NSE7_EFW-7.2 Q&As

Fortinet NSE 7 - Enterprise Firewall 7.2

Pass Fortinet NSE7_EFW-7.2 Exam with 100% Guarantee

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

https://www.geekcert.com/nse7_efw-7-2.html

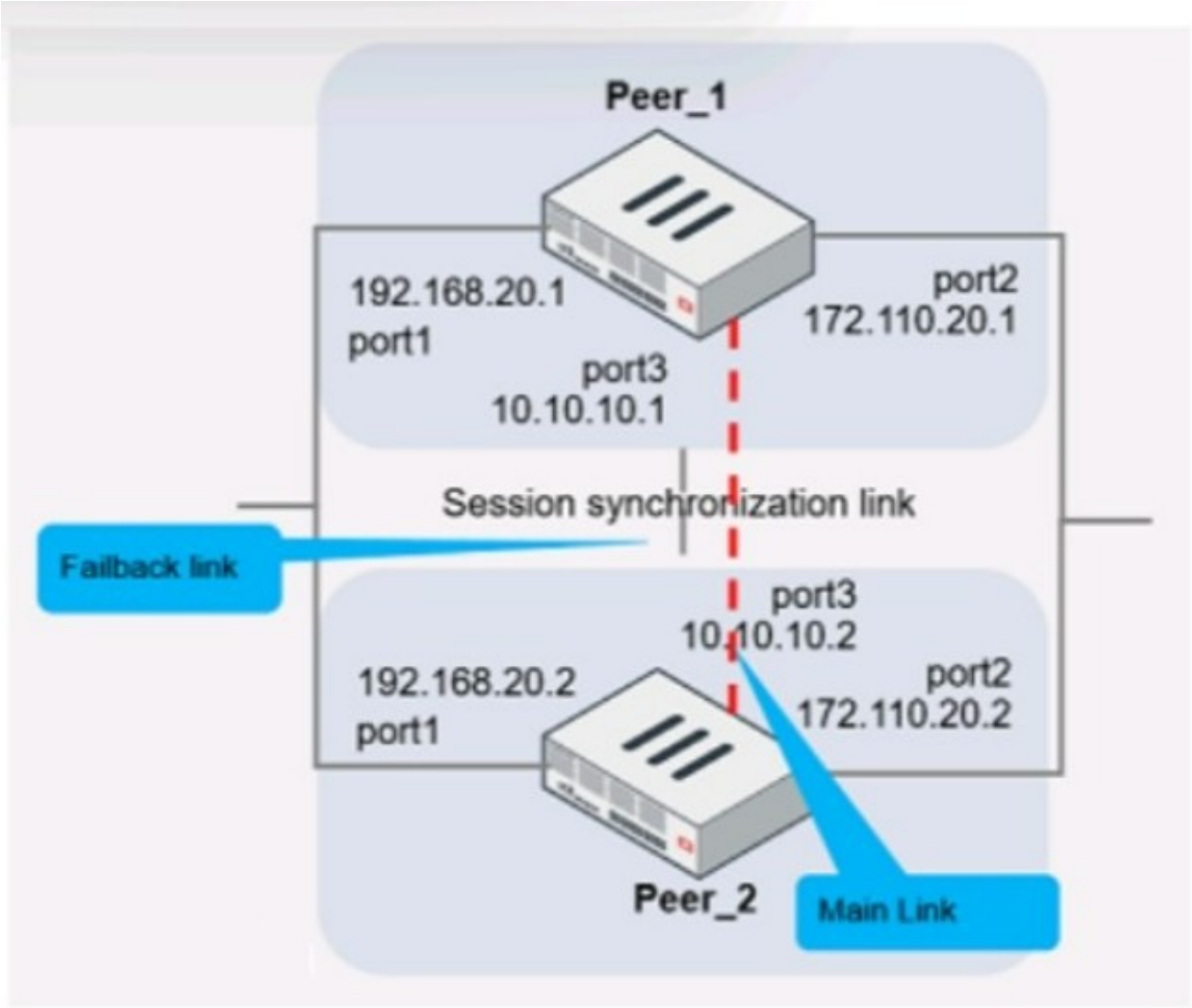
100% Passing Guarantee
100% Money Back Assurance

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, which shows two configured FortiGate devices and peering over FGSP.



The main link directly connects the two FortiGate devices and is configured using the set session-syn-dev command.

What is the primary reason to configure the main link?

A. To have both sessions and configuration synchronization in layer 2

B. To load balance both sessions and configuration synchronization between layer 2 and 3

C. To have only configuration synchronization in layer 3

D. To have both sessions and configuration synchronization in layer 3

Correct Answer: D

The primary purpose of configuring a main link between the devices is to synchronize session information so that if one unit fails, the other can continue processing traffic without dropping active sessions.

A.To have both sessions and configuration synchronization in layer 2.This is incorrect because FGSP is used for session synchronization, not configuration synchronization. B.To load balance both sessions and configuration synchronization

between layer 2 and 3.FGSP does not perform load balancing and is not used for configuration synchronization.

C.To have only configuration synchronization in layer 3.The main link is not used solely for configuration synchronization.

D.To have both sessions and configuration synchronization in layer 3.The main link in an FGSP setup is indeed used to synchronize session information across the devices, and it operates at layer 3 since it uses IP addresses to establish the

peering.

