HIGHER QUALITY
BETTER SERVICE

CERTTREE

QUESTION & ANSWER

Provide One Year
Free Update!

https://www.certtree.com

Exam : **NSE7_SDW-7.2**

Title : Fortinet NSE 7 - SD-WAN 7.2

Version : DEMO

1.Refer to the exhibits.

Exhibit A

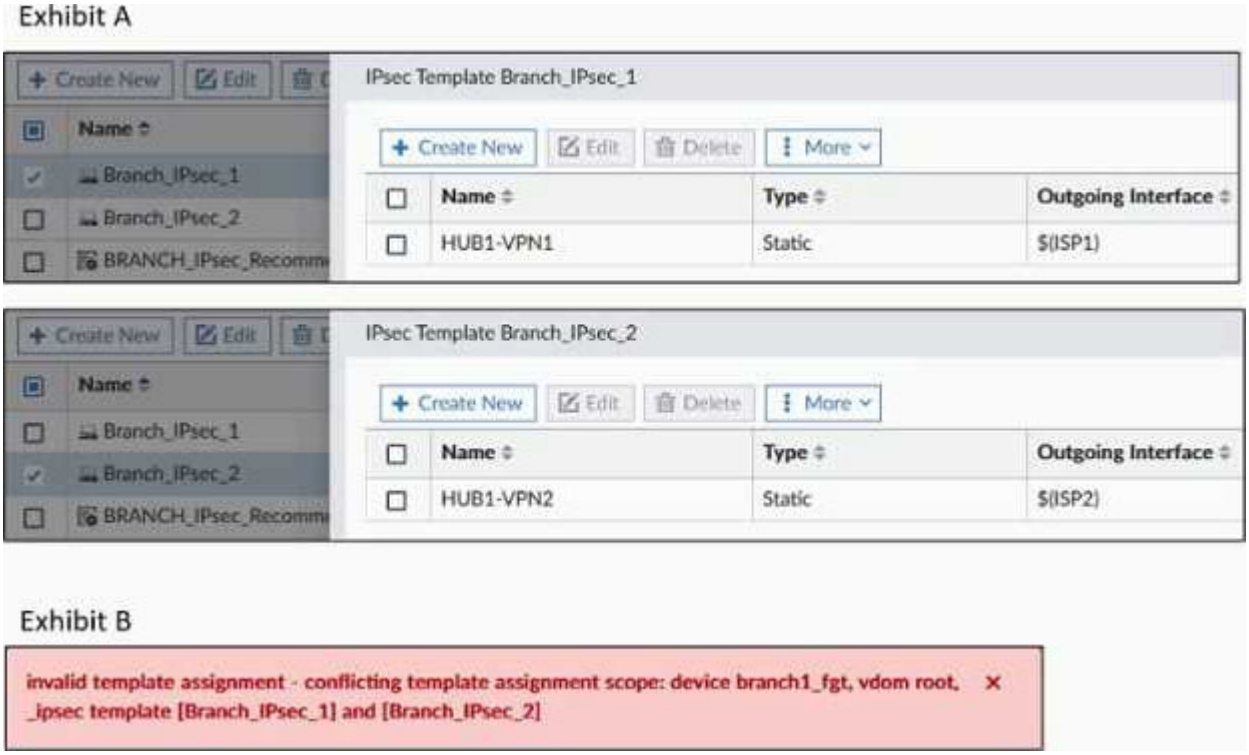

Exhibit B

Exhibit A shows two IPsec templates to define Branch_IPsec_1 and Branch_IPsec_2. Each template defines a VPN tunnel.

Exhibit B shows the error message that FortiManager displayed when the administrator tried to assign the second template to the FortiGate device.

Which statement best explain the cause for this issue?

A. You can assign only one template with a tunnel of fype static to each FortiGate device

B. You can define only one IPsec tunnel from branch devices to HUB1.

C. You can assign only one IPsec template to each FortiGate device.

D. You should review the branch1_fgt configuration for the already configured tunnel with the name HUB1-VPN2.

Answer: C

Explanation:

The error message in Exhibit B indicates a conflicting template assignment. This occurs because FortiManager does not allow the assignment of multiple IPsec templates that define VPN tunnels with the same name or settings to the same FortiGate device. The conflict arises from trying to assign a second IPsec template to a device that already has one assigned.

Reference: This is based on Fortinet's best practices and administrative guidelines which state that each FortiGate device should be assigned a unique IPsec template to avoid configuration conflicts.

2.Which statement about using BGP for ADVPN is true?

