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

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

Answer: BC

NEW QUESTION 3
Which of the following settings can be configured per VDOM? (Choose three)

A. Operating mode (NAT/route or transparent)
B. Static routes
C. Hostname
D. System time
E. Firewall Policies

Answer: ABE

NEW QUESTION 4
Examine the exhibit; then answer the question below.

The Vancouver FortiGate initially had the following information in its routing table:
S 172.20.0.0/16 [10/0] via 172.21.1.2, port2
C 172.21.0.0/16 is directly connected, port2
C 172.11.11.0/24 is directly connected, port1
Afterwards, the following static route was added:
config router static edit 6
set dst 172.20.1.0 255.255.255.0
set priority 0
set device port1
set gateway 172.11.12.1 next
Since this change, the new static route is NOT showing up in the routing table. Given the information provided, which of the following describes the cause of this problem?

A. The subnet 172.20.1.0/24 is overlapped with the subnet of one static route that is already in the routing table (172.20.0.0/16), so, we need to enable allow-subnet-overlap first.
B. The 'gateway' IP address is NOT in the same subnet as the IP address of port1.

C. The priority is 0, which means that the route will remain inactive.
D. The static route configuration is missing the distance setting.

Answer: B

NEW QUESTION 5
Your Linux email server runs on a non-standard port number, port 2525. Which statement is true?

A. IPS cannot scan that traffic for SMTP anomalies because of the non-standard port numbe
B. You must reconfigured the server to run on port 2.
C. To apply IPS to traffic to that server, you must configured FortiGate SMTP proxy to listen on port 2525
D. IPS will apply all SMTP signatures, regardless of whether they apply to clients or servers.
E. Protocol decoders automatically detect SMTP and scan for matches with appropriate IPS signature.

Answer: B

NEW QUESTION 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
Which statement best describes what the FortiGate hardware acceleration processors main task is?

A. Offload traffic processing tasks from the main CPU.
B. Offload management tasks from the main CPU.
C. Compress and optimize the network traffic.
D. Increase maximum bandwidth available in a FortiGate interface.

Answer: A

NEW QUESTION 8
Review to the network topology in the exhibit.
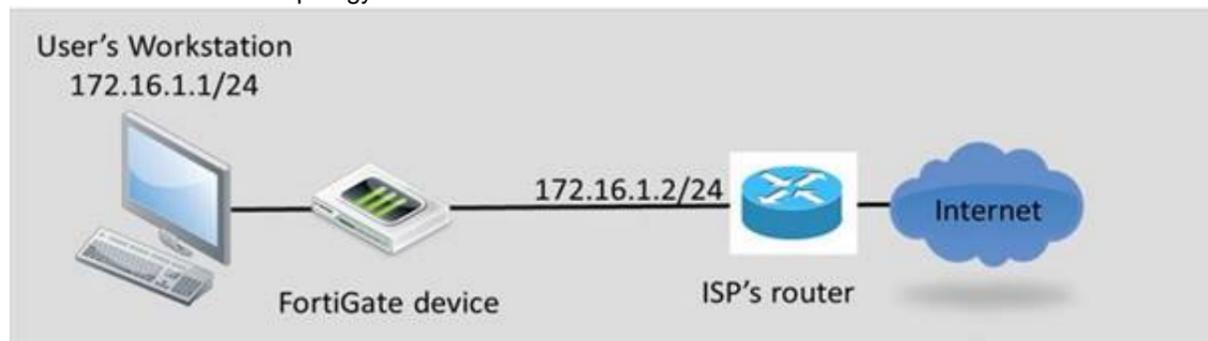
The workstation, 172.16.1.1/24, connects to port2 of the FortiGate device, and the ISP router, 172.16.1.2, connects to port1. Without changing IP addressing, which configuration changes are required to properly forward users traffic to the Internet? (Choose two)

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 9
Which best describes the authentication timeout?

