Question: 1

Which of the following are purposes of NAT traversal in IPsec? (Choose two.)

A. To delete intermediary NAT devices in the tunnel path.
B. To dynamically change phase 1 negotiation mode aggressive mode.
C. To encapsulation ESP packets in UDP packets using port 4500.
D. To force a new DH exchange with each phase 2 rekey.

Answer: AC

Question: 2

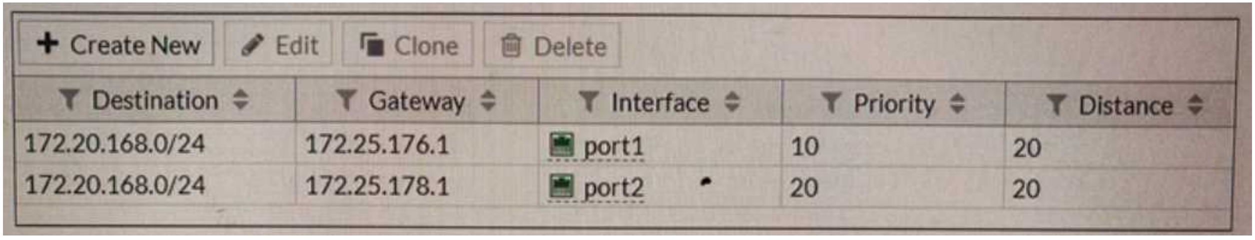
Which of the following statements correctly describes FortiGates route lookup behavior when searching for a suitable gateway? (Choose two)

A. Lookup is done on the trust packet from the session originator
B. Lookup is done on the last packet sent from the re spender
C. Lookup is done on every packet, regardless of direction
D. Lookup is done on the trust reply packet from the re spender

Answer: AB

Question: 3

Examine the two static routes shown in the exhibit, then answer title following question.



Destination	Gateway	Interface	Priority	Distance
172.20.168.0/24	172.25.176.1	port1	10	20
172.20.168.0/24	172.25.178.1	port2	20	20

Which of the following is the expected FortiGate behavior regarding these two routes to the same destination?

A. FortiGate will load balance all traffic across both routes.
B. FortiGate will use the port1 route as the primary candidate.
C. FortiGate will route twice as much traffic to the port2 route
D. FortiGate will only actuate the portl route m tlie routing table

Answer: C

Question: 4

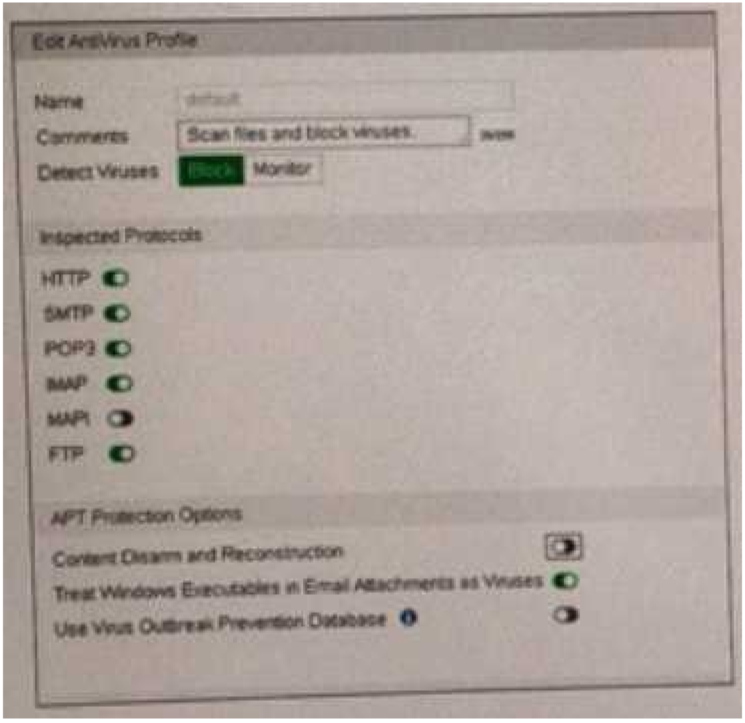
Which of the following statements about central NAT are true? (Choose two.)

