

## Exam Questions NSE4

Fortinet Network Security Expert 4 Written Exam (400)

<https://www.2passeasy.com/dumps/NSE4/>



**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**

Examine the exhibit; then answer the question below.



The Vancouver FortiGate initially had the following information in its routing table:

- S 172.20.0.0/16 [10/0] via 172.21.1.2, port2
- C 172.21.0.0/16 is directly connected, port2
- C 172.11.11.0/24 is directly connected, port1

Afterwards, the following static route was added:

```
config router static edit 6
set dst 172.20.1.0 255.255.255.0
set priority 0
set device port1
set gateway 172.11.12.1 next
```

Since this change, the new static route is NOT showing up in the routing table. Given the information provided, which of the following describes the cause of this problem?

- A. The subnet 172.20.1.0/24 is overlapped with the subnet of one static route that is already in the routing table (172.20.0.0/16), so, we need to enable allow-subnet-overlap first.
- B. The 'gateway' IP address is NOT in the same subnet as the IP address of port1.
- C. The priority is 0, which means that the route will remain inactive.
- D. The static route configuration is missing the distance setting.

**Answer: B**

**NEW QUESTION 4**

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 5**

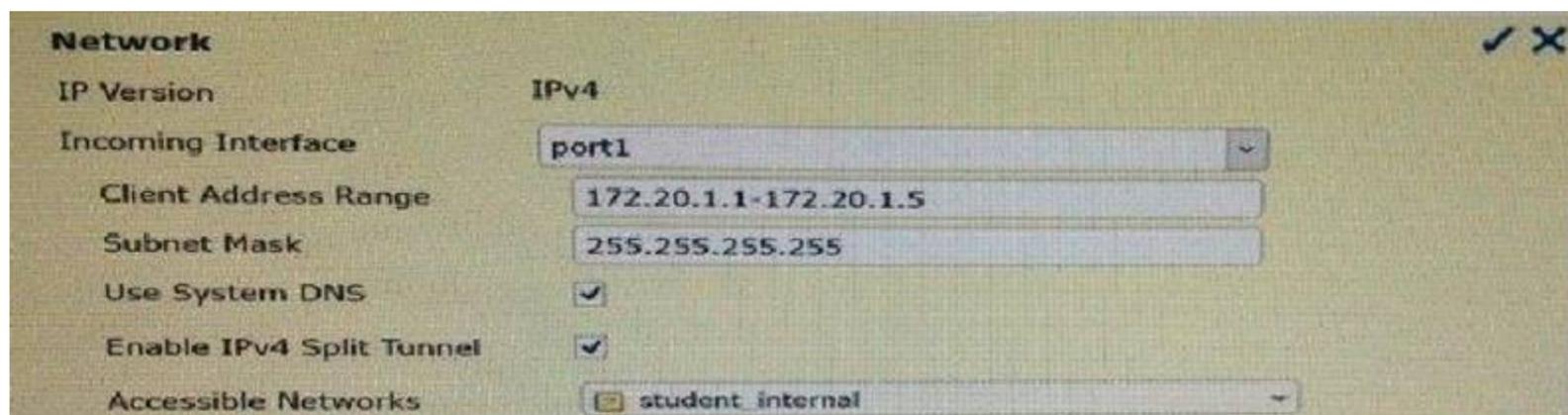
The order of the firewall policies is important. Policies can be re-ordered from either the GUI or the CLI. Which CLI command is used to perform this function?

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

**Answer: D**

**NEW QUESTION 6**

Review the configuration for FortiClient IPsec shown in the exhibit.



Which statement is correct regarding this configuration?

- A. The connecting VPN client will install a route to a destination corresponding to the student internal address object.
- B. The connecting VPN client will install a default route.
- C. The connecting VPN client will install a route to the 172.20.1.[1-5] address range.
- D. The connecting VPN client will connect in web portal mode and no route will be installed.

