Fortinet

Exam Questions NSE4

Fortinet Network Security Expert 4 Written Exam (400)

NEW QUESTION 1
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

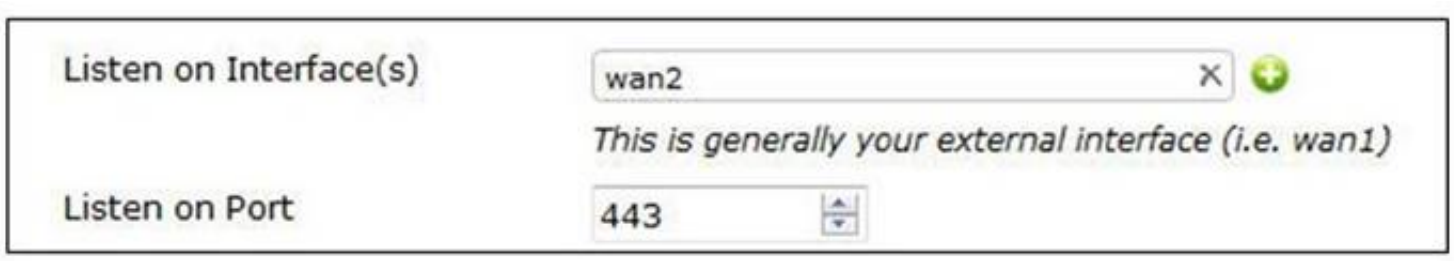
NEW QUESTION 2
Examine the exhibit; then answer the question below.

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 3
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.



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

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

Answer: BC

NEW QUESTION 6
Which is true about incoming and outgoing interfaces in firewall policies?

A. A physical interface may not be used.
B. A zone may not be used.
C. Multiple interfaces may not be used for both incoming and outgoing.
D. Source and destination interfaces are mandatory.

Answer: D

NEW QUESTION 7
What log type would indicate whether a VPN is going up or down?

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

Answer: A

NEW QUESTION 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
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 10
Which commands are appropriate for investigating high CPU? (Choose two.)

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

Answer: AD

NEW QUESTION 10
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 14
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 19
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 20
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 22
Which two methods are supported by the web proxy auto-discovery protocol (WPAD) to automatically learn the URL where a PAC file is located? (Choose two.)

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

Answer: AC

NEW QUESTION 25
When an administrator attempts to manage FortiGate from an IP address that is not a trusted host, what happens?

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

Answer: B

NEW QUESTION 27
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 29
In "diag debug flow" output, you see the message “Allowed by Policy-1: SNAT”. Which is true?

A. The packet matched the topmost policy in the list of firewall policies.
B. The packet matched the firewall policy whose policy ID is 1.
C. The packet matched a firewall policy, which allows the packet and skips UTM checks
D. The policy allowed the packet and applied session NAT.

Answer: B

NEW QUESTION 32
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 34
Which changes to IPS will reduce resource usage and improve performance? (Choose three)

A. In custom signature, remove unnecessary keywords to reduce how far into the signature tree that FortiGate must compare in order to determine whether the packet matches.
B. In IPS sensors, disable signatures and rate based statistics (anomaly detection) for protocols, applications and traffic directions that are not relevant.
C. In IPS filters, switch from 'Advanced' to 'Basic' to apply only the most essential signatures.
D. In firewall policies where IPS is not needed, disable IPS.
E. In firewall policies where IPS is used, enable session start logs.

Answer: ABD

NEW QUESTION 37
Which of the following actions can be used to back up the keys and digital certificates in a FortiGate device? (Choose two.)

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

Answer: AD

NEW QUESTION 42
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 45
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 49
Which statement best describes what SSL VPN Client Integrity Check does?

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

Answer: B

NEW QUESTION 52
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 56
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 58
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 62
A FortiGate device is configure to perform an AV & IPS scheduled update every hour.

```
Virus Definitions
---------
Version: 21.00487
Contract Expiry Date: Tue Apr 29 00:00:00 2014
Last Updated using scheduled update on Mon Jan
20 01:05:33 2014
Last Update Attempt: Mon Jan 20 10:08:56 2014
Result: Updates Installed
```

```
FG100D3G12800939 # exe time
current time is: 10:35:35
last ntp sync:Mon Jan 20 09:51:59 2014
```

Given the information in the exhibit, when will the next update happen?

A. 01:00
B. 02:05
C. 11:00
D. 11:08

Answer: D

NEW QUESTION 67
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 71
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 72
Which statement is correct concerning creating a custom signature?

