Fortinet

Exam Questions NSE4

Fortinet Network Security Expert 4 Written Exam (400)

NEW QUESTION 1
Examine the two static routes to the same destination subnet 172.20.168.0/24 as shown below; then answer the question following it.

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

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

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

Answer: C

NEW QUESTION 2
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 3
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.

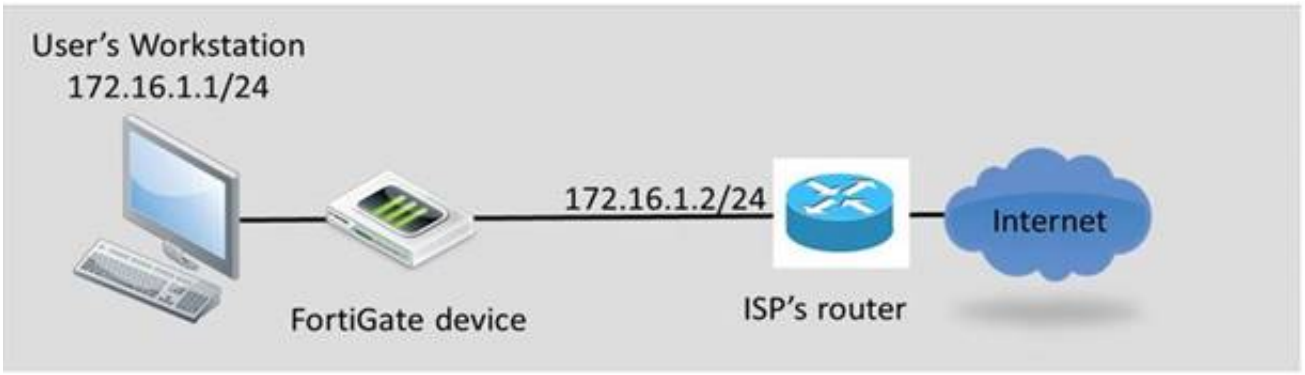
Answer: B

NEW QUESTION 4
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 5
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 6
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 7
Files reported as "suspicious" were subject to which Antivirus check"?

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

Answer: D

NEW QUESTION 8
Which statements are correct for port pairing and forwarding domains? (Choose two.)

A. They both create separate broadcast domains.
B. Port Pairing works only for physical interfaces.
C. Forwarding Domain only applies to virtual interfaces
D. They may contain physical and/or virtual interfaces.

Answer: AD

NEW QUESTION 9
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 10
Which statements are correct regarding virtual domains (VDOMs)? (Choose two)

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

Answer: BC

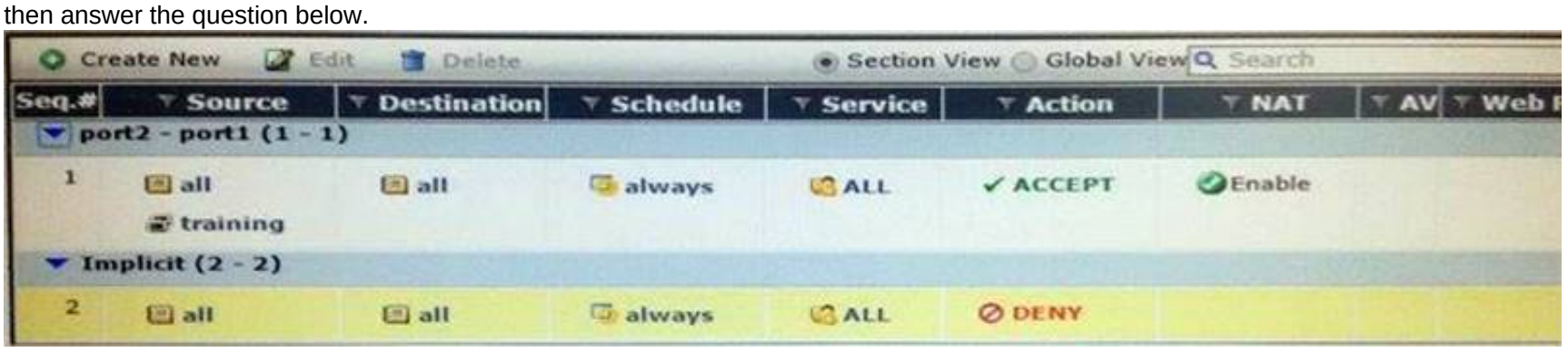
NEW QUESTION 10
Which action does the FortiGate take when link health monitor times out?

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 13
The FortiGate port1 is connected to the Internet. The FortiGate port2 is connected to the internal network. Examine the firewall configuration shown in the exhibit; then answer the question below.



