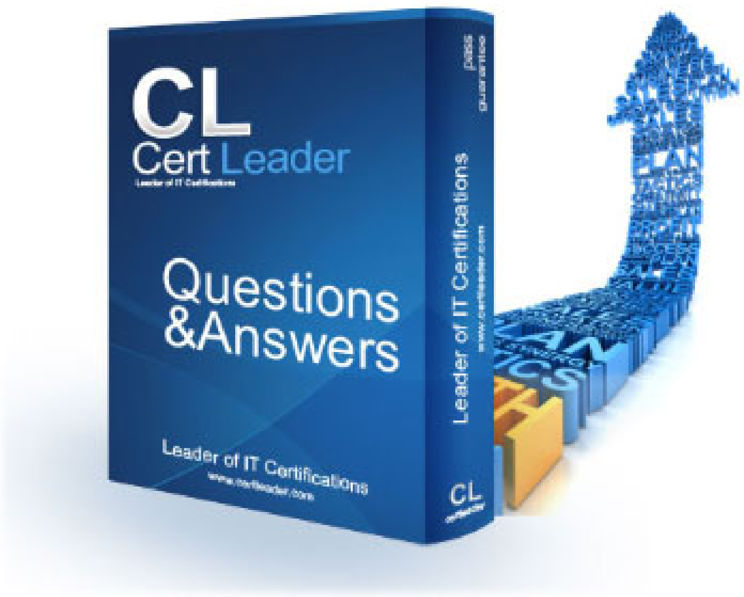
NSE4 Dumps

Fortinet Network Security Expert 4 Written Exam (400)

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



NEW QUESTION 1
A FortiGate unit operating in NAT/route mode and configured with two sub-interface on the same physical interface. Which of the following statement is correct regarding the VLAN IDs in this scenario?

A. The two VLAN sub-interfaces can have the same VLAN IDs 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 VLAN ID only if they belong to different VDOMs.
D. The two VLAN sub-interfaces can have the same VLAN if they are connected to different L2 IEEE 802.1Q complaint switches.

Answer: B

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 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 4
A new version of FortiOS firmware has just been released. When you upload new firmware, which is true?

A. If you upload the firmware image via the boot loader's menu from a TFTP server, it will not preserve the configuratio
B. But if you upload new firmware via the GUI or CLI, as long as you are following a supported upgrade path, FortiOS will attempt to convert the existing configuration to be valid with any new or changed syntax.
C. No settings are preserve
D. You must completely reconfigure.
E. No settings are preserve
F. After the upgrade, you must upload a configuration backup fil
G. FortiOS will ignore any commands that are not valid in the new O
H. In those cases, you must reconfigure settings that are not compatible with the new firmware.
I. You must use FortiConverter to convert a backup configuration file into the syntax required by the new FortiOS, then upload it to FortiGate.

Answer: A

NEW QUESTION 5
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

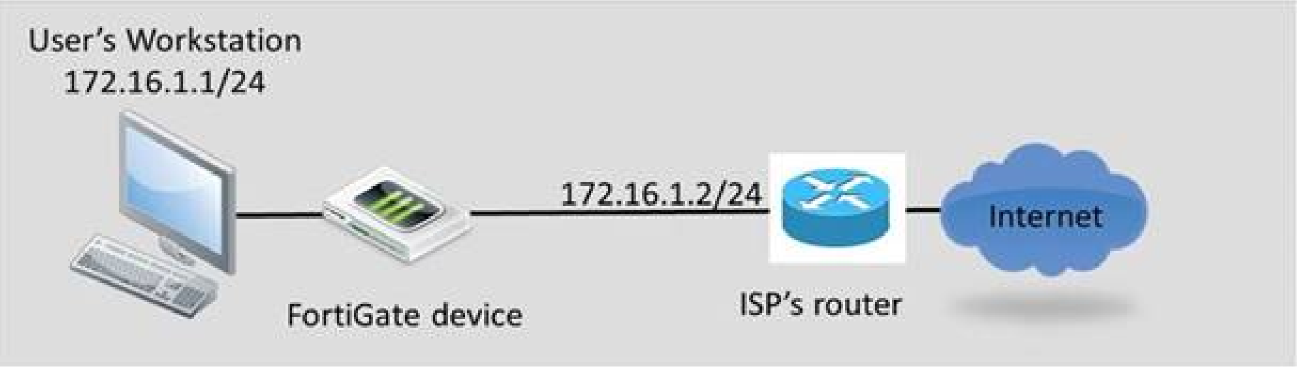
Answer: BC

NEW QUESTION 6
For traffic that does match any configured firewall policy, what is the default action taken by the FortiGate?

A. The traffic is allowed and no log is generated.
B. The traffic is allowed and logged.
C. The traffic is blocked and no log is generated.
D. The traffic is blocked and logged.

Answer: C

NEW QUESTION 7
Review to the network topology in the exhibit.



The workstation, 172.16.1.1/24, connects to port2 of the FortiGate device, and the ISP router, 172.16.1.2, connects to port1. Without changing IP addressing, which configuration changes are required to properly forward users traffic to the Internet? (Choose two)

A. At least one firewall policy from port2 to port1 to allow outgoing traffic.
B. A default route configured in the FortiGuard devices pointing to the ISP's router.
C. Static or dynamic IP addresses in both ForitGate interfaces port1 and port2.
D. The FortiGate devices configured in transparent mode.

Answer: AD

NEW QUESTION 8
Which is NOT true about source matching with firewall policies?

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

Answer: E

NEW QUESTION 9
Files reported as "suspicious" were subject to which Antivirus check"?

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

Answer: D

NEW QUESTION 10
Which header field can be used in a firewall policy for traffic matching?

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

Answer: A

NEW QUESTION 10
Which profile could IPS engine use on an interface that is in sniffer mode? (Choose three)

A. Antivirus (flow based
B. Web filtering (PROXY BASED)
C. Intrusion Protection
D. Application Control
E. Endpoint control

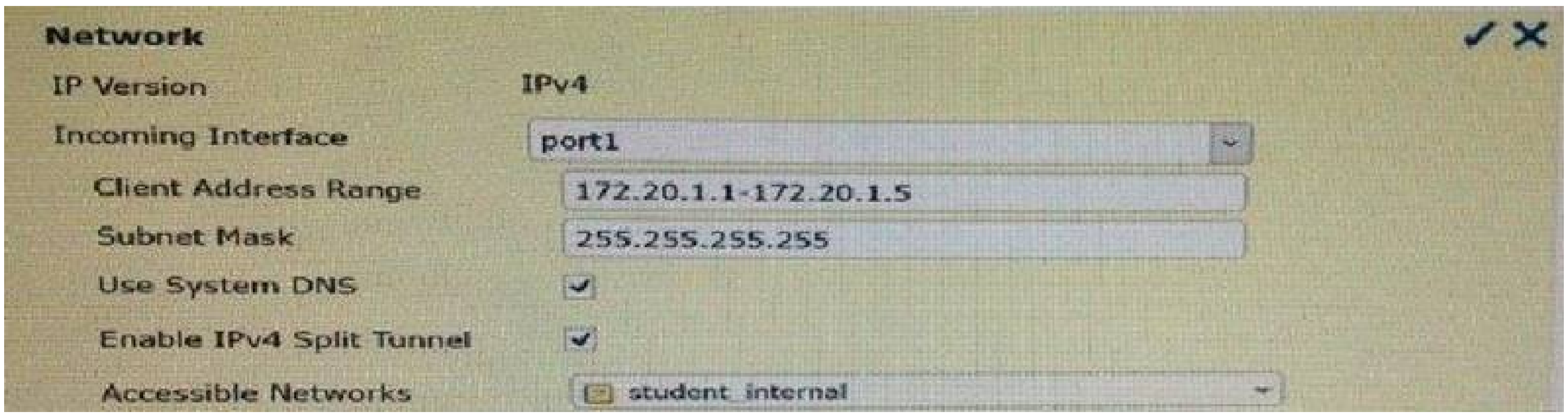
Answer: ABD

NEW QUESTION 14
The order of the firewall policies is important. Policies can be re-ordered from either the GUI or the CLI. Which CLI command is used to perform this function?