QUESTION 2

Refer to the exhibit, which contains a partial BGP combination.

You want to configure a loopback as the OGP source.

Which two parameters must you set in the BGP configuration? (Choose two)

A. ebgp-enforce-multihop

B. recursive-next-hop

C. ibgp-enfoce-multihop

D. update-source

Correct Answer: AD

To configure a loopback as the BGP source, you need to set the "ebgp- enforce-multihop" and "update-source" parameters in the BGP configuration. The "ebgp- enforce-multihop" allows EBGP connections to neighbor routers that are not directly connected, while "update-source" specifies the IP address that should be used for the BGP session1. References := BGP on loopback, Loopback interface, Technical Tip: Configuring EBGP Multihop Load-Balancing, Technical Tip: BGP routes are not installed in routing table with loopback as update source

QUESTION 3

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

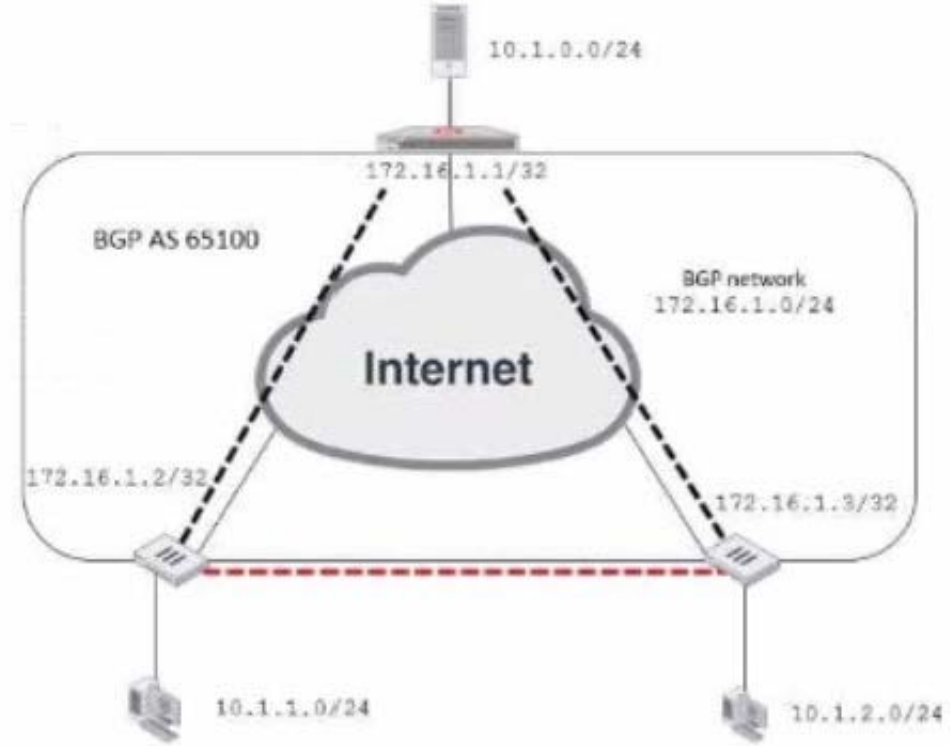
Correct Answer: BC

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 4

Exhibit.

Network diagram



Partial BGP configuration

```
Hub # show router bgp
config router bgp
    set as 65100
    set router-id 172.16.1.1
    config neighbor-group
        edit "advpn"
            set remote-as 65100
            ...
        next
    end
....
end
```

Refer to the exhibit, which contains an ADVPN network diagram and a partial BGP con figuration Which two parameters Should you configure in config neighbor range? (Choose two.)

A. set prefix 172.16.1.0 255.255.255.0

B. set route reflector-client enable

C. set neighbor-group advpn

D. set prefix 10.1.0 255.255.255.0

Correct Answer: AC

In the ADVPN configuration for BGP, you should specify the prefix that the neighbors can advertise. Option A is correct as you would configure the BGP network prefix that should be advertised to the neighbors, which matches the BGP network in the diagram. Option C is also correct since you should reference the neighbor group configured for the ADVPN setup within the BGP configuration.

QUESTION 5

You want to block access to the website ww.eicar.org using a custom IPS signature.

Which custom IPS signature should you configure?

A. `F-SBID( --name "eicar"; --protocol udp; --flow from_server; --pattern "eicar"; --context host;)`

B. `F-SBID( --name "detect_eicar"; --protocol udp; --service ssl; --flow from_client; --pattern "www.eicar.org"; --no_case; --context host;)`

C. `F-SBID( --name "detect_eicar"; --protocol tcp; --service dns; --flow from_server; --pattern "eicar"; --no_case;)`

D. `F-SBID( --name "eicar"; --protocol tcp; --service HTTP; --flow from_client; --pattern "www.eicar.org"; --no_case; --context host;)`

A. Option A

B. Option B

C. Option C

D. Option D

Correct Answer: D

Option D is the correct answer because it specifically blocks access to the website "www.eicar.org" using TCP protocol and HTTP service, which are commonly used for web browsing. The other options either use the wrong protocol (UDP), the wrong service (DNS or SSL), or the wrong pattern ("eicar" instead of "www.eicar.org"). References := Configuring custom signatures | FortiGate / FortiOS 7.4.0 - Fortinet Document Library, section "Signature to block access to example.com".