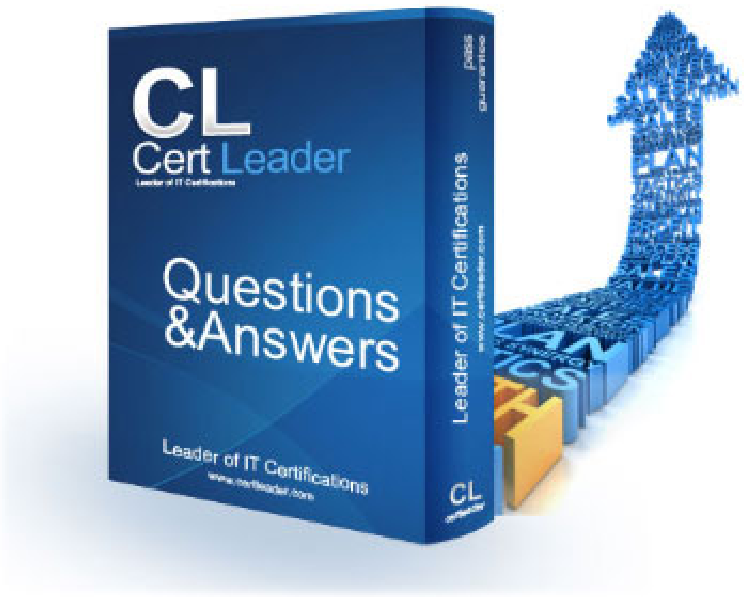
NSE4 Dumps

Fortinet Network Security Expert 4 Written Exam (400)

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



NEW QUESTION 1
Which protocols can you use for secure administrative access to a FortiGate? (Choose two)

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

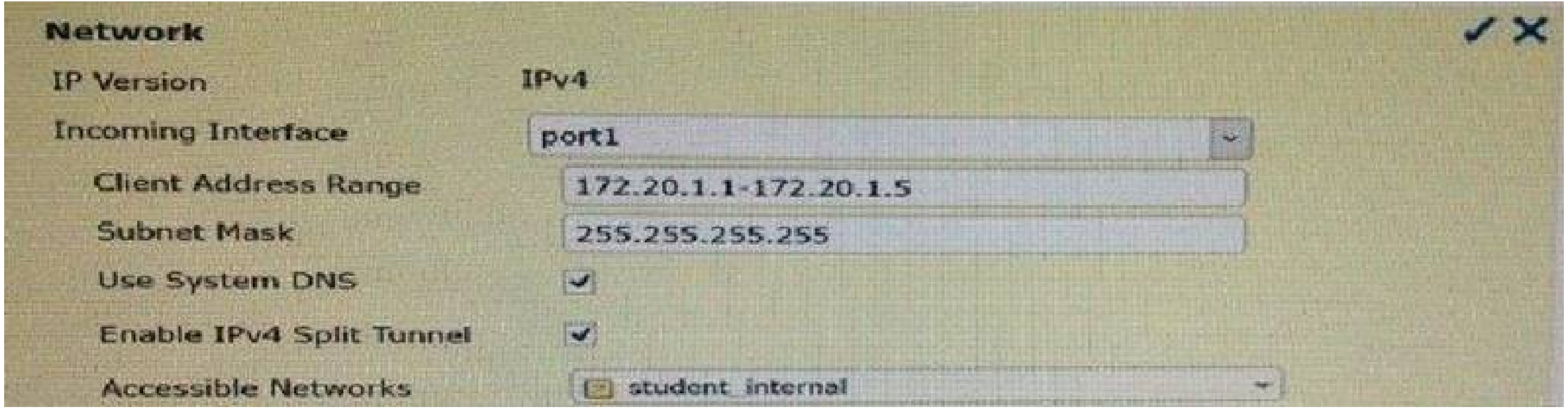
Answer: AD

NEW QUESTION 2
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 3
Review the configuration for FortiClient IPsec shown in the exhibit.



Network

IP Version	IPv4
Incoming Interface	port1
Client Address Range	172.20.1.1-172.20.1.5
Subnet Mask	255.255.255.255
Use System DNS	☑
Enable IPv4 Split Tunnel	☑
Accessible Networks	student_internal

Which statement is correct regarding this configuration?