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

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

Answer: D

NEW QUESTION 18
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 19
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 24
Two devices are in an HA cluster, the device hostnames are STUDENT and REMOTE. Exhibit A shows the command output of diagnose sys session stat for the STUDENT device. Exhibit B shows the command output of diagnose sys session stat for the REMOTE device.
Exhibit A:

```
STUDENT # diagnose sys session stat
misc info:      session_count=166 setup_rate=68 exp_count=0 clash=0
        memory_tension_drop=0 ephemeral=0/57344 removeable=0  ha_scan=0
delete=0, flush=0, dev_down=0/0
TCP sessions:
         8 in ESTABLISHED state
         3 in SYN_SENT state
         1 in FIN_WAIT state
         139 in TIME_WAIT state
firewall error stat:
error1=00000000
error2=00000000
error3=00000000
error4=00000000
tt=00000000
cont=00000000
ids_recv=00000000
url_recv=00000000
av_recv=00000000
fqdn_count=00000000
tcp reset stat:
        syncqf=0 acceptqf=0 no-listener=2 data=0 ses=0 ips=0
global: ses_limit=0 ses6_limit=0 rt_limit=0 rt6_limit=0

STUDENT # _
```

Exhibit B:

```
global: ses_limit=0 ses6_limit=0 rt_limit=0 rt6_limit=0

REMOTE # diagnose sys session stat
misc info:       session_count=11 setup_rate=0 exp_count=0 clash=4
        memory_tension_drop=0 ephemeral=0/57344 removeable=0  ha_scan=0
delete=0, flush=0, dev_down=0/0
TCP sessions:
         2 in ESTABLISHED state
         1 in SYN_SENT state
firewall error stat:
error1=00000000
error2=00000000
error3=00000000
error4=00000000
tt=00000000
cont=00000000
ids_recv=00000000
url_recv=00000000
av_recv=00000000
fqdn_count=00000000
tcp reset stat:
        syncqf=0 acceptqf=0 no-listener=7 data=0 ses=0 ips=0
global: ses_limit=0 ses6_limit=0 rt_limit=0 rt6_limit=0

REMOTE # _
```

Given the information provided in the exhibits, which of the following statements are correct? (Choose two.)

A. STUDENT is likely to be the master device.
B. Session-pickup is likely to be enabled.
C. The cluster mode is active-passive.
D. There is not enough information to determine the cluster mode.

Answer: AD

NEW QUESTION 28
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 30
You are creating a custom signature. Which has incorrect syntax?

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

Answer: A

NEW QUESTION 33
What is not true of configuring disclaimers on the FortiGate?

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

Answer: C

NEW QUESTION 38
Which statements are true regarding traffic shaping that is applied in an application sensor, and associated with the firewall policy? (Choose two.)

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

Answer: BC

NEW QUESTION 41
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 45
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 47
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 49
In a Crash log, what does a status of 0 indicate?

A. Abnormal termination of a process
B. A process closed for any reason
C. Scanunitd process crashed
D. Normal shutdown with no abnormalities
E. DHCP process crashed

Answer: D

NEW QUESTION 52
Regarding tunnel-mode SSL VPN, which three statements are correct? (Choose three.)

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

Answer: ABE

NEW QUESTION 53
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 58
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 63
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 64
Which best describes the mechanism of a TCP SYN flood?

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

Answer: D

NEW QUESTION 69
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 74
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 76
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.

