

NSE4 Dumps

Fortinet Network Security Expert 4 Written Exam (400)

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



NEW QUESTION 1

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

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

Answer: B

NEW QUESTION 2

Which protocols can you use for secure administrative access to a FortiGate? (Choose two)

- A. SSH
- B. Telnet
- C. NTLM
- D. HTTPS

Answer: AD

NEW QUESTION 3

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 4

Which of the following FSSO agents are required for a DC agent mode solution? (Choose two.)

- A. FSSO agent
- B. DC agent
- C. Collector agent
- D. Radius server

Answer: BC

NEW QUESTION 5

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 6

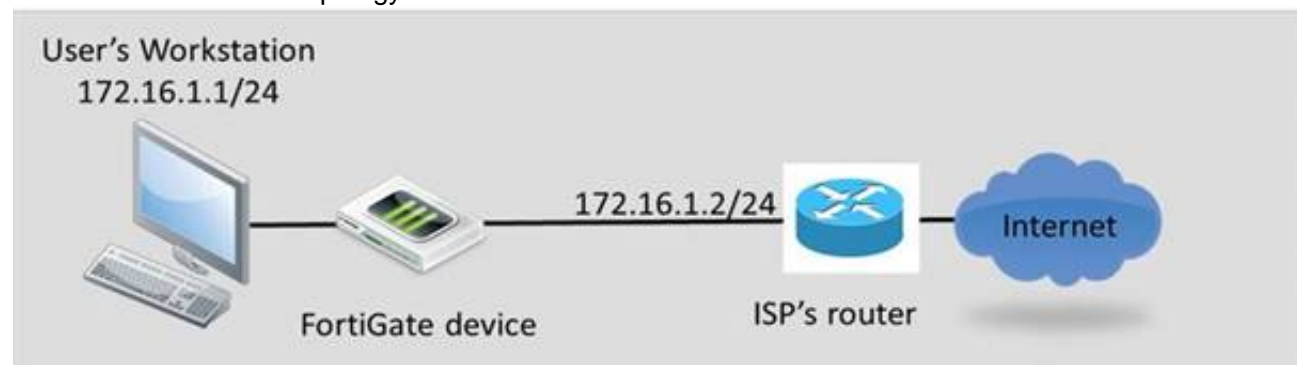
Which statement best describes what the FortiGate hardware acceleration processors main task is?

- 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 7

Review to the network topology in the exhibit.



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

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

Answer: AD

NEW QUESTION 8

Which is NOT true about source matching with firewall policies?

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

Answer: E

NEW QUESTION 9

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

Which two statements are true regarding firewall policy disclaimers? (Choose two.)

- A. They cannot be used in combination with user authentication.
- B. They can only be applied to wireless interfaces.
- C. Users must accept the disclaimer to continue.
- D. The disclaimer page is customizable.

Answer: CD

NEW QUESTION 10

Which statements are correct regarding virtual domains (VDOMs)? (Choose two)

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

Answer: BC

NEW QUESTION 12

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

- A. All routes to the destination subnet configured in the link health monitor are removed from the routing table.
- B. The distance values of all routes using interface configured in the link health monitor are increased.
- C. The priority values of all routes using configured in the link health monitor are increased.
- D. All routes using the next-hop gateway configured in the link health monitor are removed from the routing table.

Answer: D

NEW QUESTION 13

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 16

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 19

For data leak prevention, which statement describes the difference between the block and quarantine actions?

- A. A block action prevents the transactio
- B. A quarantine action blocks all future transactions, regardless of the protocol.
- C. A block action prevents the transactio
- D. A quarantine action archives the data.
- E. A block action has a finite duratio
- F. A quarantine action must be removed by an administrator.
- G. A block action is used for known user
- H. A quarantine action is used for unknown users.

Answer: A

NEW QUESTION 21

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 24

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 25

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 29

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 30

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 34

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=FCClient_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=FCClient 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=FCClient 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 38

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 43

Which of the following are benefits of using web caching? (Choose three.)

- A. Decrease bandwidth utilization
B. Reduce server load
C. Reduce FortiGate CPU usage
D. Reduce FortiGate memory usage
E. Decrease traffic delay

Answer: ABE

NEW QUESTION 48

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 50

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 55

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 58

When configuring LDAP on the FortiGate as a remote database for users, what is not a part of the configuration?

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

Answer: C

NEW QUESTION 60

Which of the following statement correct describes the use of the "diagnose sys ha reset- uptime" command?