A. The connecting VPN client will install a route to a destination corresponding to the student internal address object.
B. The connecting VPN client will install a default route.
C. The connecting VPN client will install a route to the 172.20.1.[1-5] address range.
D. The connecting VPN client will connect in web portal mode and no route will be installed.

Answer: A

NEW QUESTION 4
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 5
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 6
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 7
Which of the following statements are correct regarding a master HA unit? (Choose two)

A. There should be only one master unit is each HA virtual cluster.
B. The Master synchronizes cluster configuration with slaves.
C. Only the master has a reserved management HA interface.
D. Heartbeat interfaces are not required on a master unit.

Answer: AB

NEW QUESTION 8
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 9
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 10
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 10
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 14
Which of the following statement correct describes the use of the "diagnose sys ha reset- uptime" command?

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

Answer: A

NEW QUESTION 16
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 18
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 23
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 28
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 31
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 36
On your FortiGate 60D, you've configured firewall policies. They port forward traffic to your Linux Apache web server. Select the best way to protect your web server by using the IPS engine.

A. Enable IPS signatures for Linux servers with HTTP, TCP and SSL protocols and Apache application
B. Configured DLP to block HTTP GET request with credit card numbers.
C. Enable IPS signatures for Linux servers with HTTP, TCP and SSL protocols and Apache application
D. Configure DLP to block HTTP GET with credit card number
E. Also configure a DoS policy to prevent TCP SYn floods and port scans.
F. Non
G. FortiGate 60D is a desktop model, which does not support IPS.
H. Enable IPS signatures for Linux and windows servers with FTP, HTTP, TCP, and SSL protocols and Apache and PHP applications.

Answer: D

NEW QUESTION 39
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 43
Which statement best describes the objective of the SYN proxy feature available in SP processors?

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

Answer: D

NEW QUESTION 46
Which of the following are possible actions for static URL filtering? (Choose three.)

