# NSE4 Q&As

Fortinet Network Security Expert 4 Written Exam (400)

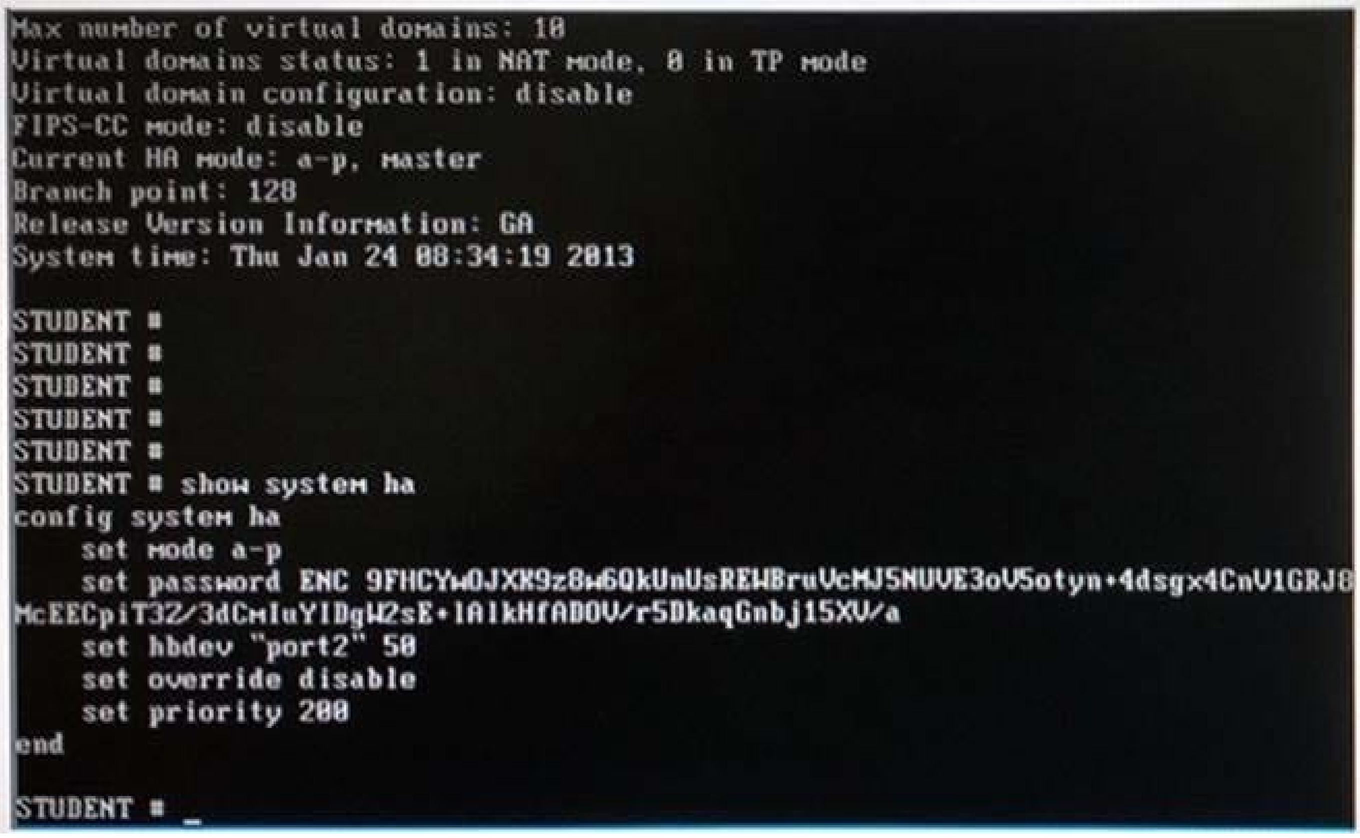
## Pass Fortinet NSE4 Exam with 100% Guarantee

Following Questions and Answers are all new published by Fortinet Official Exam Center

**QUESTION 1**

Two FortiGate devices fail to form an HA cluster, the device hostnames are STUDENT and REMOTE. Exhibit A shows the command output of show system ha for the STUDENT device. Exhibit B shows the command output of show system ha for the REMOTE device.