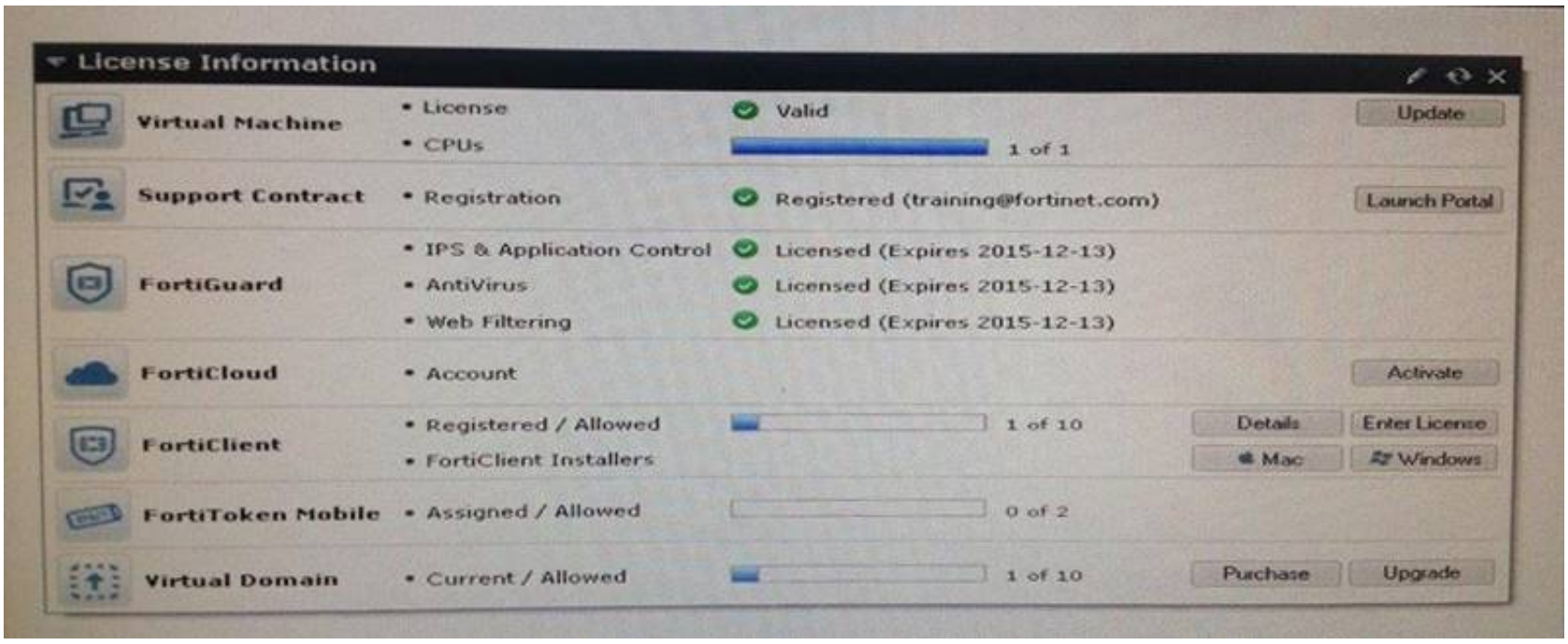
Answer: D

NEW QUESTION 81
Which of the following are possible actions for static URL filtering? (Choose three.)

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

Answer: ABC

NEW QUESTION 82
Examine the exhibit; then answer the question below.



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 85
Which of the following statements are correct concerning the FortiGate session life support protocol? (Choose two)

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

Answer: AD

NEW QUESTION 87
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 88
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 91
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 94
Which network protocols are supported for administrative access to a FortiGate unit? (Choose three.)

A. SMTP
B. WINS
C. HTTP
D. Telnet
E. SSH

Answer: CDE

NEW QUESTION 96
Which statement best describes what a Fortinet System on a Chip (SoC) is?

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

Answer: B

NEW QUESTION 99
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 100
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.

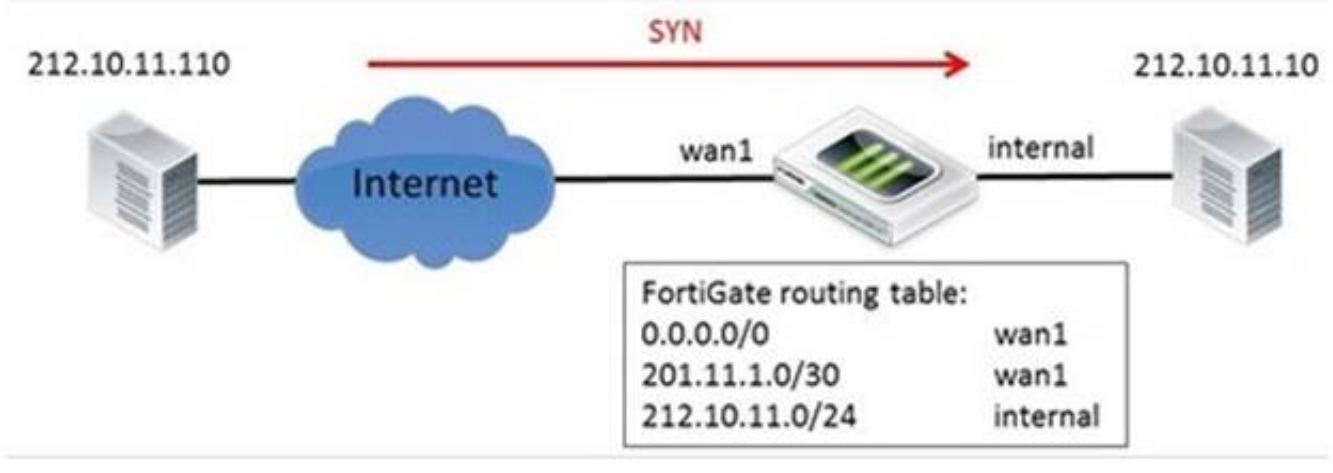
Answer: A

NEW QUESTION 104
Which of the following items is NOT a packet characteristic matched by a firewall service object?

A. ICMP type and code
B. TCP/UDP source and destination ports
C. IP protocol number
D. TCP sequence number

Answer: D

NEW QUESTION 105
Examine the network topology diagram in the exhibit; the workstation with the IP address 212.10.11.110 sends a TCP SYN packet to the workstation with the IP address 212.10.11.20.



Which of the following sentences best describes the result of the reverse path forwarding (RFP) check executed by the FortiGate on the SYN packets? (Choose two).

A. Packets is allowed if RPF is configured as loose.
B. Packets is allowed if RPF is configured as strict.
C. Packets is blocked if RPF is configured as loose.
D. Packets is blocked if RPF is configured as strict.

Answer: AD

NEW QUESTION 106
In a FSSO agentless polling mode solution, where must the collector agent be?

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

Answer: D

NEW QUESTION 110
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 114
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 119
Which of the following IPsec configuration modes can be used when the FortiGate is running in NAT mode?

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

Answer: B

NEW QUESTION 120
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 122
Which type of conserve mode writes a log message immediately, rather than when the device exits conserve mode?

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

Answer: B

NEW QUESTION 126
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 131
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 136
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 138
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 142
Which statement is one disadvantage of using FSSO NetAPI polling mode over FSSO Security Event Log (WinSecLog) polling mode?

