

## NSE4 Dumps

### Fortinet Network Security Expert 4 Written Exam (400)

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



### 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

How is traffic routed onto an SSL VPN tunnel from the FortiGate unit side?

- A. A static route must be configured by the administrator using the ssl.root interface as the outgoing interface.
- B. Assignment of an IP address to the client causes a host route to be added to the FortiGate unit's kernel routing table.
- C. A route back to the SSLVPN IP pool is automatically created on the FortiGate unit.
- D. The FortiGate unit adds a route based upon the destination address in the SSL VPN firewall policy.

**Answer: B**

### NEW QUESTION 4

Examine the exhibit; then answer the question below.



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

S 172.20.0.0/16 [10/0] via 172.21.1.2, port2

C 172.21.0.0/16 is directly connected, port2

C 172.11.11.0/24 is directly connected, port1

Afterwards, the following static route was added:

```
config router static edit 6
```

```
set dst 172.20.1.0 255.255.255.0
```

```
set priority 0
```

```
set device port1
```

```
set gateway 172.11.12.1 next
```

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

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

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

**Answer:** B

#### NEW QUESTION 5

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 6

With FSSO DC-agent mode, a domain user could authenticate either against the domain controller running the collector agent and domain controller agent, or a domain controller running only the domain controller agent.

If you attempt to authenticate with a domain controller running only the domain controller agent, which statements are correct? (Choose two.)

- A. The login event is sent to a collector agent.  
B. The FortiGate receives the user information directly from the receiving domain controller agent of the secondary domain controller.  
C. The domain collector agent may perform a DNS lookup for the authenticated client's IP address.  
D. The user cannot be authenticated with the FortiGate in this manner because each domain controller agent requires a dedicated collector agent.

**Answer:** AC

#### NEW QUESTION 7

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

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

**Answer:** AD

#### NEW QUESTION 8

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 9

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

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

**Answer:** BC

#### NEW QUESTION 10

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
ipsendjine 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 10

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 11

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 15

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 16

Which of the following web filtering modes can inspect the full URL? (Choose two.)

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

**Answer:** AD

#### NEW QUESTION 19

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 24

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 25

Which of the following are possible actions for FortiGuard web category filtering? (Choose three.)

- A. Allow  
B. Block  
C. Exempt  
D. Warning

E. Shape

**Answer:** ABD

**NEW QUESTION 26**

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 29**

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 32**

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 34**

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 38**

Review the IPsec phase 2 configuration shown in the exhibit; then answer the question below.



**Phase 2 Selectors**

Name	Local Address	Remote Address
	0.0.0.0/0.0.0.0	0.0.0.0/0.0.0.0

**Edit Phase 2** ✓✕

Name: remote

Comments: VPN: remote (Created by VPN wizard)

Local Address: Subnet 0.0.0.0/0.0.0.0

Remote Address: Subnet 0.0.0.0/0.0.0.0

▼ Advanced...

**Phase 2 Proposal** + Add

Encryption: AES256 Authentication: SHA512

Enable Replay Detection ☒

Enable Perfect Forward Secrecy (PFS) ☒

Diffie-Hellman Group:
 ☐ 21 ☐ 20 ☐ 19 ☐ 18 ☐ 17  
☐ 16 ☐ 15 ☒ 14 ☒ 5 ☐ 2 ☐ 1

Local Port: All ☒

Remote Port: All ☒

Protocol: All ☒

Autokey Keep Alive ☒

Auto-negotiate ☒

Key Lifetime: Seconds 43200

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

- A. The Phase 2 will re-key even if there is no traffic.
- B. There will be a DH exchange for each re-key.
- C. The sequence number of ESP packets received from the peer will not be checked.
- D. Quick mode selectors will default to those used in the firewall policy.

**Answer:** AB

#### NEW QUESTION 40

Examine the exhibit; then answer the question below.

**License Information**

<b>Virtual Machine</b>	• License	Valid	Update
	• CPUs	1 of 1	
<b>Support Contract</b>	• Registration	Registered (training@fortinet.com)	Launch Portal
<b>FortiGuard</b>	• IPS & Application Control	Licensed (Expires 2015-12-13)	
	• AntiVirus	Licensed (Expires 2015-12-13)	
	• Web Filtering	Licensed (Expires 2015-12-13)	
<b>FortiCloud</b>	• Account		Activate
<b>FortiClient</b>	• Registered / Allowed	1 of 10	Details Enter License
	• FortiClient Installers		Mac Windows
<b>FortiToken Mobile</b>	• Assigned / Allowed	0 of 2	
<b>Virtual Domain</b>	• Current / Allowed	1 of 10	Purchase Upgrade

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 41**

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 46**

An administrator has configured a route-based site-to-site IPsec VPN. Which statement is correct regarding this IPsec VPN configuration?