A. How long FortiGate waits for the user to enter his or her credentials.
B. How long a user is allowed to send and receive traffic before he or she must authenticate again.
C. How long an authenticated user can be idle (without sending traffic) before they must authenticate again.
D. How long a user-authenticated session can exist without having to authenticate again.

Answer: C

NEW QUESTION 10
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 10
Files reported as "suspicious" were subject to which Antivirus check"?

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

Answer: D

NEW QUESTION 14
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 16
What methods can be used to deliver the token code to a user that is configured to use
two-factor authentication? (Choose three.)

A. Browser pop-up window.
B. FortiToken.
C. Email.
D. Code books.
E. SMS phone message.

Answer: BCE

NEW QUESTION 21
A user logs into a SSL VPN portal and activates the tunnel mode. The exhibit shows the firewall policy and the user's SSL VPN portal configuration:
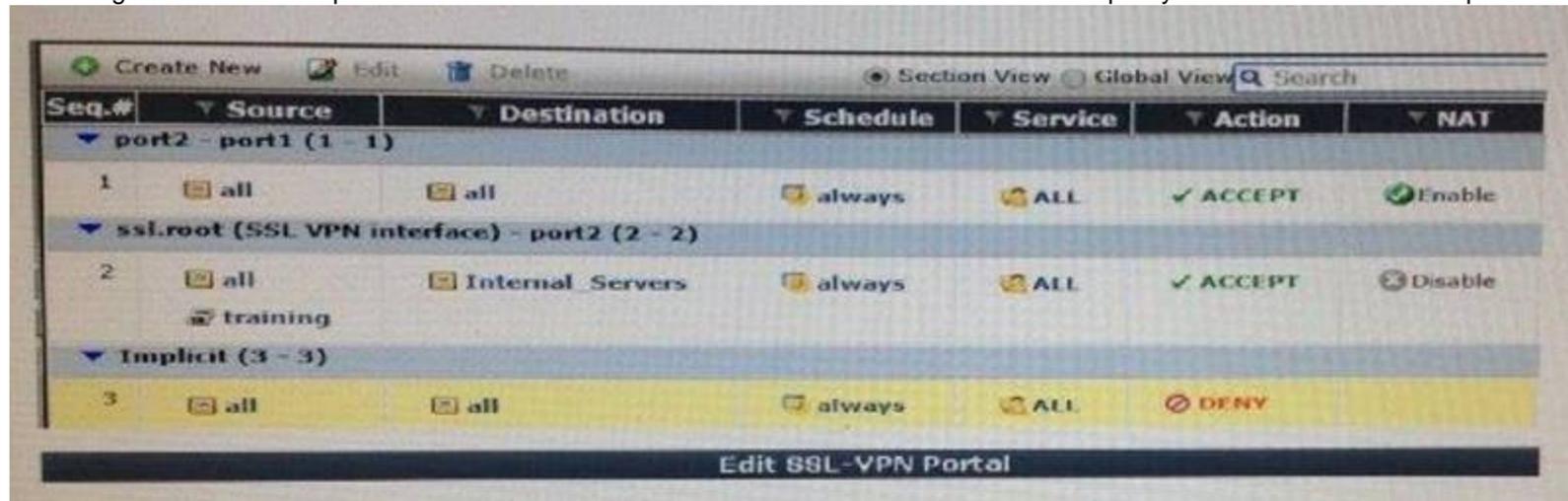
Given that the user authenticates against the SSL VPN policy shown in the image below, which statement below identifies the route that is added to the client's routing table.

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

Answer: A

NEW QUESTION 22
A FortiGate is configured with the 1.1.1.1/24 address on the wan2 interface and HTTPS Administrative Access, using the default tcp port, is enabled for that interface. Given the SSL VPN settings in the exhibit.

