Fortinet

NSE6_SDW_AD-7.6

Fortinet NSE 6 - SD-WAN 7.6 Enterprise Administrator

Latest Version: 6.0

Question: 1

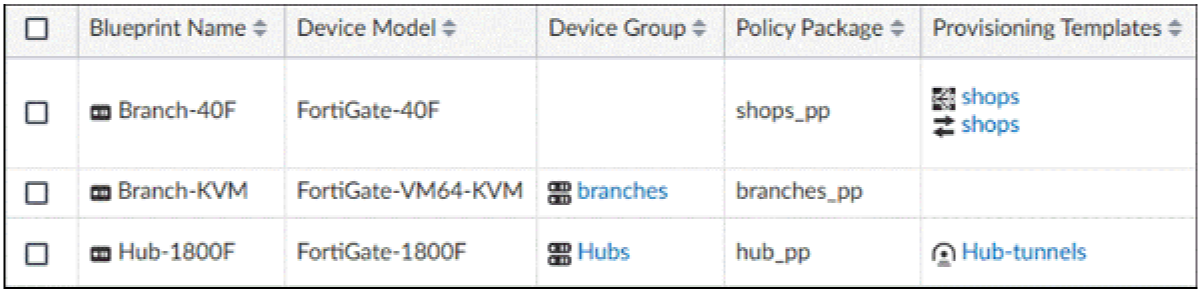
What are two advantages of using an IPsec recommended template to configure an IPsec tunnel in a hub-and-spoke topology?
(Choose two.)

A. It ensures consistent settings between phase1 and phase2.
B. It guides the administrator to use Fortinet recommended settings.
C. It automatically installs IPsec tunnels to every spoke when they are added to the FortiManager ADOM.
D. The VPN monitor tool provides additional statistics for tunnels defined with an IPsec recommended template.

Answer: A,B

Question: 2

Refer to the exhibit.



□	Blueprint Name	Device Model	Device Group	Policy Package	Provisioning Templates
□	Branch-40F	FortiGate-40F		shops_pp	shops shops
□	Branch-KVM	FortiGate-VM64-KVM	branches	branches_pp	
□	Hub-1800F	FortiGate-1800F	Hubs	hub_pp	Hub-tunnels

As a FortiManager administrator, you reviewed the device blueprint configuration. Based on the exhibit, which configuration deviates from best practices?

A. You should assign at least one provisioning template to the Branch-KVM blueprint.
B. You should assign a device group to the Branch-40F blueprint.
C. You should assign a single provisioning template to the Branch-40F blueprint.
D. You should assign a provisioning template or a device group to the Hub-1800F blueprint, but not both.

Answer: D

Question: 3

Which of the following step is necessary to use overlay links in SD-WAN?

A. Overlay links must be configured in the global VDOM on a FortiGate.
B. Overlay links must include one active IPsec interface.
C. Overlay links must be configured with a dedicated firewall policy.
D. Overlay links must be added to a SD-WAN zone.

