



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 compliant switches.

Answer: B

NEW QUESTION 3

What protocol cannot be used with the active authentication type?

- A. Local
- B. RADIUS
- C. LDAP
- D. RSSO

Answer: D

NEW QUESTION 4

Review the exhibit of an explicit proxy policy configuration.

Seq.#	To	Source	Destination	Users	Schedule	Action	AV	
web (1 - 2)								
1	port1	10.0.1.0/24	all			✓ ACCEPT		
1.1				Student	always			
2	port1	10.0.0.0/8	all		always	✓ ACCEPT		

If there is a proxy connection attempt coming from the IP address 10.0.1.5, and from a user that has not authenticated yet, what action does the FortiGate proxy take?

- A. User is prompted to authenticat
- B. Traffic from the user Student will be allowed by the policy #1. Traffic from any other user will be allowed by the policy #2.
- C. User is not prompted to authenticat
- D. The connection is allowed by the proxy policy #2.
- E. User is not prompted to authenticat
- F. The connection will be allowed by the proxy policy #1.
- G. User is prompted to authenticat
- H. Only traffic from the user Student will be allowe

I. Traffic from any other user will be blocked.

Answer: D

NEW QUESTION 5

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 6

What are examples of correct syntax for the session table diagnostics command? (Choose two.)

- A. diagnose sys session filter clear
- B. diagnose sys session src 10.0.1.254
- C. diagnose sys session filter
- D. diagnose sys session filter list dst.

Answer: AC

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

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 9

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

FSSO provides a single sign on solution to authenticate users transparently to a FortiGate unit using credentials stored in Windows active directory. Which of the following statements are correct regarding FSSO in a Windows domain environment when DC-agent mode is used? (Choose two.)

- A. An FSSO collector agent must be installed on every domain controller.
- B. An FSSO domain controller agent must be installed on every domain controller.
- C. The FSSO domain controller agent will regularly update user logon information on the FortiGate unit.
- D. The FSSO collector agent will receive user logon information from the domain controller agent and will send it to the FortiGate unit.

Answer: BD

NEW QUESTION 10

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

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

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

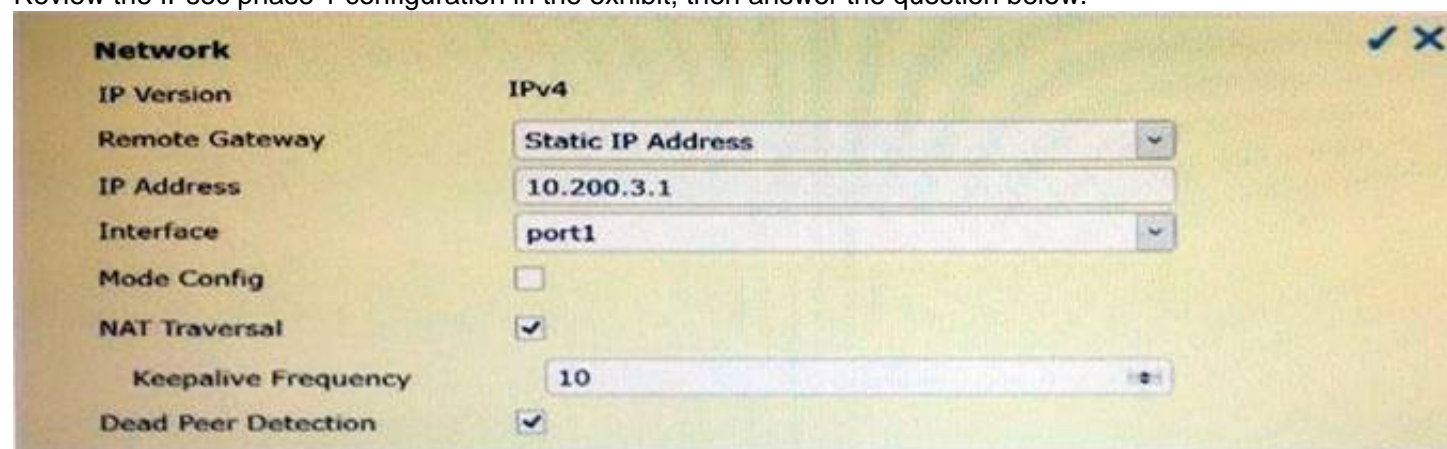
Which two statements are correct regarding this output? (Choose two.)

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

Answer: AC

NEW QUESTION 15

Review the IPsec phase 1 configuration in the exhibit; then answer the question below.