Answer: A

**NEW QUESTION 7**

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 8**

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

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

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

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

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

Answer: AC

**NEW QUESTION 9**

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 10**

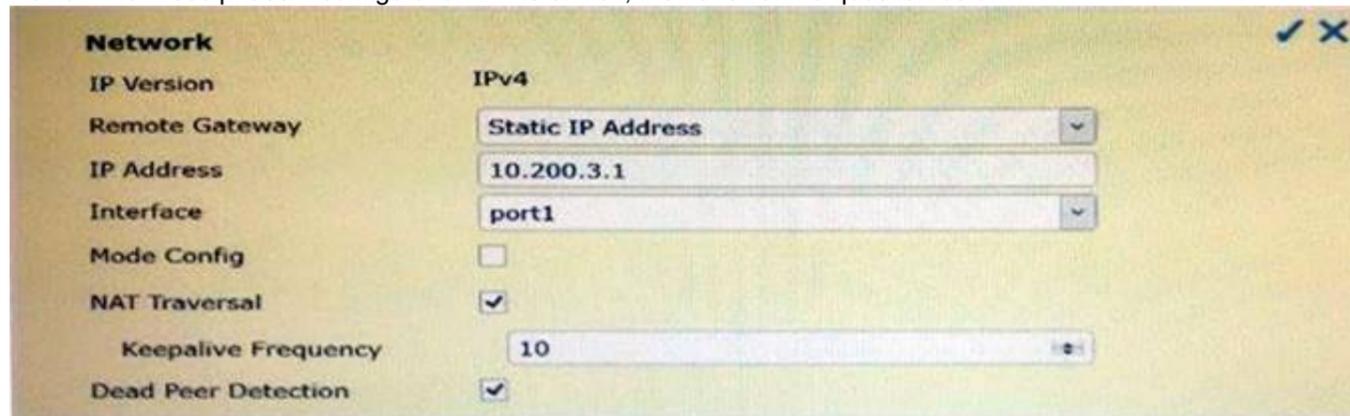
Which of the following statements is true regarding the use of a PAC file to configure the web proxy settings in an Internet browser? (Choose two.)

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

Answer: BC

**NEW QUESTION 10**

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



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 14**

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 18**

Examine the output below from the diagnose sys top command:

```
# diagnose sys top 1
Run time: 11 days, 3 hours and 29 minutes
OU,  ON,  1S,  99I;  971T,  528F,  160 KF
sshd      123      S    1.9    1.2
ipseedjine 61       S<   0.0    5.2
miglogd   45       S    0.0    4.9
pyfcgid   75       S    0.0    4.5
pyfcgid   73       S    0.0    3.9
```

Which statements are true regarding the output above (Choose two.)

- A. The sshd process is the one consuming most CPU.
- B. The sshd process is using 123 pages of memory.
- C. The command diagnose sys kill miglogd will restart the miglogd process.
- D. All the processes listed are in sleeping state.

Answer: AD

**NEW QUESTION 19**

Which commands are appropriate for investigating high CPU? (Choose two.)

- A. diag sys top
- B. diag hardware sysinfo mem
- C. diag debug flow
- D. get system performance status

