

NSE4 Dumps

Fortinet Network Security Expert 4 Written Exam (400)

<https://www.certleader.com/NSE4-dumps.html>



NEW QUESTION 1

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

- A. Filters based on file extension
- B. Filters based on fingerprints
- C. Filters based on file content
- D. File types are hard coded in the FortiOS

Answer: BC

NEW QUESTION 2

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

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

Answer: B

NEW QUESTION 3

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 4

Examine the exhibit; then answer the question below.



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

S 172.20.0.0/16 [10/0] via 172.21.1.2, port2

C 172.21.0.0/16 is directly connected, port2

C 172.11.11.0/24 is directly connected, port1

Afterwards, the following static route was added:

```
config router static edit 6
```

```
set dst 172.20.1.0 255.255.255.0
```

```
set priority 0
```

```
set device port1
```

```
set gateway 172.11.12.1 next
```

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

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

Answer: B

NEW QUESTION 5

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 6

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

- A. IPS cannot scan that traffic for SMTP anomalies because of the non-standard port number
- B. You must reconfigured the server to run on port 2.

- C. To apply IPS to traffic to that server, you must configured FortiGate SMTP proxy to listen on port 2525
D. IPS will apply all SMTP signatures, regardless of whether they apply to clients or servers.
E. Protocol decoders automatically detect SMTP and scan for matches with appropriate IPS signature.

Answer: B

NEW QUESTION 7

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

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

Answer: D

NEW QUESTION 8

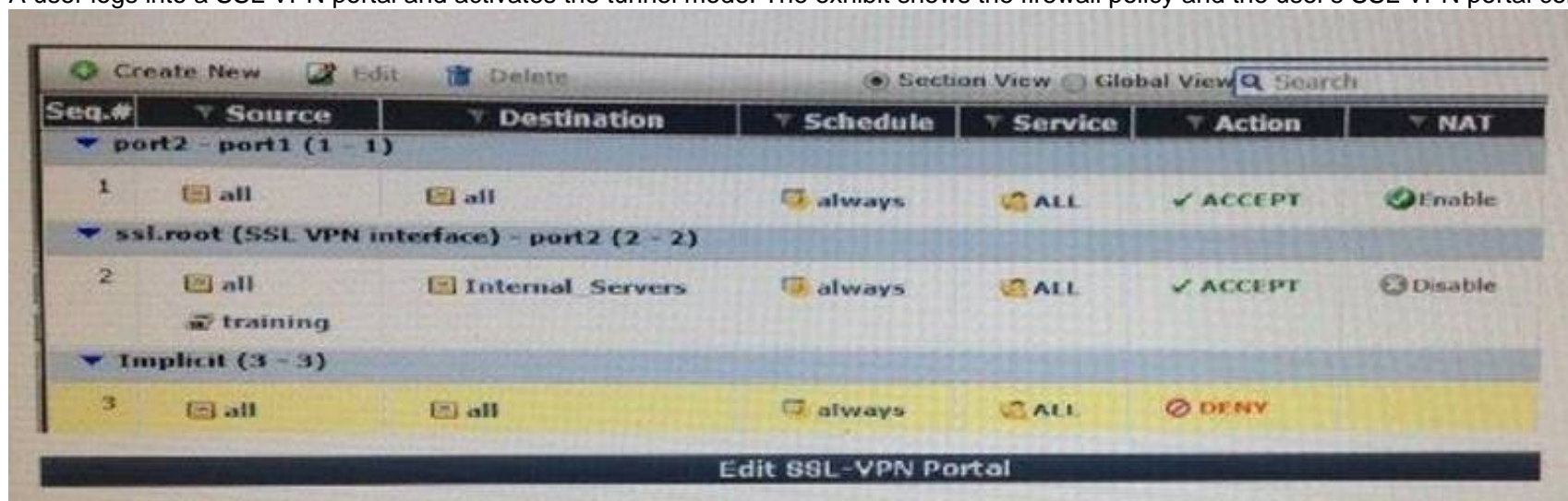
FSSO provides a single sign on solution to authenticate users transparently to a FortiGate unit using credentials stored in Windows active directory. Which of the following statements are correct regarding FSSO in a Windows domain environment when DC-agent mode is used? (Choose two.)

- A. An FSSO collector agent must be installed on every domain controller.
B. An FSSO domain controller agent must be installed on every domain controller.
C. The FSSO domain controller agent will regularly update user logon information on the FortiGate unit.
D. The FSSO collector agent will receive user logon information from the domain controller agent and will send it to the FortiGate unit.