Answer: B

Question: 4

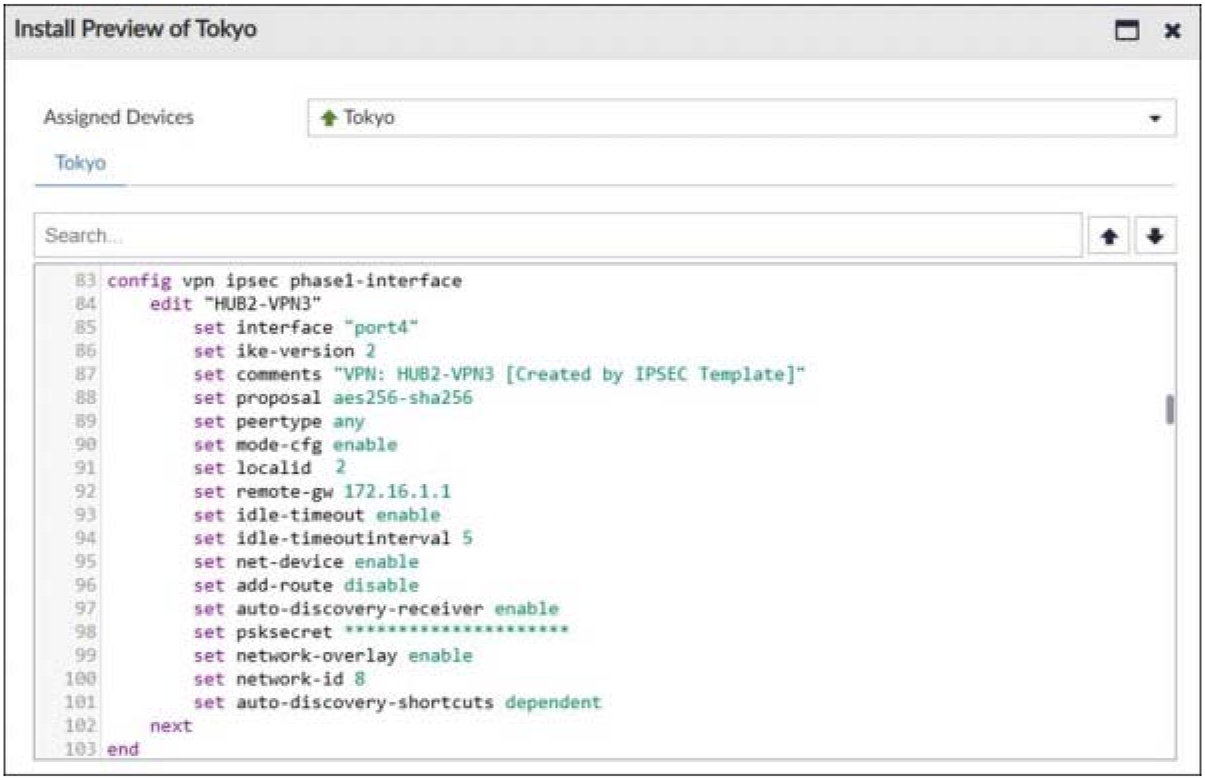
You want to configure ADVPN without route reflection on your SD-WAN topology. Which two statements apply to this scenario?
(Choose two.)

A. ADVPN without route reflection is compatible with BGP on loopback.
B. ADVPN without route reflection allows hub-side steering by route tag.
C. ADVPN without route reflection is also called ADVPN 2.0.
D. ADVPN without route reflection is compatible with static routing on the overlay.

Answer: C,D

Question: 5

Refer to the exhibit.



```
config vpn ipsec phase1-interface
    edit "HUB2-VPN3"
        set interface "port4"
        set ike-version 2
        set comments "VPN: HUB2-VPN3 [Created by IPSEC Template]"
        set proposal aes256-sha256
        set peertype any
        set mode-cfg enable
        set localid  2
        set remote-gw 172.16.1.1
        set idle-timeout enable
        set idle-timeoutinterval 5
        set net-device enable
        set add-route disable
        set auto-discovery-receiver enable
        set psksecret *********************
        set network-overlay enable
        set network-id 8
        set auto-discovery-shortcuts dependent
    next
end
```

The administrator used the SD-WAN overlay template to prepare an IPsec tunnel configuration for a hub-and-spoke SD-WAN topology. The exhibit shows the FortiManager installation preview for one FortiGate device.

Based on the exhibit, which statement best describes the configuration applied to the FortiGate device?

A. It is a spoke device. It can trigger the establishment of an ADVPN shortcut.

B. It is a hub device. It will automatically discover the spoke devices and add them to the SD-WAN topology.

C. It is a hub device in a dual-hub topology. It can participate in the establishment of ADVPN shortcuts.

D. It is a spoke device. It can establish shortcuts only if the remote spoke initiates the request.

Answer: A

Question: 6

You configured a manual SD-WAN rule to steer game and social media traffic through port2. However, when analyzing the traffic flow you notice that the volume of traffic through port2 is much smaller than expected.

What should you check on the FortiGate configuration?

