of this command is shown in the exhibit.

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

A. This is a UDP session.
B. Traffic shaping is being applied to this session.
C. This is an ICMP session.
D. This traffic has been authenticated.

E. This session matches a firewall policy with ID 5.

Answer: B

NEW QUESTION 463
What protocol cannot be used with the active authentication type?

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

Answer: D

NEW QUESTION 467
Which of the following settings can be configured per VDOM? (Choose three.)

A. Operating mode (NAT/route or transparent)
B. Static routes
C. Hostname
D. System time
E. Firewall Policies

Answer: ABE

NEW QUESTION 472
What are examples of correct syntax for the session table diagnostics command? (Choose two.)

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

Answer: AC

NEW QUESTION 477
Which statement best describes what SSL VPN Client Integrity Check does?

A. Blocks SSL VPN connection attempts from users that has been blacklisted.
B. Detects the Windows client security applications running in the SSL VPN client's PCs.
C. Validates the SSL VPN user credential.
D. Verifies which SSL VPN portal must be presented to each SSL VPN user.
E. Verifies that the latest SSL VPN client is installed in the client's PC.

Answer: B

NEW QUESTION 478
Which traffic can match a firewall policy's "Services" setting? (Choose three.)

A. HTTP
B. SSL
C. DNS
D. RSS
E. HTTPS

Answer: ACE

NEW QUESTION 481
Which of the following statements are true about the SSL Proxy certificate that must be used for SSL Content Inspection? (Choose two.)

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

Answer: CD

NEW QUESTION 486
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 490
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 495
Which of the following statements are correct concerning IKE mode config? (Choose two)

A. It can dynamically assign IP addresses to IPsec VPN clients.
B. It can dynamically assign DNS settings to IPsec VPN clients.
C. It uses the ESP protocol.
D. It can be enabled in the phase 2 configuration.

Answer: AB

NEW QUESTION 496
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 500
In a FSSO agent mode solution, how does the FSSO collector agent learn each IP address?

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

Answer: D

NEW QUESTION 504
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 508
Which of the following statements best describes what the Document Fingerprinting feature is for?

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

Answer: A

NEW QUESTION 509
Which of the following statements is correct concerning multiple vdoms configured in a FortiGate device?

A. FortiGate devices,from the FGT/FWF 60D and above, all support VDOMS.
B. All FortiGate devices scale to 250 VDOMS.
C. Each VDOM requires its own FortiGuard license.

D. FortiGate devices support more NAT/route VDOMs than Transparent Mode VDOMs.

Answer: A

NEW QUESTION 511
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 516
A FortiGate devices is configured with four VDOMs: 'root' and 'vdom1' are in NAT/route mode;
'vdom2' and 'vdom2' are in transparent mode. The management VDOM is 'root'. Which of the following statements are true? (Choose two.)

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

Answer: AB

NEW QUESTION 520
In FortiOS session table output, what are the two possible `proto_state' values for a UDP session?
(Choose two.)

A. 00
B. 11
C. 01
D. 05

Answer: AC

NEW QUESTION 524
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 525
What types of troubleshooting can you do when uploading firmware? (Choose two.)

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

Answer: AD

NEW QUESTION 528
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 530
Which of the following statements are correct concerning layer 2 broadcast domains in transparent mode VDOMs?(Choose two)

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

Answer: BC

NEW QUESTION 534
If you enable the option "Generate Logs when Session Starts", what effect does this have on the number of traffic log messages generated for each session?

A. No traffic log message is generated.
B. One traffic log message is generated.
C. Two traffic log messages are generated.
D. A log message is only generated if there is a security event.

Answer: C

NEW QUESTION 538
Which authentication methods does FortiGate support for firewall authentication? (Choose two.)

A. Remote Authentication Dial in User Service (RADIUS)
B. Lightweight Directory Access Protocol (LDAP)
C. Local Password Authentication
D. POP3
E. Remote Password Authentication

Answer: AC

NEW QUESTION 540
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 545
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 548
Which statement best describes what SSL.root is?

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

Answer: B

NEW QUESTION 549
Which of the following statements are characteristics of a FSSO solution using advanced access mode? (Choose three.)

A. Protection profiles can be applied to both individual users and user groups
B. Nested or inherited groups are supported
C. Usernames follow the LDAP convention: CN=User, OU=Name, DC=Domain
D. Usernames follow the Windows convention: Domain\username
E. Protection profiles can be applied to user groups only.

Answer: BCE

NEW QUESTION 553
Which user group types does FortiGate support for firewall authentication? (Choose three.)

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

Answer: ABE

NEW QUESTION 556
Different settings are circled and numbered. Select the number identifying the setting which will provide additional information about YouTube access, such as the name of the video watched.

A. 1
B. 2
C. 3
D. 4
E. 5

Answer: D

NEW QUESTION 560
Of the following information, what can be recorded by a Data Leak Prevention sensor configured to do a summary archiving? (Choose three.)

