

NSE8_812^{Q&As}

Network Security Expert 8 Written Exam

Pass Fortinet NSE8_812 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.leads4pass.com/nse8_812.html

100% Passing Guarantee
100% Money Back Assurance

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

-  **Instant Download** After Purchase
-  **100% Money Back** Guarantee
-  **365 Days** Free Update
-  **800,000+** Satisfied Customers



QUESTION 1

Refer to the exhibit containing the configuration snippets from the FortiGate. Customer requirements: SSLVPN Portal must be accessible on standard HTTPS port (TCP/443) Public IP address (129.11.1.100) is assigned to portl
Datacenter.acmecorp.com resolves to the public IP address assigned to portl

```
config vpn ssl settings
  set https-redirect enable
  set servercert "FortiGateLE"
  set tunnel-ip-pools "SSLVPN_TUNNEL_ADDR1"
  set tunnel-ipv6-pools "SSLVPN_TUNNEL_IPv6_ADDR1"
  set port 443
  set source-interface "port1"
  set source-address "all"
  set source-address6 "all"
  set default-portal "no-access"
end

config system global
  set admin-port 80
end

config vpn certificate local
  edit "FortiGateLE"
    set password ENC <redacted>
    set range global
    set enroll-protocol acme2
    set acme-domain "datacenter.acmecorp.com"
    set acme-email "administrator@acmecorp.com"
  next
end

config system acme
  set interface "port1"
  config accounts
    edit "ACME-.letsencrypt.org-0000"
      set status "valid"
      set ca_url "https://acme-
v02.api.letsencrypt.org/directory"
      set email "administrator@acmecorp.com"
    end
  end

config firewall address
  edit "h-fortigate_public"
    set subnet 129.11.1.100 255.255.255.255
  next
end

config firewall vip
  edit "fortimail_secure_web_admin"
    set mappedip "10.100.1.5"
    set extintf "port1"
    set portforward enable
    set extport 30443
    set mappedport 443
  next
  edit "fortimail_web_admin"
    set mappedip "10.100.1.5"
    set extintf "port1"
    set portforward enable
    set extport 30080
    set mappedport 80
  next
end

config firewall policy
  edit 1
    set name "Allow Inbound FortiMail"
    set srcintf "port1"
    set dstintf "port2"
    set action accept
    set srcaddr "all"
    set dstaddr " fortimail_secure_web_admin " "
fortimail_web_admin "
    set schedule "always"
    set service "HTTP" "HTTPS"
    set ssl-ssh-profile "no-inspection"
  next
end
```

The customer has a Let's Encrypt certificate that is going to expire soon and it reports that subsequent attempts to renew that certificate are failing.

Reviewing the requirement and the exhibit, which configuration change below will resolve this issue?

- A.

```
config vpn ssl settings
    set https-redirect disable
end
```
- B.

```
config system acme
    set interface "port2"
end
```
- C.

```
config firewall policy
    edit 1
        append dstaddr "h-fortigate_public"
    next
end
```
- D.

```
config system global
    set admin-port 8080
end
```

A. Option A

B. Option B

C. Option C

D. Option D

Correct Answer: B

Explanation: The customer's SSLVPN Portal is currently configured to use a self-signed certificate. This means that the certificate is not trusted by any browsers, and users will have to accept a security warning before they can connect to the

portal. To resolve this issue, the customer needs to configure the FortiGate to use a Let's Encrypt certificate. Let's Encrypt is a free certificate authority that provides trusted certificates for websites and other applications.

The configuration change in option B will configure the FortiGate to use a Let's Encrypt certificate for the SSLVPN Portal. This will allow users to connect to the portal without having to accept a security warning.

The other configuration changes are not necessary to resolve the issue. Option A will configure the FortiGate to use a

different port for the SSLVPN Portal, but this will not resolve the issue with the self-signed certificate. Option C will configure the FortiGate to use a different DNS name for the SSLVPN Portal, but this will also not resolve the issue with the self-signed certificate. Option D will configure the FortiGate to use a different certificate authority for the SSLVPN Portal, but this will also not resolve the issue because the customer still needs to use a trusted certificate.

References:

Configuring SSLVPN with Let's Encrypt:

<https://docs.fortinet.com/document/fortigate/7.0.0/administration-guide/822087/acme-certificate-support>

Let's Encrypt: <https://letsencrypt.org/>

QUESTION 2

Refer to the exhibit.



