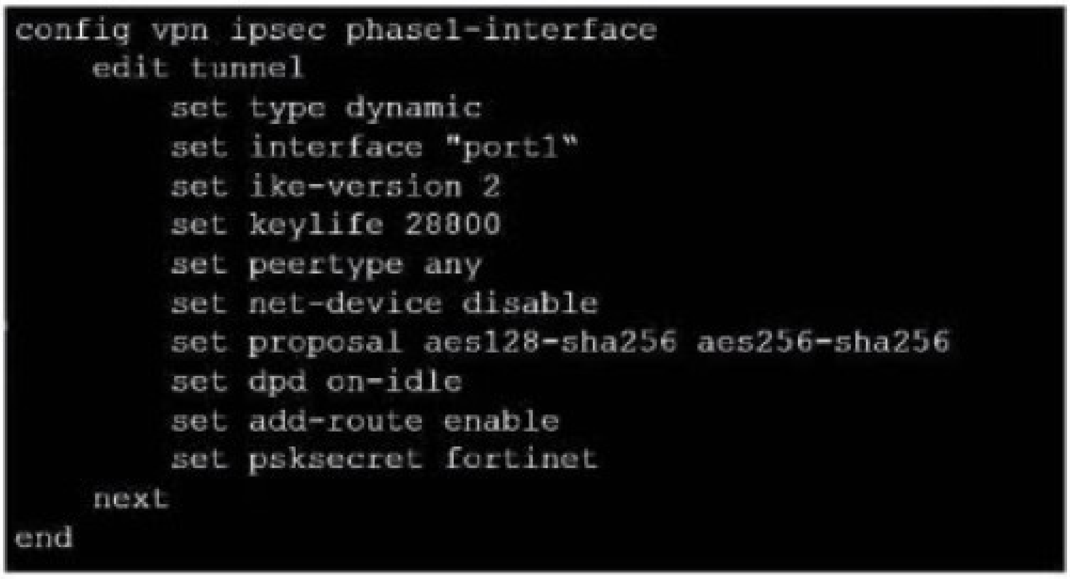
NSE7_EFW-7.2 Q&As

Fortinet NSE 7 - Enterprise Firewall 7.2

QUESTION 1

Exhibit.



```
config vpn ipsec phase1-interface
    edit tunnel
        set type dynamic
        set interface "port1"
        set ike-version 2
        set keylife 28800
        set peertype any
        set net-device disable
        set proposal aes128-sha256 aes256-sha256
        set dpd on-idle
        set add-route enable
        set psksecret fortinet
    next
end
```

Refer to the exhibit, which contains a partial VPN configuration. What can you conclude from this configuration1?

A. FortiGate creates separate virtual interfaces for each dial up client.

B. The VPN should use the dynamic routing protocol to exchange routing information Through the tunnels.

C. Dead peer detection s disabled.

D. The routing table shows a single IPSec virtual interface.

Correct Answer: C

The configuration line "set dpd on-idle" indicates that dead peer detection (DPD) is set to trigger only when the tunnel is idle, not actively disabled1. References: FortiGate IPSec VPN User Guide - Fortinet Document Library

From the given VPN configuration, dead peer detection (DPD) is set to \\'on-idle\\', indicating that DPD is enabled and will be used to detect if the other end of the VPN tunnel is still alive when no traffic is detected. Hence, option C is incorrect. The configuration shows the tunnel set to type \\'dynamic\\', which does not create separate virtual interfaces for each dial- up client (A), and it is not specified that dynamic routing will be used (B). Since this is a phase 1 configuration snippet, the routing table aspect (D) cannot be concluded from this alone.

QUESTION 2

You created a VPN community using VPN Manager on FortiManager. You also added gateways to the VPN community. Now you are trying to create firewall policies to permit traffic over the tunnel however, the VPN interfaces do not appear as available options.