- A. To force an HA failover when the HA override setting is disabled.
B. To force an HA failover when the HA override setting is enabled.
C. To clear the HA counters.
D. To restart a FortiGate unit that is part of an HA cluster.

Answer: A

NEW QUESTION 61

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 65

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

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

Answer: ABE

NEW QUESTION 69

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

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

Answer: C

NEW QUESTION 73

In "diag debug flow" output, you see the message "Allowed by Policy-1: SNAT". Which is true?

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

Answer: B

NEW QUESTION 74

What attributes are always included in a log header? (Choose three.)

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

Answer: BDE

NEW QUESTION 78

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 79

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 80

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 84

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 88

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 92

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 95

A backup file begins with this line:

```
#config-version=FGVM64-5.02-FW-build589-140613:opmode=0:vdom=0:user=admin
```

```
#conf_file_ver=3881503152630288414 #buildno=0589 #global_vdom=1
```

Can you restore it to a FortiWiFi 60D?

- A. Yes
- B. Yes, but only if you replace the "#conf_file_ver" line so that it contains the serial number of that specific FortiWiFi 60D.
- C. Yes, but only if it is running the same version of FortiOS, or a newer compatible version.
- D. No

Answer: D

NEW QUESTION 97

Which of the following statements are true regarding application control? (choose two)

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

Answer: CD

NEW QUESTION 99

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 100

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 103

What logging options are supported on a FortiGate unit? (Choose two.)

- A. LDAP
- B. Syslog
- C. FortiAnalyzer
- D. SNMP

Answer: BC

NEW QUESTION 107

Acme Web Hosting is replacing one of their firewalls with a FortiGate. It must be able to apply port forwarding to their back-end web servers while blocking virus uploads and TCP SYN floods from attackers. Which operation mode is the best choice for these requirements?

- A. NAT/route
- B. NAT mode with an interface in one-arm sniffer mode
- C. Transparent mode
- D. No appropriate operation mode exists

Answer: A

NEW QUESTION 108

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 field "Key Usage=KeyCertSign"
- C. It must be installed in the FortiGate device
- D. The subject field must contain either the FQDN, or the IP address of the FortiGate device

Answer: CD

NEW QUESTION 109

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 113

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

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

Answer: CD

NEW QUESTION 115

An Internet browser is using the WPAD DNS method to discover the PAC file's URL. The DNS server replies to the browser's request with the IP address 10.100.1.10. Which URL will the browser use to download the PAC file?

- A. http://10.100.1.10/proxy.pac
- B. https://10.100.1.10/
- C. http://10.100.1.10/wpad.dat
- D. https://10.100.1.10/proxy.pac

Answer: C

NEW QUESTION 120

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 125

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 126

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 130

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 133

What are the requirements for a HA cluster to maintain TCP connections after device or link failover? (Choose two.)

- A. Enable session pick-up.
- B. Enable override.
- C. Connections must be UDP or ICMP.
- D. Connections must not be handled by a proxy.

Answer: AD

NEW QUESTION 134

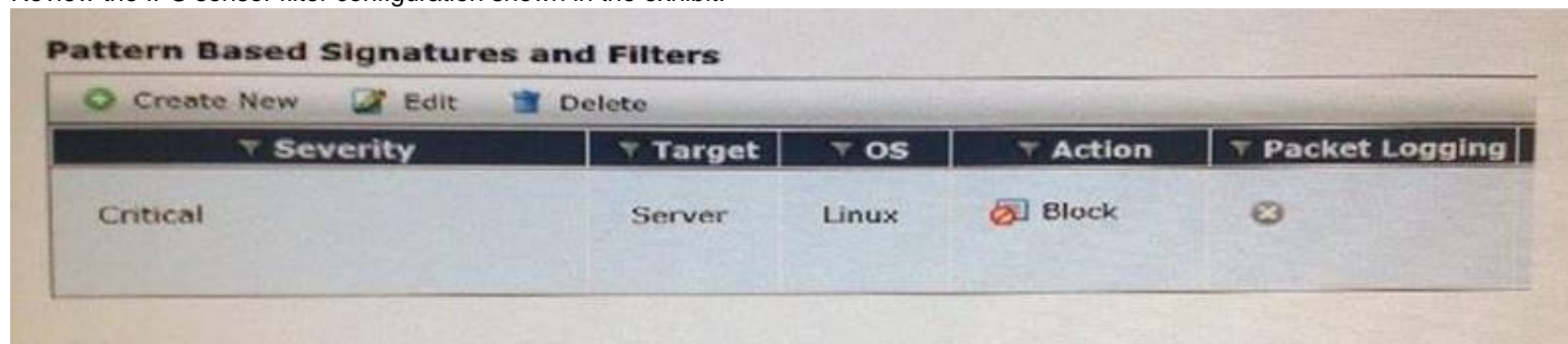
Which are outputs for the command 'diagnose hardware deviceinfo nic'? (Choose two.)