A. IP tool references must be removed from existing firewall policies before enabling central NAT.
B. Central NAT can be enabled or disabled from the CLI only.
C. Source NAT, using central NAT, requires at least one central SNAT policy.
D. Destination NAT, using central NAT, requires a VIP object as the destination address in a firewall policy.

Answer: A, B

Question: 5

Refer to the following exhibit.



Edit AntiVirus Profile

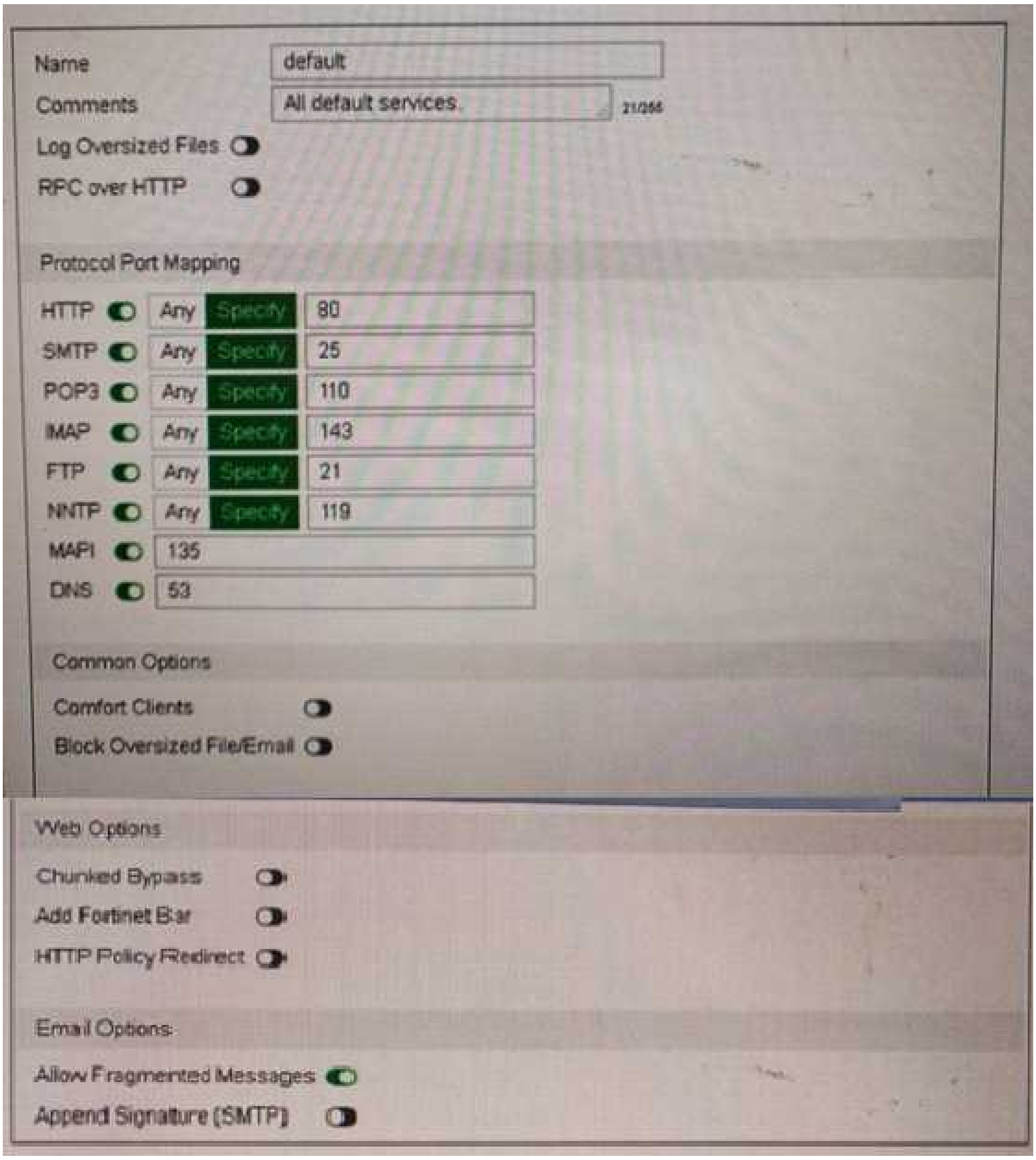
Name: default
Comments: Scan files and block viruses.
Detect Viruses: [✓ Block] Monitor