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

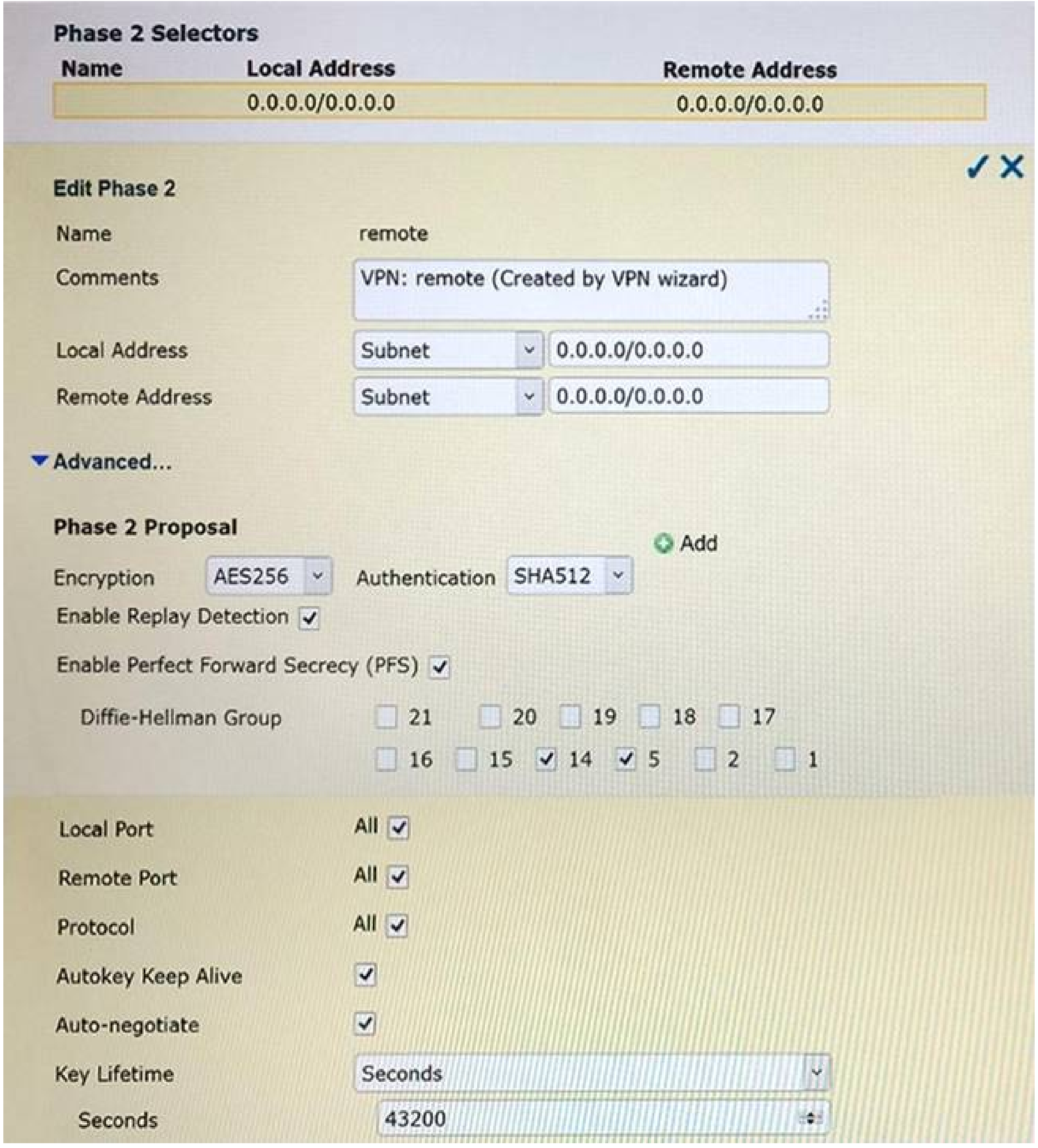
Answer: ABC

NEW QUESTION 47
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 52
Review the IPsec phase 2 configuration shown in the exhibit; then answer the question below.



Phase 2 Selectors

Name	Local Address	Remote Address
	0.0.0.0/0.0.0.0	0.0.0.0/0.0.0.0

Edit Phase 2

Name: remote
Comments: VPN: remote (Created by VPN wizard)
Local Address: Subnet 0.0.0.0/0.0.0.0
Remote Address: Subnet 0.0.0.0/0.0.0.0

Advanced...

Phase 2 Proposal

Encryption: AES256 Authentication: SHA512
Enable Replay Detection ☑
Enable Perfect Forward Secrecy (PFS) ☑
Diffie-Hellman Group: □ 21 □ 20 □ 19 □ 18 □ 17 □ 16 □ 15 ☑ 14 ☑ 5 □ 2 □ 1