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

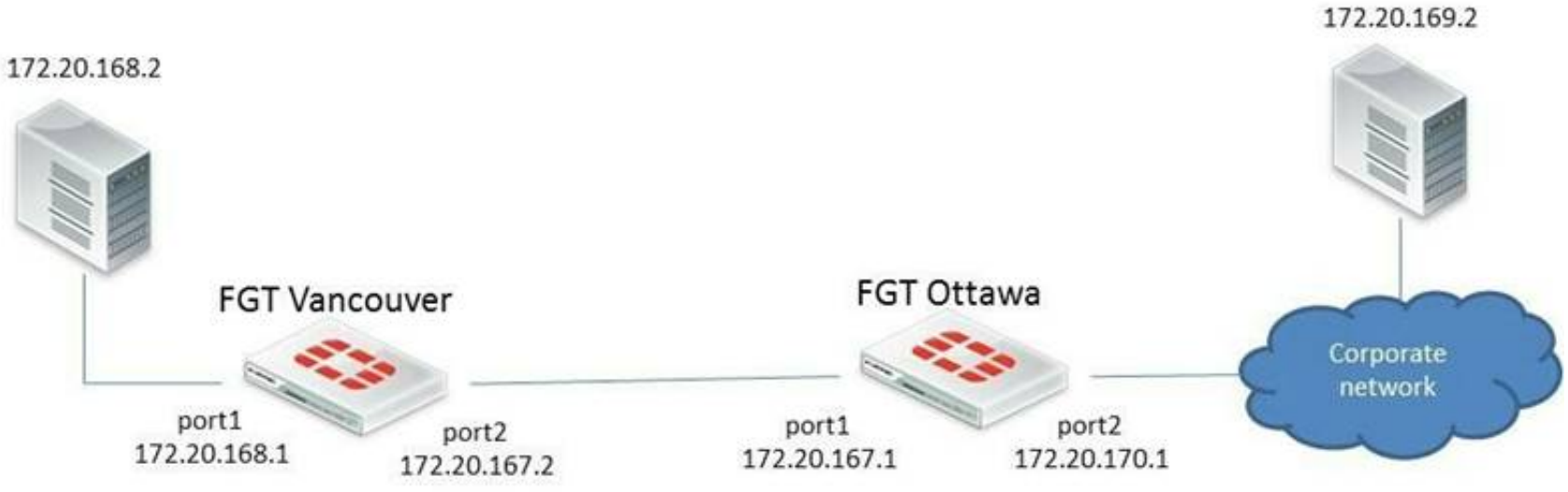
Answer: C

NEW QUESTION 143
Which of the following statements are correct about NTLM authentication? (Choose three)

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

Answer: ABC

NEW QUESTION 147
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 152
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 157
Bob wants to send Alice a file that is encrypted using public key cryptography.
Which of the following statements is correct regarding the use of public key cryptography in this scenario?

A. Bob will use his private key to encrypt the file and Alice will use her private key to decrypt the file.
B. Bob will use his public key to encrypt the file and Alice will use Bob's private key to decrypt the file.
C. Bob will use Alice's public key to encrypt the file and Alice will use her private key to decrypt the file.
D. Bob will use his public key to encrypt the file and Alice will use her private key to decrypt the file.

Answer: C

NEW QUESTION 158
What is the default criteria for selecting the HA master unit in a HA cluster?

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

Answer: B

NEW QUESTION 163
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 168
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 173
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 174
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. FortiGuard pull updates.

C. Push updates from a FortiAnalyzer.
D. execute fortiguard-AV-AS command from the CLI.

Answer: AB

NEW QUESTION 176
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 180
Which of the following statements are true about Man-in-the-middle SSL Content Inspection? (Choose three.)

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

Answer: BCE

NEW QUESTION 183
A firewall policy has been configured for the internal email server to receive email from external parties through SMTP. Exhibits A and B show the antivirus and email filter profiles applied to this policy.
Exhibit A

Exhibit B:

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

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

Answer: B

NEW QUESTION 184
In the debug command output shown in the exhibit, which of the following best described the MAC address 00:09:0f:69:03:7e ?

```
# diagnose ip arp list
index=2 ifname=port1 172.20.187.150 00:09:0f:69:03:7e
state=00000004 use=4589 confirm=4589 update=2422 ref=1
```

A. It is one of the secondary MAC addresses of the port1 interface.
B. It is the primary MAC address of the port interface.
C. It is the MAC address of another network devices located in the same LAN segment as the FortiGate unit's port1 interface.
D. It is the HA virtual MAC address.

Answer: C

NEW QUESTION 185
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 188
What are the ways FortiGate can monitor logs? (Choose three.)

A. MIB
B. SMS
C. Alert Emails
D. SNMP
E. FortiAnalyzer
F. Alert Message Console

Answer: CDF

NEW QUESTION 191
What is longest length of time allowed on a FortiGate device for the virus scan to complete?

A. 20 seconds
B. 30 seconds

C. 45 seconds
D. 10 seconds

Answer: B

NEW QUESTION 196
.....