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

Answer: D

NEW QUESTION 18
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 23
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.

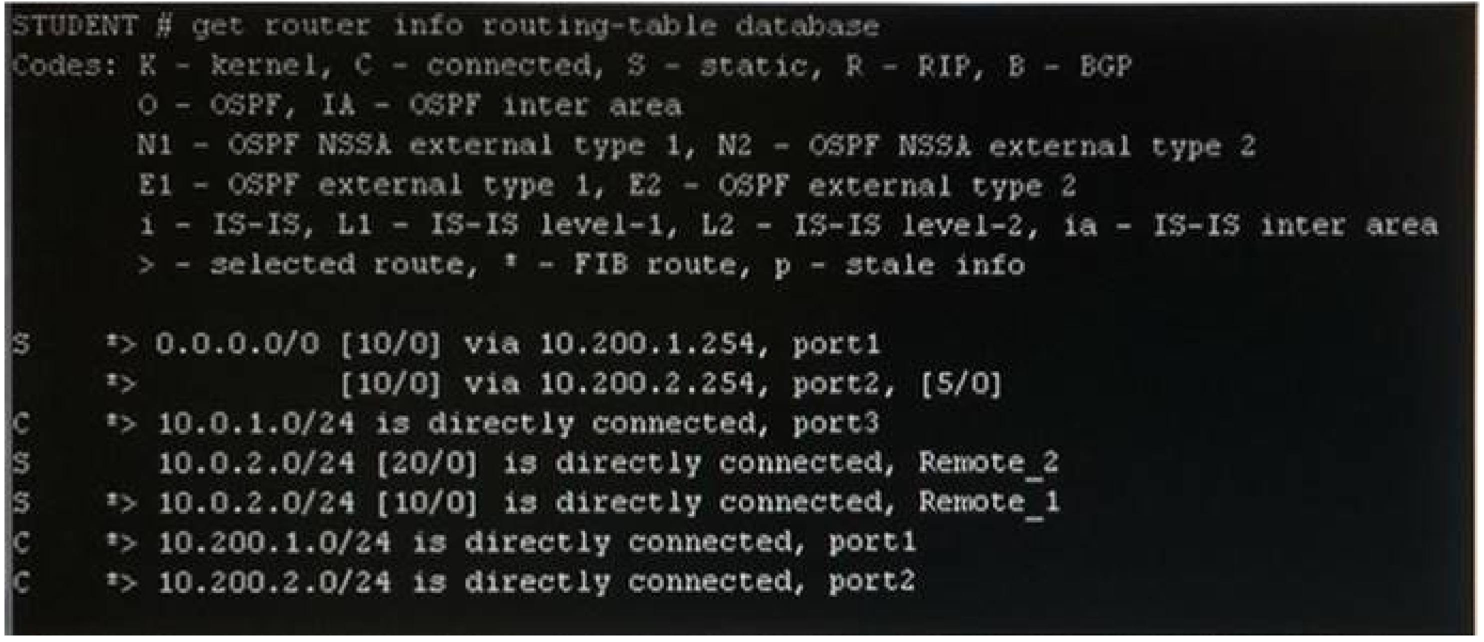
Answer: BC

NEW QUESTION 26
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 30
Review the output of the command get router info routing-table database shown in the exhibit below; then answer the question following it.



```
STUDENT # get router info routing-table database
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       > - selected route, * - FIB route, p - stale info

S     *> 0.0.0.0/0 [10/0] via 10.200.1.254, port1
      *>           [10/0] via 10.200.2.254, port2, [5/0]
C     *> 10.0.1.0/24 is directly connected, port3
S        10.0.2.0/24 [20/0] is directly connected, Remote_2
S     *> 10.0.2.0/24 [10/0] is directly connected, Remote_1
C     *> 10.200.1.0/24 is directly connected, port1
C     *> 10.200.2.0/24 is directly connected, port2
```

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

A. There will be six routes in the routing table.
B. There will be seven routes in the routing table.
C. There will be two default routes in the routing table.
D. There will be two routes for the 10.0.2.0/24 subnet in the routing table.

Answer: AC

NEW QUESTION 34
Which action does the FortiGate take when link health monitor times out?

A. All routes to the destination subnet configured in the link health monitor are removed from the routing table.
B. The distance values of all routes using interface configured in the link health monitor are increased.

C. The priority values of all routes using configured in the link health monitor are increased.
D. All routes using the next-hop gateway configured in the link health monitor are removed from the routing table.

Answer: D

NEW QUESTION 35
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 40
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 41
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 46
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 47
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 51
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 54
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 56
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 59
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 Unis 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.