A. Check whether application-group detection is allowed on the firewall policy that allows the traffic flow.

B. Check on the FortiGate CLI whether the feature that allows the detection of applications per group is enabled.

C. Check whether application filter is allowed in the FortiGuard settings.
D. Check whether application control is allowed on the firewall policy that allows the traffic flow.

Answer: D

Question: 7

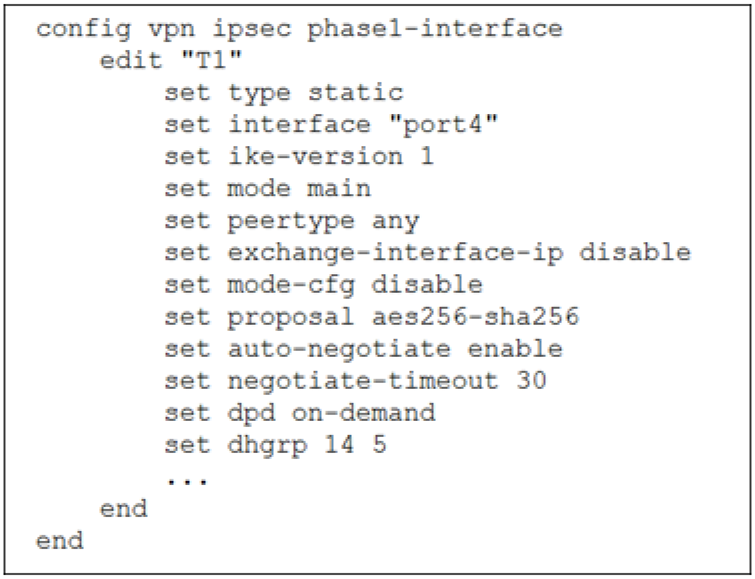
You are configuring SD-WAN zones and members on a FortiGate device. Which two facts should you take into account?
(Choose two.)

A. You can add any physical interface to a zone.
B. You can add only SD-WAN members to a zone.
C. The default zone is virtual-wan-link.
D. The default zone is sdw-default

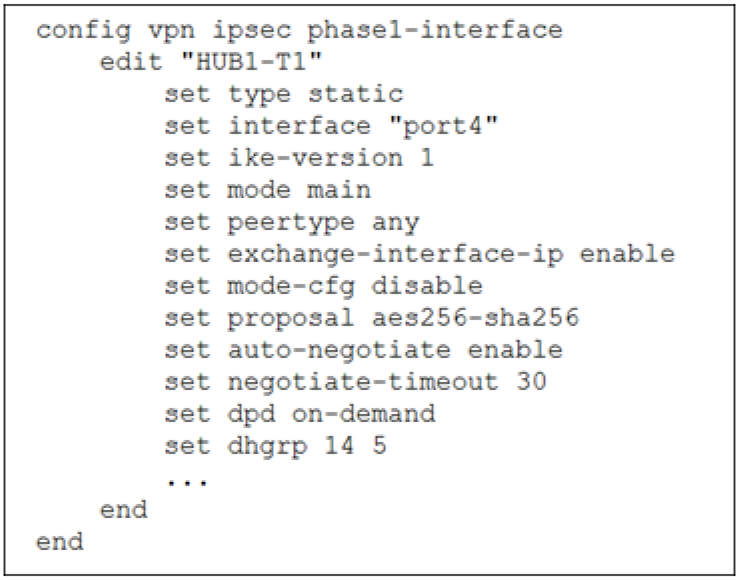
Answer: B,C

Question: 8

Refer to the exhibits.



```
config vpn ipsec phase1-interface
    edit "T1"
        set type static
        set interface "port4"
        set ike-version 1
        set mode main
        set peertype any
        set exchange-interface-ip disable
        set mode-cfg disable
        set proposal aes256-sha256
        set auto-negotiate enable
        set negotiate-timeout 30
        set dpd on-demand
        set dhgrp 14 5
        ...
    end
end
```



```
config vpn ipsec phase1-interface
    edit "HUB1-T1"
        set type static
        set interface "port4"
        set ike-version 1
        set mode main
        set peertype any
        set exchange-interface-ip enable
        set mode-cfg disable
        set proposal aes256-sha256
        set auto-negotiate enable
        set negotiate-timeout 30
        set dpd on-demand
        set dhgrp 14 5
        ...
    end
end
```

The VPN configuration on a spoke and a hub is shown.