About Exambible

Your Partner of IT Exam

Found in 1998

Exambible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, Exambible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

NEW QUESTION 1
Examine the two static routes to the same destination subnet 172.20.168.0/24 as shown below; then answer the question following it.

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

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

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

Answer: C

NEW QUESTION 2
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 3
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.

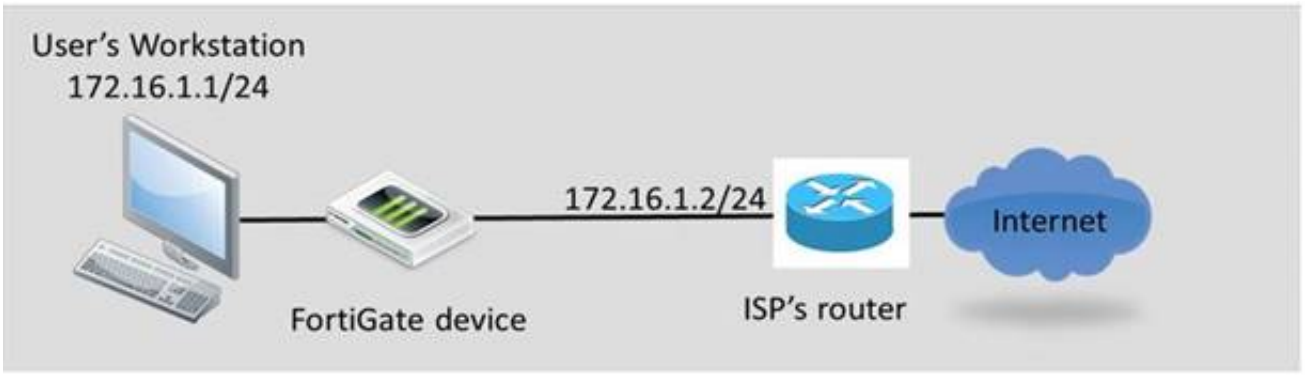
Answer: B

NEW QUESTION 4
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 5
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 6
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 7
Files reported as "suspicious" were subject to which Antivirus check"?

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

Answer: D

NEW QUESTION 8
Which statements are correct for port pairing and forwarding domains? (Choose two.)

A. They both create separate broadcast domains.
B. Port Pairing works only for physical interfaces.
C. Forwarding Domain only applies to virtual interfaces
D. They may contain physical and/or virtual interfaces.

Answer: AD

NEW QUESTION 9
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 10
Which statements are correct regarding virtual domains (VDOMs)? (Choose two)

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

Answer: BC

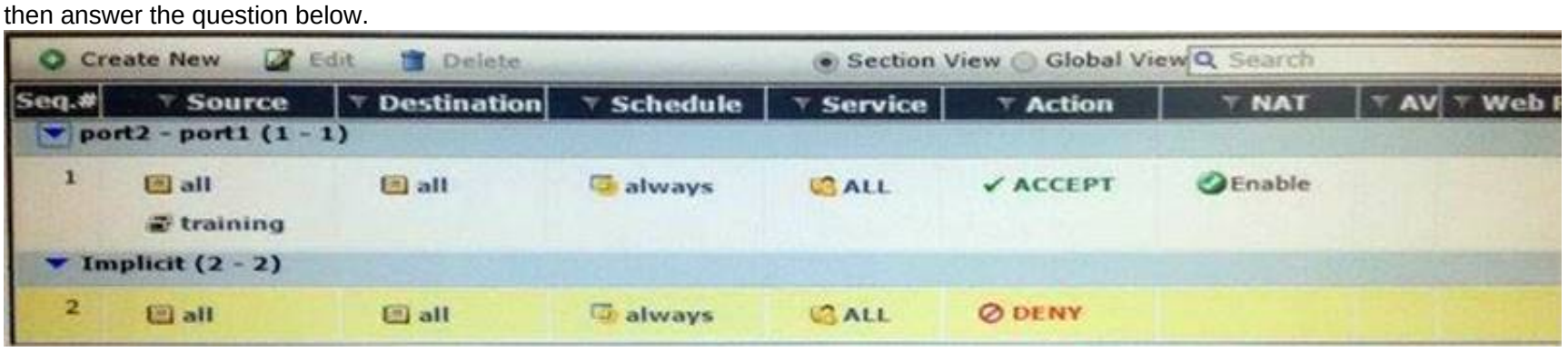
NEW QUESTION 10
Which action does the FortiGate take when link health monitor times out?

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 13
The FortiGate port1 is connected to the Internet. The FortiGate port2 is connected to the internal network. Examine the firewall configuration shown in the exhibit; then answer the question below.