Answer: BD

NEW QUESTION 9

A user logs into a SSL VPN portal and activates the tunnel mode. The exhibit shows the firewall policy and the user's SSL VPN portal configuration:



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 a destination subnet matching the Internal_Servers address object.
B. A route to the destination subnet configured in the tunnel mode widget.
C. A default route.
D. A route to the destination subnet configured in the SSL VPN global settings.

Answer: A

NEW QUESTION 10

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

Listen on Interface(s)	wan2
<i>This is generally your external interface (i.e. wan1)</i>	
Listen on Port	443

URL Path	Virtual Host	Max Concurrent U
Training		0
students		0

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

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

Answer: BD

NEW QUESTION 10

Which statements are correct regarding virtual domains (VDOMs)? (Choose two)

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

Answer: BC

NEW QUESTION 11

With FSSO DC-agent mode, a domain user could authenticate either against the domain controller running the collector agent and domain controller agent, or a domain controller running only the domain controller agent.

If you attempt to authenticate with a domain controller running only the domain controller agent, which statements are correct? (Choose two.)

- A. The login event is sent to a collector agent.
- B. The FortiGate receives the user information directly from the receiving domain controller agent of the secondary domain controller.
- C. The domain collector agent may perform a DNS lookup for the authenticated client's IP address.
- D. The user cannot be authenticated with the FortiGate in this manner because each domain controller agent requires a dedicated collector agent.

Answer: AC

NEW QUESTION 14

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 15

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 19

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 23

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

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

Answer: A

NEW QUESTION 26

Examine the output below from the diagnose sys top command:


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

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

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

Answer: AD

NEW QUESTION 30

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

- A. Two-factor authentication can be enabled on a per user basis.
- B. Local users are for administration accounts only and cannot be used to authenticate network users.
- C. Administrators can create the user accounts in a remote server and store the user passwords locally in the FortiGate.
- D. Both the usernames and passwords can be stored locally on the FortiGate.

Answer: AD

NEW QUESTION 32

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 34

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 37

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 40

Which statement is correct concerning an IPsec VPN with the remote gateway setting configured as 'Dynamic DNS'?

- A. The FortiGate will accept IPsec VPN connection from any IP address.
- B. The FQDN resolution of the local FortiGate IP address where the VPN is terminated must be provided by a dynamic DNS provider.
- C. The FortiGate will Accept IPsec VPN connections only from IP addresses included on a dynamic DNS access list.
- D. The remote gateway IP address can change dynamically.

Answer: D

NEW QUESTION 44

Which of the following statements describes the objectives of the gratuitous ARP packets sent by an HA cluster?

- A. To synchronize the ARP tables in all the FortiGate Units that are part of the HA cluster.
- B. To notify the network switches that a new HA master unit has been elected.
- C. To notify the master unit that the slave devices are still up and alive.
- D. To notify the master unit about the physical MAC addresses of the slave units.

Answer: B

NEW QUESTION 48

How do application control signatures update on a FortiGate device?

- A. Through FortiGuard updates.
- B. Upgrade the FortiOS firmware to a newer release.
- C. By running the Application Control auto-learning feature.
- D. Signatures are hard coded to the device and cannot be updated.

Answer: A

NEW QUESTION 49

In FortiOS session table output, what is the correct 'proto_state' number for an established, non-proxied TCP connection?

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

Answer: C

NEW QUESTION 51

What is the FortiGate password recovery process?

- A. Interrupt boot sequence, modify the boot registry and reboot
- B. After changing the password, reset the 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 56

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

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

Answer: C

NEW QUESTION 60

Which methods can FortiGate use to send a One Time Password (OTP) to Two-Factor Authentication users? (Choose three.)

- A. Hardware FortiToken
- B. Web Portal
- C. Email
- D. USB Token
- E. Software FortiToken (FortiToken mobile)

Answer: ACE

NEW QUESTION 61

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

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

Answer: B

NEW QUESTION 62

Which statement is not correct regarding SSL VPN Tunnel mode?

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

Answer: C

NEW QUESTION 66

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 70

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 75

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 78

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

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

Answer: ABE

NEW QUESTION 81

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

- A. SMTP
- B. SSH
- C. HTTP
- D. FTP
- E. SCP

Answer: CD

NEW QUESTION 84

Which statements are correct properties of a partial mesh VPN deployment. (Choose two.)

- A. VPN tunnels interconnect between every single location.
- B. VPN tunnels are not configured between every single location.
- C. Some location may be reachable via a hub location.
- D. There are no hub locations in a partial mesh.

Answer: BC

NEW QUESTION 87

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

- A. Allow

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

Answer: ABD

NEW QUESTION 89

A FortiGate is configured to receive push updates from the FortiGuard Distribution Network, however, they are not being received.

Which of the following statements are possible reasons for this?