Answer: AD

**NEW QUESTION 22**

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 27

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 32

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 36

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 37

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 38

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 41

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 45

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 47**

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 48**

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 51**

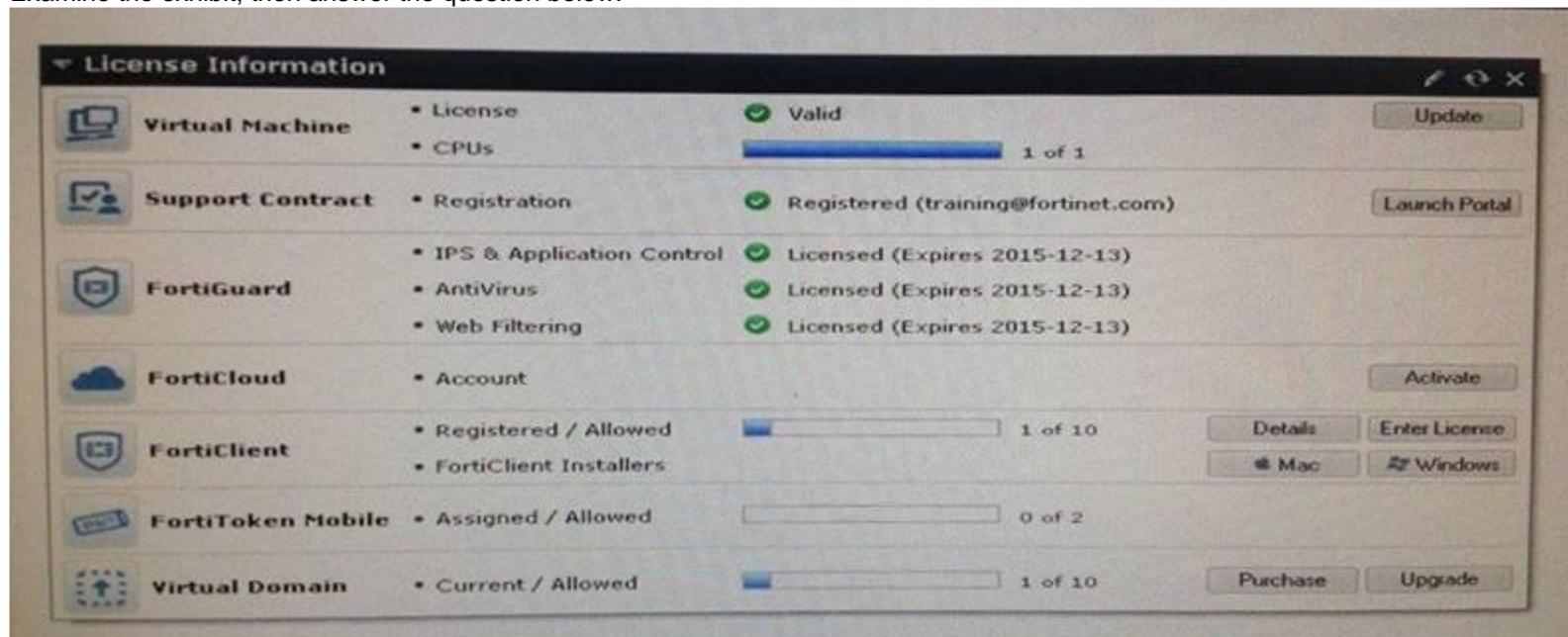
Which statements are correct regarding an IPv6 over IPv4 IPsec configuration? (Choose two.)

- 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 52**

Examine the exhibit; then answer the question below.



Which statement describes the green status indicators that appear next to the different FortiGuard Distribution Network services as illustrated in the exhibit?

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

Answer: D

**NEW QUESTION 54**

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 55

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 58

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 61

Examine the following output from the diagnose sys session list command:

```
session info: proto=6 proto_state=65 duration=3 expire=9 timeout=3600 flags=00000000
sockflag=00000000 sockport=443 av_idx=9 use=5

origin-shaper=guarantee-100kbps prio=2 guarantee 12800Bps max 134217728Bps traffic 13895Bps
reply-shaper=guarantee-100kbps prio=2 guarantee 12800Bps max 134217728Bps traffic 13895Bps
state=redir local may_dirty ndr npu nlb os rs

statistic(bytes/packets/allow_err): org=864/8/1 reply=2384/7/1 tuples=3

origin->sink: org pre->post, reply pre->post dev=7->6/6->7 gwy=172.17.87.3/10.1.10.1
hook=post dir=org act=snat 192.168.1.110:57999->74.201.86.29:443 (172.17.87.16:57999)
hook=pre dir=reply act=dnat 74.201.86.29:443->172.17.87.16:57999 (192.168.1.110:57999)
hook=post dir=reply act=noop 74.201.86.29:443->192.168.1.110:57999 (0.0.0.0:0)

misc=0 policy_id=1 id_policy_id=0 auth_info=0 chk_client_info=0 vd=0

npu info: flag=0x00/0x00, offload=0/0, ips_offload=0/0, epid=0/0, ipid=0/0, vlan=0/0
```

Which statements are true regarding the session above? (Choose two.)

- A. Session Time-To-Live (TTL) was configured to 9 seconds.
- B. FortiGate is doing NAT of both the source and destination IP address on all packets coming from the 192.168.1.110 address.
- C. The IP address 192.168.1.110 is being translated to 172.17.87.16.
- D. The FortiGate is not translating the TCP port numbers of the packets in this session.

Answer: CD

#### NEW QUESTION 64

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 65

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 68**

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 70**

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 73**

For FortiGate devices equipped with Network Processor (NP) chips, which are true? (Choose three.)

