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

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

Which two statements about the neighbor-group command are true? (Choose two.)

A. You can configure it on the GUI.

B. It applies common settings in an OSPF area.

C. It is combined with the neighbor-range parameter.

D. You can apply it in Internal BGP (IBGP) and External BGP (EBGP).

Correct Answer: BD

The neighbor-group command in FortiOS allows for the application of common settings to a group of neighbors in OSPF, and can also be used to simplify configuration by applyingcommon settings to both IBGP and EBGP neighbors. This grouping functionality is a part of the FortiOS CLI and is documented in the Fortinet CLI reference.

QUESTION 2

Exhibit.

```
config vpn ipsec phase1-interface
    edit tunnel
        set type dynamic
        set interface "port1"
        set ike-version 2
        set keylife 28800
        set peertype any
        set net-device disable
        set proposal aes128-sha256 aes256-sha256
        set dpd on-idle
        set add-route enable
        set psksecret fortinet
    next
end
```

Refer to the exhibit, which contains a partial VPN configuration. What can you conclude from this configuration1?

A. FortiGate creates separate virtual interfaces for each dial up client.

B. The VPN should use the dynamic routing protocol to exchange routing information Through the tunnels.

C. Dead peer detection s disabled.

D. The routing table shows a single IPSec virtual interface.

Correct Answer: C

The configuration line "set dpd on-idle" indicates that dead peer detection (DPD) is set to trigger only when the tunnel is idle, not actively disabled1. References: FortiGate IPSec VPN User Guide - Fortinet Document Library

From the given VPN configuration, dead peer detection (DPD) is set to \\'on-idle\\', indicating that DPD is enabled and will be used to detect if the other end of the VPN tunnel is still alive when no traffic is detected. Hence, option C is incorrect. The configuration shows the tunnel set to type \\'dynamic\\', which does not create separate virtual interfaces for each dial- up client (A), and it is not specified that dynamic routing will be used (B). Since this is a phase 1 configuration snippet, the routing table aspect (D) cannot be concluded from this alone.

QUESTION 3

Refer to the exhibits, which show the configurations of two address objects from the same FortiGate.

Engineering address object

Name	Engineering
Color	🖾 Change
Type	Subnet ▼
IP/Netmask	192.168.0.0 255.255.255.0
Interface	☐ any ▼
Static route configuration	⬤
Comments	Write a comment... ⟋ 0/255

OK   Cancel

Finance address object

Name	Finance
Color	🖾 Change
Type	Subnet ▼
IP/Netmask	192.168.1.0 255.255.255.0
Interface	☐ any ▼
Static route configuration	⬤
Comments	Write a comment... ⟋ 0/255

Return

Why can you modify the Engineering address object, but not the Finance address object?

A. You have read-only access.

B. FortiGate joined the Security Fabric and the Finance address object was configured on the root FortiGate.

C. FortiGate is registered on FortiManager.

D. Another user is editing the Finance address object in workspace mode.

Correct Answer: B

The inability to modify the Finance address object while being able to modify the Engineering address object suggests that the Finance object is being managed by a higher authority in the Security Fabric, likely the root FortiGate. When a FortiGate is part of a Security Fabric, address objects and other configurations may be managed centrally. This aligns with the Fortinet FortiGate documentation on Security Fabric and central management of address objects.

QUESTION 4

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".

QUESTION 5

Which two statements about bfd are true? (Choose two)

A. It can support neighbor only over the next hop in BGP

B. You can disable it at the protocol level

C. It works for OSPF and BGP

D. You must configure n globally only

Correct Answer: BC

BFD (Bidirectional Forwarding Detection) is a protocol that can quickly detect failures in the forwarding path between two adjacent devices. You can disable BFD at the protocol level by using the "set bfd disable" command under the OSPF or BGP configuration. BFD works for both OSPF and BGP protocols, as well as static routes and SD-WAN rules. References := BFD | FortiGate / FortiOS 7.2.0 - Fortinet Document Library, section "BFD".

NSE7_EFW-7.2 PDF Dumps

NSE7_EFW-7.2 Practice Test

NSE7_EFW-7.2 Braindumps