A FortiGate unit is configured to receive push updates from the FortiGuard Distribution Network, however, updates are not being received. Which of the following statements are possible reasons for this? (Select all that apply.)

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

Answer: ABC

NEW QUESTION 91

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

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

Which statement is correct for the above configuration?

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

Answer: B

NEW QUESTION 92

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 93

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

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

- A. The two VLAN sub-interfaces can have the same VLAN ID only if they have IP addresses in different subnets.
- B. The two VLAN sub-interfaces must have different VLAN IDs.
- C. The two VLAN sub-interfaces can have the same VLAN ID only if they belong to different VDOMs.
- D. The two VLAN sub-interfaces can have the same VLAN ID if they are connected to different L2 IEEE 802.1Q compliant switches.

Answer: B

NEW QUESTION 96

Which TCP states does the global setting 'tcp-half-open-timer' applies to? (Choose two.)

- A. SYN SENT
- B. SYN & SYN/ACK
- C. FIN WAIT
- D. TIME WAIT

Answer: AD

NEW QUESTION 99

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 104

In transparent mode, forward-domain is a CLI setting associated with .

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

Answer: C

NEW QUESTION 109

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 112

A backup file begins with this line:

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

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

Can you restore it to a FortiWiFi 60D?

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

Answer: D

NEW QUESTION 115

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

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

Answer: ABC

NEW QUESTION 119

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 are listing of all connected FSSO collector agents.
- D. Lists all DC Agents installed on all domain controllers.

Answer: B

NEW QUESTION 122

A FortiGate is configured to receive push updates from the FortiGuard Distribution Network, however, they are not being received.

Which is one reason for this problem?

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

Answer: D

NEW QUESTION 124

Which statements are correct regarding an IPv6 over IPv4 IPsec configuration? (Choose two.)

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

Answer: BC

NEW QUESTION 129

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

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

Answer: BC

NEW QUESTION 134

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

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

Answer: A

NEW QUESTION 136

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

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

Answer: CD

NEW QUESTION 138

What is the maximum number of FortiAnalyzer/FortiManager devices a FortiGate unit can be configured to send logs to?

- A. 1
- B. 2
- C. 3
- D. 4

Answer: C

NEW QUESTION 142

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

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

Answer: C

NEW QUESTION 143

Which of the following IPsec configuration modes can be used for implementing L2TP- over-IPSec VPNs?

- A. Policy-based IPsec only.
- B. Route-based IPsec only.
- C. Both policy-based and route-based VPN.
- D. L2TP-over-IPSec is not supported by FortiGate devices.

Answer: A

NEW QUESTION 148

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 153

Which of the following statements best describes the role of a DC agents in an FSSO DC?

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

Answer: C

NEW QUESTION 157

Which statement is correct concerning creating a custom signature?

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

Answer: A

NEW QUESTION 160

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

```
config web-proxy explicit
```

```
set pac-file-server-status enable set pac-file-server-port 8080
```

```
set pac-file-name wpad.dat end
```

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

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

Answer: D

NEW QUESTION 161

Data leak prevention archiving gives the ability to store session transaction data on a FortiAnalyzer unit for which of the following types of network traffic? (Choose three.)

- A. POP3
- B. SNMP
- C. IPsec
- D. SMTP
- E. HTTP

Answer: ADE

NEW QUESTION 162

Which operating system vulnerability can you protect when selecting signatures to include in an IPS sensor? (choose three)

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

Answer: CDE

NEW QUESTION 163

Which is true of FortiGate's session table?

- A. NAT/PAT is shown in the central NAT table, not the session table.
- B. It shows TCP connection states.
- C. It shows IP, SSL, and HTTP sessions.
- D. It does not show UDP or ICMP connection state codes, because those protocols are connectionless.