The screenshot shows the 'Network' configuration page for IPsec phase 1. The 'IP Version' is set to 'IPv4'. The 'Remote Gateway' is set to 'Static IP Address'. The 'IP Address' is '10.200.3.1'. The 'Interface' is 'port1'. The 'Mode Config' checkbox is unchecked. The 'NAT Traversal' checkbox is checked. The 'Keepalive Frequency' is set to '10'. The 'Dead Peer Detection' checkbox is checked.

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

- A. The remote gateway address is 10.200.3.1
- B. The local IPsec interface address is 10.200.3.1
- C. The local gateway IP is the address assigned to port1
- D. The local gateway IP is 10.200.3.1

Answer: AC

NEW QUESTION 20

Which of the following statements are correct regarding a master HA unit? (Choose two)

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

Answer: AB

NEW QUESTION 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

What capabilities can a FortiGate provide? (Choose three)

- A. Mail relay
- B. Email filtering
- C. Firewall
- D. VPN gateway
- E. Mail server

Answer: BCD

NEW QUESTION 33

Which of the following authentication methods can be used for SSL VPN authentication? (Choose three.)

- A. Remote Password Authentication (RADIUS, LDAP)
- B. Two-Factor Authentication
- C. Local Password Authentication
- D. FSSO
- E. RSSO

Answer: ABC

NEW QUESTION 38

Which antivirus inspection mode must be used to scan SMTP, FTP, POP3 and SMB protocols?

- A. Proxy-based.
- B. DNS-based.
- C. Flow-based.
- D. Man-in-the-middle.

Answer: C

NEW QUESTION 40

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 43

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 48

In FortiOS session table output, what is the correct 'proto_state' number for an established, non-proxied TCP connection?

- A. 00
- B. 11
- C. 01
- D. 05

Answer: C

NEW QUESTION 53

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 54

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 55

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 56

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 protocol.
- E. Otherwise, it does not respond.

Answer: B

NEW QUESTION 58

Which of the following actions can be used with the FortiGuard quota feature? (Choose three.)

- A. Allow
- B. Block
- C. Monitor
- D. Warning
- E. Authenticate

Answer: CDE

NEW QUESTION 61

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 interfaces.
- 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 62

Which of the following statements best describes what a Certificate Signing Request (CSR) is?

- A. A message sent by the Certificate Authority (CA) that contains a signed digital certificate.
- B. An enquiry submitted to a Certificate Authority (CA) to request a root CA certificate.
- C. An enquiry submitted to a Certificate Authority (CA) to request a signed digital certificate.
- D. An enquiry submitted to a Certificate Authority (CA) to request a Certificate Revocation List (CRL).

Answer: B

NEW QUESTION 67

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 68

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 70

Which TCP states does the global setting 'tcp-half-open-timer' apply to? (Choose two.)

- A. SYN SENT
- B. SYN & SYN/ACK
- C. FIN WAIT
- D. TIME WAIT

Answer: AD

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 79

What action does an IPsec Gateway take with the user traffic routed to an IPsec VPN when it does not match any phase 2 quick mode selector?

- A. Traffic is dropped
- B. Traffic is routed across the default phase 2.
- C. Traffic is routed to the next available route in the routing table.
- D. Traffic is routed unencrypted to the interface where the IPsec VPN is terminating.

Answer: A

NEW QUESTION 81

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 84

Which statement best describes what SSL VPN Client Integrity Check does?

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

Answer: B

NEW QUESTION 88

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 93

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 96

Which best describe the mechanism of a TCP SYN flood?

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

Answer: D

NEW QUESTION 99

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 104

Which traffic can match a firewall policy's "Services" setting? (Choose three.)

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

Answer: ACE

NEW QUESTION 105

A FortiGate device is configure to perform an AV & IPS scheduled update every hour.

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

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

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

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

Answer: D

NEW QUESTION 106

What is the maximum number of FortiAnalyzer/FortiManager devices a FortiGate unit can be configured to send logs to?

- A. 1
- B. 2
- C. 3
- D. 4

Answer: C

NEW QUESTION 110

Which of the following IPsec configuration modes can be used for implementing L2TP- over-IPSec VPNs?

- A. Policy-based IPsec only.
- B. Route-based IPsec only.
- C. Both policy-based and route-based VPN.
- D. L2TP-over-IPSec is not supported by FortiGate devices.

Answer: A

NEW QUESTION 112

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 protocol
- D. Otherwise, it could accidentally match lower-layer protocols.
- E. It is not supported by Fortinet Technical Support.