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

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

Answer: D

NEW QUESTION 18
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 19
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 24
Two devices are in an HA cluster, the device hostnames are STUDENT and REMOTE. Exhibit A shows the command output of diagnose sys session stat for the STUDENT device. Exhibit B shows the command output of diagnose sys session stat for the REMOTE device.
Exhibit A:

```
STUDENT # diagnose sys session stat
misc info:      session_count=166 setup_rate=68 exp_count=0 clash=0
        memory_tension_drop=0 ephemeral=0/57344 removeable=0  ha_scan=0
delete=0, flush=0, dev_down=0/0
TCP sessions:
         8 in ESTABLISHED state
         3 in SYN_SENT state
         1 in FIN_WAIT state
         139 in TIME_WAIT state
firewall error stat:
error1=00000000
error2=00000000
error3=00000000
error4=00000000
tt=00000000
cont=00000000
ids_recv=00000000
url_recv=00000000
av_recv=00000000
fqdn_count=00000000
tcp reset stat:
        syncqf=0 acceptqf=0 no-listener=2 data=0 ses=0 ips=0
global: ses_limit=0 ses6_limit=0 rt_limit=0 rt6_limit=0

STUDENT # _
```

Exhibit B:

```
global: ses_limit=0 ses6_limit=0 rt_limit=0 rt6_limit=0

REMOTE # diagnose sys session stat
misc info:       session_count=11 setup_rate=0 exp_count=0 clash=4
        memory_tension_drop=0 ephemeral=0/57344 removeable=0  ha_scan=0
delete=0, flush=0, dev_down=0/0
TCP sessions:
         2 in ESTABLISHED state
         1 in SYN_SENT state
firewall error stat:
error1=00000000
error2=00000000
error3=00000000
error4=00000000
tt=00000000
cont=00000000
ids_recv=00000000
url_recv=00000000
av_recv=00000000
fqdn_count=00000000
tcp reset stat:
        syncqf=0 acceptqf=0 no-listener=7 data=0 ses=0 ips=0
global: ses_limit=0 ses6_limit=0 rt_limit=0 rt6_limit=0

REMOTE # _
```

Given the information provided in the exhibits, which of the following statements are correct? (Choose two.)

A. STUDENT is likely to be the master device.
B. Session-pickup is likely to be enabled.
C. The cluster mode is active-passive.
D. There is not enough information to determine the cluster mode.

Answer: AD

NEW QUESTION 28
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 30
You are creating a custom signature. Which has incorrect syntax?

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

Answer: A

NEW QUESTION 33
What is not true of configuring disclaimers on the FortiGate?

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

Answer: C

NEW QUESTION 38
Which statements are true regarding traffic shaping that is applied in an application sensor, and associated with the firewall policy? (Choose two.)

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

Answer: BC

NEW QUESTION 41
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 45
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 47
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 49
In a Crash log, what does a status of 0 indicate?

A. Abnormal termination of a process
B. A process closed for any reason
C. Scanunitd process crashed
D. Normal shutdown with no abnormalities
E. DHCP process crashed

Answer: D

NEW QUESTION 52
Regarding tunnel-mode SSL VPN, which three statements are correct? (Choose three.)

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

Answer: ABE

NEW QUESTION 53
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 58
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 63
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 64
Which best describes the mechanism of a TCP SYN flood?

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

Answer: D

NEW QUESTION 69
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 74
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 76
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.