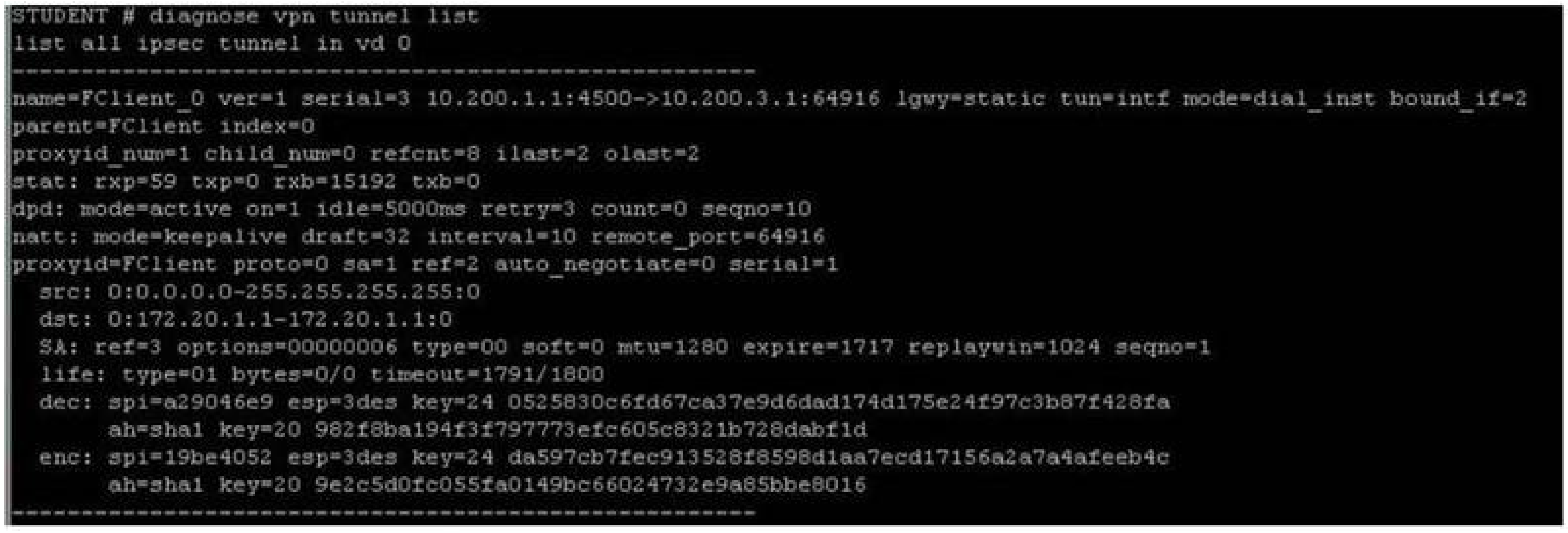
Answer: B

NEW QUESTION 64
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 67
Review the IPsec diagnostics output of the command diagnose vpn tunnel list shown in the exhibit below.



```
STUDENT # diagnose vpn tunnel list
list all ipsec tunnel in vd 0
------------------------------------------------------
name=FClient_0 ver=1 serial=3 10.200.1.1:4500->10.200.3.1:64916 lgwy=static tun=intf mode=dial_inst bound_if=2
parent=FClient index=0
proxyid_num=1 child_num=0 refcnt=8 ilast=2 olast=2
stat: rxp=59 txp=0 rxb=15192 txb=0
dpd: mode=active on=1 idle=5000ms retry=3 count=0 seqno=10
natt: mode=keepalive draft=32 interval=10 remote_port=64916
proxyid=FClient proto=0 sa=1 ref=2 auto_negotiate=0 serial=1
  src: 0:0.0.0.0-255.255.255.255:0
  dst: 0:172.20.1.1-172.20.1.1:0
  SA: ref=3 options=00000006 type=00 soft=0 mtu=1280 expire=1717 replaywin=1024 seqno=1
  life: type=01 bytes=0/0 timeout=1791/1800
  dec: spi=a29046e9 esp=3des key=24 0525830c6fd67ca37e9d6dad174d175e24f97c3b87f428fa
       ah=sha1 key=20 982f8ba194f3f797773efc605c8321b728dabf1d
  enc: spi=19be4052 esp=3des key=24 da597cb7fec913528f8598d1aa7ecd17156a2a7a4afeeb4c
       ah=sha1 key=20 9e2c5d0fc055fa0149bc66024732e9a85bbe8016
------------------------------------------------------
```

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

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

Answer: AB

NEW QUESTION 68
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 71
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 74
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 76
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 81
When configuring LDAP on the FortiGate as a remote database for users, what is not a part of the configuration?

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

Answer: C

NEW QUESTION 84
Which of the following statements best describes what a Public Certificate Authority (CA) is?

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

Answer: D

NEW QUESTION 88
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 93
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 95
A FortiGate unit has multiple VDOMs in NAT/route mode with multiple VLAN interfaces in each VDOM. Which of the following statements is correct regarding the IP addresses
assigned to each VLAN interface?

A. Different VLANs can share the same IP address as long as they have different VLAN IDs.
B. Different VLANs can share the same IP address as long as they are in different physical interface.
C. Different VLANs can share the same IP address as long as they are in different VDOMs.
D. Different VLANs can never share the same IP addresses.

Answer: C

NEW QUESTION 99
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 100
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 104
What attributes are always included in a log header? (Choose three.)

A. policyid
B. level
C. user
D. time
E. subtype
F. duration

Answer: BDE

NEW QUESTION 109
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 112
Which of the following spam filtering methods are supported on the FortiGate unit? (Select all that apply.)

A. IP Address Check
B. Open Relay Database List (ORDBL)
C. Black/White List
D. Return Email DNS Check
E. Email Checksum Check

Answer: ABCDE

NEW QUESTION 116
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 120
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 122
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 126
Which is the following statement are true regarding application control? (choose two)

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

Answer: CD

NEW QUESTION 131
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 132
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 134
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 136
Which best describe the mechanism of a TCP SYN flood?

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

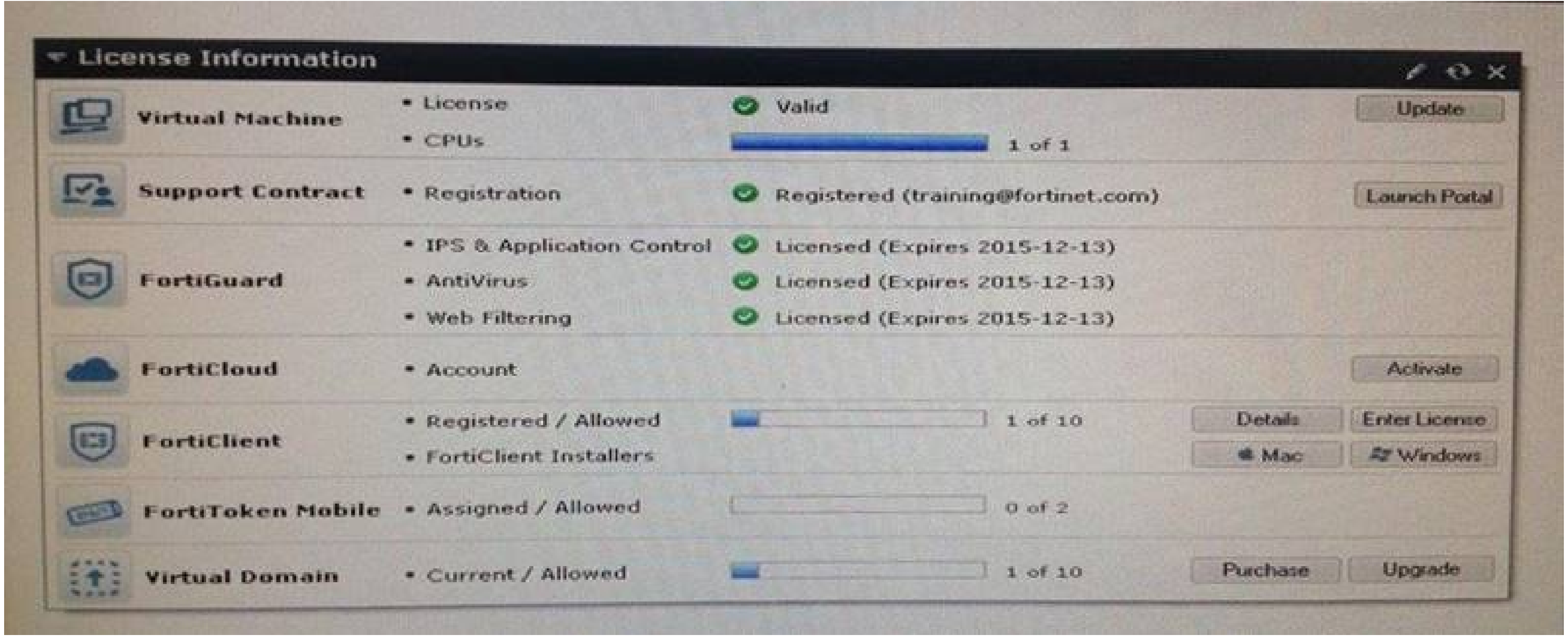
Answer: D

NEW QUESTION 141
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 142
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 146
Which traffic can match a firewall policy's "Services" setting? (Choose three.)