A. Create interface mappings for the IPsec VPN interfaces before you use them in a policy.

B. Refresh the device status using the Device Manager so that FortiGate populates the IPSec interfaces

C. Configure the phase 1 settings in the VPN community that you didnt initially configure. FortiGate automatically generates the interfaces after you configure the required settings

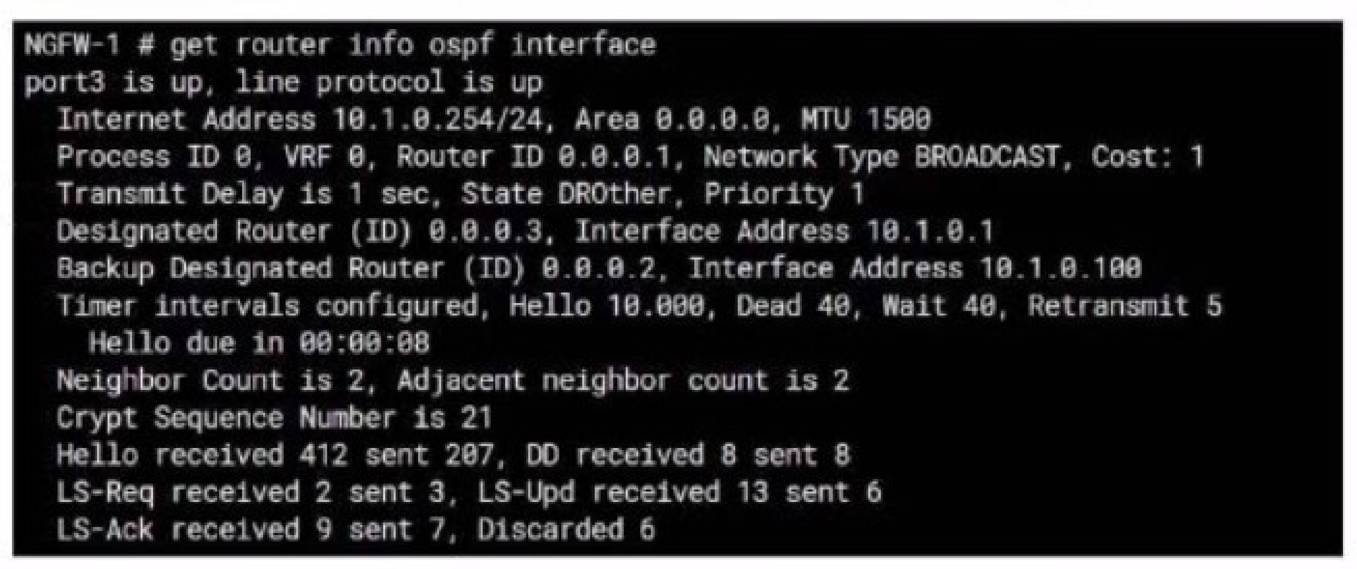
D. install the VPN community and gateway configuration on the fortiGate devices so that the VPN interfaces appear on the Policy Objects on fortiManager.

Correct Answer: D

To use the VPN interfaces in a policy, you need to install the VPN community and gateway configuration on the FortiGate devices first. This will create the VPN interfaces on the FortiGate and sync them with FortiManager. References: Creating IPsec VPN communities VPN | FortiGate / FortiOS 7.2.0

QUESTION 3

Exhibit.



```
NGFW-1 # get router info ospf interface
port3 is up, line protocol is up
  Internet Address 10.1.0.254/24, Area 0.0.0.0, MTU 1500
  Process ID 0, VRF 0, Router ID 0.0.0.1, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DROther, Priority 1
  Designated Router (ID) 0.0.0.3, Interface Address 10.1.0.1
  Backup Designated Router (ID) 0.0.0.2, Interface Address 10.1.0.100
  Timer intervals configured, Hello 10.000, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:08
  Neighbor Count is 2, Adjacent neighbor count is 2
  Crypt Sequence Number is 21
  Hello received 412 sent 207, DD received 8 sent 8
  LS-Req received 2 sent 3, LS-Upd received 13 sent 6
  LS-Ack received 9 sent 7, Discarded 6
```

Refer to the exhibit, which shows information about an OSPF interlace

What two conclusions can you draw from this command output? (Choose two.)