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

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

Answer: BD

NEW QUESTION 27
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 29
Review the configuration for FortiClient IPsec shown in the exhibit.
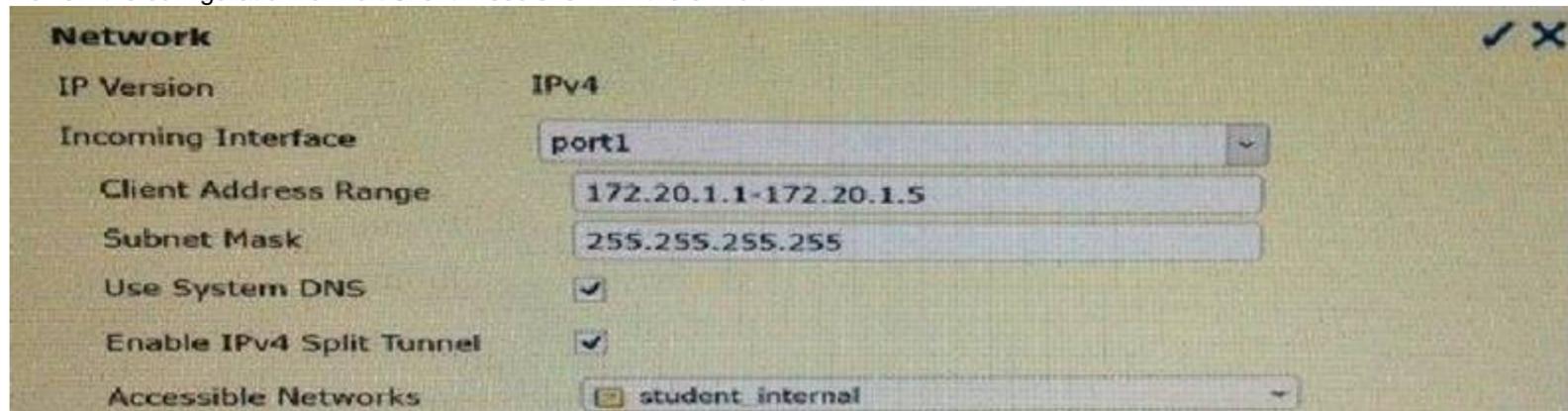
Which statement is correct regarding this configuration?

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 34
Review the output of the command get router info routing-table database shown in the exhibit below; then answer the question following it.

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 37
Which of the following fields contained in the IP/TCP/UDP headers can be used to make a routing decision when using policy-based routing? (Choose three)

A. Source IP address.
B. TCP flags
C. Source TCP/UDP ports
D. Type of service.
E. Checksum

Answer: ACD

NEW QUESTION 42
Which of the following protocols are defined in the IPsec Standard? (Choose two)

A. AH
B. GRE
C. SSL/TLS
D. ESP

Answer: AD

NEW QUESTION 47
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.
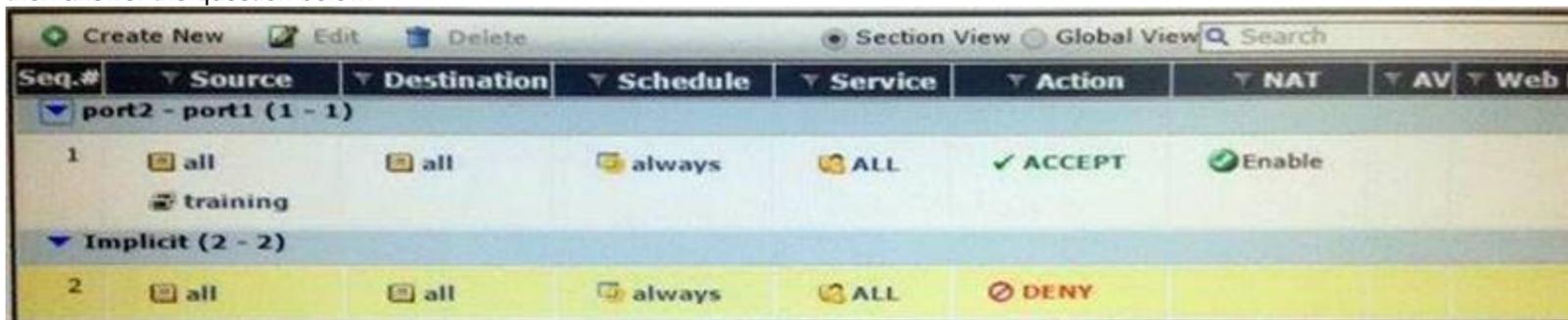
Based on the firewall configuration illustrated in the exhibit, which statement is correct?