Inspected Protocols

HTTP ●
SMTP ●
POP3 ●
IMAP ●
MAPI ○
FTP ●

APT Protection Options

Content Disarm and Reconstruction ○
Treat Windows Executables in Email Attachments as Viruses ●
Use Virus Outbreak Prevention Database ○



Name: default

Comments: All default services. 21/255

Log Oversized Files ○

RPC over HTTP ○

Protocol Port Mapping

HTTP	●	Any [✓ Specify]	80
SMTP	●	Any [✓ Specify]	25
POP3	●	Any [✓ Specify]	110
IMAP	●	Any [✓ Specify]	143
FTP	●	Any [✓ Specify]	21
NNTP	●	Any [✓ Specify]	119
MAPI	●	135	
DNS	●	53	

Common Options

Comfort Clients ○

Block Oversized File/Email ○

Web Options

Chunked Bypass ○

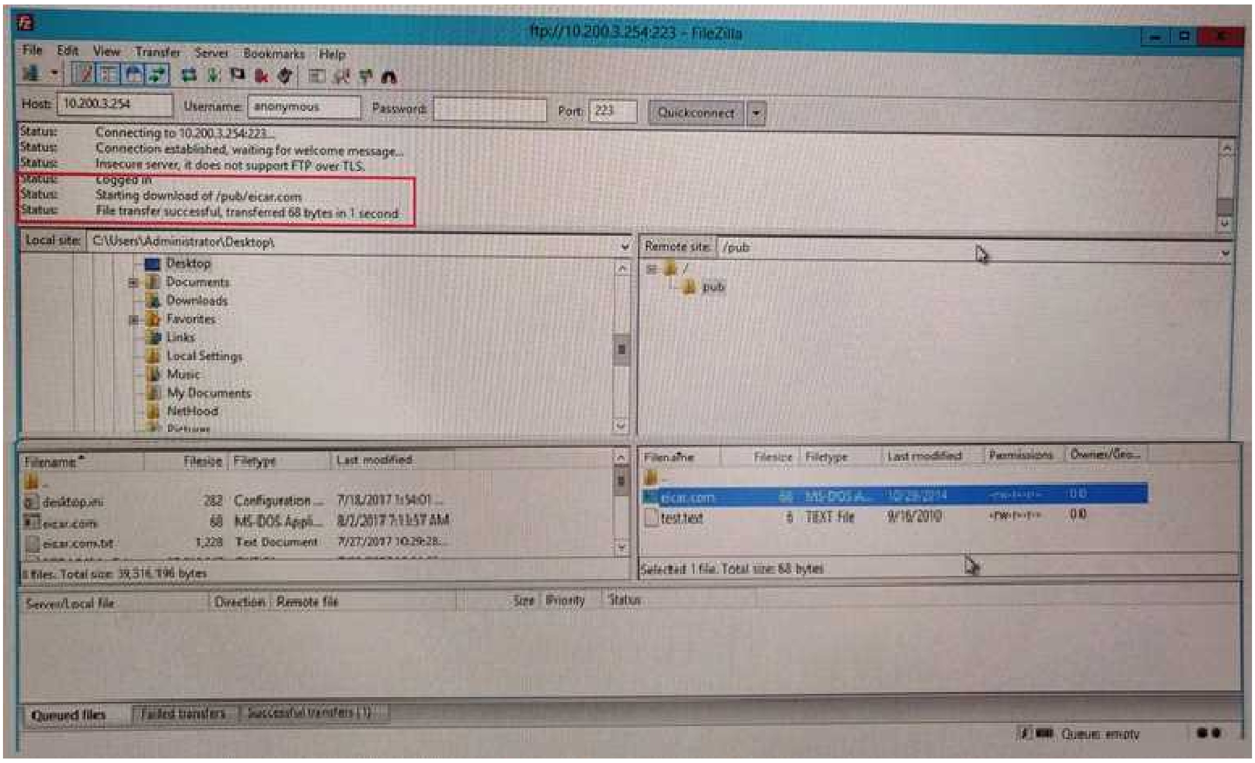
Add Fortinet Bar ○

HTTP Policy Redirect ○

Email Options

Allow Fragmented Messages ●

Append Signature (SMTP) ○



ftp://10.200.3.254:223 - FileZilla

Host: 10.200.3.254 Username: anonymous Password: Port: 223

```
Status:    Connecting to 10.200.3.254:223...
Status:    Connection established, waiting for welcome message...
Status:    Insecure server, it does not support FTP over TLS.
Status:    Logged in
Status:    Starting download of /pub/eicar.com
Status:    File transfer successful, transferred 68 bytes in 1 second
```

Local site: C:\Users\Administrator\Desktop\

Desktop
Documents
Downloads
Favorites
Links
Local Settings
Music
My Documents
NetHood

Remote site: /pub