Answer: A

NEW QUESTION 116

Which statements regarding banned words are correct? (Choose two.)

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

Answer: CD

NEW QUESTION 119

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 122

Data leak prevention archiving gives the ability to store session transaction data on a FortiAnalyzer unit for which of the following types of network traffic? (Choose three.)

- A. POP3
- B. SNMP
- C. IPsec
- D. SMTP
- E. HTTP

Answer: ADE

NEW QUESTION 126

Which Fortinet products & features could be considered part of a comprehensive solution to monitor and prevent the leakage of sensitive data?

- A. Archive non-compliant outgoing e-mails using FortiMail.
- B. Restrict unofficial methods of transferring files such as P2P using Application Control lists on a FortiGate.
- C. Monitor database activity using FortiAnalyzer.
- D. Apply a DLP sensor to a firewall policy.
- E. Configure FortiClient to prevent files flagged as sensitive from being copied to a USB disk.

Answer: ABD

NEW QUESTION 131

Which statement regarding the firewall policy authentication timeout is true?

- A. It is an idle timeout
- B. The FortiGate considers a user to be "idle" if it does not see any packets coming from the user's source IP.
- C. It is a hard timeout
- D. The FortiGate removes the temporary policy for a user's source IP address after this timer has expired.
- E. It is an idle timeout
- F. The FortiGate considers a user to be "idle" if it does not see any packets coming from the user's source MAC.
- G. It is a hard timeout
- H. The FortiGate removes the temporary policy for a user's source MAC address after this timer has expired.

Answer: A

NEW QUESTION 134

Which FSSO agents are required for a FSSO agent-based polling mode solution?

- A. Collector agent and DC agents
- B. Polling agent only
- C. Collector agent only
- D. DC agents only

Answer: A

NEW QUESTION 135

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 139

Which of the following statements best describe the main requirements for a traffic session to be offload eligible to an NP6 processor? (Choose three.)

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

Answer: CDE

NEW QUESTION 140

Which of the following statements are correct concerning IPsec dialup VPN configurations for FortiGate devices? (Choose two)

- A. Main mode must be used when there is no more than one IPsec dialup VPN configured on the same FortiGate device.
- B. A FortiGate device with an IPsec VPN configured as dialup can initiate the tunnel connection to any remote IP address.
- C. Peer ID must be used when there is more than one aggressive-mode IPsec dialup VPN on the same FortiGate device.
- D. The FortiGate will automatically add a static route to the source quick mode selector address received from each remote peer.

Answer: CD

NEW QUESTION 141

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 144

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

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

Answer: B

NEW QUESTION 145

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

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

Answer: ABC

NEW QUESTION 147

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 148

How can DLP file filters be configured to detect Office 2010 files?

- A. File Typ
- B. Microsoft Office(msoffice)
- C. File Typ
- D. Archive(zip)

- E. File Typ
- F. Unknown Filetype(unknown)
- G. File Nam
- H. "*.ppt", "*.doc", "*.xls"
- I. File Nam
- J. "*.pptx", "*.docx", "*.xlsx"

Answer: BE

NEW QUESTION 150

Which of the following statements is correct concerning multiple vdoms configured in a FortiGate device?

- A. FortiGate devices, from the FGT/FWF 60D and above, all support VDOMS.
- B. All FortiGate devices scale to 250 VDOMS.
- C. Each VDOM requires its own FortiGuard license.
- D. FortiGate devices support more NAT/route VDOMs than Transparent Mode VDOMs.

Answer: A

NEW QUESTION 155

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

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

Answer: C

NEW QUESTION 159

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. Request: internal host; slave FortiGate; master FortiGate; Internet; web server.
- B. Request: internal host; slave FortiGate; Internet; web server.
- C. Request: internal host; slave FortiGate; master FortiGate; Internet; web server.
- D. Request: internal host; master FortiGate; slave FortiGate; Internet; web server.

Answer: D

NEW QUESTION 162

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 163

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 168

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 173

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 177

What are valid options for handling DNS requests sent directly to a FortiGate's interface IP? (Choose three.)

- A. Conditional-forward.
- B. Forward-only.
- C. Non-recursive.
- D. Iterative.
- E. Recursive.

Answer: BCE

NEW QUESTION 181

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 182

Examine the exhibit shown below; then answer the question following it.