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

Answer: A

NEW QUESTION 74
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 77
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 79
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 83
An administrator configures a FortiGate unit in Transparent mode on the 192.168.11.0 subnet. Automatic Discovery is enabled to detect any available FortiAnalyzers on the
network.
Which of the following FortiAnalyzers will be detected?

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

Answer: AB

NEW QUESTION 88
Examine the following output from the diagnose sys session list command:

```
session info: proto=6 proto_state=65 duration=3 expire=9 timeout=3600 flags=00000000
sockflag=00000000 sockport=443 av_idx=9 use=5

origin-shaper=guarantee-100kbps prio=2 guarantee 12800Bps max 134217728Bps traffic 13895Bps

reply-shaper=guarantee-100kbps prio=2 guarantee 12800Bps max 134217728Bps traffic 13895Bps

state=redir local may_dirty ndr npu nlb os rs

statistic(bytes/packets/allow_err): org=864/8/1 reply=2384/7/1 tuples=3

orgin->sink: org pre->post, reply pre->post dev=7->6/6->7 gwy=172.17.87.3/10.1.10.1

hook=post dir=org act=snat 192.168.1.110:57999->74.201.86.29:443(172.17.87.16:57999)

hook=pre dir=reply act=dnat 74.201.86.29:443->172.17.87.16:57999(192.168.1.110:57999)

hook=post dir=reply act=noop 74.201.86.29:443->192.168.1.110:57999(0.0.0.0:0)

misc=0 policy_id=1 id_policy_id=0 auth_info=0 chk_client_info=0 vd=0

npu info: flag=0x00/0x00, offload=0/0, ips_offload=0/0, epid=0/0, ipid=0/0, vlan=0/0
```

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

A. Session Time-To-Live (TTL) was configured to 9 seconds.
B. FortiGate is doing NAT of both the source and destination IP address on all packets coming from the 192.168.1.110 address.

C. The IP address 192.168.1.110 is being translated to 172.17.87.16.
D. The FortiGate is not translating the TCP port numbers of the packets in this session.

Answer: CD

NEW QUESTION 92
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 96
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 97
Which two web filtering inspection modes inspect the full URL? (Choose two.)

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

Answer: BC

NEW QUESTION 101
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 105
Which of the following statements best describes what the Document Fingerprinting feature is for?

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

Answer: A

NEW QUESTION 108
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 112
Which statement is in advantage of using a hub and spoke IPsec VPN configuration instead of a fully-meshed set of IPsec tunnels?

A. Using a hub and spoke topology provides full redundancy.
B. Using a hub and spoke topology requires fewer tunnels.
C. Using a hub and spoke topology uses stronger encryption protocols.
D. Using a hub and spoke topology requires more routes.

Answer: B

NEW QUESTION 116
Files that are larger than the oversized limit are subjected to which Antivirus check?

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

Answer: C

NEW QUESTION 117
Which of the following traffic shaping functions can be offloaded to a NP processor? (Choose two.)