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 50
Which of the following statements is true regarding the use of a PAC file to configure the web proxy settings in an Internet browser? (Choose two.)

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

Answer: BC

NEW QUESTION 55
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 57
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 59
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 63
Which statements are true regarding local user authentication? (Choose two.)

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

Answer: AD

NEW QUESTION 67
Where are most of the security events logged?

A. Security log
B. Forward Traffic log
C. Event log
D. Alert log
E. Alert Monitoring Console

Answer: C

NEW QUESTION 70
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 73
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 77
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 82
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 87
Which statements are true regarding the use of a PAC file to configure the web proxy settings in an Internet browser? (Choose two.)

A. Only one proxy is supported.
B. Can be manually imported to the browser.
C. The browser can automatically download it from a web server.
D. Can include a list of destination IP subnets where the browser can connect directly to without using a proxy.

Answer: CD

NEW QUESTION 92

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 95
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 98
What is the FortiGate password recovery process?

A. Interrupt boot sequence, modify the boot registry and reboo
B. After changing thepassword, reset the boot registry.
C. Log in through the console port using the ''maintainer'' account within several seconds of physically power cycling the FortiGate.
D. Hold down the CTRL + Esc (Escape) keys during reboot, then reset the admin password.
E. Interrupt the boot sequence and restore a configuration file for which the password has been modified.

Answer: B

NEW QUESTION 101
Which is one of the conditions that must be met for offloading the encryption and decryption of IPsec traffic to an NP6 processor?

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

Answer: C

NEW QUESTION 102
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 105
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 109
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 114
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 117
Which statement is not correct regarding SSL VPN Tunnel mode?

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

Answer: C

NEW QUESTION 120
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 124
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 125
Which is not a FortiGate feature?

A. Database auditing
B. Intrusion prevention
C. Web filtering
D. Application control

Answer: A

NEW QUESTION 127
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 128
A FortiGate is configured to receive push updates from the FortiGuard Distribution Network, however, they are not being received.
Which of the following statements are possible reasons for this?
A FortiGate unit is configured to receive push updates from the FortiGuard Distribution Network, however, updates are not being received. Which of the following statements are possible reasons for this? (Select all that apply.)

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

Answer: ABC

NEW QUESTION 133
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 136
A FortiGate is operating in NAT/Route mode and configured with two virtual LAN (VLAN) sub-interfaces added to the same physical interface.
Which one of the following statements is correct regarding the VLAN IDs in this scenario?

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

Answer: B

NEW QUESTION 137
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 140
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 143
Which of the following actions can be used to back up the keys and digital certificates in a FortiGate device? (Choose two.)

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

Answer: AD

NEW QUESTION 148
On your FortiGate 60D, you've configured firewall policies. They port forward traffic to your Linux Apache web server. Select the best way to protect your web server by using the IPS engine.

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

Answer: D

NEW QUESTION 153
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 158
Which statement describes what the CLI command diagnose debug authd fsso list is used for?

A. Monitors communications between the FSSO collector agent and FortiGate unit.
B. Displays which users are currently logged on using FSSO.
C. Displays are listing of all connected FSSO collector agents.
D. Lists all DC Agents installed on all domain controllers.

Answer: B

NEW QUESTION 163
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 164
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 168
Which of the following statements are true about the SSL Proxy certificate that must be used for SSL Content Inspection? (Choose two.)

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

Answer: CD

NEW QUESTION 169
Which of the following statements best describes the role of a DC agents in an FSSO DC?

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

Answer: C

NEW QUESTION 171
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 172
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 175
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 178
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 182
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 187
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 190
Which of the following statements are correct concerning IKE mode config? (Choose two)

A. It can dynamically assign IP addresses to IPsec VPN clients.
B. It can dynamically assign DNS settings to IPsec VPN clients.
C. It uses the ESP protocol.
D. It can be enabled in the phase 2 configuration.