FortiGuard Subscription Services

AntiVirus	Valid License (Expires 2013-05-12)	
AV Definitions	1.00000 (Updated 2012-10-17 via Manual Update) [Update]	
AV Engine	5.00032 (Updated 2012-10-16 via Manual Update)	
<hr/>		
IPS	Valid License (Expires 2013-05-12)	
IPS Definitions	4.00269 (Updated 2012-11-28 via Manual Update) [Update]	
IPS Engine	2.00043 (Updated 2012-10-29 via Manual Update)	
<hr/>		
Vulnerability Scan	Valid License (Expires 2013-05-12)	
VCM Plugins	1.00288 (Updated 2012-11-30 via Manual Update) [Update]	
VCM Engine	1.00288 (Updated 2012-11-30 via Manual Update)	
<hr/>		
Web Filtering	Valid License (Expires 2013-05-11)	
<hr/>		
Email Filtering	Valid License (Expires 2013-05-11)	
<hr/>		

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

Answer: A

NEW QUESTION 183

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 188

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 lgvy=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 lgvy=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 582af59d71635b835c9208878e0e3f3fe31ba1dfd88ff63ca9bab1ed66ac325e
    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 189

When does a FortiGate load-share traffic between two static routes to the same destination subnet?

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

Answer: D

NEW QUESTION 191

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

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

Answer: BC

NEW QUESTION 195

What configuration objects are automatically added when using the FortiGate's FortiClient VPN Configurations Wizard?(Choose two)

- A. Static route
- B. Phase 1
- C. Users group
- D. Phase 2

Answer: BD

NEW QUESTION 200

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 205

Which of the following statements are correct about the HA command `diagnose sys ha reset-uptime?` (Choose two.)

- A. The device this command is executed on is likely to switch from master to slave status if override is disabled.
- B. The device this command executed on is likely to switch from master to slave status if override is enabled.
- C. The command has no impact on the HA algorithm.
- D. This commands resets the uptime variable used in the HA algorithm so it may cause a new master to become elected.

Answer: AD

NEW QUESTION 209

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 213

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 215

The exhibit shows a part output of the diagnostic command `'diagnose debug application ike 255'`, taken during establishment of a VPN. Which of the following statement are correct concerning this output? (choose two)

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

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

Answer: BD

NEW QUESTION 216

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 217

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 219

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 221

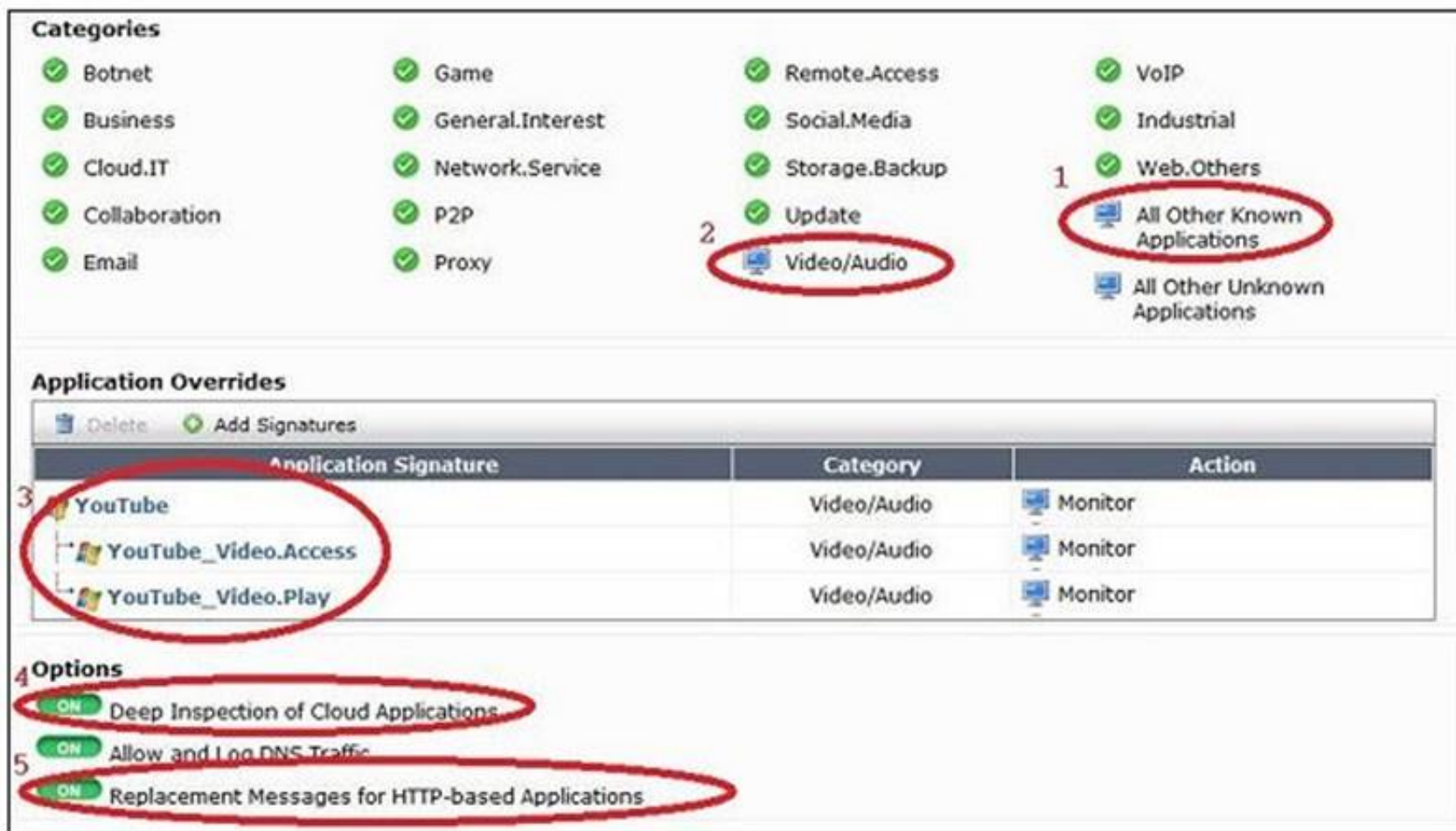
Which user group types does FortiGate support for firewall authentication? (Choose three.)