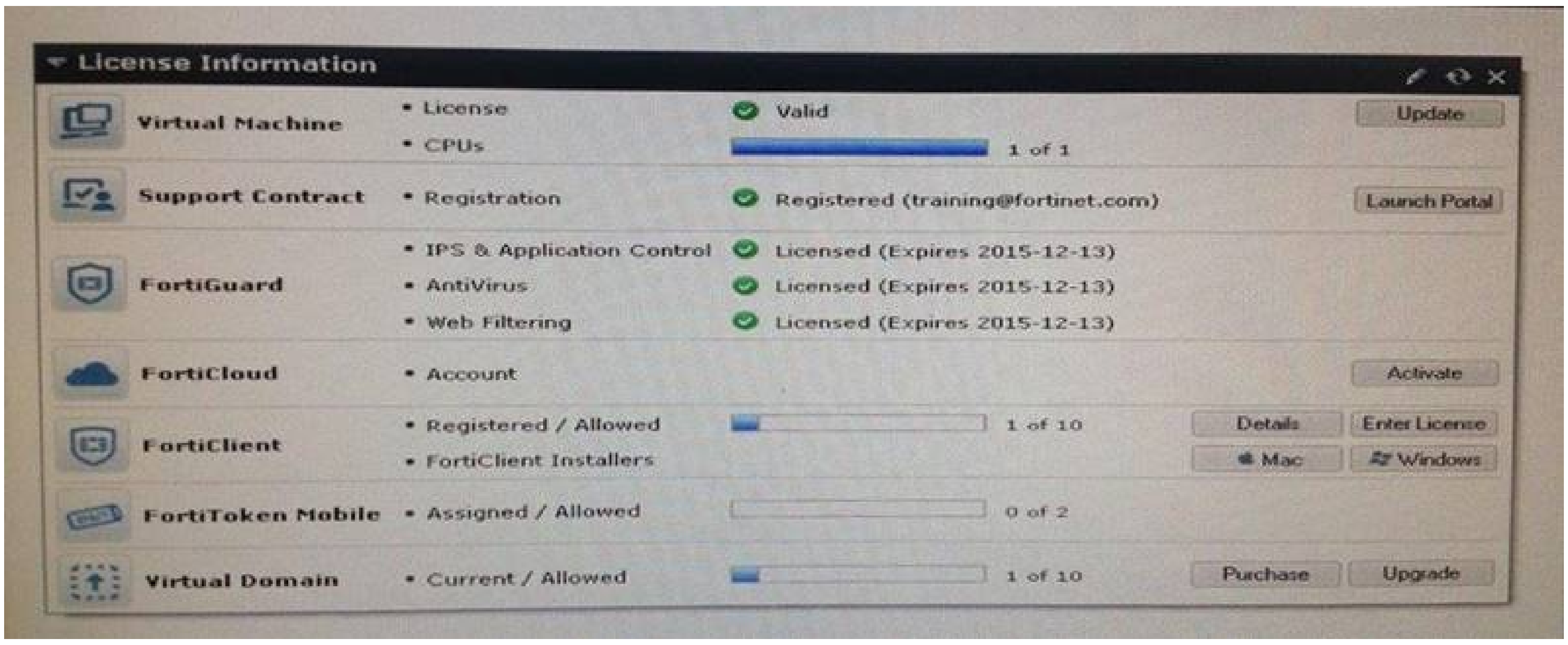
Local Port: All ☑
Remote Port: All ☑
Protocol: All ☑
Autokey Keep Alive ☑
Auto-negotiate ☑
Key Lifetime: Seconds
Seconds: 43200

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

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

Answer: AB

NEW QUESTION 56
Examine the exhibit; then answer the question below.



License Information

Virtual Machine	• License • CPUs	✓ Valid 1 of 1	Update
Support Contract	• Registration	✓ Registered (training@fortinet.com)	Launch Portal
FortiGuard	• IPS & Application Control • AntiVirus • Web Filtering	✓ Licensed (Expires 2015-12-13) ✓ Licensed (Expires 2015-12-13) ✓ Licensed (Expires 2015-12-13)	
FortiCloud	• Account		Activate
FortiClient	• Registered / Allowed • FortiClient Installers	1 of 10	Details Enter License Mac Windows
FortiToken Mobile	• Assigned / Allowed	0 of 2	
Virtual Domain	• Current / Allowed	1 of 10	Purchase Upgrade

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

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

Answer: D

NEW QUESTION 58
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 62
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 63
Which statements regarding banned words are correct? (Choose two.)

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

Answer: CD

NEW QUESTION 67
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 71
Examine the static route configuration shown below; then answer the question following it.
config router static edit 1
set dst 172.20.1.0 255.255.255.0
set device port1

```
set gateway 172.11.12.1
set distance 10
set weight 5 next
edit 2
set dst 172.20.1.0 255.255.255.0
set blackhole enable set distance 5
set weight 10 next
end
```

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

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

Answer: AC

NEW QUESTION 75
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 77
Which IPsec configuration mode can be used for implementing GRE-over-IPsec VPNs?

A. Policy-based only.
B. Route-based only.
C. Either policy-based or route-based VPN.
D. GRE-based only.

Answer: B

NEW QUESTION 82
If there are no changes in the routing table and in the case of TCP traffic, which of the following correctly describes the routing table lookups performed by a FortiGate in NAT
/Route mode, when searching for a suitable gateway?

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

Answer: B

NEW QUESTION 86
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 91
Which statement best describes what a Fortinet System on a Chip (SoC) is?

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

Answer: B

NEW QUESTION 92
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 93
Examine the following log message for IPS:
2012-07-01 09:54:28 oid=2 log_id=18433 type=ips subtype=anomaly pri=alert vd=root severity="critical" src="192.168.3.168" dst="192.168.3.170" src_int="port2" serial=0 status="detected" proto=1 service="icmp" count=1 attack_name="icmp_flood"
icmp_id="0xa8a4"
icmp_type="0x08" icmp_code="0x00" attack_id=16777316 sensor="1" ref="http://www.fortinet.com/ids/VID16777316" msg="anomaly: icmp_flood, 51 > threshold 50"
Which statement is correct about the above log? (Choose two.)