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

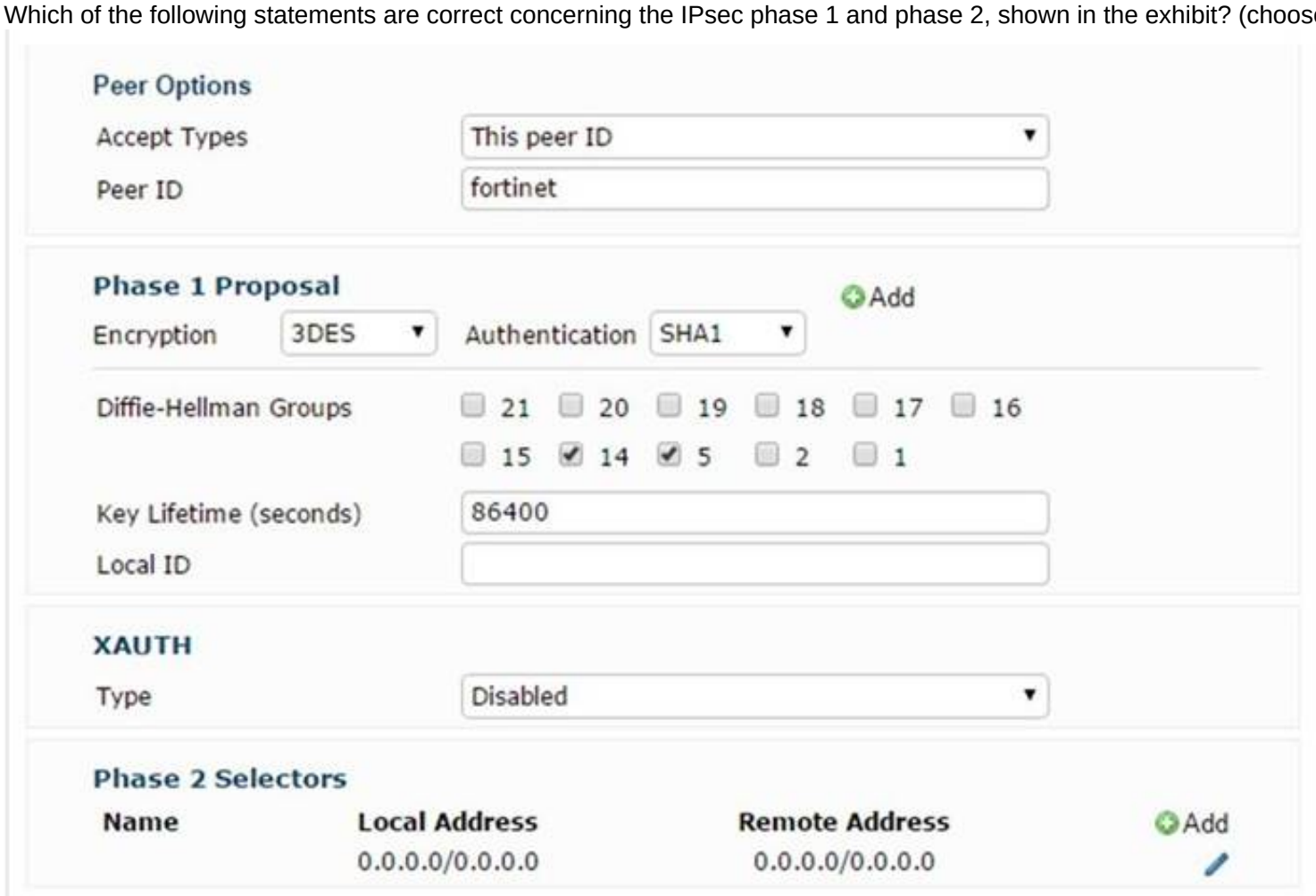
Answer: CD

NEW QUESTION 119
Which statements are true regarding the factory default configuration? (Choose three.)

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

Answer: BDE

NEW QUESTION 122
Which of the following statements are correct concerning the IPsec phase 1 and phase 2, shown in the exhibit? (choose two)



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 125
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 126
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 130
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 135
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 140
Examine the following CLI configuration:
config system session -ttl set default 1800
end
What statement is true about the effect of the above configuration line?