- A. ARP cache
- B. Physical MAC address
- C. Errors and collisions
- D. Listening TCP ports

Answer: BC

NEW QUESTION 139

Review the IPS sensor filter configuration shown in the exhibit.



Pattern Based Signatures and Filters				
 Create New	 Edit	 Delete		
Severity	Target	OS	Action	Packet Logging
Critical	Server	Linux	 Block	

Based on the information in the exhibit, which statements are correct regarding the filter? (Choose two.)

- A. It does not log attacks targeting Linux servers.
- B. It matches all traffic to Linux servers.
- C. Its action will block traffic matching these signatures.
- D. It only takes affect when the sensor is applied to a policy.

Answer: CD

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 143

In which process states is it impossible to interrupt/kill a process? (Choose two.)

- A. S – Sleep
- B. R – Running
- C. D – Uninterruptable Sleep
- D. Z – Zombie

Answer: CD

NEW QUESTION 146

Which two web filtering inspection modes inspect the full URL? (Choose two.)

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

Answer: BC

NEW QUESTION 148

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 153

In a FSSO agent mode solution, how does the FSSO collector agent learn each IP address?

- A. The DC agents get each user IP address from the event logs and forward that information to the collector agent
- B. The collector agent does not know, and does not need, each user IP address
- C. Only workstation names are known by the collector agent.
- D. The collector agent frequently polls the AD domain controllers to get each user IP address.
- E. The DC agent learns the workstation name from the event logs and DNS is then used to translate those names to the respective IP addresses.

Answer: D

NEW QUESTION 157

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 159

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 160

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

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

Answer: B

NEW QUESTION 164

A static route is configured for a FortiGate unit from the CLI using the following commands:

```
config router static edit 1
set device "wan1" set distance 20
set gateway 192.168.100.1 next
end
```

Which of the following conditions are required for this static default route to be displayed in the FortiGate unit's routing table? (Choose two.)

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

Answer: BD

NEW QUESTION 166

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 167

A FortiGate devices is configured with four VDOMs: 'root' and 'vdom1' are in NAT/route mode; 'vdom2' and 'vdom2' are in transparent mode. The management VDOM is 'root'. Which of the following statements are true? (Choose two.)

- A. An inter-VDOM link between 'root' and 'vdom1' can be created.
- B. An inter-VDOM link between 'vdom1' and vdom2' can created.
- C. An inter-VDOM link between 'vdom2' and vdom3' can created.
- D. Inter-VDOM link links must be manually configured for FortiGuard traffic.

Answer: AB

NEW QUESTION 172

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 176

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 178

Which of the following email spam filtering features is NOT supported on a FortiGate unit?

- A. Multipurpose Internet Mail Extensions (MIME) Header Check
- B. HELO DNS Lookup
- C. Greylisting
- D. Banned Word

Answer: C

NEW QUESTION 181

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 182

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 186



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

The screenshot displays the FortiGate IPsec configuration interface. It is divided into four main sections: Peer Options, Phase 1 Proposal, XAUTH, and Phase 2 Selectors. In the Peer Options section, 'Accept Types' is set to 'This peer ID' and 'Peer ID' is 'fortinet'. The Phase 1 Proposal section shows 'Encryption' as 3DES and 'Authentication' as SHA1. Under Diffie-Hellman Groups, the options 14 and 5 are selected. 'Key Lifetime (seconds)' is set to 86400. The XAUTH section shows 'Type' as 'Disabled'. The Phase 2 Selectors section shows a table with 'Local Address' and 'Remote Address' both set to 0.0.0.0/0.0.0.0.