A customer has deployed a FortiGate 300E with virtual domains (VDOMs) enabled in the multi-VDOM mode. There are three VDOMs: Root is for management and internet access, while VDOM 1 and VDOM 2 are used for segregating internal traffic. AccountVlnk and SalesVlnk are standard VDOM links in Ethernet mode.

Given the exhibit, which two statements below about VDOM behavior are correct? (Choose two.)

- A. You can apply OSPF routing on the VDOM link in either PPP or Ethernet mode
- B. Traffic on AccountVlnk and SalesVlnk will not be accelerated.
- C. The VDOM links are in Ethernet mode because they have IP addressed assigned on both sides.
- D. Root VDOM is an Admin type VDOM, while VDOM 1 and VDOM 2 are Traffic type VDOMs.
- E. OSPF routing can be configured between VDOM 1 and Root VDOM without any configuration changes to AccountVlnk

Correct Answer: AD

A. You can apply OSPF routing on the VDOM link in either PPP or Ethernet mode. This is because VDOM links can be configured in either PPP or Ethernet mode, and OSPF routing can be configured on both types of links. D. Root VDOM is

an Admin type VDOM, while VDOM 1 and VDOM 2 are Traffic type VDOMs. This is because the Root VDOM is the default VDOM, and it is used for management and internet access. VDOM 1 and VDOM 2 are traffic type VDOMs,

which are

used for segregating internal traffic.

The other options are not correct.

B. Traffic on AccountVlnk and SalesVlnk will not be accelerated. This is because VDOM links are not accelerated by default. However, you can configure acceleration on VDOM links if you want.

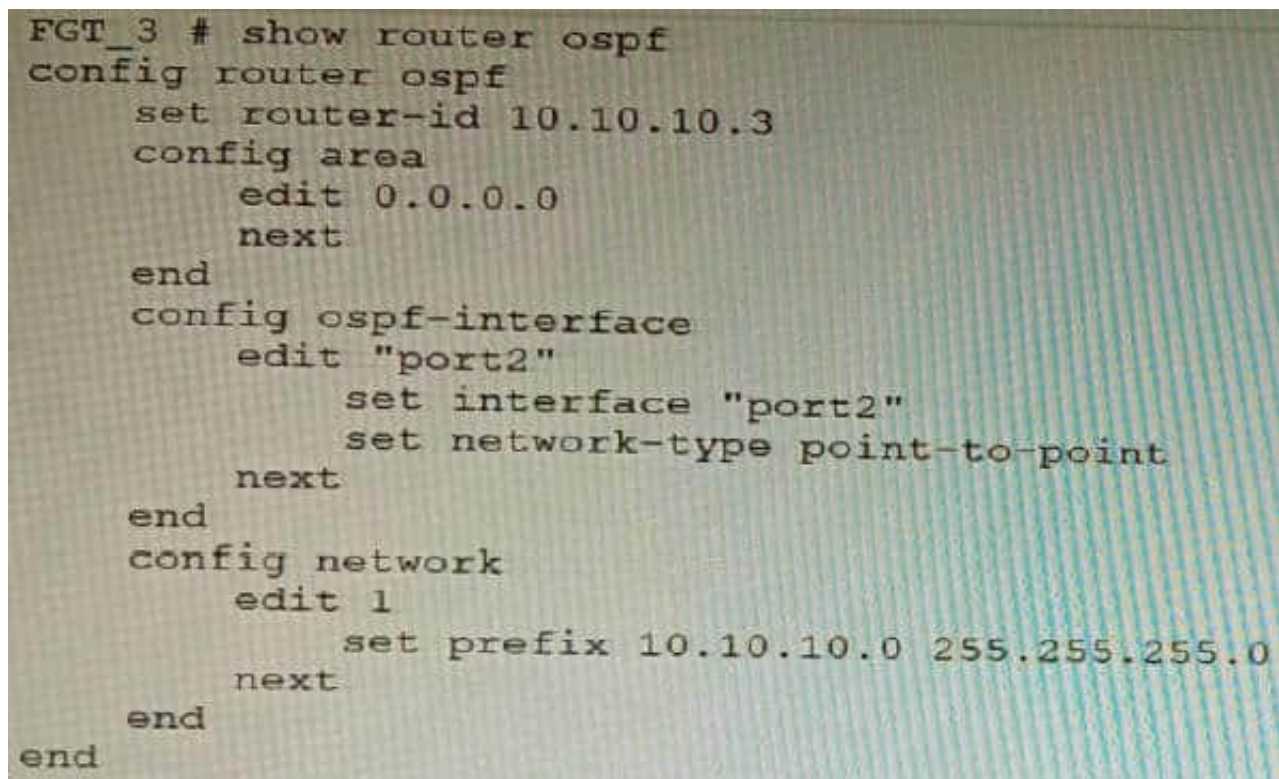
C. The VDOM links are in Ethernet mode because they have IP addresses assigned on both sides. This is not necessarily true. The VDOM links could be in PPP mode even if they have IP addresses assigned on both sides. E. OSPF routing