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

Answer: ACE

NEW QUESTION 147
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 150
Which of the following statements describe some of the differences between symmetric and asymmetric cryptography? (Choose two.)

A. In symmetric cryptography, the keys are publicly availabl
B. In asymmetric cryptography, the keys must be kept secret.
C. Asymmetric cryptography can encrypt data faster than symmetric cryptography
D. Symmetric cryptography uses one pre-shared ke
E. Asymmetric cryptography uses a pair or keys
F. Asymmetric keys can be sent to the remote peer via digital certificate
G. Symmetric keys cannot

Answer: CD

NEW QUESTION 155
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 157
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 160
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 161
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 165
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.

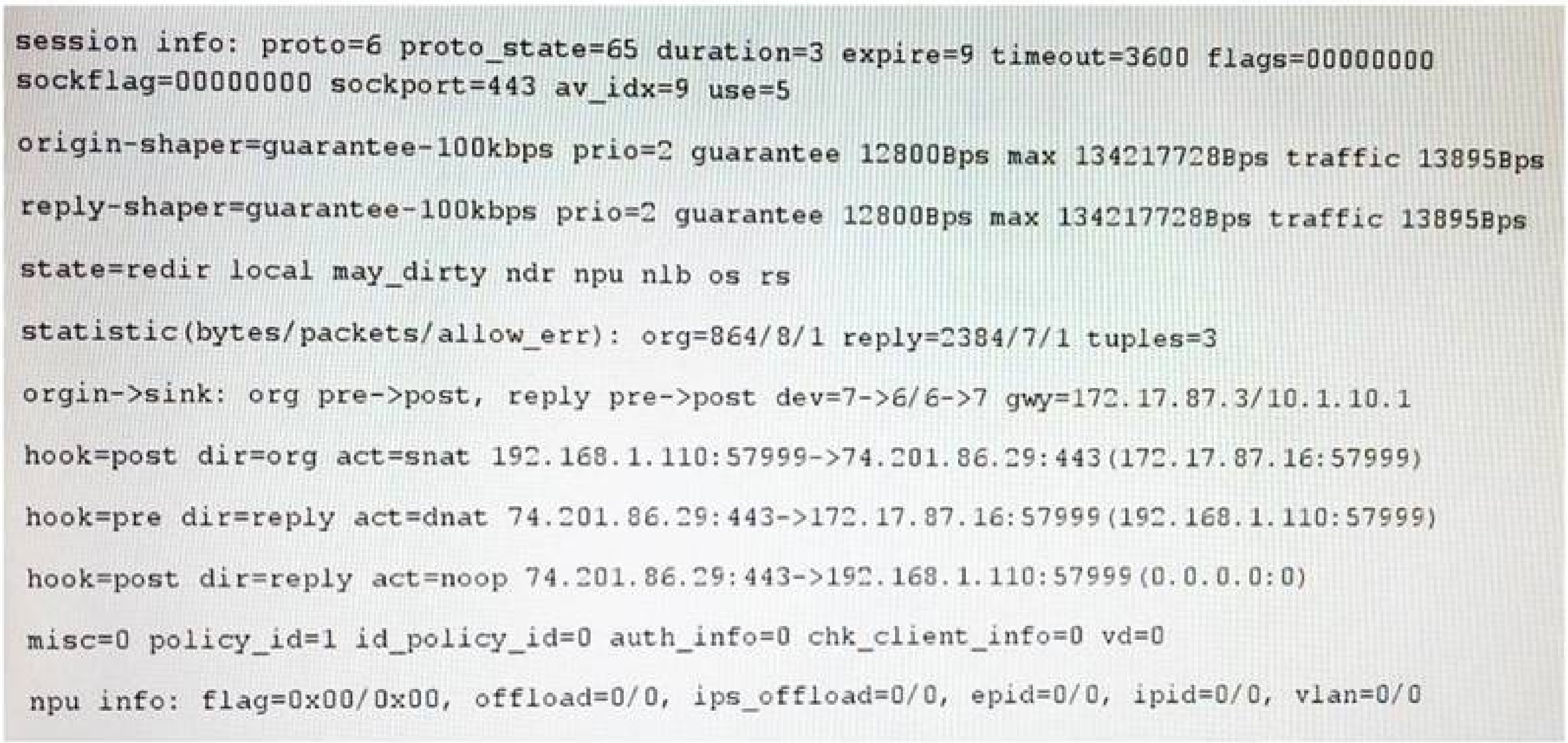
Answer: AD

NEW QUESTION 168
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 170
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 174
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 175
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 176
Which of the following statements best describe the main requirements for a traffic session to be offload eligible to an NP6 processor? (Choose three.)

A. Session packets do NOT have an 802.1Q VLAN tag.
B. It is NOT multicast traffic.
C. It does NOT require proxy-based inspection.
D. Layer 4 protocol must be UDP, TCP, SCTP or ICMP.
E. It does NOT require flow-based inspection.

Answer: CDE

NEW QUESTION 180
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 183
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 184
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 185
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 186
Which of the following statements are true regarding WAN Link Load Balancing? (Choose two).

A. There can be only one virtual WAN Link per VDOM.
B. FortiGate can measure the quality of each link based on latency, jitter, or packets percentage.
C. Link health checks can be performed over each link member if the virtual WAN interface.
D. Distance and priority values are configured in each link member if the virtual WAN interface.

Answer: AC

NEW QUESTION 190
Which antivirus and attack definition update options are supported by FortiGate units? (Choose two.)

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

Answer: ABC

NEW QUESTION 192
Which statement describes how traffic flows in sessions handled by a slave unit in an active-active HA cluster?

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

Answer: D

NEW QUESTION 195
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 199
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 203
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 206
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 211
A static route is configured for a FortiGate unit from the CLI using the following commands:
config router static edit 1
set device “wan1” set distance 20
set gateway 192.168.100.1 next
end
Which of the following conditions are required for this static default route to be displayed in the FortiGate unit's routing table? (Choose two.)

A. The administrative status of the wan1 interface is displayed as down.
B. The link status of the wan1 interface is displayed as up.
C. All other default routers should have a lower distance.
D. The wan1 interface address and gateway address are on the same subnet.

Answer: BD

NEW QUESTION 214
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 215
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 218
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 222
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 227
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 232
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 236
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 241
What types of troubleshooting can you do when uploading firmware? (Choose two.)

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

Answer: AD

NEW QUESTION 242
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 245
Examine the following log message attributes and select two correct statements from the list below. (Choose two.)
hostname=www.youtube.com profiletype="Webfilter_Profile" profile="default" status="passthrough" msg="URL belongs to a category with warnings enabled"

A. The traffic was blocked.
B. The user failed authentication.
C. The category action was set to warning.
D. The website was allowed

Answer: CD

NEW QUESTION 250
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 255
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 258
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 263
When does a FortiGate load-share traffic between two static routes to the same destination subnet?

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

Answer: D

NEW QUESTION 268
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 273
Which IP packets can be hardware-accelerated by a NP6 processor? (Choose two.)

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

Answer: BC

NEW QUESTION 275
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.