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

Answer: BCE

NEW QUESTION 565
Which are the three different types of Conserve Mode that can occur on a FortiGate device? (Choose three.)

A. Proxy
B. Operating system
C. Kernel
D. System
E. Device

Answer: ACD

NEW QUESTION 568
Which of the following statements are correct about NTLM authentication? (Choose three)

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

Answer: ABC

NEW QUESTION 569
Which UTM feature sends a UDP query to FortiGuard servers each time FortiGate scans a packet (unless the response is locally cached)?

A. Antivirus
B. VPN
C. IPS
D. Web Filtering

Answer: D

NEW QUESTION 570
Which of the following combinations of two FortiGate device configurations (side A and side B), can be used to successfully establish an IPsec VPN between them? (choose two)

A. Side A:main mode, remote gateway as static IP address, policy based VP
B. Side B: aggressive mode, remote Gateway as static IP address policy-based VPN.
C. Side A:main mode, remote gateway as static IP address, policy based VP
D. Side B: main mode, remote gateway as static IP address, route-based VPN
E. Side A:main mode, remote gateway as static IP address, policy based VP
F. Side B: main mode, remote gateway as dialup, route-based VPN.
G. Side A: main mode, remote gateway as dialup policy based VPN, Side B: main mode, remote gateway as dialup, policy based VPN.

Answer: BC

NEW QUESTION 574
A FortiGate devices has two VDOMs in NAT/route mode. Which of the following solutions can be implemented by a network administrator to route traffic between the two VDOMs. (Choose two.)

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

Answer: BC

NEW QUESTION 579
Which of the following are considered log types? (Choose three.)

A. Forward log
B. Traffic log
C. Syslog
D. Event log
E. Security log

Answer: BDE

NEW QUESTION 583
The exhibit shoes three static routes.
Which routes will be used to route the packets to the destination IP address 172.20.168.1?

A. The route with the ID number 2 and 3.
B. Only the route with the ID number 3.
C. Only the route with the ID number 2.
D. Only the route with the ID number 1.

Answer: D

NEW QUESTION 588
Which of the following authentication methods are supported in an IPsec phase 1? (Choose two.)

A. Asymmetric Keys
B. CA root digital certificates
C. RSA signature
D. Pre-shared keys

Answer: CD

NEW QUESTION 589
Which of the following statements best describe what a FortiGate does when packets match a black hole route?

A. Packets are dropped.
B. Packets are routed based on the information in the policy-based routing table.
C. An ICMP error message is sent back to the originator.
D. Packet are routed back to the originator.

Answer: A

NEW QUESTION 592
What actions are possible with Application Control? (Choose three.)

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

Answer: BCD

NEW QUESTION 595
What are required to be the same for two FortiGate units to form an HA cluster? (Choose two)

A. Firmware.
B. Model.
C. Hostname.
D. System time zone.

Answer: AB

NEW QUESTION 600
Which of the following FSSO agents are required for a DC agent mode solution? (Choose two.)

A. FSSO agent
B. DC agent
C. Collector agent
D. Radius server

Answer: BC

NEW QUESTION 601
Which statement best describes what the FortiGate hardware acceleration processors main task is?

A. Offload traffic processing tasks from the main CPU.
B. Offload management tasks from the main CPU.
C. Compress and optimize the network traffic.
D. Increase maximum bandwidth available in a FortiGate interface.

Answer: A

NEW QUESTION 603
Which best describes the authentication timeout?

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

Answer: C

NEW QUESTION 604
Which is NOT true about source matching with firewall policies?

A. A source address object must be selected in the firewall policy.
B. A source user/group may be selected in the firewall policy.
C. A source device may be defined in the firewall policy.
D. A source interface must be selected in the firewall policy.
E. A source user/group and device must be specified in the firewall policy.

Answer: E

NEW QUESTION 607
A FortiGate is configured with the 1.1.1.1/24 address on the wan2 interface and HTTPS Administrative Access, using the default tcp port, is enabled for that interface. Given the SSL VPN settings in the exhibit.

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

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

Answer: BD

NEW QUESTION 612
Which of the following protocols are defined in the IPsec Standard? (Choose two)

A. AH
B. GRE
C. SSL/TLS
D. ESP

Answer: AD

NEW QUESTION 615
Which of the following statements 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 618
Which of the following statements is true regarding the use of a PAC file to configure the web proxy settings in an Internet browser? (Choose two.)

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

Answer: BC

NEW QUESTION 620
Which of the following statements is true regarding a FortiGate device operating in transparent mode? (Choose three.)

A. It acts as a layer 2 bridge
B. It acts as a layer 3 router
C. It forwards frames using the destination MAC address.
D. It forwards packets using the destination IP address.
E. It can perform content inspection (antivirus, web filtering, etc)

Answer: ACE

NEW QUESTION 624
What is the maximum number of different virus databases a FortiGate can have?