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

Answer: BD

NEW QUESTION 94
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 98
You have created a new administrator account, and assign it the prof_admin profile. Which is false about that account's permissions?

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

Answer: A

NEW QUESTION 100
Which of the following statements are true regarding traffic accelerated by an NP processor? (Choose two.)

A. TCP SYN packets are always handled by the NP Processor
B. The initial packets go to the NP Processor, where a decision is taken on if the session can be offloaded or not.
C. Packets for a session termination are always handled by the CPU.
D. The initial packets go to the CPU, where a decision is taken on if the session can be offloaded or not.

Answer: AD

NEW QUESTION 105
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.

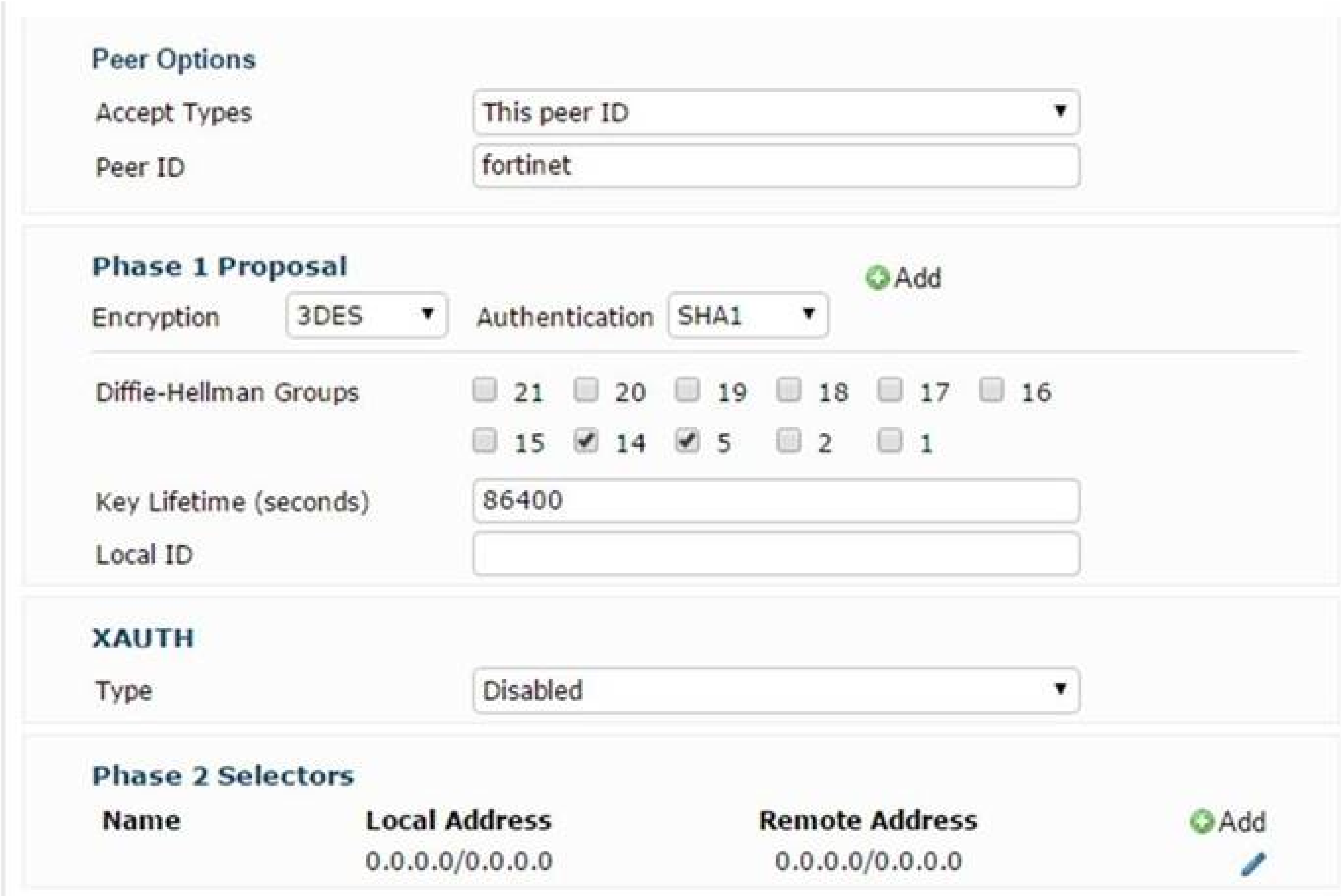
Answer: BD

NEW QUESTION 107
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 110
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