Answer: AB

NEW QUESTION 193
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 195
Which of the following statements best describes what the Document Fingerprinting feature is for?

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

Answer: A

NEW QUESTION 196
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 201
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 205
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
Alert emails enable the FortiGate unit to send email notifications to an email address upon detection of a pre-defined event type.
Which of the following are some of the available event types in Web Config?

A. Intrusion detected.
B. Successful firewall authentication.
C. Oversized file detected.
D. DHCP address assigned.
E. FortiGuard Web Filtering rating error detected.

Answer: A

NEW QUESTION 208
Examine the following log message for IPS:
2012-07-01 09:54:28 oid=2 log_id=18433 type=ips subtype=anomaly pri=alert vd=root severity="critical" src="192.168.3.168" dst="192.168.3.170" src_int="port2"
serial=0 status="detected" proto=1 service="icmp" count=1 attack_name="icmp_flood"
icmp_id="0xa8a4"
icmp_type="0x08" icmp_code="0x00" attack_id=16777316 sensor="1" ref="http://www.fortinet.com/ids/VID16777316" msg="anomaly: icmp_flood, 51 > threshold 50"
Which statement is correct about the above log? (Choose two.)

A. The target is 192.168.3.168.
B. The target is 192.168.3.170.

C. The attack was NOT blocked.
D. The attack was blocked.

Answer: BD

NEW QUESTION 209
Which statements are correct regarding application control? (Choose two.)

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

Answer: AC

NEW QUESTION 211
Which define device identification? (Choose two.)

A. Device identification is enabled by default on all interfaces.
B. Enabling a source device in a firewall policy enables device identification on the source interfaces of that policy.
C. You cannot combine source user and source device in the same firewall policy.
D. FortiClient can be used as an agent based device identification technique.
E. Only agentless device identification techniques are supported.

Answer: BD

NEW QUESTION 213
Which does FortiToken use as input when generating a token code? (Choose two.)

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

Answer: AD

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

NEW QUESTION 214
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 218
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 220
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 222
Which of the following statements are correct concerning the IPsec phase 1 and phase 2, shown in the exhibit? (choose two)

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

Answer: CD

NEW QUESTION 223
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 226
Which action is taken by the FortiGate device when a file matches more than one rule in a Data Leak Prevention sensor?

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

Answer: D

NEW QUESTION 229
Review the IPsec diagnostics output of the command diagnose vpn tunnel list shown in the exhibit.

```
STUDENT # diagnose vpn tunnel list
list all ipsec tunnel in vd 0
------------------------------------------------------------
name=Remote_1 ver=1 serial=1 10.200.1.1:0->10.200.3.1:0 lgwy=static tun=intf mode=auto bound_if=2
proxyid_num=1 child_num=0 refcnt=6 ilast=2 olast=2
stat: rxp=8 txp=8 rxb=960 txb=480
dpd: mode=active on=1 idle=5000ms retry=3 count=0 seqno=128
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=P2_Remote_1 proto=0 sa=1 ref=2 auto_negotiate=0 serial=1
   src: 0:0.0.0.0/0.0.0.0:0
   dst: 0:0.0.0.0/0.0.0.0:0
   SA: ref=3 options=0000000f type=00 soft=0 mtu=1412 expire=1486 replaywin=1024 seqno=1
   life: type=01 bytes=0/0 timeout=1753/1800
   dec: spi=b95a77fe esp=aes key=32 84ed410c1bb9f61e635a49563c4e7646e9e110628b79b0ac03482d05e3b6a0e6
        ah=sha1 key=20 6bddbfad7161237daa46c19725dd0292b062dda5
   enc: spi=9293e7d4 esp=aes key=32 951befd87860cdb59b98b170a17dcb75f77bd541bdc3a1847e54c78c0d43aa13
        ah=sha1 key=20 8a5bedd6a0ce0f8daf7593601acfe2c618a0d4e2
------------------------------------------------------------
name=Remote_2 ver=1 serial=2 10.200.2.1:0->10.200.4.1:0 lgwy=static tun=intf mode=auto bound_if=3
proxyid_num=1 child_num=0 refcnt=6 ilast=0 olast=0
stat: rxp=0 txp=0 rxb=0 txb=0
dpd: mode=active on=1 idle=5000ms retry=3 count=0 seqno=0
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=P2_Remote_2 proto=0 sa=1 ref=2 auto_negotiate=0 serial=1
   src: 0:0.0.0.0/0.0.0.0:0
   dst: 0:0.0.0.0/0.0.0.0:0
   SA: ref=3 options=0000000f type=00 soft=0 mtu=1280 expire=1732 replaywin=1024 seqno=1
   life: type=01 bytes=0/0 timeout=1749/1800
   dec: spi=b95a77ff esp=aes key=32 582af59d71635b835c9208878e0e3f3fe31ba1dfd88ff83ca9bab1ed66ac325e
        ah=sha1 key=20 0d951e62a1bcb63232df6d0fb86df49ab714f53b
   enc: spi=9293e7d5 esp=aes key=32 eeeecacf3a58161f3390fa612b794c776654c86aef51fbc7542906223d56ebb3
        ah=sha1 key=20 09eaa3085bc30a59091f182eb3d11550385b8304
```