The administrator wants to use those tunnels to build an SD-WAN topology.
Which one parameter must you modify to allow the tunnel to come up and be used in the SD-WAN topology?

A. Set exchange-interface-ip to enable on the hub side.
B. Set mode-cfg to enable on the spoke side.
C. Set the type to dynamic on the hub side.
D. Change ike-version to 2 on the hub and the spoke.

Answer: A

Question: 9

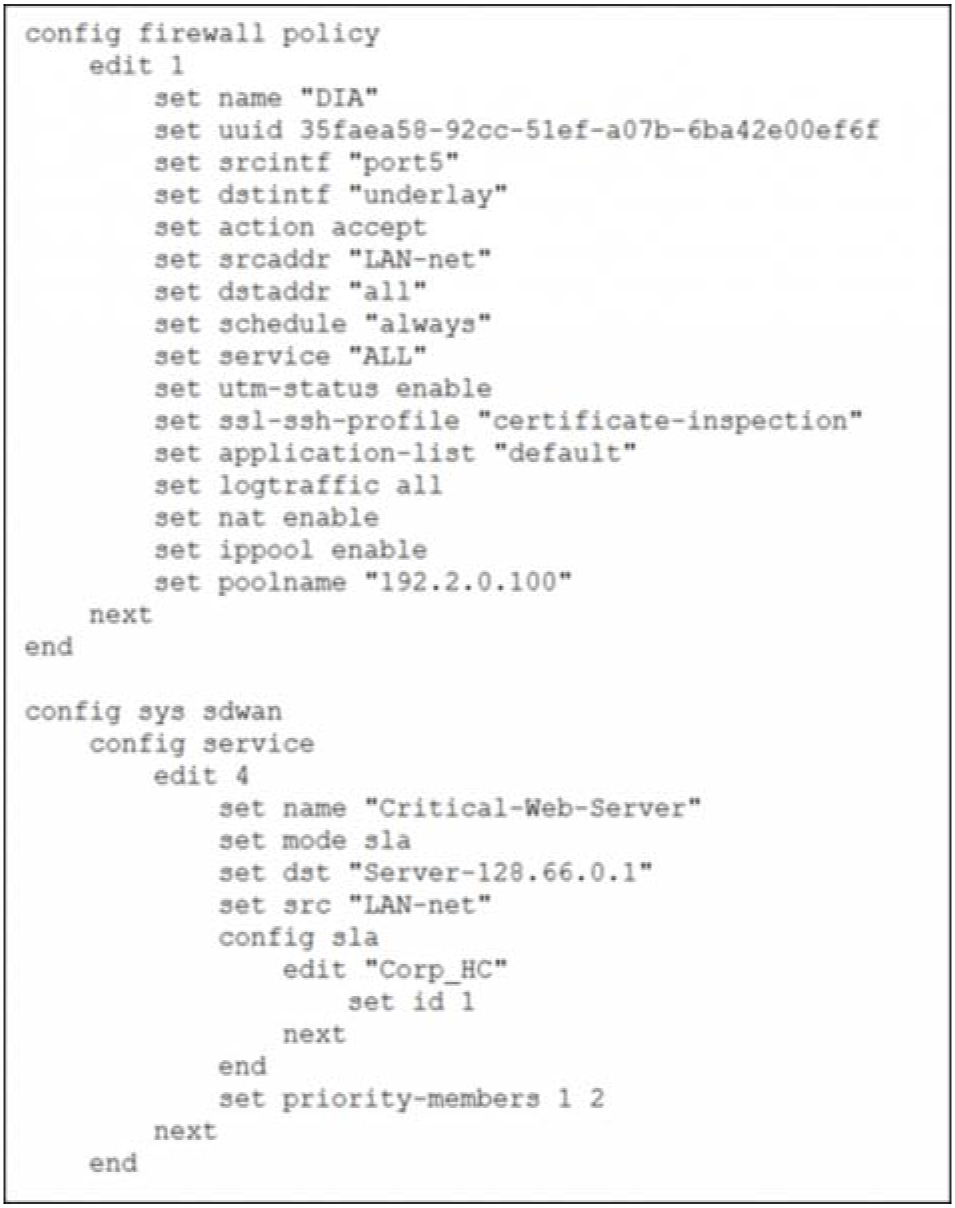
Which two statements correctly describe what happens when traffic matches the implicit SD-WAN rule? (Choose two.)

