Passcert

Higher Quality, better service!

Q&A

Http://www.passcert.com

We offer free update service for one year.

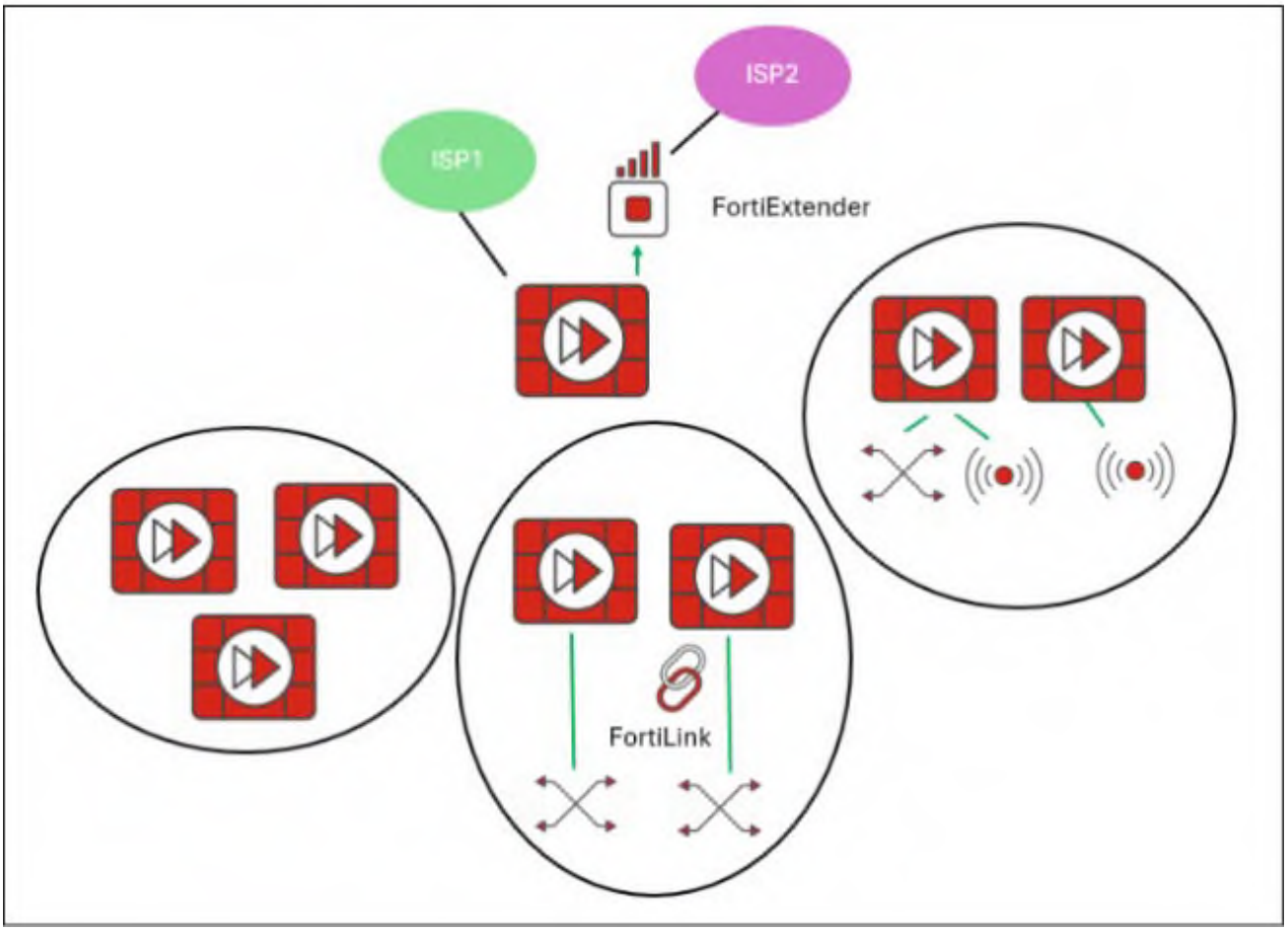
Exam : **NSE7_FSN_AR-7.6**

Title : Fortinet NSE 7 - Secure Networking 7.6 Architect

Version : DEMO

1.Refer to the exhibit.