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

Answer: ABE

NEW QUESTION 226

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



Categories

- ☒ Botnet
- ☒ Business
- ☒ Cloud.IT
- ☒ Collaboration
- ☒ Email
- ☒ Game
- ☒ General.Interest
- ☒ Network.Service
- ☒ P2P
- ☒ Proxy
- ☒ Remote.Access
- ☒ Social.Media
- ☒ Storage.Backup
- ☒ Update
- ☒ Video/Audio
- ☒ VoIP
- ☒ Industrial
- ☒ Web.Others
- ☒ All Other Known Applications
- ☐ All Other Unknown Applications

Application Overrides

Application Signature	Category	Action
YouTube	Video/Audio	Monitor
YouTube_Video.Access	Video/Audio	Monitor
YouTube_Video.Play	Video/Audio	Monitor

Options

- ☒ Deep Inspection of Cloud Applications
- ☒ Allow and Log DNS Traffic
- ☒ Replacement Messages for HTTP-based Applications

Different settings are circled and numbered. Select the number identifying the setting which will provide additional information about YouTube access, such as the name of the video watched.

- A. 1
- B. 2
- C. 3
- D. 4
- E. 5

Answer: D

NEW QUESTION 231

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

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

Answer: D

NEW QUESTION 235

The exhibit shows a FortiGate routing table.


```
# get router info routing-table all
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       E1 - OSPF external type 1, E2 - OSPF external type 2
       * - candidate default
O*E2  0.0.0.0/0 [110/10] via 192.168.11.254, wan1, 01:29:24
C      172.16.78.0/24 is directly connected, wan2
O      192.168.1.0/24 [110/200] via 192.168.11.59, internal, 01:30:28
C      192.168.3.0/24 is directly connected, dmz
C      192.168.11.0/24 is directly connected, internal
```

Which of the following statements are correct?(Choose two)

- A. There is only one active default route.
- B. The distance values for the route to 192.168.1.0/24 is 200
- C. An IP address in the subnet 172.16.78.0/24 has been assigned to the dmz interface.
- D. The FortiGate will route the traffic to 172.17.1.2 to next hop with the IP address 192.168.11.254

Answer: AD

NEW QUESTION 240

Which IPSec mode includes the peer id information in the first packet?

- A. Main mode.
- B. Quick mode.
- C. Aggressive mode.
- D. IKEv2 mode.

Answer: C

NEW QUESTION 244

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 245

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 248

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 252

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 255

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 259

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 264

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 266

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 268

What are the advantages of FSSO DC mode over polling mode?