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

Answer: B

NEW QUESTION 629
Which are valid replies from a RADIUS server to an ACCESS-REQUEST packet from a FortiGate? (Choose two.)

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

Answer: AD

NEW QUESTION 633
Which of the following authentication methods can be used for SSL VPN authentication? (Choose three.)

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

Answer: ABC

NEW QUESTION 638
What log type would indicate whether a VPN is going up or down?

A. Event log
B. Security log
C. Forward log
D. Syslog

Answer: A

NEW QUESTION 639
Where are most of the security events logged?

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

Answer: C

NEW QUESTION 642
Which commands are appropriate for investigating high CPU? (Choose two.)

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

Answer: AD

NEW QUESTION 645
You are creating a custom signature. Which has incorrect syntax?

A. F-SBID(--attack_id 1842,--name "Ping.Death";--protocol icmp; --data_size>32000;)
B. F-SBID(--name "Block.SMTP.VRFY.CMD";--pattern "vrfy";-- service SMTP; --no_case;-- context header;)
C. F-SBID(--name "Ping.Death";--protocol icmp;--data_size>32000;)
D. F-SBID(--name "Block".HTTP.POST"; --protocol tcp;-- service HTTP;-- flow from_client; -- pattern "POST"; -- context uri;--within 5,context;)

Answer: A

NEW QUESTION 648
What is not true of configuring disclaimers on the FortiGate?

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

Answer: C

NEW QUESTION 653
Which of the following are benefits of using web caching? (Choose three.)

A. Decrease bandwidth utilization
B. Reduce server load
C. Reduce FortiGate CPU usage
D. Reduce FortiGate memory usage
E. Decrease traffic delay

Answer: ABE

NEW QUESTION 658
When an administrator attempts to manage FortiGate from an IP address that is not a trusted host,
what happens?

A. FortiGate will still subject that person's traffic to firewall policies; it will not bypass them.

B. FortiGate will drop the packets and not respond.
C. FortiGate responds with a block message, indicating that it will not allow that person to log in.
D. FortiGate responds only if the administrator uses a secure protoco
E. Otherwise, it does not respond

Answer: B

NEW QUESTION 660
When configuring LDAP on the FortiGate as a remote database for users, what is not a part of the configuration?

A. The name of the attribute that identifies each user (Common Name Identifier).
B. The user account or group element names (user DN).
C. The server secret to allow for remote queries (Primary server secret).
D. The credentials for an LDAP administrator (password).

Answer: C

NEW QUESTION 662
Which of the following statements best describes what a Public Certificate Authority (CA) is?

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

Answer: D

NEW QUESTION 664
Which of the following web filtering modes can inspect the full URL? (Choose two.)

A. Proxy based
B. DNS based
C. Policy based
D. Flow based

Answer: AD

NEW QUESTION 666
What determines whether a log message is generated or not?

A. Firewall policy setting
B. Log Settings in the GUI
C. 'config log' command in the CLI
D. Syslog
E. Webtrends

Answer: A

NEW QUESTION 667
Which of the following actions can be used with the FortiGuard quota feature? (Choose three.)

A. Allow
B. Block
C. Monitor
D. Warning
E. Authenticate

Answer: CDE

NEW QUESTION 671
Which is not a FortiGate feature?

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

Answer: A

NEW QUESTION 673
What attributes are always included in a log header? (Choose three.)

A. policyid
B. level

C. user
D. time
E. subtype
F. duration

Answer: BDE

NEW QUESTION 677
Which best describes the mechanism of a TCP SYN flood?

A. The attackers keeps open many connections with slow data transmission so that other clients cannot start new connections.
B. The attackers sends a packets designed to sync with the FortiGate
C. The attacker sends a specially crafted malformed packet, intended to crash the target by exploiting its parser.
D. The attacker starts many connections, but never acknowledges to fully form them.

Answer: D

NEW QUESTION 679
What action does an IPsec Gateway take with the user traffic routed to an IPsec VPN when it does not match any phase 2 quick mode selector?

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

Answer: A

NEW QUESTION 683
Which statements about virtual domains (VDOMs) are true? (Choose two.)

A. Transparent mode and NAT/Route mode VDOMs cannot be combined on the same FortiGate.
B. Each VDOM can be configured with different system hostnames.
C. Different VLAN sub-interfaces of the same physical interface can be assigned to different VDOMs.
D. Each VDOM has its own routing table.

Answer: CD

NEW QUESTION 684
.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questons and Answers in PDF Format

NSE4-5.4 Practice Exam Features:

* NSE4-5.4 Questions and Answers Updated Frequently

* NSE4-5.4 Practice Questions Verified by Expert Senior Certified Staff

* NSE4-5.4 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* NSE4-5.4 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year