can be configured between VDOM 1 and Root VDOM without any configuration changes to AccountVlnk. This is correct. OSPF routing can be configured between any two VDOMs, even if they are not directly connected. In this case, the

OSPF routing would be configured on the AccountVlnk link.

QUESTION 3

Refer to the exhibit.



```
FGT_3 # show router ospf
config router ospf
  set router-id 10.10.10.3
  config area
    edit 0.0.0.0
    next
  end
  config ospf-interface
    edit "port2"
      set interface "port2"
      set network-type point-to-point
    next
  end
  config network
    edit 1
      set prefix 10.10.10.0 255.255.255.0
    next
  end
end
```

You are operating an internal network with multiple OSPF routers on the same LAN segment. FGT_3 needs to be added to the OSPF network and has the configuration shown in the exhibit. FGT_3 is not establishing any OSPF connection. What needs to be changed to the configuration to make sure FGT_3 will establish OSPF neighbors without affecting the DR/BDR election?

- A.
- ```
config router ospf
 config ospf-interface
 edit "port2"
 set priority 255
 set network-type point-to-multipoint
 next
 end
end
```
- B.
- ```
config router ospf
  config ospf-interface
    edit "port2"
      set priority 0
      set network-type broadcast
    next
  end
end
```
- C.
- ```
config router ospf
 config ospf-interface
 edit "port2"
 set priority 255
 set network-type broadcast
 next
 end
end
```
- D.
- ```
config router ospf
  config ospf-interface
    edit "port2"
      set priority 0
      set network-type point-to-multipoint
    next
  end
end
```