Exhibit A:

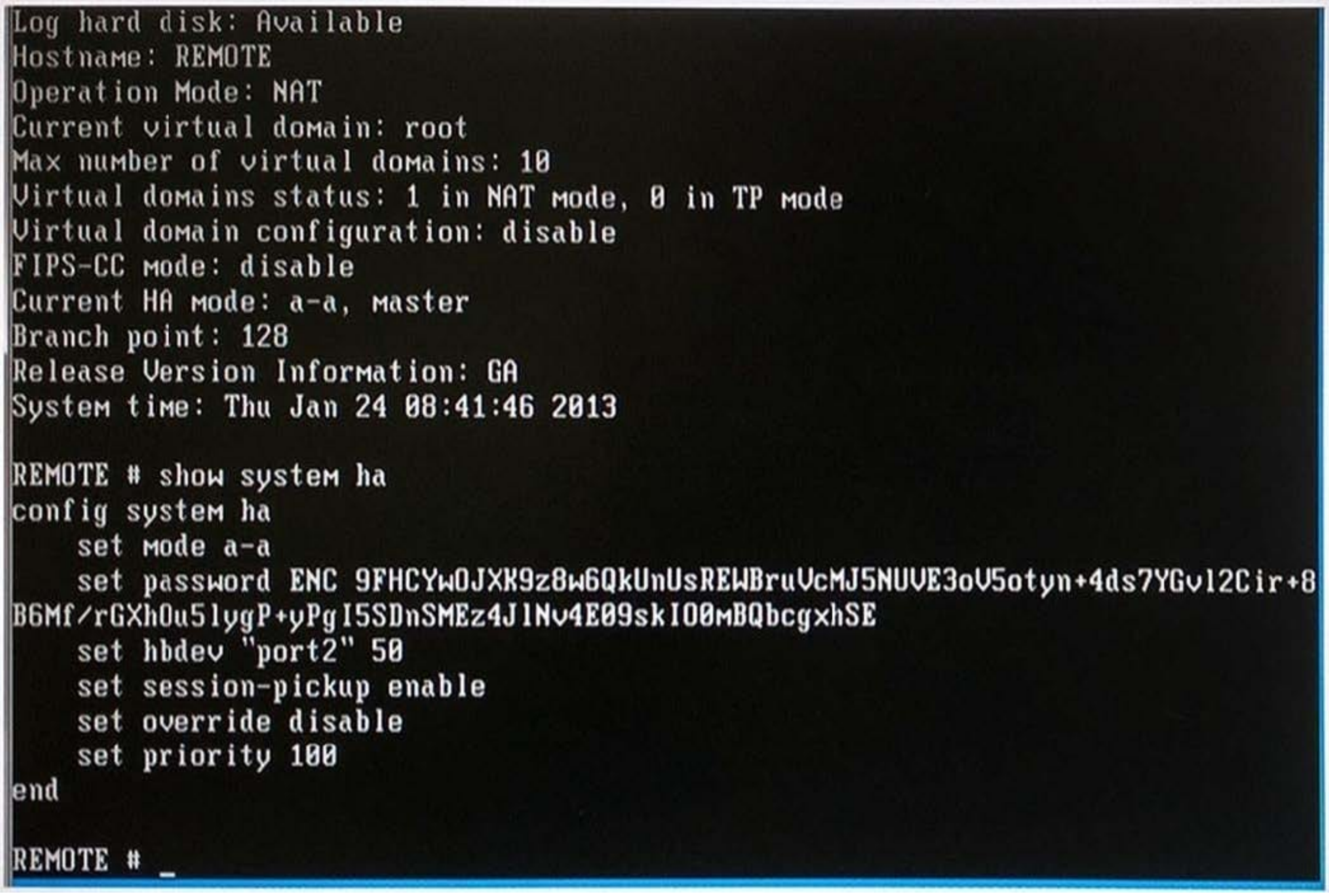


```
Max number of virtual domains: 10
Virtual domains status: 1 in NAT mode, 0 in TP mode
Virtual domain configuration: disable
FIPS-CC mode: disable
Current HA mode: a-p, master
Branch point: 128
Release Version Information: GA
System time: Thu Jan 24 08:34:19 2013

STUDENT #
STUDENT #
STUDENT #
STUDENT #
STUDENT #
STUDENT # show system ha
config system ha
    set mode a-p
    set password ENC 9FHCYwOJXK9z8w6QkUnUsREWBruVcMJ5NUVE3oV5otyn+4dsgx4CnV1GRJ8
McEECpiT32/3dCmIuYIDgW2sE+lAlkHfADOV/r5DkaqGnbj15XV/a
    set hbdev "port2" 50
    set override disable
    set priority 200
end

STUDENT # _
```