Peer Options			
Accept Types	This peer ID ▼		
Peer ID	fortinet		

Phase 1 Proposal			
Encryption	3DES ▼	Authentication	SHA1 ▼
Diffie-Hellman Groups	<input type="checkbox"/> 21 <input type="checkbox"/> 20 <input type="checkbox"/> 19 <input type="checkbox"/> 18 <input type="checkbox"/> 17 <input type="checkbox"/> 16 <input type="checkbox"/> 15 <input checked="" type="checkbox"/> 14 <input checked="" type="checkbox"/> 5 <input type="checkbox"/> 2 <input type="checkbox"/> 1		
Key Lifetime (seconds)	86400		
Local ID			

XAUTH	
Type	Disabled ▼

Phase 2 Selectors			
Name	Local Address	Remote Address	
	0.0.0.0/0.0.0.0	0.0.0.0/0.0.0.0	 

- 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 189

A FortiGate device is configured with two VDOMs. The management VDOM is 'root' , and is configured in transparent mode,'vdom1' is configured as NAT/route mode. Which traffic is generated only by 'root' and not 'vdom1'? (Choose three.)

- A. SNMP traps
- B. FortiGaurd
- C. ARP
- D. NTP
- E. ICMP redirect

Answer: ABD

NEW QUESTION 191

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 6bddbfa7161237daa46c19725dd0292b062dda5
enc: spi=9293e7d4 esp=aes key=32 951be1d87860c0b59b98b170a17dcb75f77bd541bdc3a1847e54c78c0d43aa13
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 582af59d71635b835c9208878e0e3f3fe31ba1df88ff83ca9bab1ed66ac325e
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 193

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 194

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 198

If you enable the option "Generate Logs when Session Starts", what effect does this have on the number of traffic log messages generated for each session?

- A. No traffic log message is generated.
- B. One traffic log message is generated.
- C. Two traffic log messages are generated.
- D. A log message is only generated if there is a security event.

Answer: C

NEW QUESTION 200

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 201

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 204

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 208

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

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

Answer: D

NEW QUESTION 209

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 213

How many packets are interchanged between both IPSec ends during the negotiation of a main-mode phase 1?

- A. 5
- B. 3
- C. 2
- D. 6

Answer: D

NEW QUESTION 216

Which is NOT true about the settings for an IP pool type port block allocation?

- A. A Block Size defines the number of connections.
- B. Blocks Per User defines the number of connection blocks for each user.
- C. An Internal IP Range defines the IP addresses permitted to use the pool.
- D. An External IP Range defines the IP addresses in the pool.

Answer: B

NEW QUESTION 220

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 222

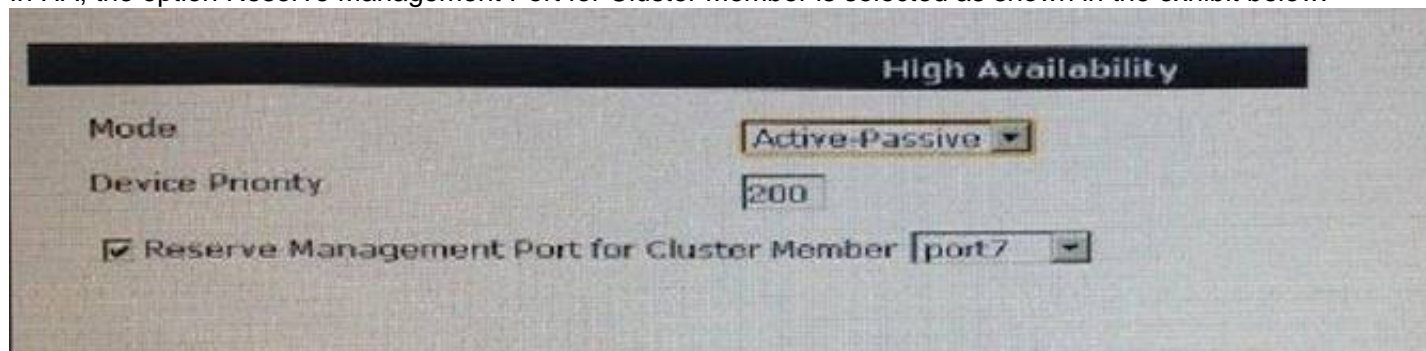
A FortiGate is configured with multiple VDOMs. An administrative account on the device has been assigned a Scope value of VDOM:root. Which of the following settings will this administrator be able to configure? (Choose two.)

- A. Firewall addresses
- B. DHCP servers
- C. FortiGuard Distribution Network configuration.
- D. System hostname.

Answer: AB

NEW QUESTION 224

In HA, the option Reserve Management Port for Cluster Member is selected as shown in the exhibit below.