Answer: B

NEW QUESTION 168

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

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

Answer: AD

NEW QUESTION 172

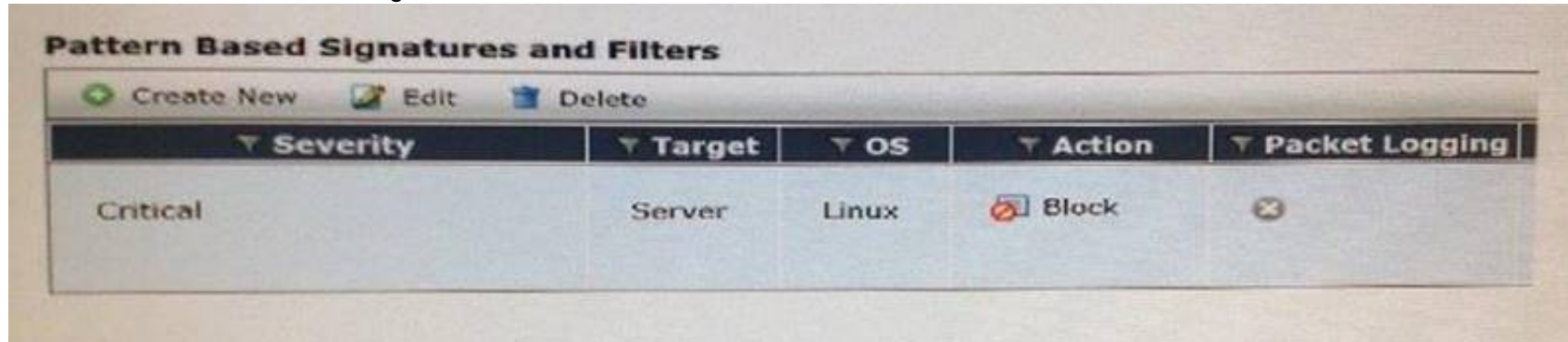
Which are outputs for the command 'diagnose hardware deviceinfo nic'? (Choose two.)

- A. ARP cache
- B. Physical MAC address
- C. Errors and collisions
- D. Listening TCP ports

Answer: BC

NEW QUESTION 174

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 affect when the sensor is applied to a policy.

Answer: CD

NEW QUESTION 179

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

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

Answer: D

NEW QUESTION 183

In which process states is it impossible to interrupt/kill a process? (Choose two.)

- A. S – Sleep
- B. R – Running
- C. D – Uninterruptable Sleep
- D. Z – Zombie

Answer: CD

NEW QUESTION 185

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 189

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 190

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

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

Answer: D

NEW QUESTION 193

Which statement describes how traffic flows in sessions handled by a slave unit in an active-active HA cluster?

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

Answer: D

NEW QUESTION 198

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

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

Answer: BCD

NEW QUESTION 202

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 206

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

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

Answer: AC

NEW QUESTION 211

Which of the following email spam filtering features is NOT supported on a FortiGate unit?

- A. Multipurpose Internet Mail Extensions (MIME) Header Check
- B. HELO DNS Lookup
- C. Greylisting
- D. Banned Word

Answer: C

NEW QUESTION 213

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 218

Which does FortiToken use as input when generating a token code? (Choose two.)

- A. User password
- B. Time
- C. User name
- D. Seed

Answer: AD

Explanation:

The token passcode is generated using a combination of the time and a secret key which is known only by the token and the FortiAuthenticator device. The token password changes at regular time intervals, and the FortiAuthenticator unit is able to validate the entered passcode using the time and the secret seed information for that token.

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 225

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

- A. Both proxy-based and flow-based inspection are supported.
- B. A replacement message cannot be presented to users when a virus has been detected.
- C. It saves CPU resources.
- D. The ingress and egress interfaces can be in different SPs.

Answer: BC

NEW QUESTION 229

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

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

Answer: C

NEW QUESTION 231

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

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

Answer: BCE

NEW QUESTION 232

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

Peer Options
Accept Types This peer ID ▼
Peer ID fortinet

Phase 1 Proposal + Add
Encryption 3DES ▼ Authentication SHA1 ▼
Diffie-Hellman Groups ☐ 21 ☐ 20 ☐ 19 ☐ 18 ☐ 17 ☐ 16 ☐ 15 ☒ 14 ☒ 5 ☐ 2 ☐ 1
Key Lifetime (seconds) 86400
Local ID

XAUTH
Type Disabled ▼

Phase 2 Selectors

Name	Local Address	Remote Address	+ Add
	0.0.0.0/0.0.0.0	0.0.0.0/0.0.0.0	✎

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

Answer: CD

NEW QUESTION 234

You are the administrator in charge of a FortiGate acting as an IPsec VPN gateway using routebased 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 238

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






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

Answer: ACE

NEW QUESTION 239

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

FortiGuard Subscription Services

Antivirus	Valid License (Expires 2013-05-12)	
AV Definitions	1.00000 (Updated 2012-10-17 via Manual Update) [Update]	
AV Engine	5.00032 (Updated 2012-10-16 via Manual Update)	
<hr/>		
IPS	Valid License (Expires 2013-05-12)	
IPS Definitions	4.00269 (Updated 2012-11-28 via Manual Update) [Update]	
IPS Engine	2.00043 (Updated 2012-10-29 via Manual Update)	
<hr/>		
Vulnerability Scan	Valid License (Expires 2013-05-12)	
VCM Plugins	1.00288 (Updated 2012-11-30 via Manual Update) [Update]	
VCM Engine	1.00288 (Updated 2012-11-30 via Manual Update)	
<hr/>		
Web Filtering	Valid License (Expires 2013-05-11)	
<hr/>		
Email Filtering	Valid License (Expires 2013-05-11)	
<hr/>		

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

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

Answer: A

NEW QUESTION 241

Which protocol can an Internet browser use to download the PAC file with the web proxy configuration?