/
pub

Filename	Filesize	Filetype	Last modified
..			
desktop.ini	282	Configuration ...	7/18/2017 1:54:01 ...
eicar.com	68	MS-DOS Appli...	8/2/2017 7:11:57 AM
eicar.com.txt	1,228	Text Document	7/27/2017 10:29:28...

8 files. Total size: 39,516,196 bytes

Filename	Filesize	Filetype	Last modified	Permissions	Owner/Gro...
..					
eicar.com	68	MS-DOS A...	10/28/2014	-rw-r--r--	0 0
test.text	6	TEXT File	9/16/2010	-rw-r--r--	0 0

Selected 1 file. Total size: 68 bytes

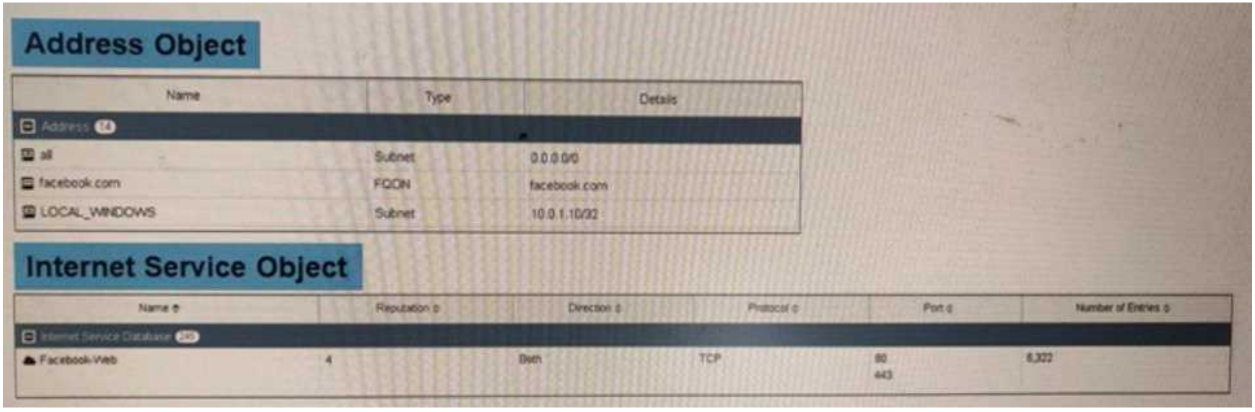
Why is FortiGate not blocking the test file over FTP download?

A. Deep-inspection must be enabled for FortiGate to fully scan FTP traffic.
B. FortiGate needs to be operating in flow-based inspection mode in order to scan FTP traffic.
C. The FortiSandbox signature database is required to successfully scan FTP traffic.
D. The proxy options profile needs to scan FTP traffic on a non-standard port.

Answer: D

Question: 6

View the following exhibit, which shows the firewall policies and the object uses in the firewall policies.



Address Object

Name	Type	Details
Address 14		
all	Subnet	0.0.0.0/0
facebook.com	FQDN	facebook.com
LOCAL_WINDOWS	Subnet	10.0.1.10/32

Internet Service Object

Name	Reputation	Direction	Protocol	Port	Number of Entries
Internet Service Database 245					
Facebook-Web	4	Both	TCP	80 443	6,322