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

- A. Interface settings on port7 will not be synchronized with other cluster members.
- B. The IP address assigned to this interface must not overlap with the IP address subnet assigned to another interface.
- C. When connecting to port7 you always connect to the master device.
- D. A gateway address may be configured for port7.

Answer: AD

NEW QUESTION 227

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 228

Which of the following statements are characteristics of a FSSO solution using advanced access mode? (Choose three.)

- A. Protection profiles can be applied to both individual users and user groups
- B. Nested or inherited groups are supported
- C. Usernames follow the LDAP convention: CN=User, OU=Name, DC=Domain
- D. Usernames follow the Windows convention: Domain\username
- E. Protection profiles can be applied to user groups only.

Answer: BCE

NEW QUESTION 230

Which of the following statements are correct regarding FortiGate virtual domains (VDMs)? (Choose two)

- A. VDMs 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 234

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 239

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 241

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

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

Answer: D

NEW QUESTION 245

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 247

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 248

Which of the following statements are correct regarding SSL VPN Web-only mode? (Choose two.)

- A. It can only be used to connect to web services.
- B. IP traffic is encapsulated over HTTPS.
- C. Access to internal network resources is possible from the SSL VPN portal.
- D. The standalone FortiClient SSL VPN client CANNOT be used to establish a Web-only SSL VPN.
- E. It is not possible to connect to SSH servers through the VPN.

Answer: BC

NEW QUESTION 250

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 252

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 9E2606AC7AE83D7A612DA78D3AB3F9450810050115B107050000005C26E2A7EC8461AC15E9B9C705B6C1F667A41957AED11F37003C07A1
07B0934D938E1A2C74348ED8FD6B39146C618525C6EC51E2F26385B63B8E035F52B4
ike 0:Remote_1:10: dec 9E2606AC7AE83D7A612DA78D3AB3F9450810050115B107050000005C0B000018E281874EECF170EB5222B6A4E3A027C714
C0000C02000000001011089289E2606AC7AE83D7A612DA78D3AB3F9450000009C17511ED6EE549507
ike 0:Remote_1:10: notify msg received: R-U-THERE
ike 0:Remote_1:10: enc 9E2606AC7AE83D7A612DA78D3AB3F94508100501734C5CDF000000540B0000181C047F014CEEF1B0EC8DA915F3B18AEB20
A0000C02000000001011089299E2606AC7AE83D7A612DA78D3AB3F9450000009C
ike 0:Remote_1:10: out 9E2606AC7AE83D7A612DA78D3AB3F94508100501734C5CDF0000005CB3CC431065A1737144B02F1AAE79C1BE712B84255
EB84E5FA7A9677E99C7B731057FF33728BB42AA983E79C919DA9B64EBC087EFOA02666C1FBD2C62F
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/612da78d3ab31
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 254

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 257

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 259

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 262

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 265

Caching improves performance by reducing FortiGate unit requests to the FortiGuard server. Which of the following statements are correct regarding the caching of FortiGuard responses?

- A. Caching is available for web filtering, antispam, and IPS requests.
- B. The cache uses a small portion of the FortiGate system memory.
- C. When the cache is full, the least recently used IP address or URL is deleted from the cache.
- D. An administrator can configure the number of seconds to store information in the cache before the FortiGate unit contacts the FortiGuard server again.
- E. The size of the cache will increase to accommodate any number of cached queries.

Answer: BCD

NEW QUESTION 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

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 272

An end user logs into the full-access SSL VPN portal and selects the Tunnel Mode option by clicking on the "Connect" button. The administrator has enabled split tunneling.



Given that the user authenticates against the SSL VPN policy shown in the image below, which statement below identifies the route that is added to the client's routing table.

- A. A route to destination matching the `WIN2K3' address object.
- B. A route to the destination matching the `all' address object.
- C. A default route.
- D. No route is added.

Answer: A

NEW QUESTION 274

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 279

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 283

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 285

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 289

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 290

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 291

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 296

When the SSL proxy is NOT doing man-in-the-middle interception of SSL traffic, which certificate field can be used to determine the rating of a website?

- A. Organizational Unit.
B. Common name.
C. Serial Number.
D. Validity.

Answer: B

NEW QUESTION 297

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 302

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

- A. 20 seconds
B. 30 seconds
C. 45 seconds
D. 10 seconds

Answer: B

NEW QUESTION 304

.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your NSE4 Exam with Our Prep Materials Via below:

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