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

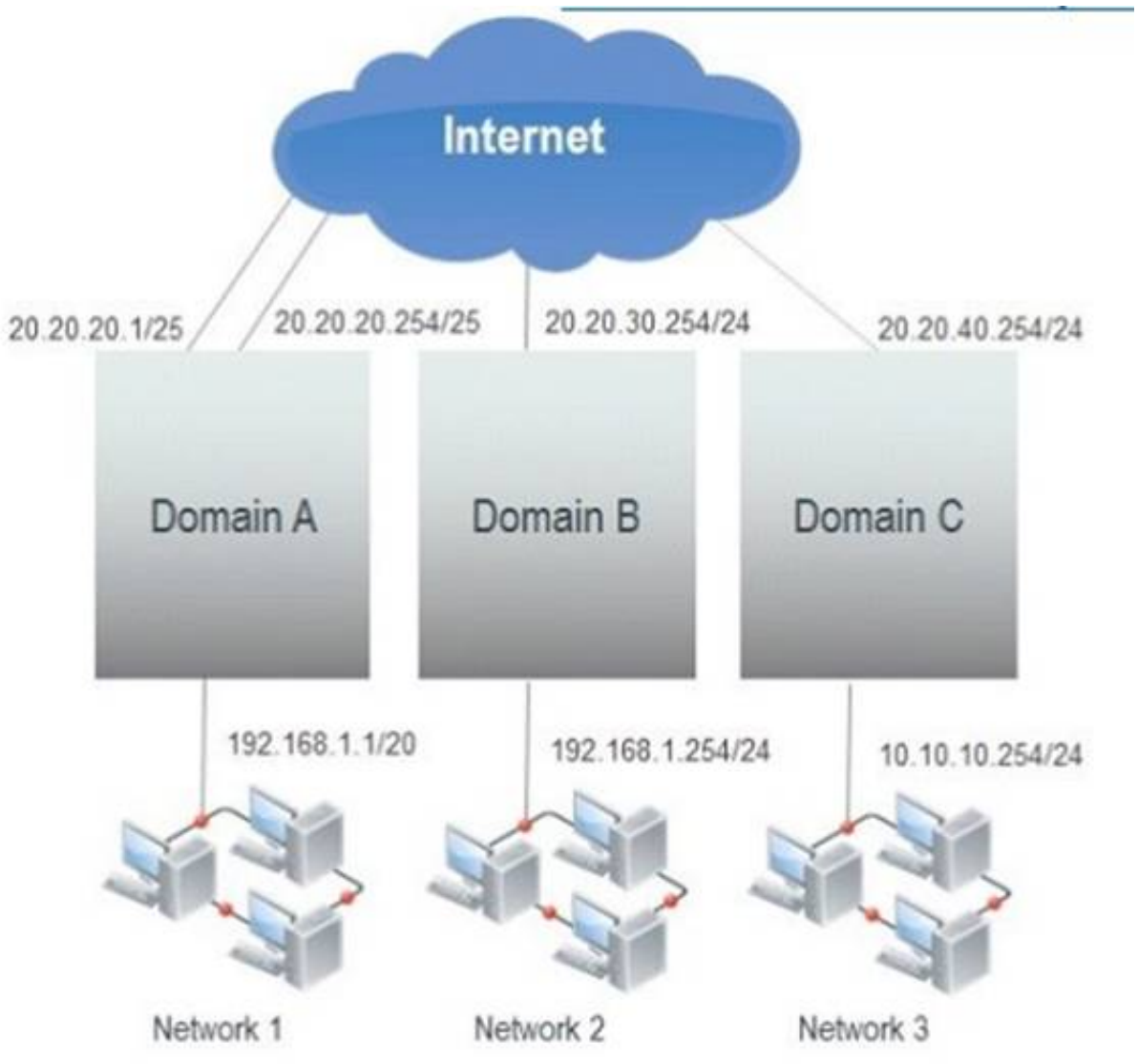
Answer: A

NEW QUESTION 141
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 143
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 146
Which authentication methods does FortiGate support for firewall authentication? (Choose two.)

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

Answer: AC

NEW QUESTION 151
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 152
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 153
The exhibit shows a part output of the diagnostic command 'diagnose debug application ike 255', taken during establishment of a VPN. Which of the following

statement are correct concerning this output? (choose two)

```
Ike 0:Remote:7:22: responder received first quick-mode message
ike 0:Remote:7:22: peer proposal is: peer:0:0.0.0.0-255.255.255.255:0, me:0:0.0.0.0-255.255.255.255:0
ike 0:Remote:7: sent IKE msg (quick_r1send): 172.20.186.222:500->172.20.187.114:500, len=356
ike 0: comes 172.20.187.114:500->172.20.186.222:500,ifindex=2....
ike 0:Remote:7:P2:22: replay protection enabled
ike 0:Remote:7:P2:22: SA life soft seconds=1750.
ike 0:Remote:7:P2:22: SA life hard seconds=1800.
ike 0:Remote:7:P2:22: IPsec SA selectors #src=1 #dst=1
ike 0:Remote:7:P2:22: src 0 7 0:0.0.0.0-255.255.255.255:0
ike 0:Remote:7:P2:22: dst 0 7 0:0.0.0.0-255.255.255.255:0
ike 0:Remote:7:P2:22: add IPsec SA: SPIs=6e13ca19/8f1ce9ae
ike 0:Remote:7:P2:22: added IPsec SA: SPIs=6e13ca19/8f1ce9ae
ike 0:Remote:7:P2:22: sending SNMP tunnel UP trap
```

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

Answer: BD

NEW QUESTION 156
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 157
Which of the following IKE modes is the one used during the IPsec phase 2 negotiation?

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

Answer: B

NEW QUESTION 159
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 160
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 165
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 170
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 173
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 175
Which are the three different types of Conserve Mode that can occur on a FortiGate device? (Choose three.)

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

Answer: ACD

NEW QUESTION 180
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 183
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 184
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 187
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 189
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 191
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 194
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 195
Which of the following options best defines what Diffie-Hellman is?

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

Answer: B

NEW QUESTION 199
What is IPsec Perfect Forwarding Secrecy (PFS)?

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

Answer: B

NEW QUESTION 204
.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questons and Answers in PDF Format

NSE4 Practice Exam Features:

* NSE4 Questions and Answers Updated Frequently

* NSE4 Practice Questions Verified by Expert Senior Certified Staff

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

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