- A. The IPsec firewall policies must be placed at the top of the list.
- B. This VPN cannot be used as a part of a hub and spoke topology.
- C. Routes are automatically created based on the quick mode selectors.
- D. A virtual IPsec interface is automatically created after the Phase 1 configuration is completed.

**Answer:** D

**NEW QUESTION 48**

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 51**

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 55**

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 60**

An administrator configures a FortiGate unit in Transparent mode on the 192.168.11.0 subnet. Automatic Discovery is enabled to detect any available FortiAnalyzers on the network.

Which of the following FortiAnalyzers will be detected?

- A. 192.168.11.100
- B. 192.168.11.251
- C. 192.168.10.100
- D. 192.168.10.251

**Answer:** AB

**NEW QUESTION 64**

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



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

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

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

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

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

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

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

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

**Answer:** CD

#### NEW QUESTION 66

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 71

There are eight (8) log severity levels that indicate the importance of an event. Not including Debug, which is only needed to log diagnostic data, what are both the lowest AND highest severity levels?

- A. Notification, Emergency
- B. Information, Critical
- C. Error, Critical
- D. Information, Emergency
- E. Information, Alert

**Answer:** D

#### NEW QUESTION 74

Which IPsec configuration mode can be used for implementing GRE-over-IPsec VPNs?

- A. Policy-based only.
- B. Route-based only.
- C. Either policy-based or route-based VPN.
- D. GRE-based only.

**Answer:** B

#### NEW QUESTION 79

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 82**

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 84**

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 86**

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 88**

You have created a new administrator account, and assign it the prof\_admin profile. Which is false about that account's permissions?

- A. It cannot upgrade or downgrade firmware.
- B. It can create and assign administrator accounts to parts of its own VDOM.
- C. It can reset forgotten passwords for other administrator accounts such as "admin".
- D. It has a smaller permissions scope than accounts with the "super\_admin" profile.

**Answer:** A

**NEW QUESTION 91**

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 94**

Which of the following FSSO modes must be used for Novell eDirectory networks?

- A. Agentless polling
- B. LDAP agent
- C. eDirectory agent
- D. DC agent

**Answer:** C

**NEW QUESTION 98**

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

**Peer Options**  
Accept Types This peer ID ▼  
Peer ID fortinet

**Phase 1 Proposal** ➕ Add  
Encryption 3DES ▼ Authentication SHA1 ▼  
Diffie-Hellman Groups ☐ 21 ☐ 20 ☐ 19 ☐ 18 ☐ 17 ☐ 16 ☐ 15 ☒ 14 ☒ 5 ☐ 2 ☐ 1  
Key Lifetime (seconds) 86400  
Local ID

**XAUTH**  
Type Disabled ▼

**Phase 2 Selectors**  

Name	Local Address	Remote Address	➕ Add
	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 99

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 102

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 105

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 109

Which of the following statements are correct concerning layer 2 broadcast domains in transparent mode VDOMs?(Choose two)

- A. The whole VDOM is a single broadcast domain even when multiple VLAN are used.
- B. Each VLAN is a separate broadcast domain.
- C. Interfaces configured with the same VLAN ID can belong to different broadcast domains.
- D. All the interfaces in the same broadcast domain must use the same VLAN ID.

**Answer:** BC

#### NEW QUESTION 112

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 114

Examine the following CLI configuration:  
config system session -ttl set default 1800  
end

What statement is true about the effect of the above configuration line?

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

**Answer:** A

#### NEW QUESTION 118

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 120

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 125

Which statement concerning IPS is false?

- A. IPS packages contain an engine and signatures used by both IPS and other flow-based scans.
- B. One-arm topology with sniffer mode improves performance of IPS blocking.
- C. IPS can detect zero-day attacks.
- D. The status of the last service update attempt from FortiGuard IPS is shown on System>Config>FortiGuard and in output from 'diag autoupdate version'



**Answer:** D

**NEW QUESTION 128**

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 130**

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

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

**Answer:** BD

**NEW QUESTION 133**

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

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

**Answer:** D

**NEW QUESTION 134**

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 138**

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 142**

Which UTM feature sends a UDP query to FortiGuard servers each time FortiGate scans a packet (unless the response is locally cached)?