A. The port3 network has more man one OSPF router

B. The OSPF routers are in the area ID of 0.0.0.1.

C. The interfaces of the OSPF routers match the MTU value that is configured as 1500.

D. NGFW-1 is the designated router

Correct Answer: AC

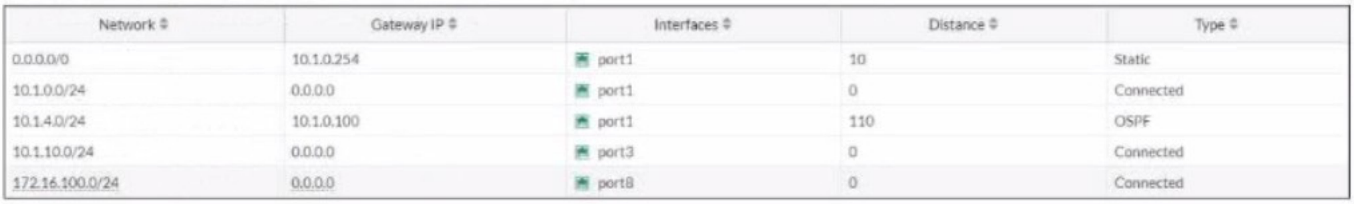
From the OSPF interface command output, we can conclude that the port3 network has more than one OSPF router because the Neighbor Count is 2, indicating the presence of another OSPF router besides NGFW-1. Additionally, we can deduce that the interfaces of the OSPF routers match the MTU value configured as 1500, which is necessary for OSPF neighbors to form adjacencies. The MTU mismatch would prevent OSPF from forming a neighbor relationship.

References:

Fortinet FortiOS Handbook: OSPF Configuration

QUESTION 4

Refer to the exhibit, which shows a routing table.



Network ⇕	Gateway IP ⇕	Interfaces ⇕	Distance ⇕	Type ⇕
0.0.0.0/0	10.1.0.254	port1	10	Static
10.1.0.0/24	0.0.0.0	port1	0	Connected
10.1.4.0/24	10.1.0.100	port1	110	OSPF
10.1.10.0/24	0.0.0.0	port3	0	Connected
172.16.100.0/24	0.0.0.0	port8	0	Connected

What two options can you configure in OSPF to block the advertisement of the 10.1.10.0 prefix? (Choose two.)

A. Remove the 16.1.10.C prefix from the OSPF network

B. Configure a distribute-list-out

C. Configure a route-map out

D. Disable Redistribute Connected

Correct Answer: BC

To block the advertisement of the 10.1.10.0 prefix in OSPF, you can configure a distribute-list-out or a route-map out. A distribute-list-out is used to filter outgoing routing updates from being advertised to OSPF neighbors1. A route-map out can also be used for filtering and is applied to outbound routing updates2. References := Technical Tip: Inbound route filtering in OSPF usi ... - Fortinet Community, OSPF | FortiGate / FortiOS 7.2.2 - Fortinet Documentation

QUESTION 5

You want to improve reliability over a lossy IPSec tunnel.

Which combination of IPSec phase 1 parameters should you configure?

A. fec-ingress and fec-egress

B. Odpd and dpd-retryinterval

C. fragmentation and fragmentation-mtu

D. keepalive and keylive

Correct Answer: C

For improving reliability over a lossy IPSec tunnel, the fragmentation and fragmentation-mtu parameters should be configured. In scenarios where there might be issues with packet size or an unreliable network, setting the IPsec phase 1 to allow for fragmentation will enable large packets to be broken down, preventing them from being dropped due to size or poor network quality. The fragmentation-mtu specifies the size of the fragments. This is aligned with Fortinet\\'s recommendations for handling IPsec VPN over networks with potential packet loss or size limitations.

NSE7_EFW-7.2 VCE Dumps NSE7_EFW-7.2 Practice Test NSE7_EFW-7.2 Exam Questions