Exhibit B:



```
Log hard disk: Available
Hostname: REMOTE
Operation Mode: NAT
Current virtual domain: root
Max number of virtual domains: 10
Virtual domains status: 1 in NAT mode, 0 in TP mode
Virtual domain configuration: disable
FIPS-CC mode: disable
Current HA mode: a-a, master
Branch point: 128
Release Version Information: GA
System time: Thu Jan 24 08:41:46 2013

REMOTE # show system ha
config system ha
    set mode a-a
    set password ENC 9FHCYwOJXK9z8w6QkUnUsREWBruVcMJ5NUVE3oV5otyn+4ds7YGvl2Cir+8
B6Mf/rGXhOu5lygP+yPgI5SDnSMEz4JlNv4E09skIO0mBQbcgxhSE
    set hbdev "port2" 50
    set session-pickup enable
    set override disable
    set priority 100
end

REMOTE # _
```

Which one of the following is the most likely reason that the cluster fails to form?

A. Password

B. HA mode

C. Hearbeat

D. Override

Correct Answer: B

### QUESTION 2

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

Correct Answer: A

**QUESTION 3**

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.

Correct Answer: A

**QUESTION 4**

Which network protocols are supported for administrative access to a FortiGate unit? (Choose three.)

A. SMTP

B. WINS

C. HTTP

D. Telnet

E. SSH

Correct Answer: CDE

**QUESTION 5**

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

A. Traffic is dropped

B. Traffic is routed across the default phase 2.

C. Traffic is routed to the next available route in the routing table.

D. Traffic is routed unencrypted to the interface where the IPsec VPN is terminating.

Correct Answer: A

**QUESTION 6**

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

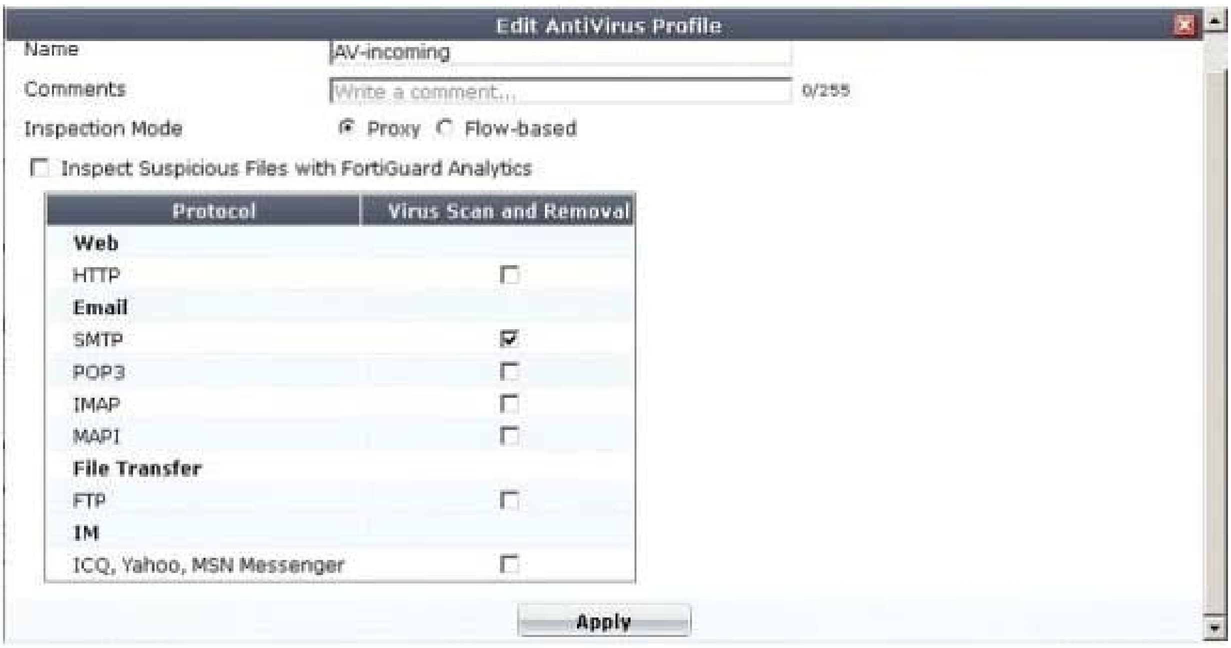