- A. Antivirus
- B. VPN
- C. IPS
- D. Web Filtering

**Answer:** D

**NEW QUESTION 144**

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 149**

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 153**

Which of the following authentication methods are supported in an IPsec phase 1? (Choose two.)

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

**Answer:** CD

**NEW QUESTION 158**

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 161**

What actions are possible with Application Control? (Choose three.)

- A. Warn
- B. Allow
- C. Block
- D. Traffic Shaping
- E. Quarantine

**Answer:** BCD

**NEW QUESTION 166**

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

Exhibit A

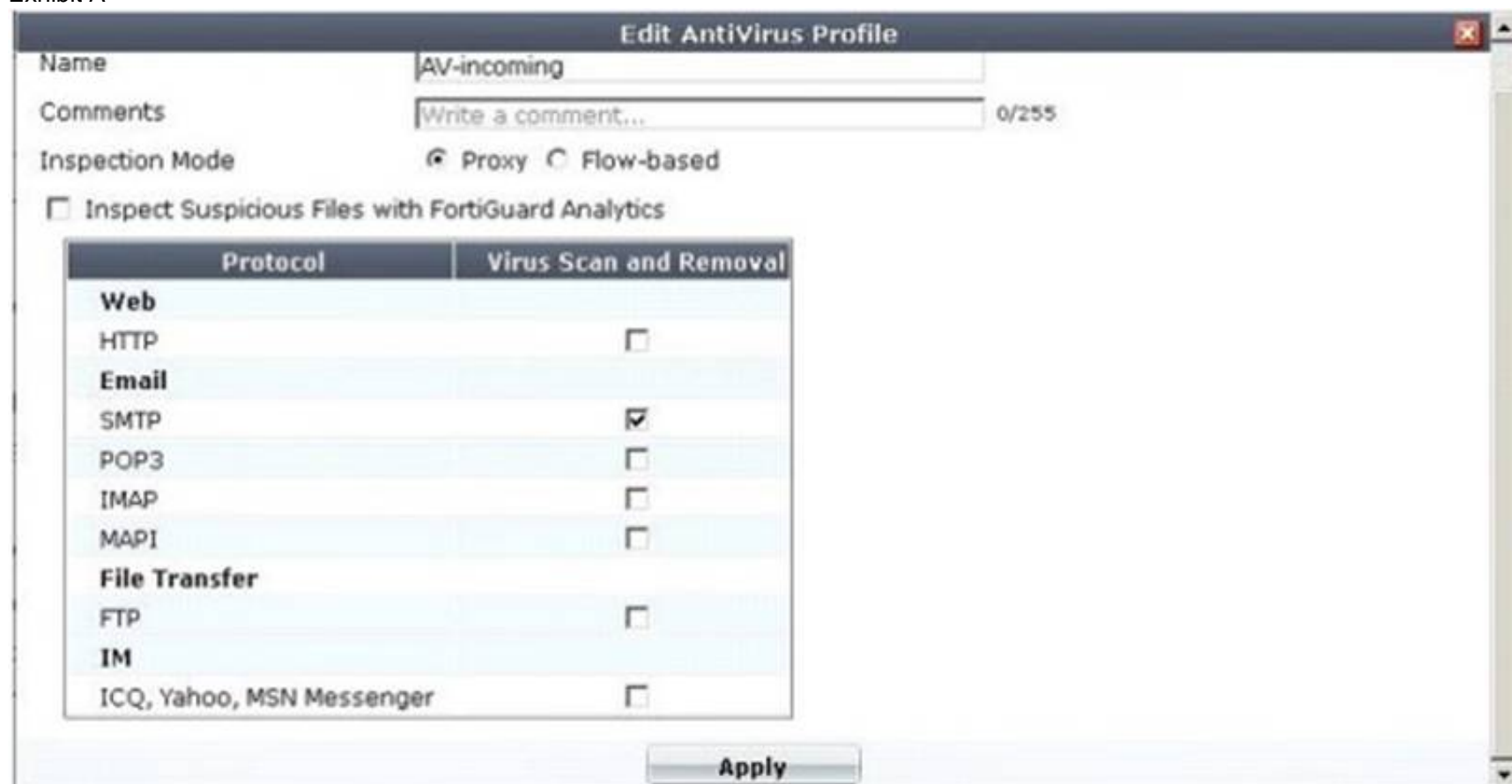


Exhibit B:

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

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

**Answer: B**

#### NEW QUESTION 167

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 172

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 173

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 177

.....



## 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>