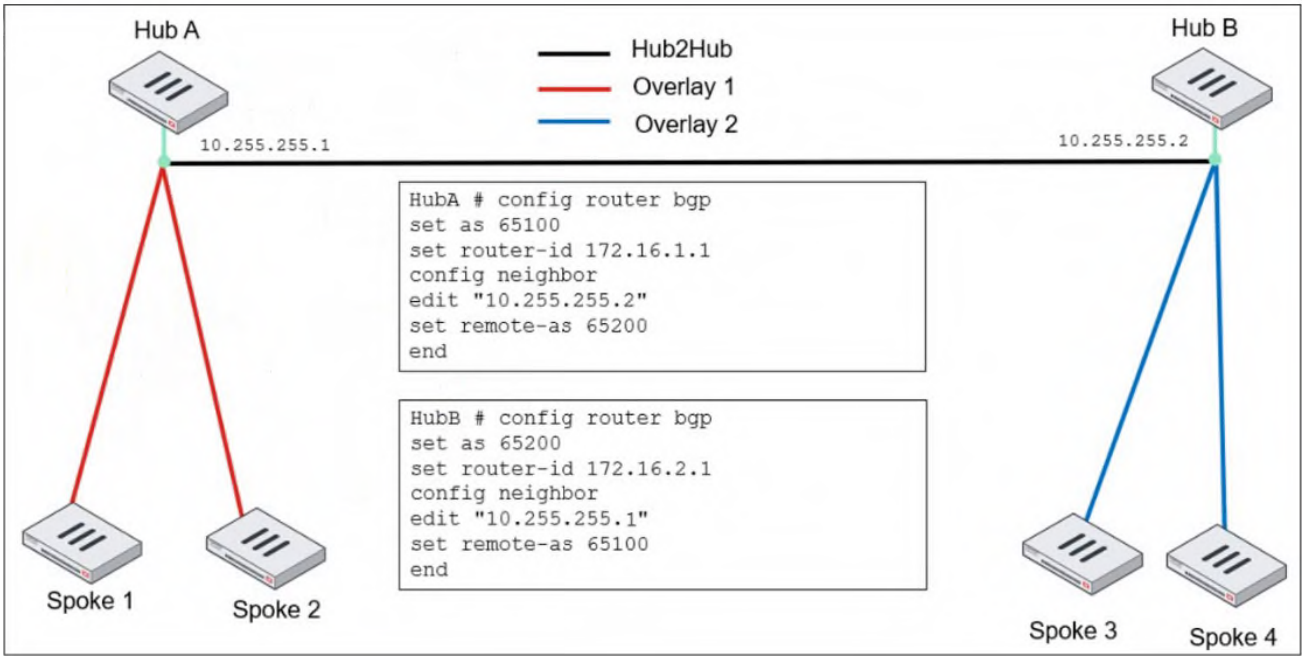
SD-WAN Network Topology



You want to configure SD-WAN on a network, as shown in the exhibit.
The network contains many FortiGate devices. Some are used as next-generation firewalls (NGFW), and some are installed with extensions such as FortiSwitch, FortiAP, or FortiExtender.
Which factors should you consider when planning your deployment?
A. You can build an SD-WAN topology that includes all devices. The hubs must be devices without extensions.
B. You can build an SD-WAN topology that includes all devices. The hubs can be FortiGate devices with FortiExtender.
C. You should exclude the FortiGate devices with FortiLink connection from the SD-WAN topology.
D. You should build multiple SD-WAN topologies. Each topology should contain only one type of extension.
Answer: A

2.Refer to the exhibit.

Network topology



An ADVPN network is shown.

You must configure an ADVPN using IBGP for each local region and EBGP across regions to connect Overlay 1 with Overlay 2.

Which two options must you configure in the Hub2Hub BGP peering? (Choose two.)