Which statements is correct regarding this output?

A. One tunnel is rekeying.
B. Two tunnels are rekeying.
C. Two tunnels are up.
D. One tunnel is up.

Answer: C

NEW QUESTION 234
Which protocol can an Internet browser use to download the PAC file with the web proxy configuration?

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

Answer: D

NEW QUESTION 239
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 241
Examine the following CLI configuration:
config system session -ttl set default 1800
end
What statement is true about the effect of the above configuration line?

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

Answer: A

NEW QUESTION 244
What is required in a FortiGate configuration to have more than one dialup IPsec VPN using aggressive mode?

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

Answer: C

NEW QUESTION 246
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 248
Which authentication methods does FortiGate support for firewall authentication? (Choose two.)

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

Answer: AC

NEW QUESTION 253
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 257
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 261
Review the static route configuration for IPsec shown in the exhibit; then answer the question below.
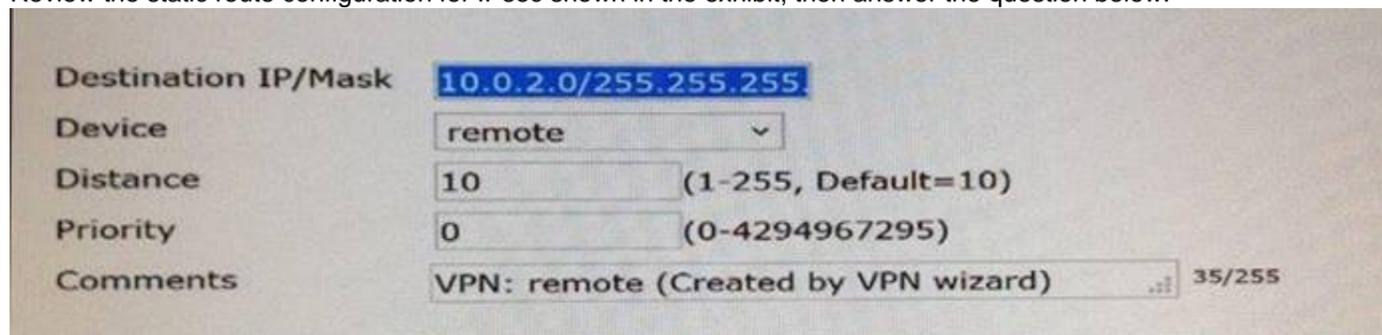
Which statements are correct regarding this configuration? (Choose two.)