- A. Option A
- B. Option B
- C. Option C
- D. Option D

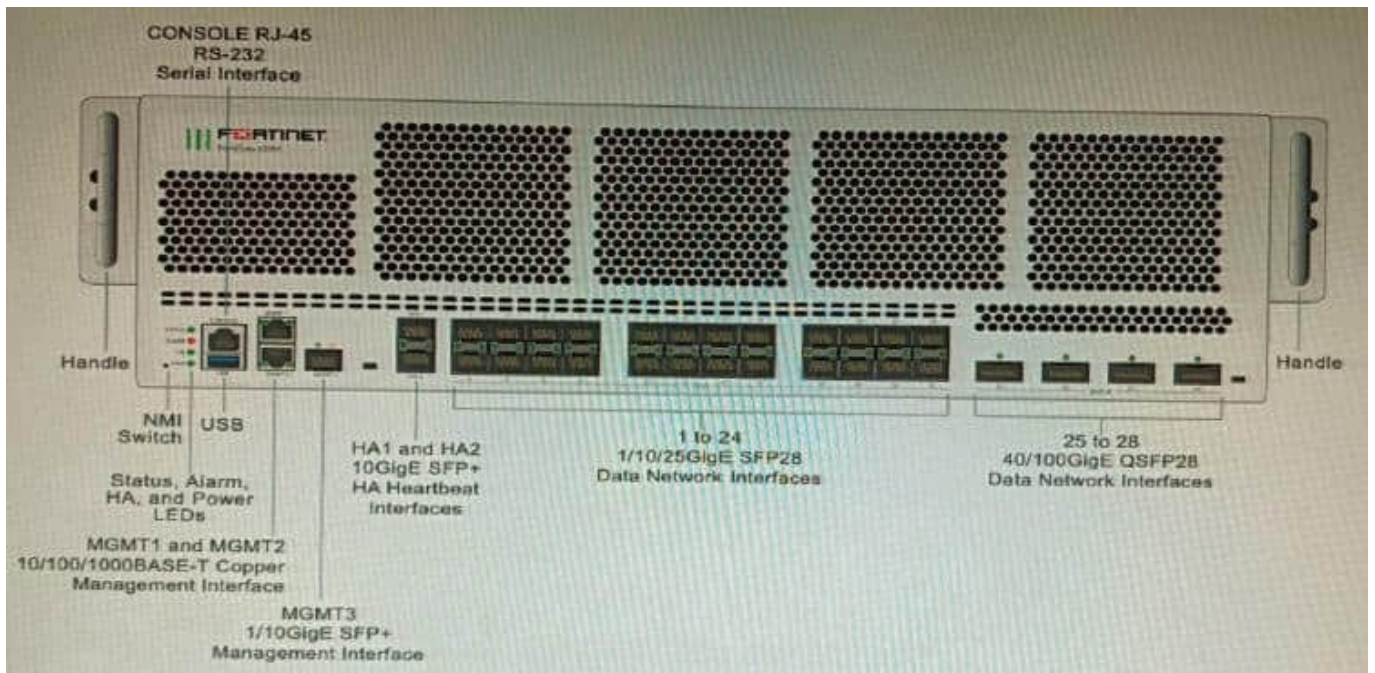
Correct Answer: B

Explanation: The OSPF configuration shown in the exhibit is using the default priority value of 1 for the interface port1. This means that FGT_3 will participate in the DR/BDR election process with the other OSPF routers on the same LAN segment. However, this is not desirable because FGT_3 is a new device that needs to be added to the OSPF network without affecting the existing DR/BDR election. Therefore, to make sure FGT_3 will establish OSPF neighbors without affecting the DR/BDR election, the priority value of the interface port1 should be changed to 0. This will prevent FGT_3 from becoming a DR or BDR and allow it to form OSPF adjacencies with the current DR and BDR. Option B shows the correct configuration that changes the priority value to 0. Option A is incorrect because it does not change the priority value. Option C is incorrect because it changes the network type to point-to-point, which is not suitable for a LAN segment with multiple OSPF routers. Option D is incorrect because it changes the area ID to 0.0.0.1, which does not match the area ID of the other OSPF routers on the same LAN segment.

References: <https://docs.fortinet.com/document/fortigate/7.0.0/administration-guide/358640/basic-ospf-example>

QUESTION 4

Refer to the exhibit.



You are deploying a FortiGate 6000F. The device should be directly connected to a switch. In the future, a new hardware module providing higher speed will be installed in the switch, and the connection to the FortiGate must be moved to this higher-speed port.

You must ensure that the initial FortiGate interface connected to the switch does not affect any other port when the new module is installed and the new port speed is defined.

How should the initial connection be made?

- A. Connect the switch on any interface between ports 21 to 24
- B. Connect the switch on any interface between ports 25 to 28
- C. Connect the switch on any interface between ports 1 to 4
- D. Connect the switch on any interface between ports 5 to 8.

Correct Answer: C

Explanation: The FortiGate 6000F has 24 1/10/25-Gbps SFP28 data network interfaces (1 to 24). These interfaces are divided into the following interface groups: 1 to 4, 5 to 8, 9 to 12, 13 to 16, 17 to 20, and 21 to 24. The ports 25 to 28 are

40/100-Gbps QSFP28 data network interfaces.

The initial connection should be made to any interface between ports 1 to 4. This is because the ports 21 to 24 are part of the same interface group, and changing the speed of one of these ports will affect the speeds of all of the ports in the group. The ports 5 to 8 are also part of the same interface group, so they should not be used for the initial connection. The new hardware module that will be installed in the switch will provide higher speed ports. When this module is installed,

the speed of the ports 21 to 24 will be increased. However, this will not affect the ports 1 to 4, because they are not part of the same interface group.

Therefore, the initial connection should be made to any interface between ports 1 to 4, in order to ensure that the FortiGate interface connected to the switch does not affect any other port when the new module is installed and the new port

speed is defined.