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
	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 111
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 112
Which action is taken by the FortiGate device when a file matches more than one rule in a Data Leak Prevention sensor?

A. The actions specified by the rule that most specifically matched the file
B. The actions specified in the first rule from top to bottom
C. All actions specified by all the matched rules.
D. The actions specified in the rule with the higher priority number

Answer: D

NEW QUESTION 113
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 116
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 119
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 122
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 126
Which of the following IPsec configuration modes can be used when the FortiGate is running in NAT mode?

A. Policy-based VPN only
B. Both policy-based and route-based VPN.
C. Route-based VPN only.
D. IPSec VPNs are not supported when the FortiGate is running in NAT mode.

Answer: B

NEW QUESTION 131
Which of the following are operating mode supported in FortiGate devices? (Choose two)

A. Proxy
B. Transparent
C. NAT/route
D. Offline inspection

Answer: BC

NEW QUESTION 134
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 136
Which portion of the configuration does an administrator specify the type of IPsec configuration (either policy-based or route-based)?

A. Under the IPsec VPN global settings.
B. Under the phase 2 settings.
C. Under the phase 1 settings.
D. Under the firewall policy settings.

Answer: D

NEW QUESTION 140
Which of the following statements is true regarding the TCP SYN packets that go from a client, through an implicit web proxy (transparent proxy), to a web server listening at TCP port 80? (Choose three.)

A. The source IP address matches the client IP address.
B. The source IP address matches the proxy IP address.
C. The destination IP address matches the proxy IP address.
D. The destination IP address matches the server IP addresses.
E. The destination TCP port number is 80.

Answer: ADE

NEW QUESTION 143
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 146
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 149
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.