A. You must use BGP to route traffic for both overlay and underlay links.

B. You must configure AS path prepending.

C. You must configure BGP communities.

D. IBGP is preferred over EBGP, because IBGP preserves next hop information.

Answer: D

Explanation:
ADVPN is a technology that allows dynamic creation of IPsec tunnels between branch sites without requiring pre-configured policies or keys. BGP is a routing protocol that can be used to exchange routes between ADVPN peers. IBGP is a type of BGP that runs between routers in the same autonomous system (AS), while EBGP is a type of BGP that runs between routers in different ASes. IBGP is preferred over EBGP for ADVPN, because IBGP preserves the next hop information of the routes, which is needed to establish the IPsec tunnels. EBGP changes the next hop information to the EBGP peer address, which may not be reachable by the ADVPN peers. Therefore, using IBGP for ADVPN avoids the need to configure additional static routes or redistribute routes between BGP and another routing protocol.
Reference = ADVPN with BGP as the routing protocol, ADVPN, SD-WAN self-healing with BGP, Technical Tip: ADVPN with BGP as the routing protocol
The statement that IBGP is preferred over EBGP for ADVPN because IBGP preserves next hop information (D) is true. In a typical ADVPN deployment, it's beneficial to maintain next hop information across the network to ensure proper routing and optimal path selection.
Reference: This understanding comes from my knowledge of Fortinet's SD-WAN and ADVPN configurations, where BGP's behavior in terms of next hop preservation is a key consideration.

3.Which are three key routing principles in SD-WAN? (Choose three.)
A. FortiGate performs route lookups for new sessions only.
B. Regular policy routes have precedence over SD-WAN rules.
C. SD-WAN rules have precedence over ISDB routes.
D. By default, SD-WAN members are skipped if they do not have a valid route to the destination.
E. By default, SD-WAN rules are skipped if the best route to the destination is not an SD-WAN member.
Answer: BDE
Explanation:
Study Guide 7.2, pages 125, 129, 151

4.Refer to the exhibit.

```
session info: proto=6 proto_state=11 duration=242 expire=3349 timeout=3600
flags=00000000 socktype=0 sockport=0 av_idx=0 use=4
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
state=log dirty may_dirty ndr f00 app_valid
statistic(bytes/packets/allow_err): org=3421/20/1 reply=3777/17/1 tuples=3
tx speed(Bps/kbps): 0/0 rx speed(Bps/kbps): 0/0
orgin->sink: org pre->post, reply pre->post dev=7->3/3->7 gwy=0.0.0.0/0.0.0.0
hook=post dir=org act=snat 10.0.1.101:34676->128.66.0.1:22(192.2.0.1:34676)
hook=pre dir=reply act=dnat 128.66.0.1:22->192.2.0.1:34676(10.0.1.101:34676)
hook=post dir=reply act=noop 128.66.0.1:22->10.0.1.101:34676(0.0.0.0:0)
pos/(before,after) 0/(0,0), 0/(0,0)
misc=0 policy_id=2 pol_uuid_idx=14721 auth_info=0 chk_client_info=0 vd=0
serial=000032d9 tos=ff/ff app_list=2000 app=16060 url_cat=0
sdwan_mbr_seq=1 sdwan_service_id=2
rpdb_link_id=ff000002 rpdb_svc_id=0 ngfwid=n/a
npu_state=0x001008
```

Which statement explains the output shown in the exhibit?
A. FortiGate performed standard FIB routing on the session.
B. FortiGate will not re-evaluate the session following a firewall policy change.

C. FortiGate used 192.2.0.1 as the gateway for the original direction of the traffic.
D. FortiGate must re-evaluate the session due to routing change.
Answer: D
Explanation:
The snat-route-change option is enabled by default. This option enables FortiGate to re-evaluate the routing table and select a new egress interface if the next hop IP address changes. This option only applies to sessions in the dirty state. Sessions in the log state are not affected by routing changes.

5.What are two common use cases for remote internet access (RIA)? (Choose two.)
A. Provide direct internet access on spokes
B. Provide internet access through the hub
C. Centralize security inspection on the hub
D. Provide thorough inspection on spokes
Answer: BC
Explanation:
B) Provide internet access through the hub: This involves routing branch or remote office internet traffic through a central hub, ensuring consistent security policies and possibly better management of network resources.
C) Centralize security inspection on the hub: With this approach, all internet-bound traffic from various spokes is inspected at the hub, leveraging centralized security mechanisms for thorough inspection and policy enforcement.