Reference:

FortiGate 6000F Front Panel Interfaces: <https://docs.fortinet.com/document/fortigate-6000/hardware/fortigate-6000f-system-guide/827055/front-panel-interfaces>

QUESTION 5

Refer to the exhibit showing an SD-WAN configuration. According to the exhibit, if an internal user pings 10.1.100.2 and 10.1.100.22 from subnet 172.16.205.0/24, which outgoing interfaces will be used?

```

        set interface "port15"
        set zone "z1"
        set gateway 172.16.209.2
    next
    edit 4
        set interface "port16"
        set zone "z1"
        set gateway 172.16.210.2
    next
end
config health-check
    edit "1"
        set server "10.1.100.2"
        set members 4 1 2 1
        config sla
            edit 1
                set id 1
            next
        end
        set priority-members 1 2 3 4
        set tie-break fib-best-match
    next
end
end

#####

FGT_A (root) # diagnose sys sdwan service

Service(1): Address Mode(IPV4) flags=0x200 use-shortcut-sla
Gen(4), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(sla), sla-
compare-order
Members(4):
  1: Seq_num(1 port1), alive, sla(0x1), gid(0), cfg_order(0),
cost(0), selected
  2: Seq_num(2 dmz), alive, sla(0x1), gid(0), cfg_order(1),
cost(0), selected
  3: Seq_num(3 port15), alive, sla(0x1), gid(0), cfg_order(2),
cost(0), selected
  4: Seq_num(4 port16), alive, sla(0x1), gid(0), cfg_order(3),
cost(0), selected
Src address(1):
  172.16.205.0-172.16.205.255
Dst address(1):
  0.0.0.0-255.255.255.255

#####

FGT_A (root) # get router info routing-table static
Routing table for VRF=0
S*   0.0.0.0/0 [1/0] via 172.16.200.2, port1
      [1/0] via 172.16.209.2, dmz
      [1/0] via 172.16.209.2, port15
      [1/0] via 172.16.210.2, port16
S    10.1.100.22/32 [10/0] via 172.16.209.2, port15
      [10/0] via 172.16.210.2, port16

```

- A. port16 and port1
- B. port1 and port1
- C. port16 and port15
- D. port1 and port15

Correct Answer: A

Explanation: According to the exhibit, the SD-WAN configuration has two rules: one for traffic to 10.1.100.0/24 subnet, and one for traffic to 10.1.100.16/28 subnet. The first rule uses the best quality strategy, which selects the SD-WAN member with the best measured quality based on performance SLA metrics. The second rule uses the manual strategy, which specifies port1 as the SD-WAN member to select. Therefore, if an internal user pings 10.1.100.2 and 10.1.100.22 from subnet 172.16.205.0/24, the outgoing interfaces will be port16 and port1 respectively, assuming that port16 has the best quality among the SD-WAN members.

References: <https://docs.fortinet.com/document/fortigate/6.2.14/cookbook/218559/configuring-the-sd-wan-interface>

QUESTION 6

You must configure an environment with dual-homed servers connected to a pair of FortiSwitch units using an MLAG.

Multicast traffic is expected in this environment, and you should ensure unnecessary traffic is pruned from links that do not have a multicast listener.

In which two ways must you configure the igmps-flood-traffic and igmps-flood-report settings? (Choose two.)

- A. disable on ICL trunks
- B. enable on ICL trunks
- C. disable on the ISL and FortiLink trunks
- D. enable on the ISL and FortiLink trunks

Correct Answer: AD

Explanation: To ensure that unnecessary multicast traffic is pruned from links that do not have a multicast listener, you must disable IGMP flood traffic on the ICL trunks and enable IGMP flood reports on the ISL and FortiLink trunks.
Disabling

IGMP flood traffic will prevent the FortiSwitch units from flooding multicast traffic to all ports on the ICL trunks. This will help to reduce unnecessary multicast traffic on the network.

Enabling IGMP flood reports will allow the FortiSwitch units to learn which ports are interested in receiving multicast traffic. This will help the FortiSwitch units to prune multicast traffic from links that do not have a multicast listener.

QUESTION 7

You are creating the CLI script to be used on a new SD-WAN deployment. You will have branches with a different number of internet connections and want to be sure there is no need to change the Performance SLA configuration in case more connections are added to the branch.

