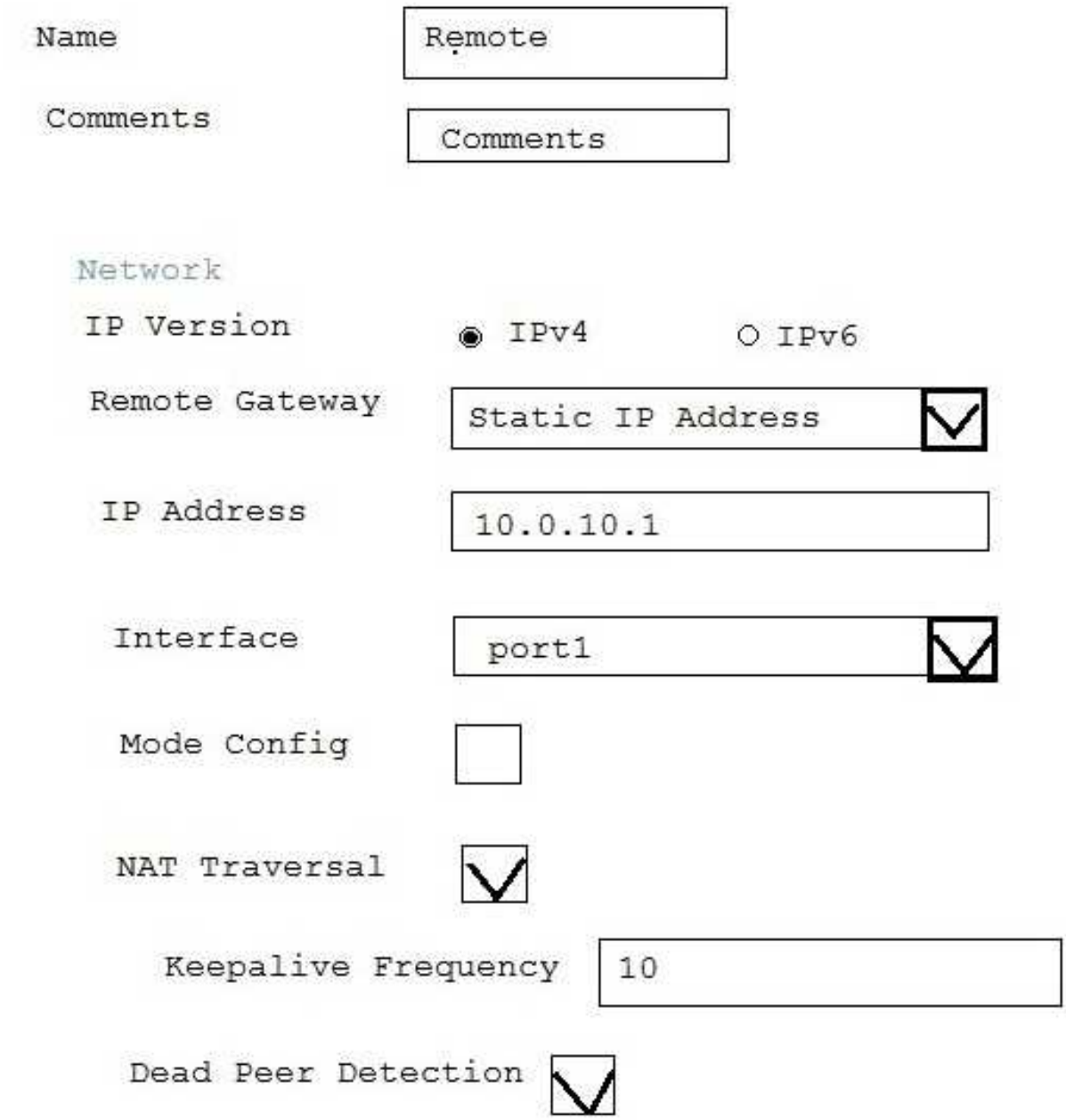
Fortinet

NSE7_EFW-6.4 Exam

Fortinet NSE 7 - Enterprise Firewall 6.4

Question: 1

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



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: B

Explanation:

Question: 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

Explanation:

Question: 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 xxxxxxx
   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: B

Explanation:

https://kb.fortinet.com/kb/viewContent.do?externalId=FD37516

Question: 4

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 fsso list' 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: A,D

Explanation:
https://kb.fortinet.com/kb/documentLink.do?externalID=FD38828

Question: 5

An administrator has decreased all the TCP session timers to optimize the FortiGate memory usage. However, after the changes, one network application started to have problems. During the troubleshooting, the administrator noticed that the FortiGate deletes the sessions after the clients send the SYN packets, and before the arrival of the SYN/ACKs. When the SYN/ACK packets arrive to the FortiGate, the unit has already deleted the respective sessions. Which TCP session timer must be increased to fix this problem?

A. TCP half open.
B. TCP half close.
C. TCP time wait.
D. TCP session time to live.

Answer: A

Explanation:
http://docs-legacy.fortinet.com/fos40hlp/43prev/wwhelp/wwhimpl/common/html/wwhelp.htm?context=fgt&file=CLI_get_Commands.58.25.html
The tcp-halfopen-timer controls for how long, after a SYN packet, a session without SYN/ACK remains in the table.
The tcp-halfclose-timer controls for how long, after a FIN packet, a session without FIN/ACK remains in the table.
The tcp-timewait-timer controls for how long, after a FIN/ACK packet, a session remains in the table. A closed session remains in the session table for a few seconds more to allow any out-of-sequence packet.