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

Answer: C

NEW QUESTION 269

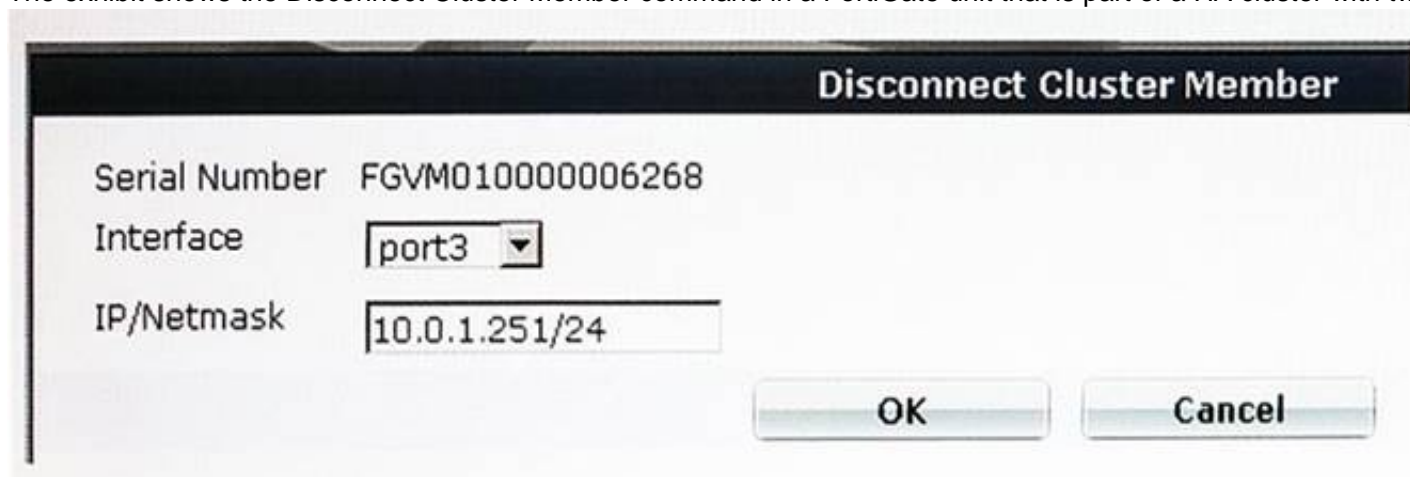
When creating FortiGate administrative users, which configuration objects specify the account rights?

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

Answer: C

NEW QUESTION 274

The exhibit shows the Disconnect Cluster Member command in a FortiGate unit that is part of a HA cluster with two HA members.



What is the effect of the Disconnect Cluster Member command as given in the exhibit. (Choose two.)

- A. Port3 is configured with an IP address management access.
- B. The firewall rules are purged on the disconnected unit.
- C. The HA mode changes to standalone.
- D. The system hostname is set to the unit serial number.

Answer: AC

NEW QUESTION 275

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 276

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 280

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 285

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 290

To which remote device can the FortiGate send logs? (Choose three.)

- A. Syslog
- B. FortiAnalyzer
- C. Hard drive
- D. Memory
- E. FortiCloud

Answer: ABE

NEW QUESTION 295

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 296

What is IPsec Perfect Forwarding Secrecy (PFS)?

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

Answer: B

NEW QUESTION 297

The exhibit shows two static routes to the same destinations subnet 172.20.168.0/24.

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

Which of the following statements correctly describes this static routing configuration? (choose two)

- A. Both routes will show up in the routing table.
- B. The FortiGate unit will evenly share the traffic to 172.20.168.0/24 between routes.
- C. Only one route will show up in the routing table.
- D. The FortiGate will route the traffic to 172.20.168.0/24 only through one route.

Answer: CD

NEW QUESTION 301

What is valid reason for using session based authentication instead of IP based authentication in a FortiGate web proxy solution?

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

Answer: C

NEW QUESTION 303

A client can establish a secure connection to a corporate network using SSL VPN in tunnel mode. Which of the following statements are correct regarding the use of tunnel mode SSL VPN? (Select all that apply.)

- A. Split tunneling can be enabled when using tunnel mode SSL VPN.
- B. Client software is required to be able to use a tunnel mode SSL VPN.
- C. Users attempting to create a tunnel mode SSL VPN connection must be authenticated by at least one SSL VPN policy.
- D. The source IP address used by the client for the tunnel mode SSL VPN is assigned by the FortiGate unit.

Answer: ABCD

NEW QUESTION 308

.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questions 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 First Try
- * NSE4 Practice Test Questions in Multiple Choice Formats and Updates for 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The NSE4 Practice Test Here](#)