E. ICQ

Correct Answer: ABD

**QUESTION 7**

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



Name: AV-incoming

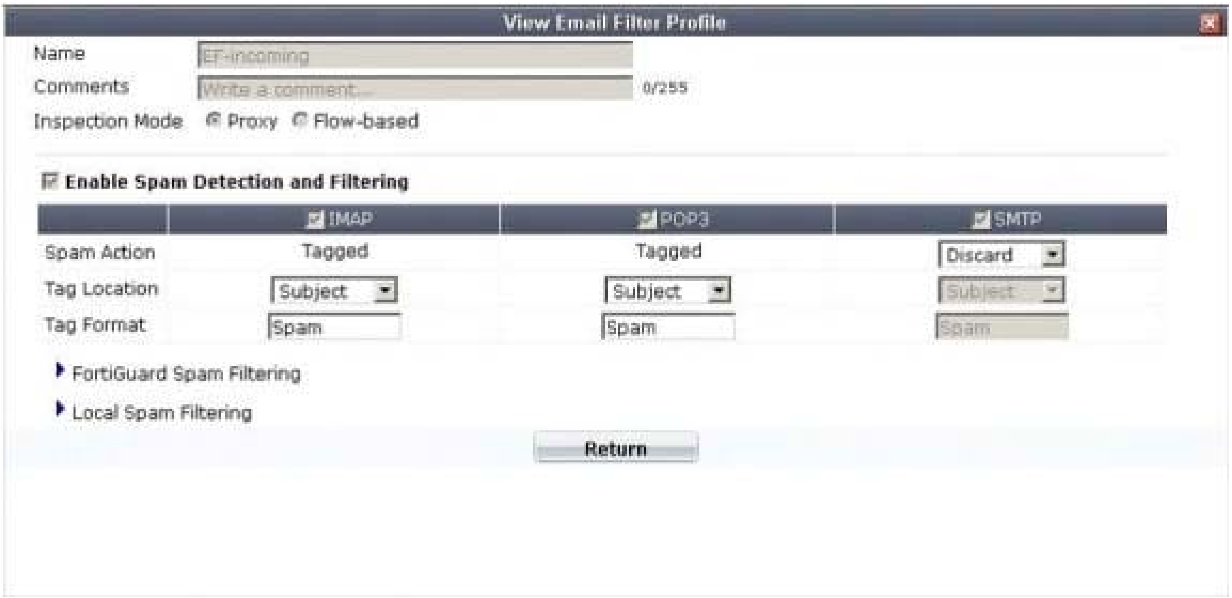
Comments: Write a comment... 0/255

Inspection Mode: ● Proxy ○ Flow-based

□ Inspect Suspicious Files with FortiGuard Analytics

| Protocol | Virus Scan and Removal |
|---|---|
| **Web** | |
| HTTP | □ |
| **Email** | |
| SMTP | ☑ |
| POP3 | □ |
| IMAP | □ |
| MAPI | □ |
| **File Transfer** | |
| FTP | □ |
| **IM** | |
| ICQ, Yahoo, MSN Messenger | □ |

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



View Email Filter Profile

| | |
|---|---|
| Name | EF-incoming |
| Comments | Write a comment... 0/255 |
| Inspection Mode | ● Proxy ○ Flow-based |

☑ Enable Spam Detection and Filtering

| | ☑ IMAP | ☑ POP3 | ☑ SMTP |
|---|---|---|---|
| Spam Action | Tagged | Tagged | Discard |
| Tag Location | Subject | Subject | Subject |
| Tag Format | Spam | Spam | Spam |

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 message. Both sender and recipient are notified that the infected file has been removed.

D. The FortiGate unit will reject the infected email and notify the sender.

Correct Answer: B

**QUESTION 8**

Which is an advantage of using SNMP v3 instead of SNMP v1/v2 when querying a FortiGate unit?

A. MIB-based report uploads.

B. SNMP access limited by access lists.

C. Packet encryption.

D. Running SNMP service on a non-standard port is possible.

Correct Answer: C

**QUESTION 9**

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.

Correct Answer: AB

**QUESTION 10**

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.