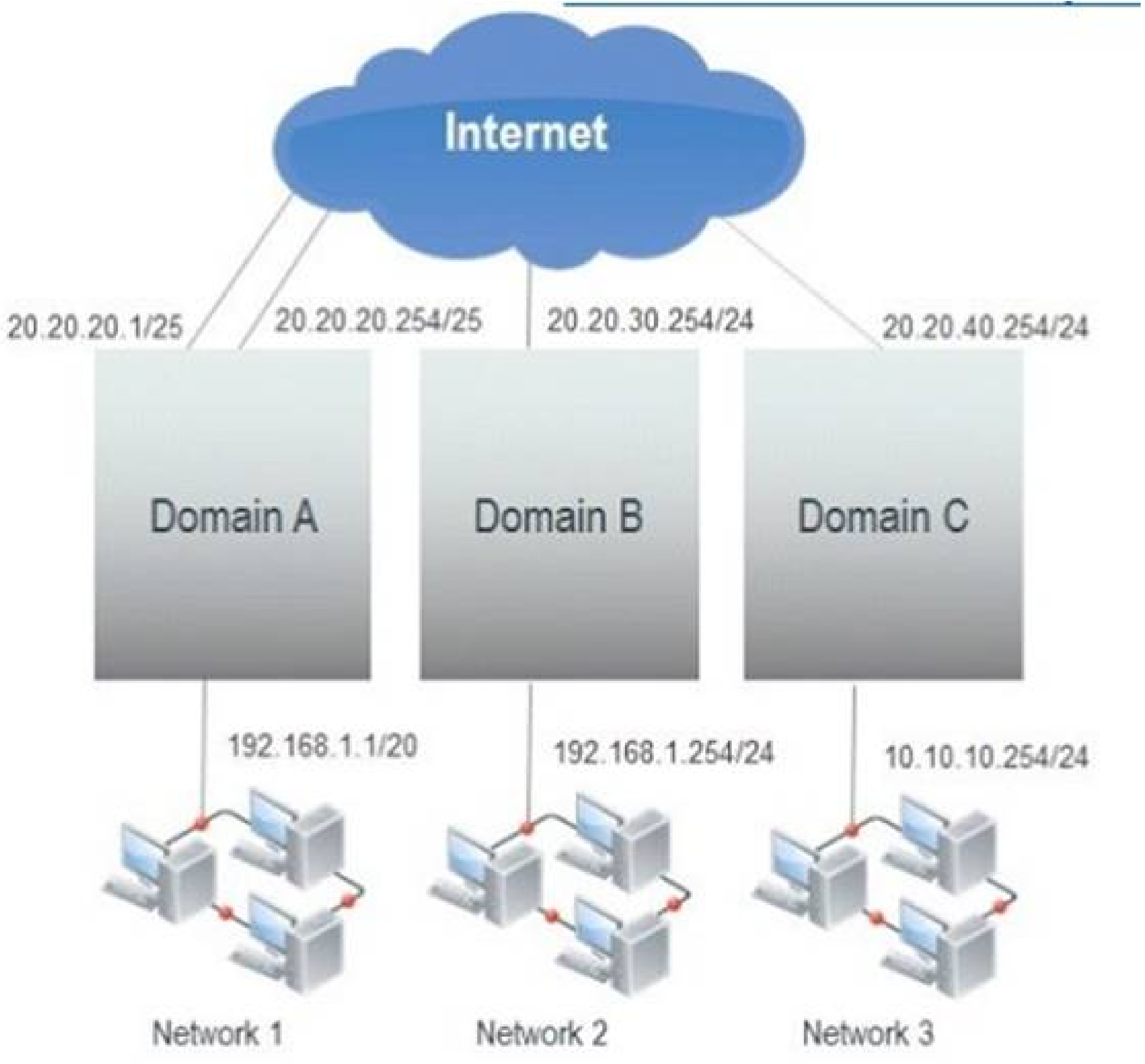
Answer: AD

NEW QUESTION 280
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 282
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 287
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 290
Regarding the use of web-only mode SSL VPN, which statement is correct?

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

Answer: C

NEW QUESTION 294
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

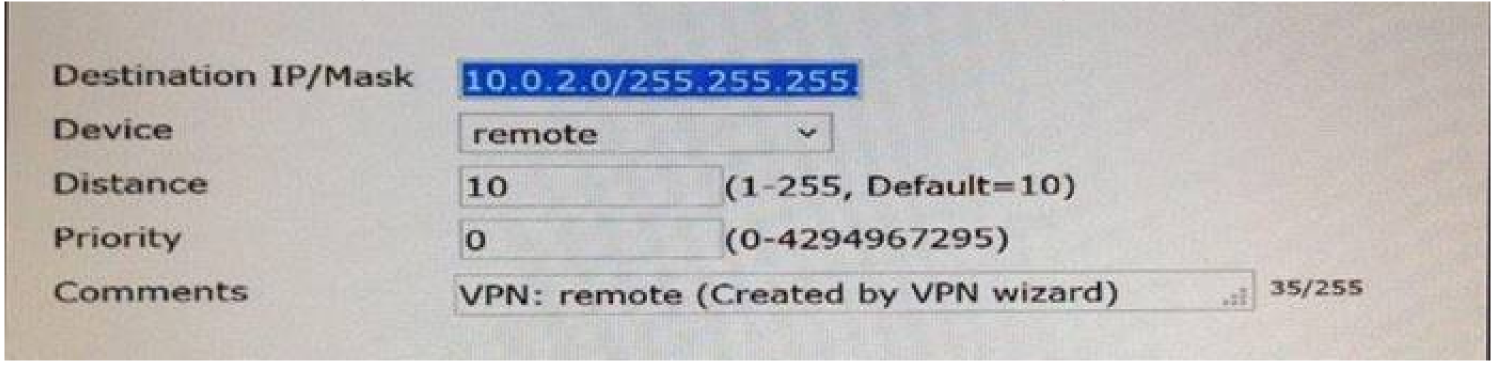
Answer: ABD

NEW QUESTION 297
Which web filtering inspection mode inspects DNS traffic?

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

Answer: A

NEW QUESTION 301
Review the static route configuration for IPsec shown in the exhibit; then answer the question below.



Destination IP/Mask 10.0.2.0/255.255.255
Device remote
Distance 10 (1-255, Default=10)
Priority 0 (0-4294967295)
Comments VPN: remote (Created by VPN wizard) 35/255

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

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

Answer: AB

NEW QUESTION 304
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 305
Which of the following statements are correct differences between NAT/route and transparent mode? (Choose two.)

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

Answer: AC

NEW QUESTION 310
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 314
Which of the following regular expression patterns makes the terms “confidential data” case insensitive?

A. [confidential data]
B. /confidential data/i
C. i/confidential data/
D. “confidential data”

Answer: B

NEW QUESTION 319
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 321
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 326
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 330
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 333
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.