The current configuration is:

```
config health-check
  edit "Default_AWS"
    set server "aws.amazon.com"
    set protocol http
    set interval 1000
    set probe-timeout 1000
    set recoverytime 10
  config sla
    edit 1
      set latency-threshold 250
      set jitter-threshold 50
      set packetloss-threshold 5
    next
  end
next
end
```

Which configuration do you use for the Performance SLA members?

- A. set members any
- B. set members 0
- C. current configuration already fulfills the requirement
- D. set members all

Correct Answer: A

Explanation: The set members any option will ensure that all of the SD-WAN interfaces are included in the Performance SLA. This is the best option if you want to be sure that the Performance SLA will be triggered even if more connections are added to the branch in the future. The set members 0 option will exclude all of the SD-WAN interfaces from the Performance SLA. This is not a good option because it will prevent the Performance SLA from being triggered even if there is a problem with the network. The current configuration already fulfills the requirement option is incorrect because it does not ensure that all of the SD-WAN interfaces will be included in the Performance SLA. The set members all

option will include all of the SD-WAN interfaces in the Performance SLA, but it is not the best option because it is not scalable. If you have a large number of SD-WAN interfaces, this option will cause the Performance SLA to be triggered too often. References: Performance SLA | FortiGate / FortiOS 7.4.0 Configuring Performance SLA | FortiGate / FortiOS 7.4.0

QUESTION 8

Refer to the exhibit.

```
config vpn ipsec phase1-interface
  edit "vpn-hub02-1"
    set interface "wan1"
    set ike-version 2
    set authmethod signature
    set net-device enable
    set proposal aes256-sha256
    set auto-discovery-receiver enable
    set remote-gw 192.168.168.100
    set certificate "BR01FGTLOCAL"
    set peer "vpn-hub02-1_peer"
  next
end
```

To facilitate a large-scale deployment of SD-WAN/ADVPN with FortiGate devices, you are tasked with configuring the FortiGate devices to support injecting of IKE routes on the ADVPN shortcut tunnels. Which three commands must be added or changed to the FortiGate spoke config vpn ipsec phase1-interface options referenced in the exhibit for the VPN interface to enable this capability? (Choose three.)

- A. set net-device disable
- B. set mode-cfg enable
- C. set ike-version 1
- D. set add-route enable
- E. set mode-cfg-allow-client-selector enable

Correct Answer: BDE

B must be set to enable mode-cfg, which is required for injecting IKE routes on the ADVPN shortcut tunnels.

D must be set to enable add-route, which is the command that actually injects the IKE routes.

E must be set to enable mode-cfg-allow-client-selector, which allows custom phase 2 selectors to be configured.

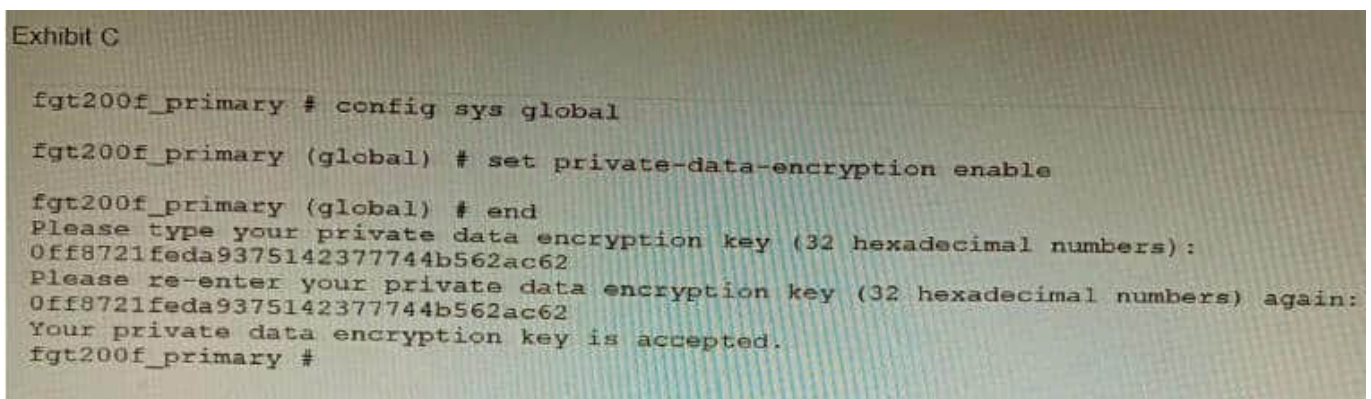
The other options are incorrect. Option A is incorrect because net-device disable is not required for injecting IKE routes on the ADVPN shortcut tunnels. Option C is incorrect because IKE version 1 is not supported for ADVPN.