- A. HTTPS
- B. FTP
- C. TFTP
- D. HTTP

Answer: D

NEW QUESTION 244

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 245

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

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

Answer: ADE

NEW QUESTION 250

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

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

Answer: C

NEW QUESTION 251

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

- A. The device this command is executed on is likely to switch from master to slave status if override is disabled.

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

Answer: AD

NEW QUESTION 255

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

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

Answer: B

NEW QUESTION 258

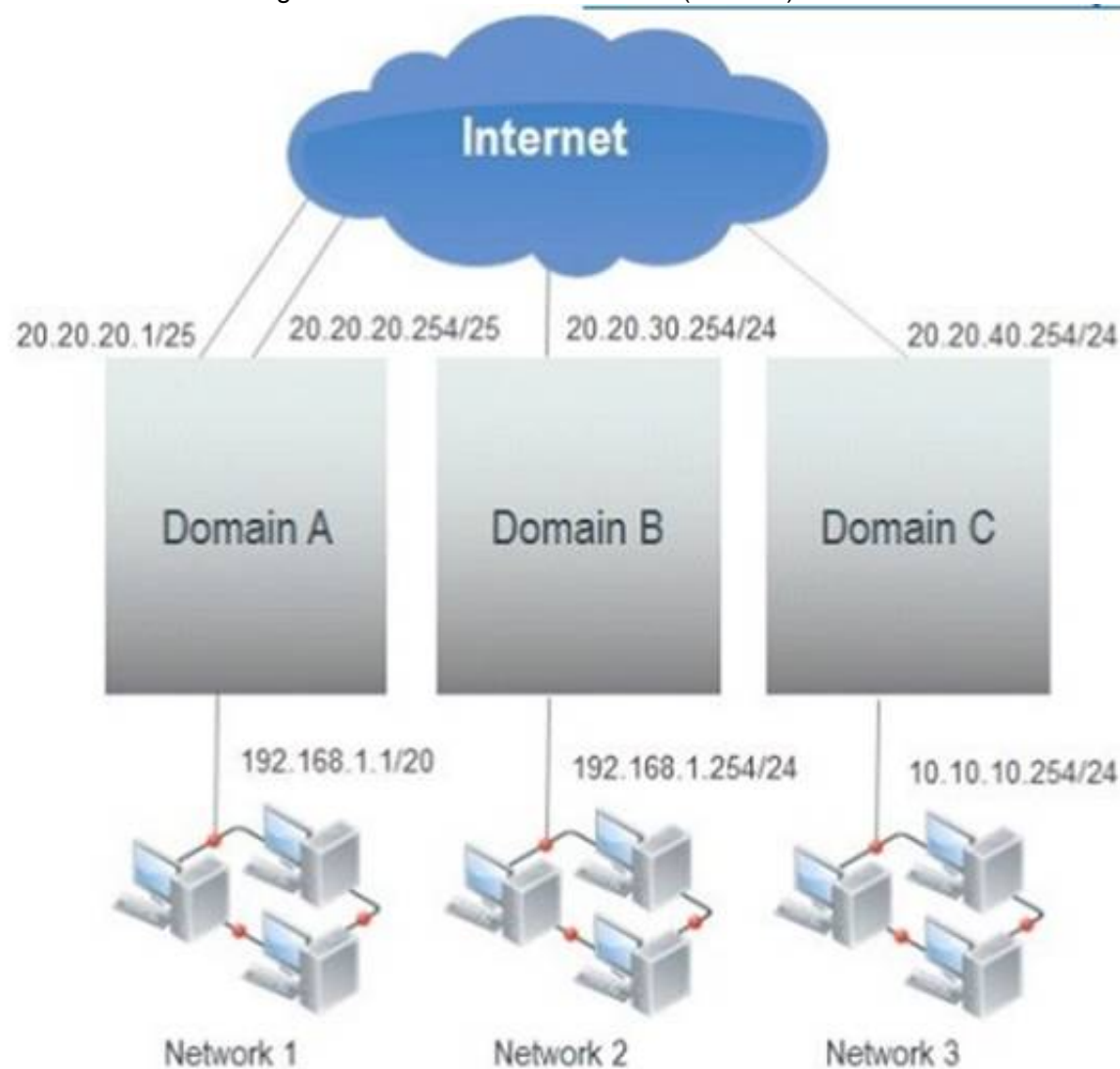
In a FSSO agentless polling mode solution, where must the collector agent be?