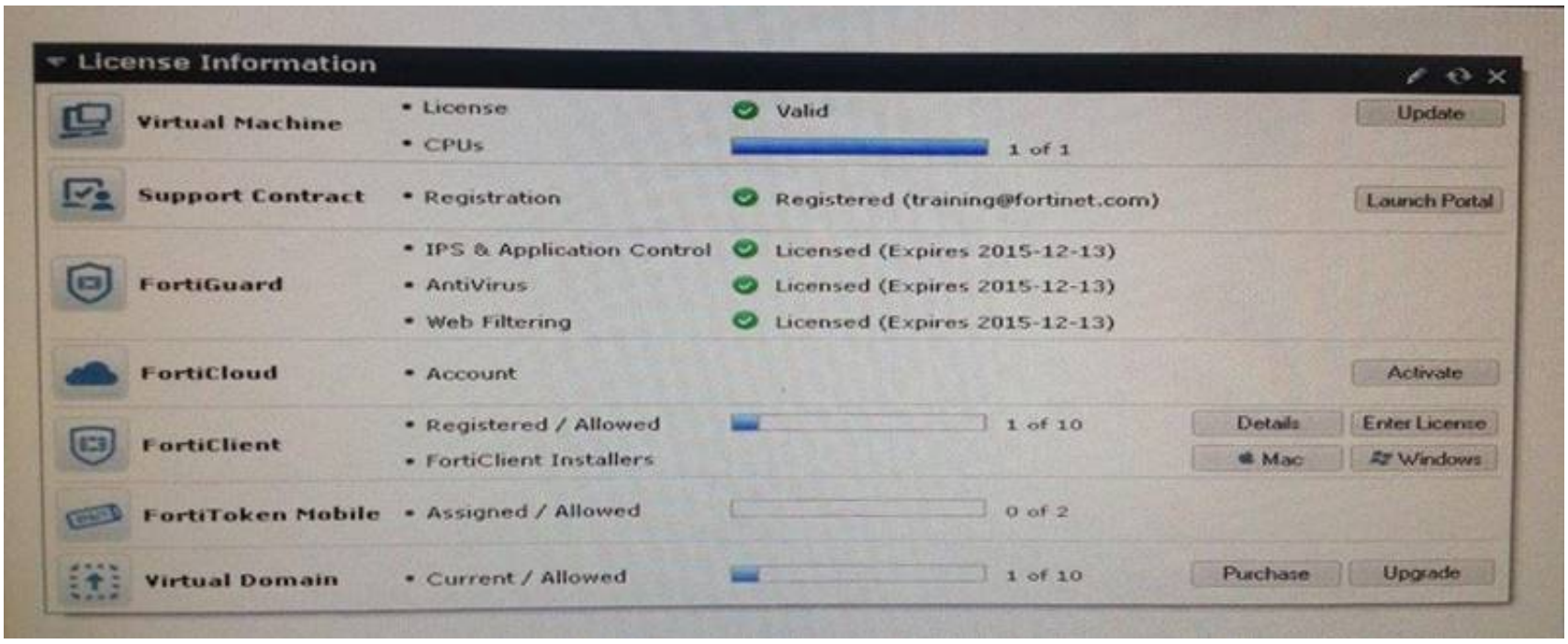
Answer: D

NEW QUESTION 81
Which of the following are possible actions for static URL filtering? (Choose three.)

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

Answer: ABC

NEW QUESTION 82
Examine the exhibit; then answer the question below.



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 85
Which of the following statements are correct concerning the FortiGate session life support protocol? (Choose two)

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

Answer: AD

NEW QUESTION 87
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 88
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 91
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 94
Which network protocols are supported for administrative access to a FortiGate unit? (Choose three.)

A. SMTP
B. WINS
C. HTTP
D. Telnet
E. SSH

Answer: CDE

NEW QUESTION 96
Which statement best describes what a Fortinet System on a Chip (SoC) is?

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

Answer: B

NEW QUESTION 99
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 100
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.

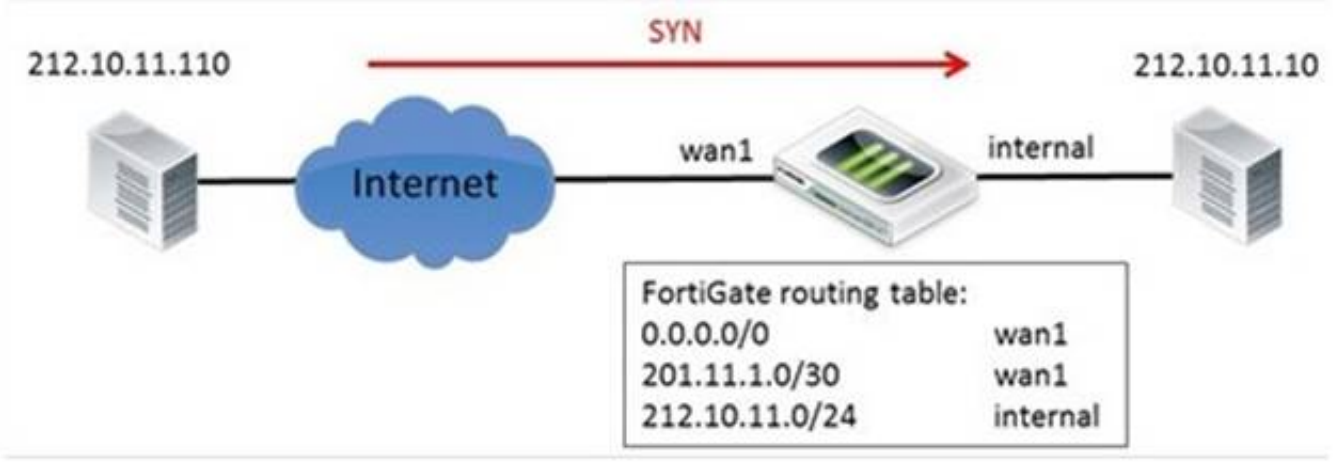
Answer: A

NEW QUESTION 104
Which of the following items is NOT a packet characteristic matched by a firewall service object?

A. ICMP type and code
B. TCP/UDP source and destination ports
C. IP protocol number
D. TCP sequence number

Answer: D

NEW QUESTION 105
Examine the network topology diagram in the exhibit; the workstation with the IP address 212.10.11.110 sends a TCP SYN packet to the workstation with the IP address 212.10.11.20.



Which of the following sentences best describes the result of the reverse path forwarding (RFP) check executed by the FortiGate on the SYN packets? (Choose two).

A. Packets is allowed if RPF is configured as loose.
B. Packets is allowed if RPF is configured as strict.
C. Packets is blocked if RPF is configured as loose.
D. Packets is blocked if RPF is configured as strict.

Answer: AD

NEW QUESTION 106
In a FSSO agentless polling mode solution, where must the collector agent be?

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

Answer: D

NEW QUESTION 110
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 114
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 119
Which of the following IPsec configuration modes can be used when the FortiGate is running in NAT mode?

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

Answer: B

NEW QUESTION 120
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 122
Which type of conserve mode writes a log message immediately, rather than when the device exits conserve mode?

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

Answer: B

NEW QUESTION 126
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 131
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 136
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 138
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 142
Which statement is one disadvantage of using FSSO NetAPI polling mode over FSSO Security Event Log (WinSecLog) polling mode?