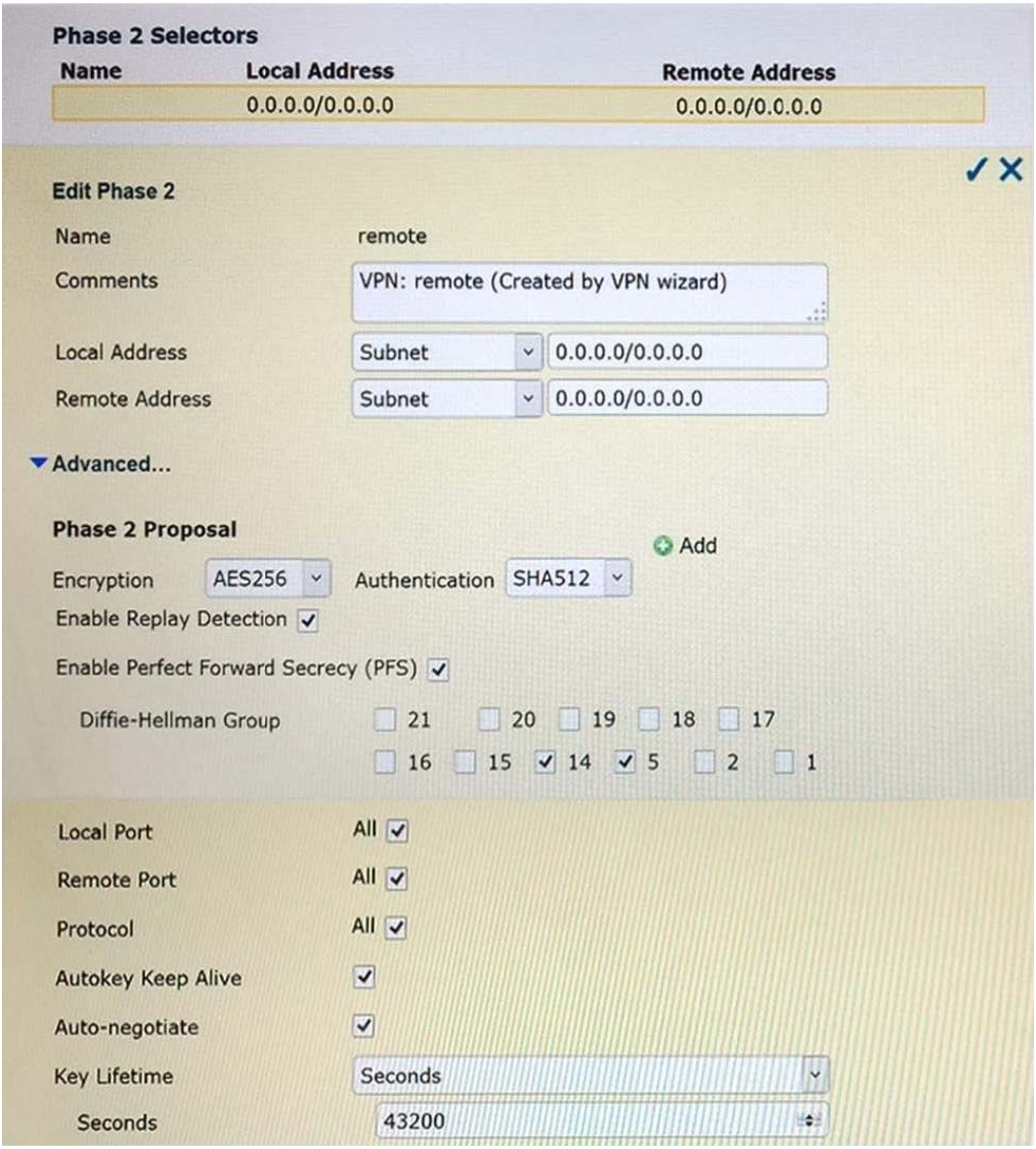
C. Administrators can create the user accounts in a remote server and store the user passwords locally in the FortiGate.

D. Both the usernames and passwords can be stored locally on the FortiGate.

Correct Answer: AD

**QUESTION 11**

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

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 |
| 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.

Correct Answer: AB

**QUESTION 12**

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.

Correct Answer: BD

**QUESTION 13**

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

Correct Answer: ADE

**QUESTION 14**

What is not true of configuring disclaimers on the FortiGate?

A. Disclaimers can be used in conjunction with captive portal.

B. Disclaimers appear before users authenticate.

C. Disclaimers can be bypassed through security exemption lists.

D. Disclaimers must be accepted in order to continue to the authentication login or originally intended destination.

Correct Answer: C

**QUESTION 15**

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.

Correct Answer: BC