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

Answer: D

NEW QUESTION 260

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



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

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

Answer: ABE

NEW QUESTION 261

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

- A. 5
- B. 3
- C. 2
- D. 6

Answer: D

NEW QUESTION 263

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

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

Answer: C

NEW QUESTION 266

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

- A. SMTP
- B. HTTP-POST
- C. AIM
- D. MAPI
- E. ICQ

Answer: ABD

NEW QUESTION 267

Which web filtering inspection mode inspects DNS traffic?

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

Answer: A

NEW QUESTION 268

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 269

Which statement concerning IPS is false?

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

Answer: D

NEW QUESTION 271

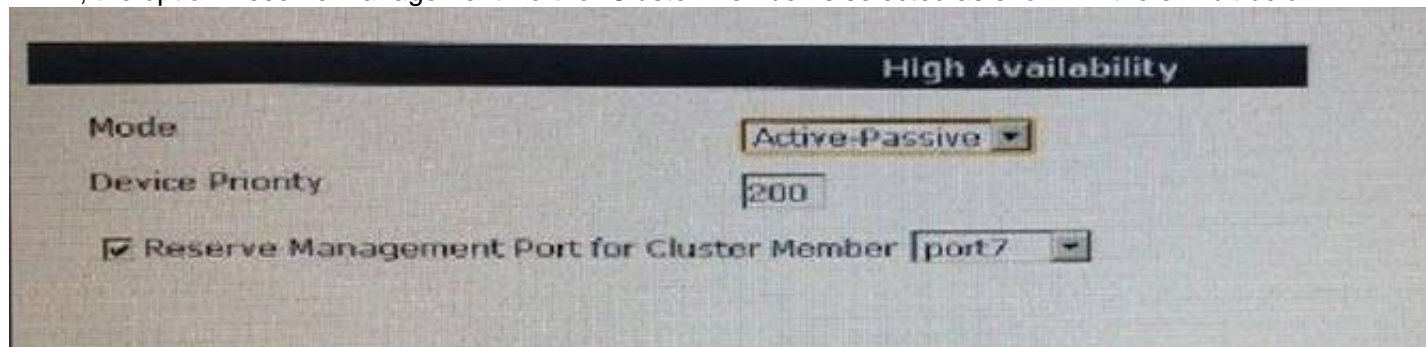
Which of the following statements are correct differences between NAT/route and transparent mode? (Choose two.)

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

Answer: AC

NEW QUESTION 275

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 279

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

- A. Kernel
- B. Proxy
- C. System
- D. Device

Answer: B

NEW QUESTION 282

Which of the following statements are true regarding the web filtering modes? (Choose two.)

- A. Proxy based mode allows for customizable block pages to display when sites are prevented.
- B. Proxy based mode requires more resources than flow-based.
- C. Flow based mode offers more settings under the advanced configuration section of the GUI.
- D. Proxy based mode offers higher throughput than flow-based mode.

Answer: AB

NEW QUESTION 285

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 290

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

- A. They are accelerated by hardware in the master unit.
- B. They are not accelerated by hardware in the master unit.
- C. They are accelerated by hardware in the slave unit.
- D. They are not accelerated by hardware in the slave unit.

Answer: AD

NEW QUESTION 292

Which of the following statements is correct regarding FortiGate interfaces and spanning tree protocol? (Choose Two)

- A. Only FortiGate switch interfaces Participate in spanning tree.
- B. All FortiGate interfaces in transparent mode VDOMs participate in spanning tree.
- C. All FortiGate interfaces in NAT/route mode VDOMs Participate in spanning tree.
- D. All FortiGate interfaces in transparent mode VDOMs may block or forward BPDUs.

Answer: BD

NEW QUESTION 296

Which of the following statements are correct regarding FortiGate virtual domains (VDOMs)? (Choose two)

- A. VDOMs divide a single FortiGate unit into two or more independent firewall.
- B. A management VDOM handles SNM
- C. logging, alert email and FortiGuard updates.
- D. Each VDOM can run different firmware versions.
- E. Administrative users with a 'super_admin' profile can administrate only one VDOM.

Answer: AB

NEW QUESTION 298

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

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

Answer: BC

NEW QUESTION 299

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

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

Answer: D

NEW QUESTION 302

The exhibit is a screen shot of an Application Control profile.

Categories

- Botnet
- Business
- Cloud.IT
- Collaboration
- Email
- Game
- General.Interest
- Network.Service
- P2P
- Proxy
- Remote.Access
- Social.Media
- Storage.Backup
- Update
- Video/Audio
- VoIP
- Industrial
- Web.Others
- All Other Known Applications
- All Other Unknown Applications

Application Overrides

Application Signature	Category	Action
YouTube	Video/Audio	Monitor
YouTube_Video.Access	Video/Audio	Monitor
YouTube_Video.Play	Video/Audio	Monitor

Options

- Deep Inspection of Cloud Applications
- Allow and Log DNS Traffic
- Replacement Messages for HTTP-based Applications

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 306

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

- A. Negotiate the encryption parameters to use.
- B. Auto-adjust the MTU setting.
- C. Autoconfigure addresses and prefixes.
- D. Determine other nodes reachability.