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

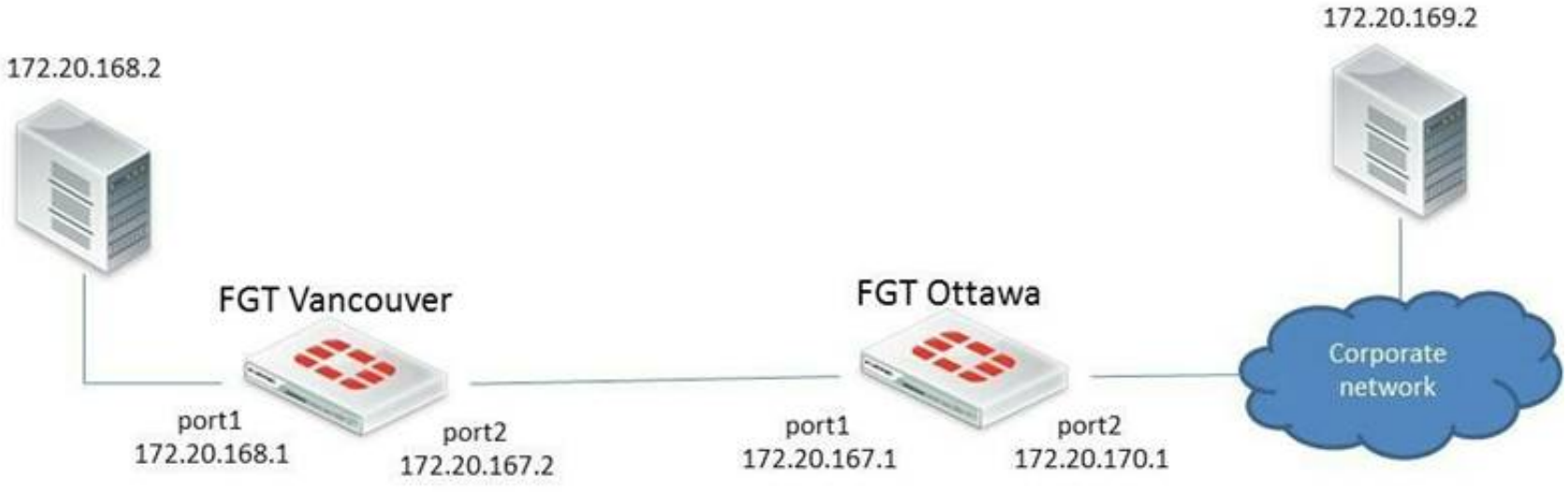
Answer: C

NEW QUESTION 143
Which of the following statements are correct about NTLM authentication? (Choose three)

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

Answer: ABC

NEW QUESTION 147
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 152
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 157
Bob wants to send Alice a file that is encrypted using public key cryptography.
Which of the following statements is correct regarding the use of public key cryptography in this scenario?

A. Bob will use his private key to encrypt the file and Alice will use her private key to decrypt the file.
B. Bob will use his public key to encrypt the file and Alice will use Bob's private key to decrypt the file.
C. Bob will use Alice's public key to encrypt the file and Alice will use her private key to decrypt the file.
D. Bob will use his public key to encrypt the file and Alice will use her private key to decrypt the file.

Answer: C

NEW QUESTION 158
What is the default criteria for selecting the HA master unit in a HA cluster?

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

Answer: B

NEW QUESTION 163
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 168
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 173
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 174
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. FortiGuard pull updates.

C. Push updates from a FortiAnalyzer.
D. execute fortiguard-AV-AS command from the CLI.

Answer: AB

NEW QUESTION 176
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 180
Which of the following statements are true about Man-in-the-middle SSL Content Inspection? (Choose three.)

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

Answer: BCE

NEW QUESTION 183
A firewall policy has been configured for the internal email server to receive email from external parties through SMTP. Exhibits A and B show the antivirus and email filter profiles applied to this policy.
Exhibit A

Exhibit B:

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

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

Answer: B

NEW QUESTION 184
In the debug command output shown in the exhibit, which of the following best described the MAC address 00:09:0f:69:03:7e ?

```
# diagnose ip arp list
index=2 ifname=port1 172.20.187.150 00:09:0f:69:03:7e
state=00000004 use=4589 confirm=4589 update=2422 ref=1
```

A. It is one of the secondary MAC addresses of the port1 interface.
B. It is the primary MAC address of the port interface.
C. It is the MAC address of another network devices located in the same LAN segment as the FortiGate unit's port1 interface.
D. It is the HA virtual MAC address.

Answer: C

NEW QUESTION 185
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 188
What are the ways FortiGate can monitor logs? (Choose three.)

A. MIB
B. SMS
C. Alert Emails
D. SNMP
E. FortiAnalyzer
F. Alert Message Console

Answer: CDF

NEW QUESTION 191
What is longest length of time allowed on a FortiGate device for the virus scan to complete?

A. 20 seconds
B. 30 seconds

C. 45 seconds
D. 10 seconds

Answer: B

NEW QUESTION 196
.....

Relate Links

100% Pass Your NSE4 Exam with Exambible Prep Materials

https://www.exambible.com/NSE4-exam/

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - https://www.exambible.com/