Fortinet

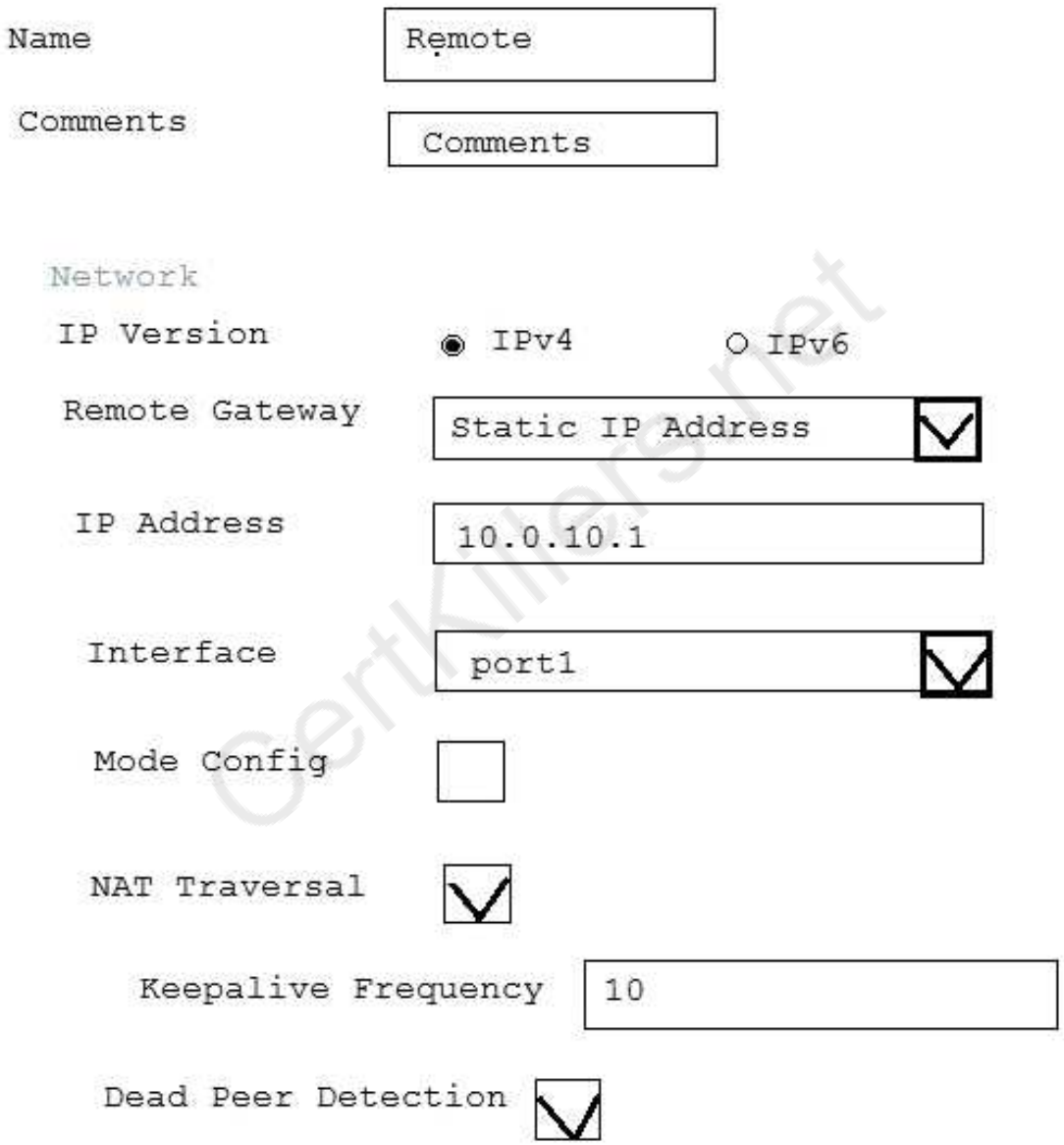
NSE7_EFW Exam

Fortinet NSE7 Enterprise Firewall - FortiOS 5.4 Exam

Version: 12.0

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: A

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

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: A

Question: 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

Question: 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 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: B,D

Question: 6

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

Question: 7

An administrator is running the following sniffer in a FortiGate:
diagnose sniffer packet any “host 10.0.2.10” 2
What information is included in the output of the sniffer? (Choose two.)

A. Ethernet headers.
B. IP payload.
C. IP headers.
D. Port names.

Answer: B,C

Question: 8

Examine the partial output from two web filter debug commands; then answer the question below:

```
# diagnose test application urlfilter 3
Domain | IP    DB Ver   T URL
34000000| 34000000  16.40224 P Bhttp://www.fgt99.com/
# get webfilter categories
g07 General Interest - Business:
    34 Finance and Banking
    37 Search Engines and Portals
    43 General Organizations
    49 Business
    50 Information and Computer Security
    51 Government and Legal Organizations
    52 Information Technology
```

Based on the above outputs, which is the FortiGuard web filter category for the web site www.fgt99.com?

A. Finance and banking
B. General organization.
C. Business.

D. Information technology.

Answer: C

Question: 9

Examine the output of the 'get router info ospf interface' command shown in the exhibit; then answer the question below.

```
# get router info ospf interface port4
port4 is up, line protocol is up
   Internet Address 172.20.121.236/24, Area 0.0.0.0, MTU 1500
   Process ID 0, Router ID 0.0.0.4, Network Type BROADCAST, Cost: 1
   Transmit Delay is 1 sec, State DROther, Priority 1
   Designated Router (ID) 172.20.140.2, Interface Address 172.20.121.2
Backup Designated Router (ID) 0.0.0.1, Interface Address
172.20.121.239
Timer intervals configured, Hello 10.000, Dead 40, Wait 40, Retransmit
5
     Hello due in 00:00:05
   Neighbor Count is 4, Adjacent neighbor count is 2
   Crypt Sequence Number is 411
   Hello received 106, sent 27, DD received 7 sent 9
   LS-Req received 2 sent 2, LS-Upd received 7 sent 5
   LS-Ack received 4 sent 3, Discarded 1
```

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

A. The port4 interface is connected to the OSPF backbone area.
B. The local FortiGate has been elected as the OSPF backup designated router.
C. There are at least 5 OSPF routers connected to the port4 network.
D. Two OSPF routers are down in the port4 network.

Answer: A,D

Question: 10

Examine the output of the 'get router info bgp summary' command shown in the exhibit; then answer the question below.

```
# get router info bgp summary
BGP router identifier 0.0.0.117, local AS number 65117
BGP table version is 104
3 BGP AS-PATH entries
0 BGP community entries

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
10.125.0.60     4 65060    1698    1756      103    0    0 03:02:49        1
10.127.0.75     4 65075    2206    2250      102    0    0 02:45:55        1
10.200.3.1      4 65501     101     115        0    0    0 never         Active

Total number of neighbors 3
```

Which statements are true regarding the output in the exhibit? (Choose two.)

A. BGP state of the peer 10.125.0.60 is Established.
B. BGP peer 10.200.3.1 has never been down since the BGP counters were cleared.
C. Local BGP peer has not received an OpenConfirm from 10.200.3.1.
D. The local BGP peer has received a total of 3 BGP prefixes.

Answer: A,C

Thank You for trying NSE7_EFW PDF Demo

To Buy Latest NSE7_EFW Full Version Download visit link below

https://www.certkillers.net/Exam/NSE7_EFW

Start Your NSE7_EFW Preparation

[Limited Time Offer] Use Coupon "CKNET" for Further discount on your purchase. Test your NSE7_EFW preparation with actual exam questions.