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 266
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 267
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 272
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 277
Which of the following statements is correct regarding FortiGate interfaces and spanning tree protocol? (Choose Two)

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

Answer: BD

NEW QUESTION 280
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 282
Which of the following IKE modes is the one used during the IPsec phase 2 negotiation?

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

Answer: B

NEW QUESTION 287
Which user group types does FortiGate support for firewall authentication? (Choose three.)

A. RSSO
B. Firewall
C. LDAP
D. NTLM
E. FSSO

Answer: ABE

NEW QUESTION 290
Which authentication scheme is not supported by the RADIUS implementation on FortiGate?

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

Answer: D

NEW QUESTION 295
The exhibit is a screen shot of an Application Control profile.

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 296
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 300
In a high availability cluster operating in active-active mode, which of the following correctly describes the path taken by the SYN packet of an HTTP session that is offloaded to a slave unit?

A. Client - > slave FortiGate - > master FortiGate - > web server.
B. Client - > slave FortiGate - > web server.
C. Client - > master FortiGate - > slave FortiGate - > master FortiGate - >web server.
D. Client - > master FortiGate - >slave FortiGate - > web server.

Answer: D

NEW QUESTION 301
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 302
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 305
Which are the three different types of Conserve Mode that can occur on a FortiGate device? (Choose three.)

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

Answer: ACD

NEW QUESTION 309
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 311
Examine this log entry.
What does the log indicate? (Choose three.)
date=2013-12-04 time=09:30:18 logid=0100032001 type=event subtype=system level=information vd="root" user="admin" ui=http(192.168.1.112) action=login status=success reason=none profile="super_admin" msg="Administrator admin logged in successfully from http(192.168.1.112)"

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

Answer: BEG

NEW QUESTION 316
How do you configure a FortiGate to apply traffic shaping to P2P traffic, such as BitTorrent?

A. Apply a traffic shaper to a BitTorrent entry in an application control list, which is then applied to a firewall policy.
B. Enable the shape option in a firewall policy with service set to BitTorrent.
C. Define a DLP rule to match against BitTorrent traffic and include the rule in a DLP sensor with traffic shaping enabled.
D. Apply a traffic shaper to a protocol options profile.

Answer: A

NEW QUESTION 318
Which of the following statements are true about IPsec VPNs? (Choose three.)

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

Answer: ADE

NEW QUESTION 320
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 321

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 324
Review the IKE debug output for IPsec shown in the exhibit below.


```
STUDENT # ike 0: comes 10.200.3.1:500->10.200.1.1:500,ifindex=2....
ike 0: IKEv1 exchange=Informational id=9e2606ac7ae83d7a/612da78d3ab3f945:15b10705 len=92
ike 0: in 9E2606AC7AE83D7A612DA78D3AB3F94508100501158107050000005C26E2A7EC8461AC15E9BBC705B6C1F667A41957AED11FB7003C07A1
37B0934DD08E1A2074348E08FD6B39149C618525C6EC51E2F26885B6BB8E035F52B4
ike 0:Remote_1:10: dec 9E2606AC7AE83D7A612DA78D3AB3F94508100501158107050000005C08000018E2B1874EECF170EB5222B6A4E3A027C71-
000000020000000010110BD289E2606AC7AE83D7A612DA78D3AB3F9450000009C17511ED8EE5495O7
ike 0:Remote_1:10: notify msg received: R-U-THERE
ike 0:Remote_1:10: enc 9E2606AC7AE83D7A612DA78D3AB3F94508100501734C5CDF00000054080000181C047F014CBEF1B0EC80A915F3B18AEBC0
A00000020000000010110BD299E2606AC7AE83D7A612DA78D3AB3F9450000009C
ike 0:Remote_1:10: out 9E2606AC7AE83D7A612DA78D3AB3F94508100501734C5CDF0000005CB3CC431065A1737144B02F1AACE79C1BE712B84255
EB84E5FA7A967FE99C7B731057FF33728BB42AA983E79C919DA9B64EBCE087EF0A02666C1FBD2C62F
ike 0:Remote_1:10: sent IKE msg (R-U-THERE-ACK): 10.200.1.1:500->10.200.3.1:500, len=92, id=9e2606ac7ae83d7a/612da78d3ab3
734c5cdf
ike 0:Remote_1: link is idle 2 10.200.1.1->10.200.3.1:500 dpd=1 seqno=34
```

Which statements is correct regarding this output?