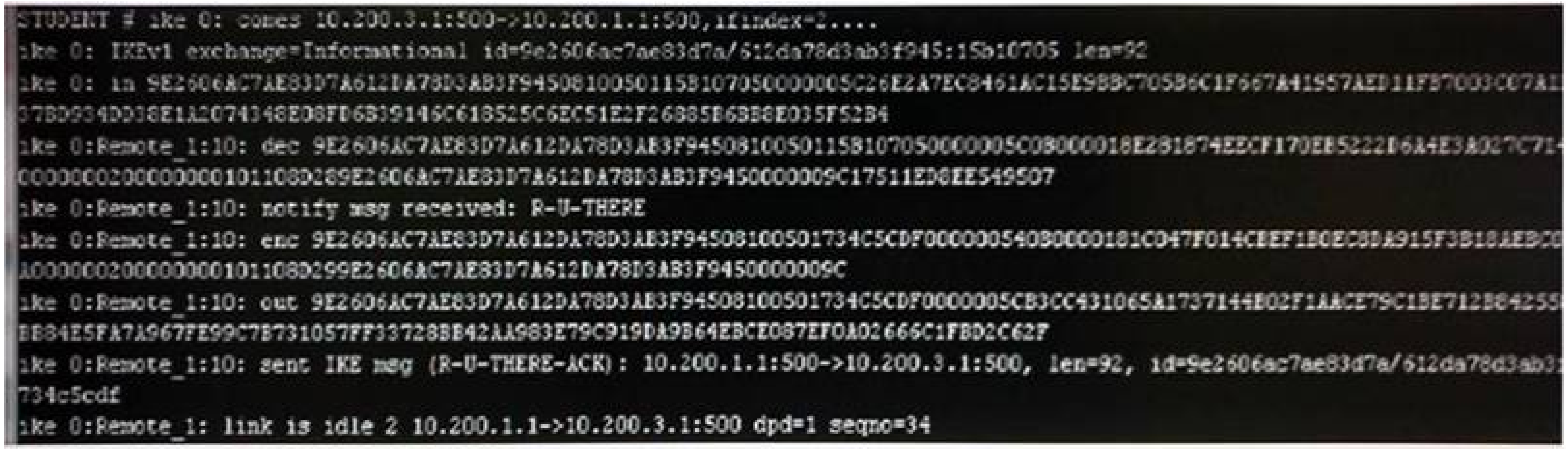
Answer: BEG

NEW QUESTION 154
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 158
Review the IKE debug output for IPsec shown in the exhibit below.



```
STUDENT # ike 0: comes 10.200.3.1:500->10.200.1.1:500,ifindex=2....
ike 0: IKEv1 exchange=Informational id=9e2606ac7ae83d7a/612da78d3ab3f945:15b10705 len=92
ike 0: in 9E2606AC7AE83D7A612DA78D3AB3F9450810050115B1070500000005C26E2A7EC8461AC15E9BBC705B6C1F667A41957AED11FB7003C07A1
37BD934DD18E1A2074348ED8FD6B39146C618525C6EC51E2F26885B6BB8ED35F52B4
ike 0:Remote_1:10: dec 9E2606AC7AE83D7A612DA78D3AB3F9450810050115B107050000005C08000018E281874EECF170EB5222B6A4E3A027C71
000000020000000101108D289E2606AC7AE83D7A612DA78D3AB3F9450000009C17511ED8EE549507
ike 0:Remote_1:10: notify msg received: R-U-THERE
ike 0:Remote_1:10: enc 9E2606AC7AE83D7A612DA78D3AB3F94508100501734C5CDF000000540800001 81C047F014CBEF1B0EC8DA915F3B18AEBC0
A000000200000000101108D299E2606AC7AE83D7A612DA78D3AB3F9450000009C
ike 0:Remote_1:10: out 9E2606AC7AE83D7A612DA78D3AB3F94508100501734C5CDF0000005CB3CC431065A1737144B02F1AACE79C1BE712B8425
BB84E5FA7A967FE99C7B731057FF337288B42AA983E79C919DA9B64EBCE087EF0A02666C1FBD2C62F
ike 0:Remote_1:10: sent IKE msg (R-U-THERE-ACK): 10.200.1.1:500->10.200.3.1:500, len=92, id=9e2606ac7ae83d7a/612da78d3ab3
734c5cdf
ike 0:Remote_1: link is idle 2 10.200.1.1->10.200.3.1:500 dpd=1 seqno=34
```

Which statements is correct regarding this output?

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

Answer: C

NEW QUESTION 161
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.