A. set ibgp-enforce-multihop advpn

B. set ebgp-enforce-multihop enable

C. set next-hop-self enable

D. set attribute-unchanged next-hop

Answer: BD

3.Refer to the exhibits.

OSPF configuration

```
FGT # show router ospf
config router ospf
    set router-id 0.0.0.113
    set distribute-list-in "Allow-172.16"
    config area
        edit 0.0.0.0
---omitted---
end
```

Prefix-list configuration

```
FGT # show router prefix-list
config router prefix-list
    edit "Allow-172.16"
        config rule
            edit 1
                set prefix 172.16.0.0 255.255.0.0
                unset ge
                unset le
---omitted---
end
```

An OSPF peer is advertising route 172.16.52.0/24. The local FortiGate is configured with an inbound distribution list that allows the 172.16.0.0/16 network to be injected into its routing table. However, the 172.16.52.0/24 subnet cannot be seen in the FIB.

Which two steps can the administrator of the local FortiGate take to ensure that the advertised 172.16.52.0/24 subnet will be injected into the routing table? (Choose two.)

A. Modify the default prefix-list behavior from implicit deny to implicit allow.

B. Add another entry to the prefix list to specifically allow the 172.16.52.0/24 network.

C. Change the le value to 16.

D. Change the ge value to 17.

Answer: BD

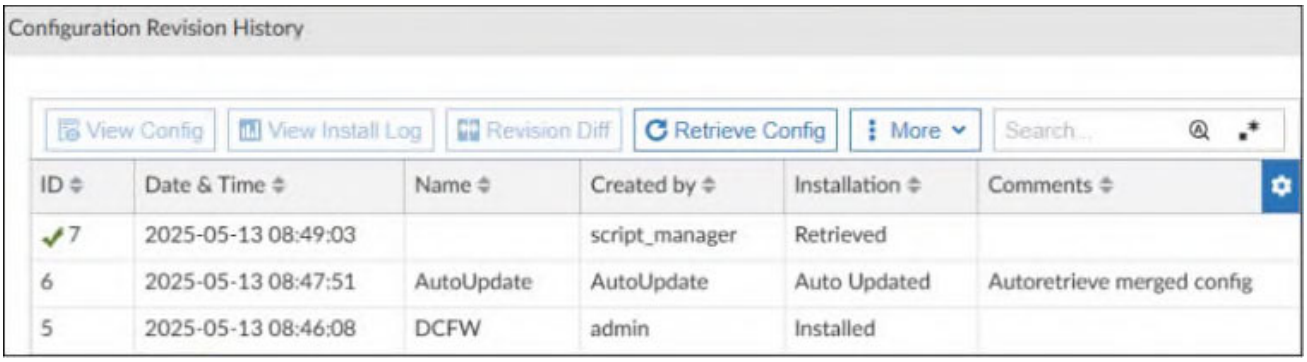
4.In which two ways does FortiGate utilize the Internet Service Database (ISDB) within firewall policies and SD-WAN rules? (Choose two.)

A. The ISDB limits access by URL and domain.

B. The ISDB works in proxy mode only, allowing the analysis of packets in layers 3 and 4 of the OSI

model.
C. FortiGate has a predefined list of all IP addresses and ports for specific applications downloaded from FortiGuard.
D. The ISDB blocks the IP addresses and ports of an application predefined by FortiGuard.
Answer: CD

5.Refer to the exhibit.



A revision history window at the FortiManager device layer is shown.
The IT team is trying to identify the administrator responsible for the most recent update to the FortiGate device database.
What can the IT team conclude?
A. To identify the user who created the event, they must view it on the Configuration and Installation widget on FortiGate at the FortiManager device layer.
B. The user script_manager, an API user from the Fortinet Developer Network (FDN), is retrieving a configuration.
C. To identify the user who created the event, in the FortiManager system logs, they must use the type=script filter in the user field.
D. The retrieve process was automatically triggered by a Remote FortiGate Directly (via CLI) script.
Answer: D