- A. For each new IP session, the first packet always goes to the CPU.
- B. The kernel does not need to program the NP
- C. When the NPU sees the traffic, it determines by itself whether it can process the traffic
- D. Once offloaded, unless there are errors, the NP forwards all subsequent packet
- E. The CPU does not process them.
- F. When the last packet is sent or received, such as a TCP FIN or TCP RST signal, the NP returns this session to the CPU for tear down.
- G. Sessions for policies that have a security profile enabled can be NP offloaded.

**Answer:** ACD

**NEW QUESTION 77**

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 78**

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 81**

In FortiOS session table output, what are the two possible 'proto\_state' values for a UDP session? (Choose two.)

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

**Answer:** AC

**NEW QUESTION 82**

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

- A. ICMP type and code

- B. TCP/UDP source and destination ports
- C. IP protocol number
- D. TCP sequence number

Answer: D

**NEW QUESTION 84**

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 88**

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 91**

What types of troubleshooting can you do when uploading firmware? (Choose two.)

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

Answer: AD

**NEW QUESTION 95**

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 99**

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)	
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)	
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)	
Web Filtering	Valid License (Expires 2013-05-11)	
Email Filtering	Valid License (Expires 2013-05-11)	

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 104

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 108

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 110

You have configured the DHCP server on a FortiGate's port1 interface (or internal, depending on the model) to offer IPs in a range of 192.168.1.65-192.168.1.253. When the first host sends a DHCP request, what IP will the DHCP offer?

- A. 192.168.1.99
- B. 192.168.1.253
- C. 192.168.1.65
- D. 192.168.1.66

**Answer:** C

#### NEW QUESTION 111

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 116

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

- A. They are accelerated by hardware in the master unit.
- B. They are not accelerated by hardware in the master unit.
- C. They are accelerated by hardware in the slave unit.
- D. They are not accelerated by hardware in the slave unit.

**Answer:** AD

#### NEW QUESTION 121

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 123

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

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

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

**Answer:** D

#### NEW QUESTION 126

Which of the following statements is true regarding the TCP SYN packets that go from a client, through an implicit web proxy (transparent proxy), to a web server listening at TCP port 80? (Choose three.)

- A. The source IP address matches the client IP address.
- B. The source IP address matches the proxy IP address.
- C. The destination IP address matches the proxy IP address.
- D. The destination IP address matches the server IP addresses.
- E. The destination TCP port number is 80.

**Answer:** ADE

#### NEW QUESTION 128

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

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

**Answer:** ABC

#### NEW QUESTION 131

What must be configured in order to keep two static routes to the same destination in the routing table?

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

**Answer:** B

#### NEW QUESTION 133

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 137

Which of the following statements best describe what a FortiGate does when packets match a black hole route?

- A. Packets are dropped.
- B. Packets are routed based on the information in the policy-based routing table.
- C. An ICMP error message is sent back to the originator.
- D. Packet are routed back to the originator.

**Answer:** A

#### NEW QUESTION 139

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 142

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 143**

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

Seq.#	Source	Destination	Schedule	Service	Authentication	Action	UTM Profile	Log	NA
port3 - port1 (1 - 1)									
1	all	all	always	ALL		ACCEPT			
port1 - port3 (2 - 2)									
2	all	WIN2K3				SSL-VPN			
ssl.root (sslvpn tunnel interface) - port3 (3 - 3)									
3	all	all	always	ALL		ACCEPT			
Implicit (4 - 4)									
4	any	any	always	ALL		DENY			

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

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

Answer: A

**NEW QUESTION 147**

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 150**

An administrator wants to create an IPsec VPN tunnel between two FortiGate devices. Which three configuration steps must be performed on both units to support this scenario? (Choose three.)

- A. Create firewall policies to allow and control traffic between the source and destination IP addresses.
- B. Configure the appropriate user groups to allow users access to the tunnel.
- C. Set the operating mode to IPsec VPN mode.
- D. Define the phase 2 parameters.
- E. Define the Phase 1 parameters.

Answer: ADE

**NEW QUESTION 153**

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 154**

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 158**

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 160**

.....

## THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual NSE4 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the NSE4 Product From:

<https://www.2passeasy.com/dumps/NSE4/>

### Money Back Guarantee

#### **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