Answer: CD

NEW QUESTION 308

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 309

The exhibit shows a FortiGate routing table.

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

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

- A. There is only one active default route.
- B. The distance values for the route to 192.168.1.0/24 is 200
- C. An IP address in the subnet 172.16.78.0/24 has been assigned to the dmz interface.
- D. The FortiGate will route the traffic to 172.17.1.2 to next hop with the IP address 192.168.11.254

Answer: AD

NEW QUESTION 313

Which of the following sequences describes the correct order of criteria used for the selection of a master unit within a FortiGate high availability (HA) cluster when override is disabled?

- A. 1. port monitor, 2. unit priority, 3. up time, 4. serial number.
- B. 1. port monitor, 2. up time, 3. unit priority, 4. serial number.
- C. 1. unit priority, 2. up time, 3. port monitor, 4. serial number.
- D. 1. up time, 2. unit priority, 3. port monitor, 4. serial number.

Answer: B

NEW QUESTION 314

Examine this log entry.

What does the log indicate? (Choose three.)

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

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

Answer: BEG

NEW QUESTION 316

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

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

Answer: C

NEW QUESTION 319

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

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

Answer: ADE

NEW QUESTION 321

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 326

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 327

What is the default criteria for selecting the HA master unit in a HA cluster?

- A. port monitor, priority, uptime, serial number
- B. Port monitor, uptime, priority, serial number
- C. Priority, uptime, port monitor, serial number
- D. uptime, priority, port monitor, serial number

Answer: B

NEW QUESTION 330

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 332

The exhibit shoes three static routes.

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

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

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

Answer: D

NEW QUESTION 334

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

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

Answer: AD

NEW QUESTION 337

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 342

What are two requirements for DC-agent mode FSSO to work properly in a Windows AD environment? (Choose two.)

- A. DNS server must properly resolve all workstation names
- B. The remote registry service must be running in all workstations
- C. The collector agent must be installed in one of the Windows domain controllers
- D. A same user cannot be logged in into two different workstations at the same time

Answer: AB

NEW QUESTION 346

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 348

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 349

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

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

Answer: BCD

NEW QUESTION 354

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

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

Answer: BC

NEW QUESTION 359

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

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

Answer: C

NEW QUESTION 362

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

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

Answer: BCD

NEW QUESTION 364

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

- A. The FortiGate device “re-signs” all the certificates coming from the HTTPS servers
- B. The FortiGate device acts as a sub-CA
- C. The local service certificate of the web server must be installed in the FortiGate device
- D. The FortiGate device does man-in-the-middle inspection.
- E. The required SSL Proxy certificate must first be requested to a public certificate authority (CA).

Answer: BCE

NEW QUESTION 367

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

Exhibit A:

```
Max number of virtual domains: 18
Virtual domains status: 1 in NAT mode, 0 in TP mode
Virtual domain configuration: disable
FIPS-CC mode: disable
Current HA mode: a-p, master
Branch point: 128
Release Version Information: GA
System time: Thu Jan 24 08:34:19 2013

STUDENT #
STUDENT #
STUDENT #
STUDENT #
STUDENT #
STUDENT # show system ha
config system ha
    set mode a-p
    set password ENC 9FHCYw0JXK9z8w6QkUnUsRE4BruUcMJ5NUUE3oU5otyn+4dsgx4CnV1GRJ8
McEECPiT32/3dCmIuYIDgW2sE+1A1kHfAD0V/r5DkaqGnbj15XU/a
    set hbdev "port2" 58
    set override disable
    set priority 200
end

STUDENT # _
```

Exhibit B:

```
Log hard disk: Available
Hostname: REMOTE
Operation Mode: NAT
Current virtual domain: root
Max number of virtual domains: 10
Virtual domains status: 1 in NAT mode, 0 in TP mode
Virtual domain configuration: disable
FIPS-CC mode: disable
Current HA mode: a-a, master
Branch point: 128
Release Version Information: GA
System time: Thu Jan 24 08:41:46 2013

REMOTE # show system ha
config system ha
    set mode a-a
    set password ENC 9FHCYw0JXK9z8w6QkUnUsREWBruUcMJ5NUUE3oV5otyn+4ds7YGv12Cir+8
B6Mf/rGXh0u5lygP+yPgI5SDnSMEz4JINv4E09skI00MBQbcgxhSE
    set hbdev "port2" 50
    set session-pickup enable
    set override disable
    set priority 100
end

REMOTE # _
```