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

Answer: C

NEW QUESTION 329
A FortiGate devices has two VDOMs in NAT/route mode. Which of the following solutions can be implemented by a network administrator to route traffic between the two VDOMs.(Choose two)

A. Use the inter-VDOMs links automatically created between all VDOMS.
B. Manually create and configured an inter-VDOM link between yours.
C. Interconnect and configure an external physical interface in one VDOM to another physical interface in the second VDOM.
D. Configure both VDOMs to share the same table.

Answer: BC

NEW QUESTION 331
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 335
The exhibit shoes three static routes.

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

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

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

Answer: D

NEW QUESTION 339
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 340
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 341
Which of the following authentication methods are supported in an IPsec phase 1? (Choose two.)

A. Asymmetric Keys
B. CA root digital certificates
C. RSA signature
D. Pre-shared keys

Answer: CD

NEW QUESTION 344
A FortiGate is configured with three virtual domains (VDOMs). Which of the following statements is correct regarding multiple VDOMs?

A. The FortiGate must be a model 1000 or above to support multiple VDOMs.
B. A license has to be purchased and applied to the FortiGate before VDOM mode could be enabled.
C. Changing the operational mode of a VDOM requires a reboot of the FortiGate.
D. The FortiGate supports any combination of VDOMs in NAT/Route and transparent modes.

Answer: D

NEW QUESTION 349
Two FortiGate units with NP6 processors form an active-active cluster. The cluster is doing security profile (UTM) inspection over all the user traffic.
What statements are true regarding the sessions that the master unit is offloading to the slave unit for inspection? (Choose two.)

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

Answer: BC

NEW QUESTION 351
Which answer best describes what an "Unknown Application" is?

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

Answer: C

NEW QUESTION 352
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:

Exhibit B:

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 356
When creating FortiGate administrative users, which configuration objects specify the account rights?

A. Remote access profiles.
B. User groups.
C. Administrator profiles.
D. Local-in policies.

Answer: C

NEW QUESTION 357
Which correctly define "Section View" and "Global View" for firewall policies? (Choose two.)

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

Answer: AD

NEW QUESTION 358
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 360
An administrator has formed a high availability cluster involving two FortiGate units.
[Multiple upstream Layer 2 switches] – [FortiGate HA Cluster] – [Multiple downstream Layer 2 Switches]
The administrator wishes to ensure that a single link failure will have minimal impact upon the overall throughput of traffic through this cluster.
Which of the following options describes the best step the administrator can take? The administrator should

A. Increase the number of FortiGate units in the cluster and configure HA in active-active mode.
B. Enable monitoring of all active interfaces.
C. Set up a full-mesh design which uses redundant interfaces.
D. Configure the HA ping server feature to allow for HA failover in the event that a path is disrupted.

Answer: C

NEW QUESTION 365
Which of the following options best defines what Diffie-Hellman is?

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

Answer: B

NEW QUESTION 370
Which statements are correct regarding URL filtering on a FortiGate unit? (Choose two.)

A. The allowed actions for URL filtering include allow, block, monitor and exempt.
B. The allow actions for URL filtering and Allow and Block only.
C. URL filters may be based on patterns using simple text, wildcards and regular expressions.
D. URL filters are based on simple text only and require an exact match.

Answer: AC

NEW QUESTION 375
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 376
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 379
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 384
......

Thank You for Trying Our Product

We offer two products:

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

2nd - Questons and Answers in PDF Format

NSE4 Practice Exam Features:

* NSE4 Questions and Answers Updated Frequently

* NSE4 Practice Questions Verified by Expert Senior Certified Staff

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

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

100% Actual & Verified — Instant Download, Please Click
Order The NSE4 Practice Test Here