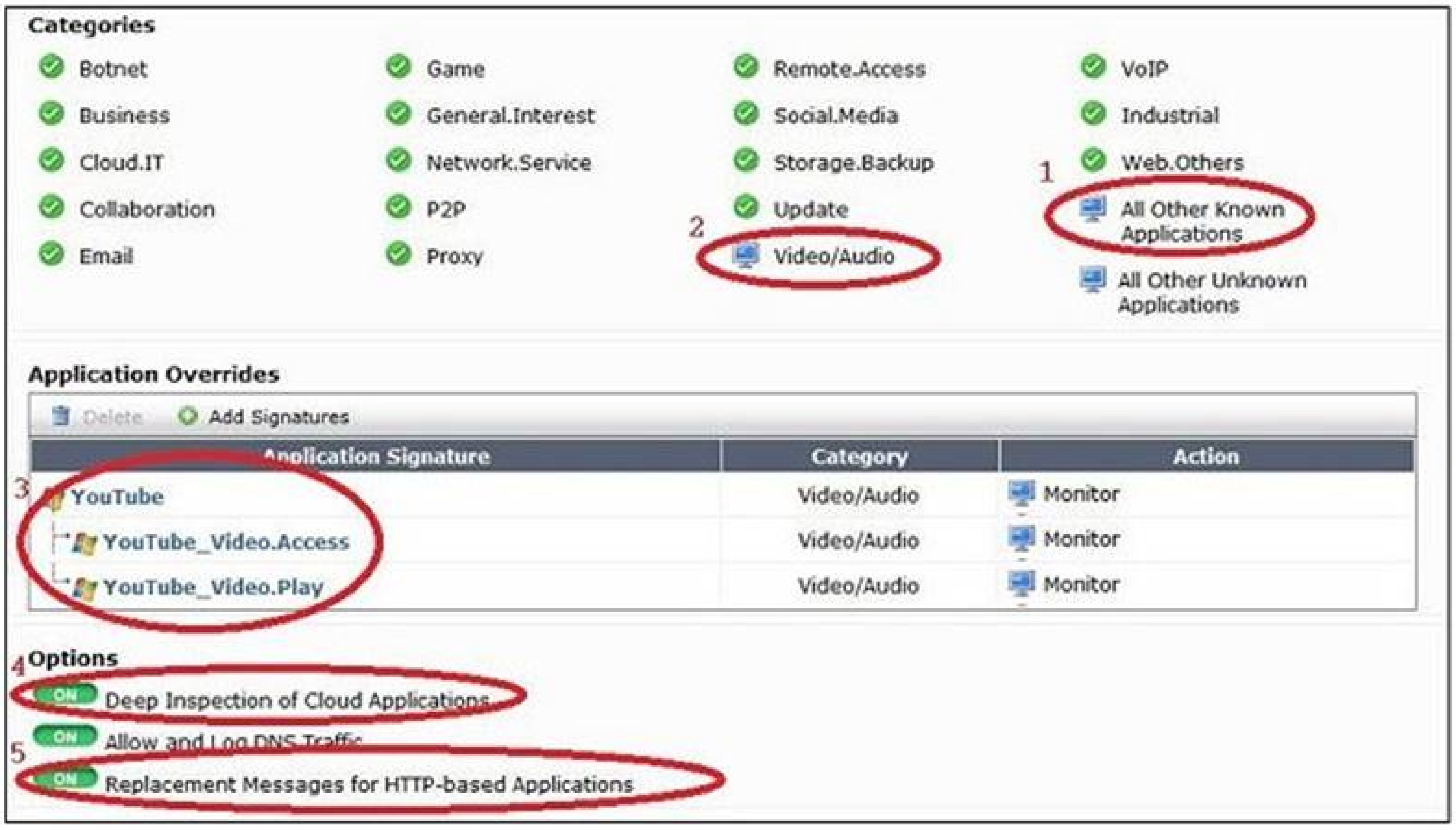
Answer: BC

NEW QUESTION 336
Which authentication scheme is not supported by the RADIUS implementation on FortiGate?

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

Answer: D

NEW QUESTION 340
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

- ON Deep Inspection of Cloud Applications
- ON Allow and Log DNS Traffic
- ON 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 343

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 348

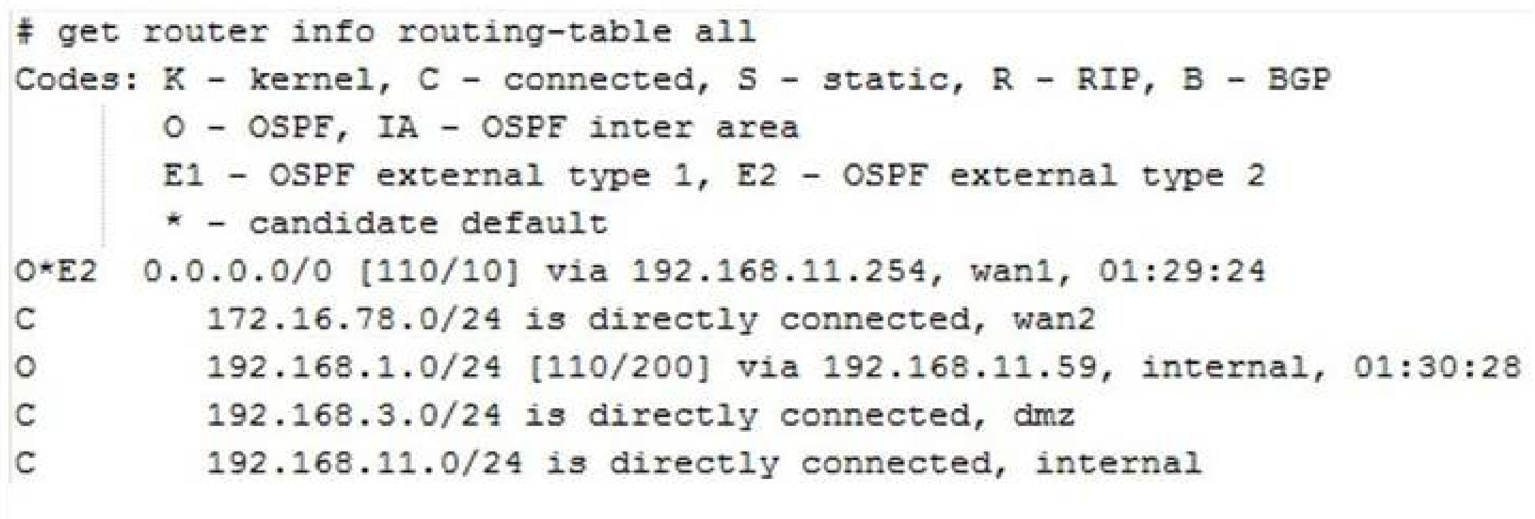
Which of the following statements are correct regarding logging to memory on a FortiGate unit?

A. When the system has reached its capacity for log messages, the FortiGate unit will stop logging to memory.
B. When the system has reached its capacity for log messages, the FortiGate unit overwrites the oldest messages.
C. If the FortiGate unit is reset or loses power, log entries captured to memory will be lost.
D. None of the above.

Answer: BC

NEW QUESTION 352

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 357
Which statements correctly describe transparent mode operation? (Choose three.)