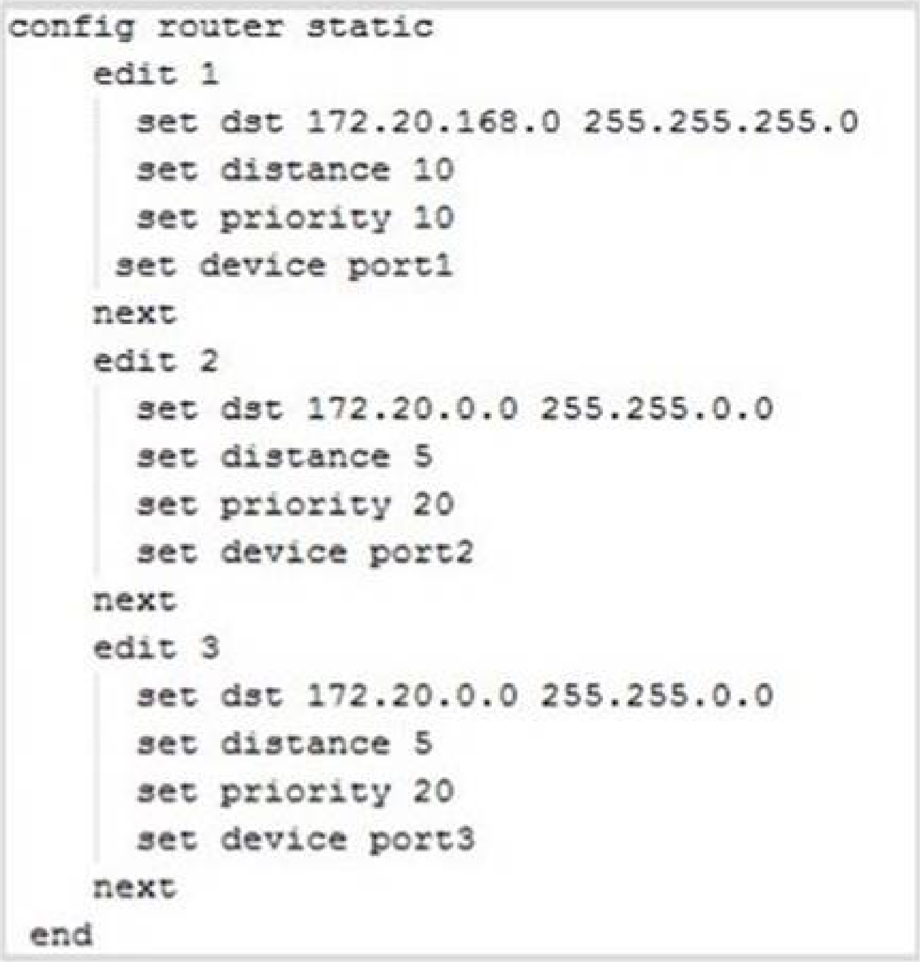
Answer: BC

NEW QUESTION 163
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 168
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 170
Which statements are true regarding IPv6 anycast addresses? (Choose two.)

A. Multiple interfaces can share the same anycast address.
B. They are allocated from the multicast address space.
C. Different nodes cannot share the same anycast address.
D. An anycast packet is routed to the nearest interface.

Answer: AD

NEW QUESTION 175
In which order are firewall policies processed on a FortiGate unit?

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

Answer: A

NEW QUESTION 180
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 181
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.

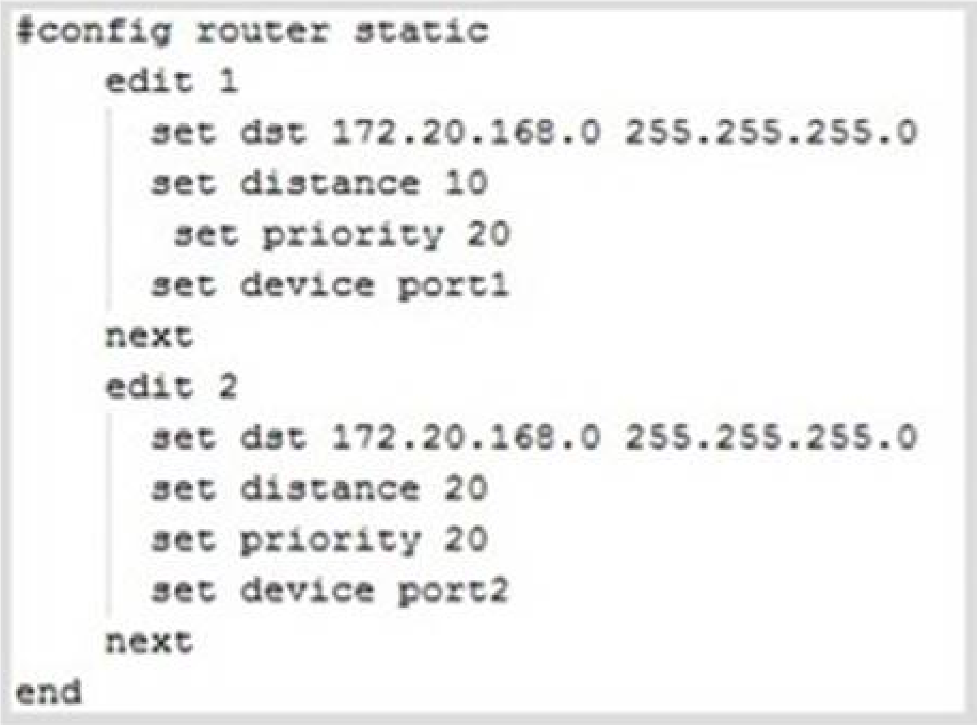
Answer: C

NEW QUESTION 186
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 188
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 190
What is valid reason for using session based authentication instead of IP based authentication in a FortiGate web proxy solution?

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

Answer: C

NEW QUESTION 191
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?

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 192
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 194
......

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