References:

Phase 2 selectors and ADVPN shortcut tunnels | FortiGate / FortiOS 7.2.0 Configuring SD-WAN/ADVPN with FortiGate | FortiGate / FortiOS 7.2.0

QUESTION 9

Refer to the exhibit.



```
Exhibit C

fgt200f_primary # config sys global
fgt200f_primary (global) # set private-data-encryption enable
fgt200f_primary (global) # end
Please type your private data encryption key (32 hexadecimal numbers):
Off8721feda9375142377744b562ac62
Please re-enter your private data encryption key (32 hexadecimal numbers) again:
Off8721feda9375142377744b562ac62
Your private data encryption key is accepted.
fgt200f_primary #
```

A customer has deployed a FortiGate 200F high-availability (HA) cluster that contains and TPM chip. The exhibit shows output from the FortiGate CLI session where the administrator enabled TPM.

Following these actions, the administrator immediately notices that both FortiGate high availability (HA) status and FortiManager status for the FortiGate are negatively impacted.

What are the two reasons for this behavior? (Choose two.)

- A. The private-data-encryption key entered on the primary did not match the value that the TPM expected.
- B. Configuration for TPM is not synchronized between FortiGate HA cluster members.
- C. The FortiGate has not finished the auto-update process to synchronize the new configuration to FortiManager yet.
- D. TPM functionality is not yet compatible with FortiGate HA D The administrator needs to manually enter the hex private data encryption key in FortiManager

Correct Answer: AB

Explanation: The two reasons for the negative impact on the FortiGate HA status and FortiManager status after enabling TPM are: The private-data-encryption key entered on the primary unit did not match the value that the TPM expected. This could happen if the TPM was previously enabled and then disabled, and the key was changed in between. The TPM will reject the new key and cause an error in the configuration synchronization. Configuration for TPM is not synchronized between FortiGate HA cluster members. Each cluster member must have the same private-data-encryption key to form a valid HA cluster and synchronize their configurations. However, enabling TPM on one unit does not automatically enable it on the other units, and the key must be manually entered on each unit. To resolve these issues, the administrator should disable TPM on all units, clear the TPM data, and then enable TPM again with the

same private-data-encryption key on each unit. References:

<https://docs.fortinet.com/document/fortigate/6.4.0/cookbook/103437/inbound-ssl-inspection>

<https://docs.fortinet.com/document/fortigate/6.4.0/cookbook/103438/application-detection-on-ssl-offloaded-traffic>

QUESTION 10

SD-WAN is configured on a FortiGate. You notice that when one of the internet links has high latency the time to resolve names using DNS from FortiGate is very high.

You must ensure that the FortiGate DNS resolution times are as low as possible with the least amount of work. What should you configure?

- A. Configure local out traffic to use the outgoing interface based on SD-WAN rules with a manual defined IP associated to a loopback interface and configure an SD-WAN rule from the loopback to the DNS server.
- B. Configure an SD-WAN rule to the DNS server and use the FortiGate interface IPs in the source address.
- C. Configure two DNS servers and use DNS servers recommended by the two internet providers.
- D. Configure local out traffic to use the outgoing interface based on SD-WAN rules with the interface IP and configure an SD-WAN rule to the DNS server.

Correct Answer: D

Explanation: SD-WAN is a feature that allows users to optimize network performance and reliability by using multiple WAN links and applying rules based on various criteria, such as latency, jitter, packet loss, etc. One way to ensure that the FortiGate DNS resolution times are as low as possible with the least amount of work is to configure local out traffic to use the outgoing interface based on SD-WAN rules with the interface IP and configure an SD-WAN rule to the DNS server. This means that the FortiGate will use the best WAN link available to send DNS queries to the DNS server according to the SD-WAN rule, and use its own interface IP as the source address. This avoids NAT issues and ensures optimal DNS performance. References: <https://docs.fortinet.com/document/fortigate/7.0.0/sd-wan/19662/sd-wan>

[Latest NSE8_812 Dumps](#)

[NSE8_812 VCE Dumps](#)

[NSE8_812 Brindumps](#)