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

Answer: ABD

NEW QUESTION 360
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 362
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

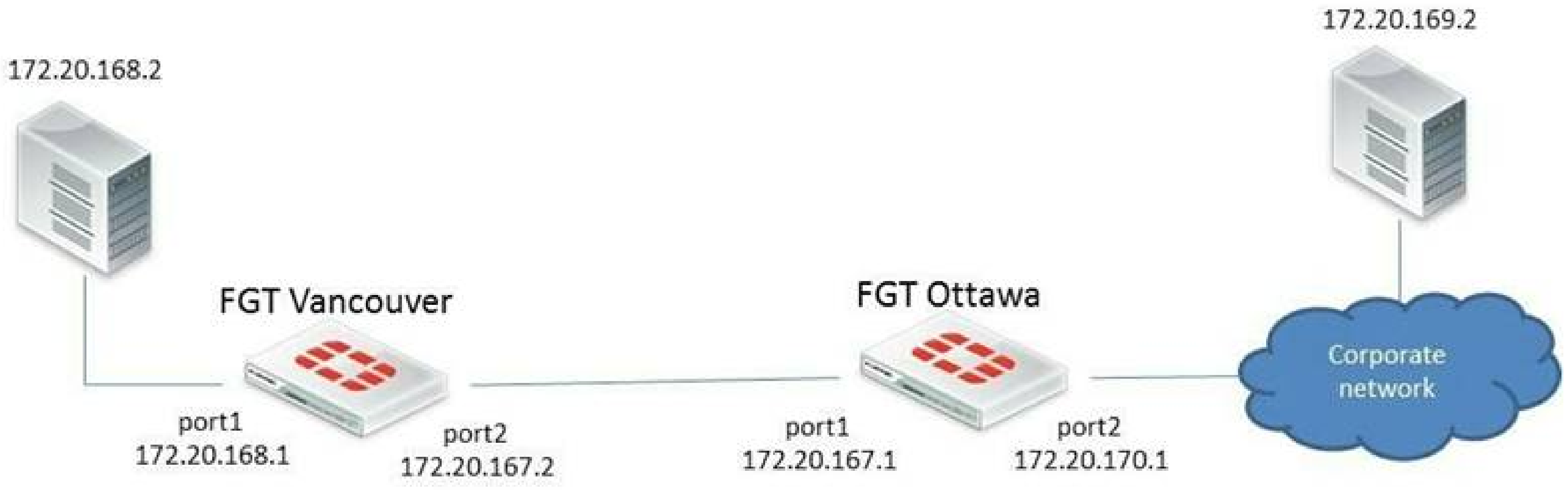
NEW QUESTION 367
Examine this log entry.
What does the log indicate? (Choose three.)

```
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 370
Examine the exhibit below; then answer the question following it.



In this scenario. The FortiGate unit in Ottawa has the following routing table:
s*0.0.0.0/0 [10/0] via 172.20.170.254, port2
c172.20.167.0/24 is directly connected, port1 c172.20.170.0/24 is directly connected, port2
Sniffer tests show that packets sent from the source IP address 170.20.168.2 to the destination IP address 172.20.169.2 are being dropped by the FortiGate

located in Ottawa.
Which of the following correctly describes the cause for the dropped packets?

A. The forward policy check.
B. The reserve path forwarding check.
C. The subnet 172.20.169.0/24 is NOT in the Ottawa FortiGate's routing table.
D. The destination workstation 172.20.169.2 does NOT have the subnet 172.20.168.0/24 in its routing table.

Answer: B

NEW QUESTION 373
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 377
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 379
What must be configured in order to keep two static routes to the same destination in the routing table?

A. The same priority.
B. The same distance and same priority.
C. The same distance.
D. The same metric.

Answer: B

NEW QUESTION 380
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 382
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 383
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 384
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 389
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 392
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.

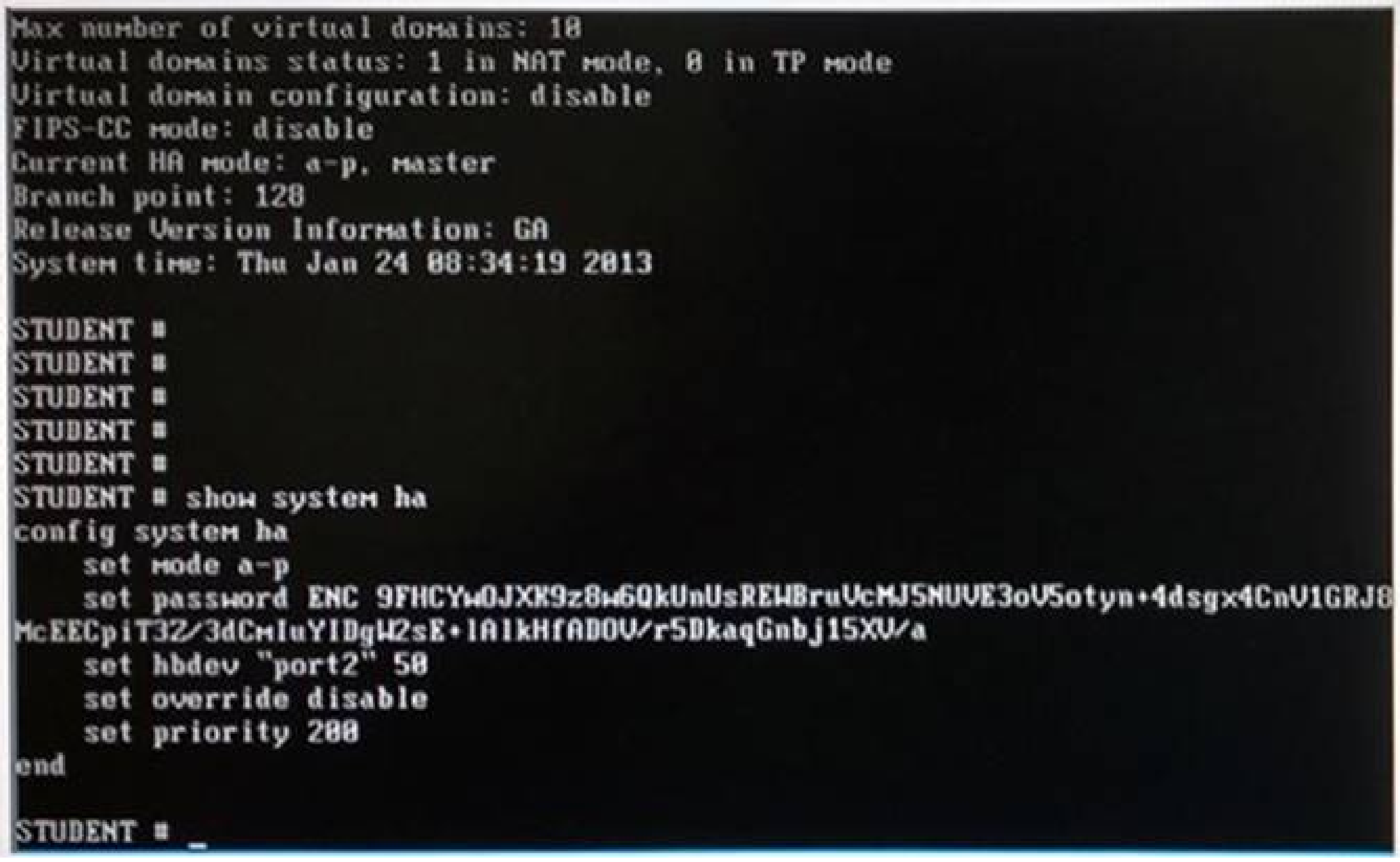
Answer: D

NEW QUESTION 395
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 397
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:

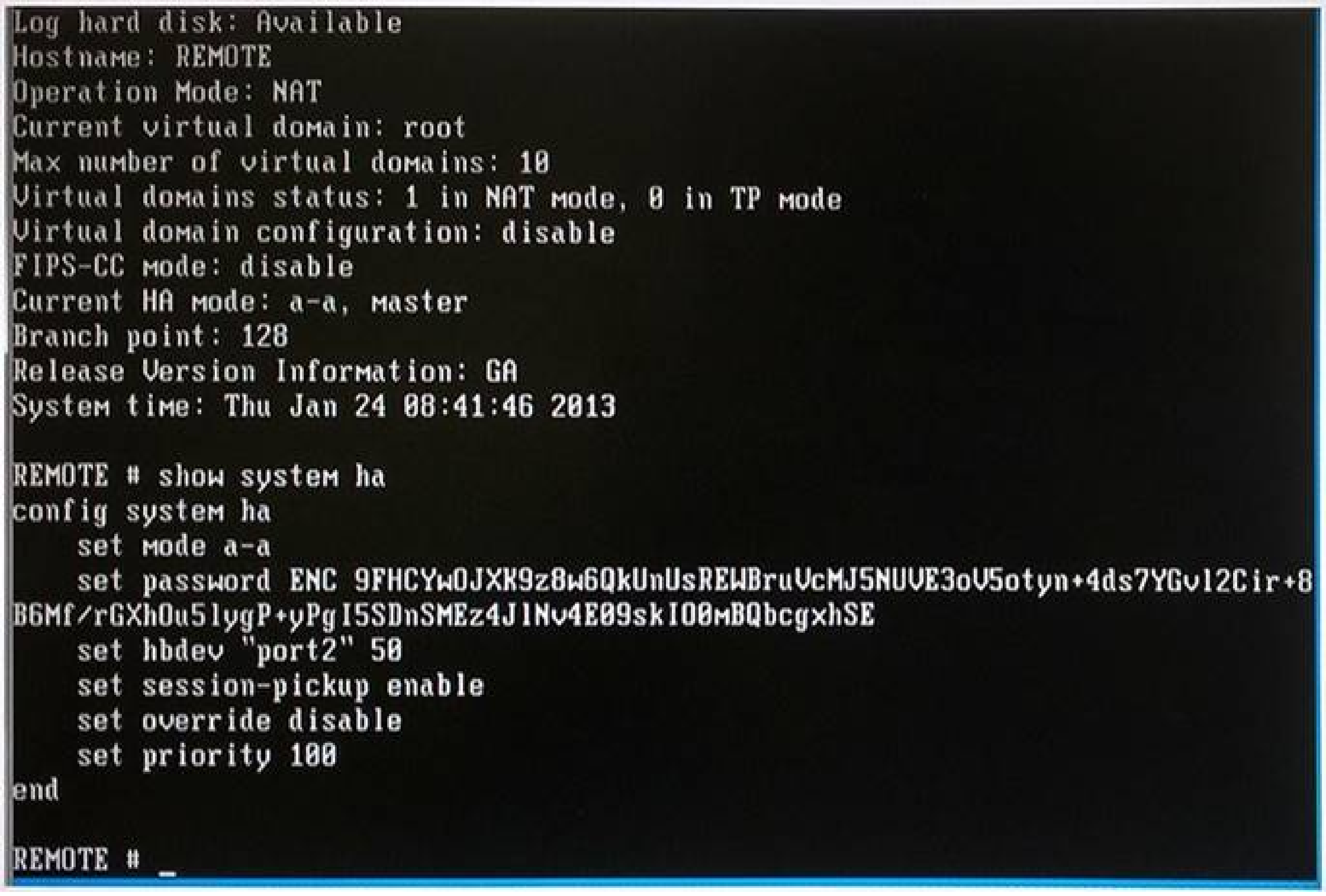