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

- A. Password
- B. HA mode
- C. Hearbeat
- D. Override

Answer: B

NEW QUESTION 369

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 371

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

Disconnect Cluster Member

Serial Number FGVM010000006268

Interface

IP/Netmask

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 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 375

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

- A. Virus scanning is enabled by default.
- B. Fortinet customer support enables virus scanning remotely for you.
- C. Virus scanning must be enabled in a security profile, which must be applied to a firewall policy.
- D. Enabling virus scanning in a UTM security profile enables virus scanning for all traffic flowing through the FortiGate device.

Answer: C

NEW QUESTION 376

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

Protocol	Virus Scan and Removal
Web	
HTTP	<input type="checkbox"/>
Email	
SMTP	<input checked="" type="checkbox"/>
POP3	<input type="checkbox"/>
IMAP	<input type="checkbox"/>
MAPI	<input type="checkbox"/>
File Transfer	
FTP	<input type="checkbox"/>
IM	
ICQ, Yahoo, MSN Messenger	<input type="checkbox"/>

Exhibit B:

	<input checked="" type="checkbox"/> IMAP	<input checked="" type="checkbox"/> POP3	<input checked="" type="checkbox"/> SMTP
Spam Action	Tagged	Tagged	Discard
Tag Location	Subject	Subject	Subject
Tag Format	Spam	Spam	Spam

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: B

NEW QUESTION 378

Which of the following Fortinet products can receive updates from the FortiGuard Distribution Network?

- A. FortiGate
- B. FortiClient
- C. FortiMail
- D. FortiAnalyzer

Answer: ABC

NEW QUESTION 380

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.



Seq.#	Source	Destination	Schedule	Service	Authentication	Action	UTM Profile	Log	NA
▼ port3 - port1 (1 - 1)									
1	all	all	always	ALL		✓ ACCEPT		✕	✓
▼ port1 - port3 (2 - 2)									
2	all	WIN2K3				SSL-VPN			✕
▼ ssl.root (sslvpn tunnel interface) - port3 (3 - 3)									
3	all	all	always	ALL		✓ ACCEPT		✕	✓
▼ Implicit (4 - 4)									
4	any	any	always	ALL		✗ DENY		✕	

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 384

Which correctly define "Section View" and "Global View" for firewall policies? (Choose two.)

- A. Section View lists firewall policies primarily by their interface pairs.
- B. Section View lists firewall policies primarily by their sequence number.
- C. Global View lists firewall policies primarily by their interface pairs.
- D. Global View lists firewall policies primarily by their policy sequence number.
- E. The 'any' interface may be used with Section View.

Answer: AD

NEW QUESTION 385

Which of the following statements is true regarding the differences between route-based and policy-based IPsec VPNs? (Choose two.)

- A. The firewall policies for policy-based are bidirectiona
- B. The firewall policies for route- based are unidirectional.
- C. In policy-based VPNs the traffic crossing the tunnel must be routed to the virtual IPsec interfac
- D. In route-based, it does not.
- E. The action for firewall policies for route-based VPNs may be Accept or Deny, for policy- based VPNs it is Encrypt.
- F. Policy-based VPN uses an IPsec interface, route-based does not.

Answer: AC

NEW QUESTION 389

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

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

Answer: CD

NEW QUESTION 393

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 396

The exhibit shows two static routes to the same destinations subnet 172.20.168.0/24.

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

Which of the following statements correctly describes this static routing configuration? (choose two)

- A. Both routes will show up in the routing table.
- B. The FortiGate unit will evenly share the traffic to 172.20.168.0/24 between routes.
- C. Only one route will show up in the routing table.
- D. The FortiGate will route the traffic to 172.20.168.0/24 only through one route.

Answer: CD

NEW QUESTION 399

A client can establish a secure connection to a corporate network using SSL VPN in tunnel mode. Which of the following statements are correct regarding the use of tunnel mode SSL VPN? (Select all that apply.)

- A. Split tunneling can be enabled when using tunnel mode SSL VPN.
- B. Client software is required to be able to use a tunnel mode SSL VPN.
- C. Users attempting to create a tunnel mode SSL VPN connection must be authenticated by at least one SSL VPN policy.
- D. The source IP address used by the client for the tunnel mode SSL VPN is assigned by the FortiGate unit.

Answer: ABCD

NEW QUESTION 404

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

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

Answer: B

NEW QUESTION 409

.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your NSE4 Exam with Our Prep Materials Via below:

<https://www.certleader.com/NSE4-dumps.html>