A. The session information output displays no SD-WAN service ID.
B. By default, FortiGate load balance the traffic according to the source IP address.
C. FortiGate flags the session with sdw-imp.
D. The traffic is distributed through only static routes or directly connected routes.

Answer: A,B

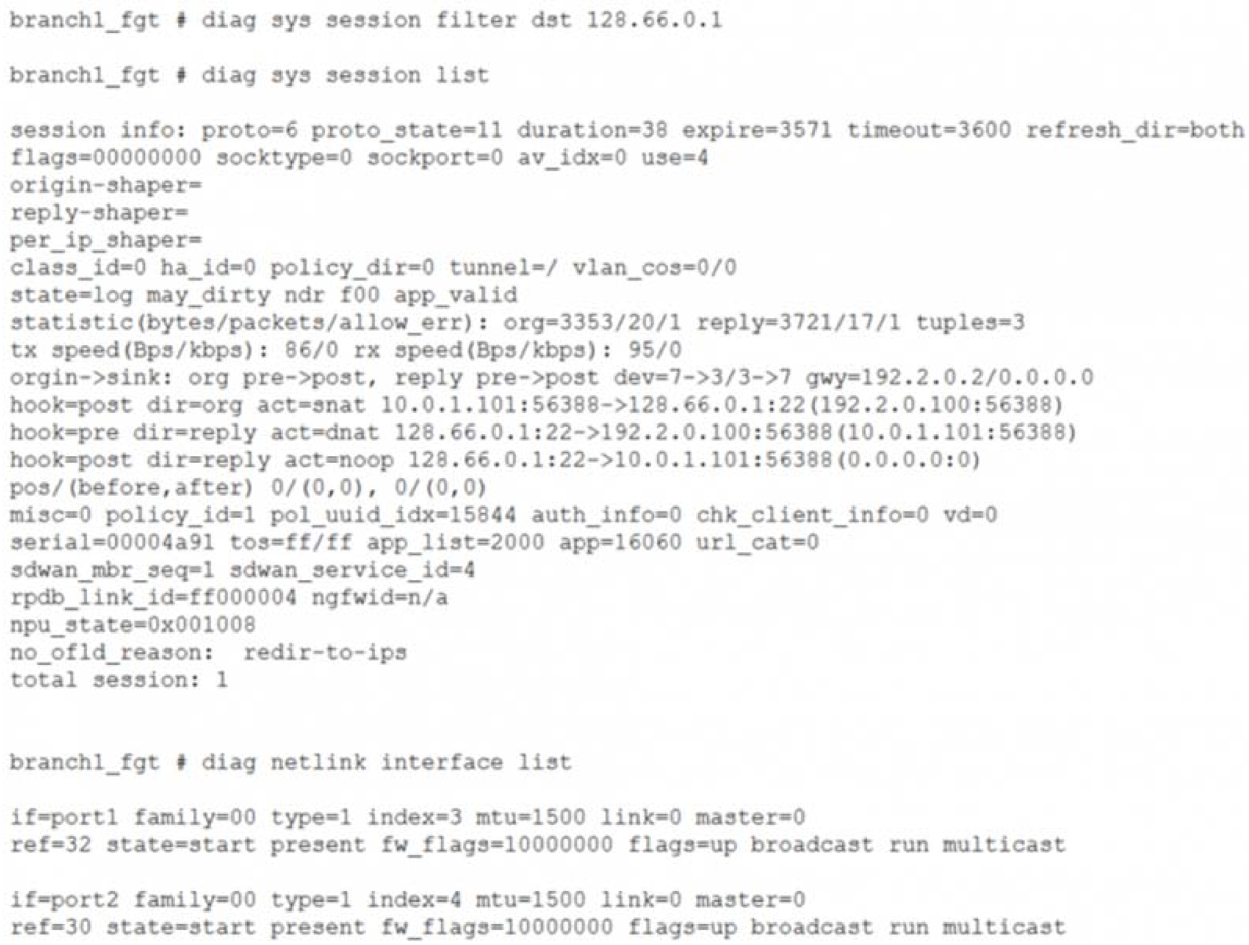
Question: 10

Refer to the exhibits.



```
config firewall policy
    edit 1
        set name "DIA"
        set uuid 35faea58-92cc-51ef-a07b-6ba42e00ef6f
        set srcintf "port5"
        set dstintf "underlay"
        set action accept
        set srcaddr "LAN-net"
        set dstaddr "all"
        set schedule "always"
        set service "ALL"
        set utm-status enable
        set ssl-ssh-profile "certificate-inspection"
        set application-list "default"
        set logtraffic all
        set nat enable
        set ippool enable
        set poolname "192.2.0.100"
    next
end

config sys sdwan
    config service
        edit 4
            set name "Critical-Web-Server"
            set mode sla
            set dst "Server-128.66.0.1"
            set src "LAN-net"
            config sla
                edit "Corp_HC"
                    set id 1
                next
            end
            set priority-members 1 2
        next
    end
```



```
branch1_fgt # diag sys session filter dst 128.66.0.1

branch1_fgt # diag sys session list

session info: proto=6 proto_state=11 duration=38 expire=3571 timeout=3600 refresh_dir=both
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=0/0
state=log may_dirty ndr f00 app_valid
statistic(bytes/packets/allow_err): org=3353/20/1 reply=3721/17/1 tuples=3