```
Max number of virtual domains: 10
Virtual domains status: 1 in NAT mode, 0 in TP mode
Virtual domain configuration: disable
FIPS-CC mode: disable
Current HA mode: a-p, master
Branch point: 128
Release Version Information: GA
System time: Thu Jan 24 08:34:19 2013

STUDENT #
STUDENT #
STUDENT #
STUDENT #
STUDENT #
STUDENT # show system ha
config system ha
    set mode a-p
    set password ENC 9FHCYwOJXK9z8w6QkUnUsREWBruVcMJ5NUVE3oV5otyn+4dsgx4CnV1GRJ8
McEECpiT32/3dCmIuYIDgW2sE+1A1kHfADOV/r5DkaqGnbj15XV/a
    set hbdev "port2" 50
    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 9FHCYwOJXK9z8w6QkUnUsREWBruVcMJ5NUVE3oV5otyn+4ds7YGvl2Cir+8
B6Mf/rGXhOu5lygP+yPgI5SDnSMEz4JlNv4E09skI00mBQbcgxhSE
    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 400
What are the advantages of FSSO DC mode over polling mode?

A. Redundancy in the collector agent.
B. Allows transparent authentication.
C. DC agents are not required in the AD domain controllers.
D. Scalability

Answer: C

NEW QUESTION 403
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.

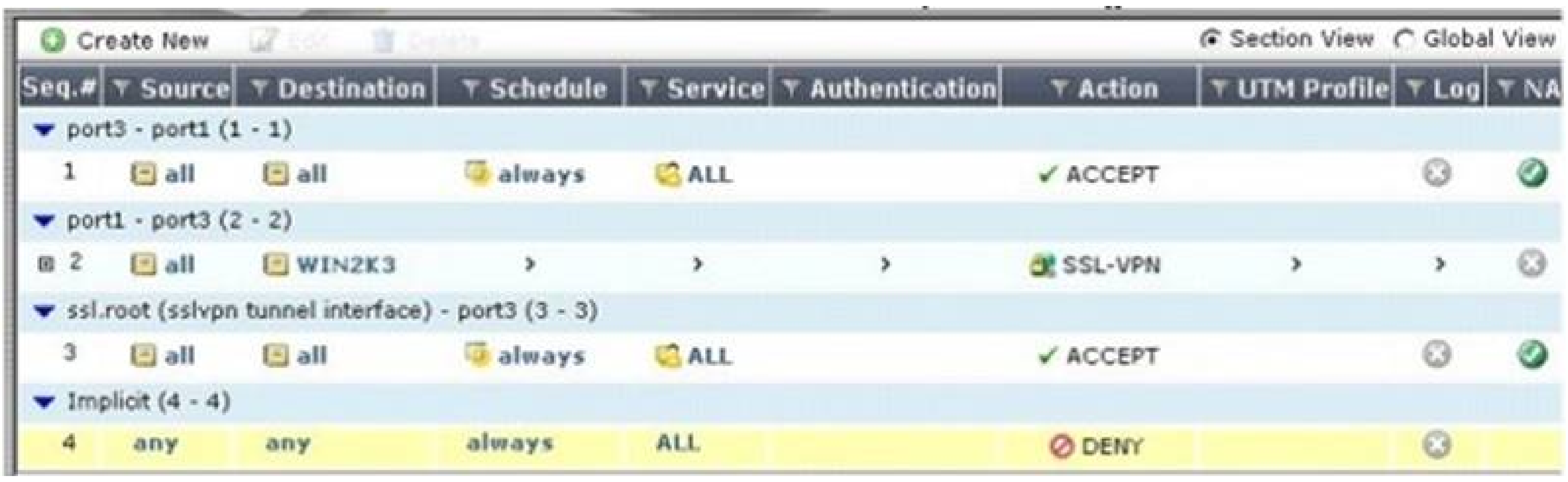
Answer: C

NEW QUESTION 406
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 408
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 411
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 414
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 418
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 419
Which tasks fall under the responsibility of the SSL proxy in a typical HTTPS connection?
(Choose two.)

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

Answer: AB

NEW QUESTION 423
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 426
Which of the following statements are true about PKI users created in a FortiGate device? (Choose two.)

A. Can be used for token-based authentication
B. Can be used for two-factor authentication
C. Are used for certificate-based authentication
D. Cannot be members of user groups

Answer: AB

NEW QUESTION 431
......