

PASSTCERT

QUESTION & ANSWER

Higher Quality
Better Service!

We offer free update service for one year
[HTTP://WWW.PASSTCERT.COM](http://www.passtcert.com)

Exam : **NSE7**

Title : **NSE7 Enterprise Firewall -
FortiOS 5.4**

Version : **DEMO**

1.Examine the IPsec configuration shown in the exhibit; then answer the question below.

Name	<input type="text" value="Remote"/>
Comments	<input type="text" value="Comments"/>
Network	
IP Version	<input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6
Remote Gateway	<input type="text" value="Static IP Address"/> <input checked="" type="checkbox"/>
IP Address	<input type="text" value="10.0.10.1"/>
Interface	<input type="text" value="port1"/> <input checked="" type="checkbox"/>
Mode Config	<input type="checkbox"/>
NAT Traversal	<input checked="" type="checkbox"/>
Keepalive Frequency	<input type="text" value="10"/>
Dead Peer Detection	<input checked="" type="checkbox"/>

An administrator wants to monitor the VPN by enabling the IKE real time debug using these commands:

- diagnose vpn ike log-filter src-addr4 10.0.10.1
- diagnose debug application ike -1
- diagnose debug enable

The VPN is currently up, there is no traffic crossing the tunnel and DPD packets are being interchanged between both IPsec gateways.

However, the IKE real time debug does NOT show any output.

Why isn't there any output?

- A. The IKE real time shows the phases 1 and 2 negotiations only. It does not show any more output once the tunnel is up.
- B. The log-filter setting is set incorrectly. The VPN's traffic does not match this filter.
- C. The IKE real time debug shows the phase 1 negotiation only. For information after that, the administrator must use the IPsec real time debug instead: diagnose debug application ipsec -1.
- D. The IKE real time debug shows error messages only. If it does not provide any output, it indicates that the tunnel is operating normally.

Answer: A

2.Which of the following statements are true regarding the SIP session helper and the SIP application layer gateway (ALG)? (Choose three.)

- A. SIP session helper runs in the kernel; SIP ALG runs as a user space process.
- B. SIP ALG supports SIP HA failover; SIP helper does not.
- C. SIP ALG supports SIP over IPv6; SIP helper does not.
- D. SIP ALG can create expected sessions for media traffic; SIP helper does not.
- E. SIP helper supports SIP over TCP and UDP; SIP ALG supports only SIP over UDP.

Answer: B,C,D

3.A FortiGate device has the following LDAP configuration:

```
config user ldap
  edit "WindowsLDAP"
    set server "10.0.1.10"
    set cnid "cn"
    set dn "cn=Users, dc=trainingAD, dc=training, dc=lab"
    set type regular
    set username "dc=trainingAD, dc=training, dc=lab"
    set password xxxxxxxx
  next
end
```

The administrator executed the 'dsquery' command in the Windows LDAP server 10.0.1.10, and got the following output:

```
>dsquery user -samid administrator
```

```
"CN=Administrator, CN=Users, DC=trainingAD, DC=training, DC=lab"
```

Based on the output, what FortiGate LDAP setting is configured incorrectly?

- A. cnid.
- B. username.
- C. password.
- D. dn.

Answer: A

4.Which of the following statements is true regarding a FortiGate configured as an explicit web proxy?

- A. FortiGate limits the number of simultaneous sessions per explicit web proxy user. This limit CANNOT be modified by the administrator.
- B. FortiGate limits the total number of simultaneous explicit web proxy users.
- C. FortiGate limits the number of simultaneous sessions per explicit web proxy user. The limit CAN be modified by the administrator.
- D. FortiGate limits the number of workstations that authenticate using the same web proxy user credentials. This limit CANNOT be modified by the administrator.

Answer: C

5.A corporate network allows Internet Access to FSSO users only. The FSSO user student does not have Internet access after successfully logged into the Windows AD network. The output of the 'diagnose debug authd fssolist' command does not show student as an active FSSO user. Other FSSO users can access the Internet without problems.

What should the administrator check? (Choose two.)

- A. The user student must not be listed in the CA's ignore user list.
- B. The user student must belong to one or more of the monitored user groups.
- C. The student workstation's IP subnet must be listed in the CA's trusted list.
- D. At least one of the student's user groups must be allowed by a FortiGate firewall policy.

Answer: B,D