tx speed(Bps/kbps): 86/0 rx speed(Bps/kbps): 95/0
orgin->sink: org pre->post, reply pre->post dev=7->3/3->7 gwy=192.2.0.2/0.0.0.0
hook=post dir=org act=snat 10.0.1.101:56388->128.66.0.1:22(192.2.0.100:56388)
hook=pre dir=reply act=dnat 128.66.0.1:22->192.2.0.100:56388(10.0.1.101:56388)
hook=post dir=reply act=noop 128.66.0.1:22->10.0.1.101:56388(0.0.0.0:0)
pos/(before,after) 0/(0,0), 0/(0,0)
misc=0 policy_id=1 pol_uuid_idx=15844 auth_info=0 chk_client_info=0 vd=0
serial=00004a91 tos=ff/ff app_list=2000 app=16060 url_cat=0
sdwan_mbr_seq=1 sdwan_service_id=4
rpdb_link_id=ff000004 ngfwid=n/a
npu_state=0x001008
no_ofld_reason:  redir-to-ips
total session: 1


branch1_fgt # diag netlink interface list

if=port1 family=00 type=1 index=3 mtu=1500 link=0 master=0
ref=32 state=start present fw_flags=10000000 flags=up broadcast run multicast

if=port2 family=00 type=1 index=4 mtu=1500 link=0 master=0
ref=30 state=start present fw_flags=10000000 flags=up broadcast run multicast
```

You have configured an SD-WAN rule and a firewall policy. You check the interface list, and the sessions established between a LAN device and a server located on another side.

Based on the exhibits, if the performances of port1 falls outside SLA, what can you expect for traffic matching the session shown?

A. FortiGate will drop the session. The user must establish a new session that FortiGate will steer through port2.

B. You must check the underlay zone configuration to know the answer.

C. You must check the system global configuration to know the answer.

D. FortiGate will flag the session as dirty, and reevaluate the interface to use when the next packet arrives.

Answer: C