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:

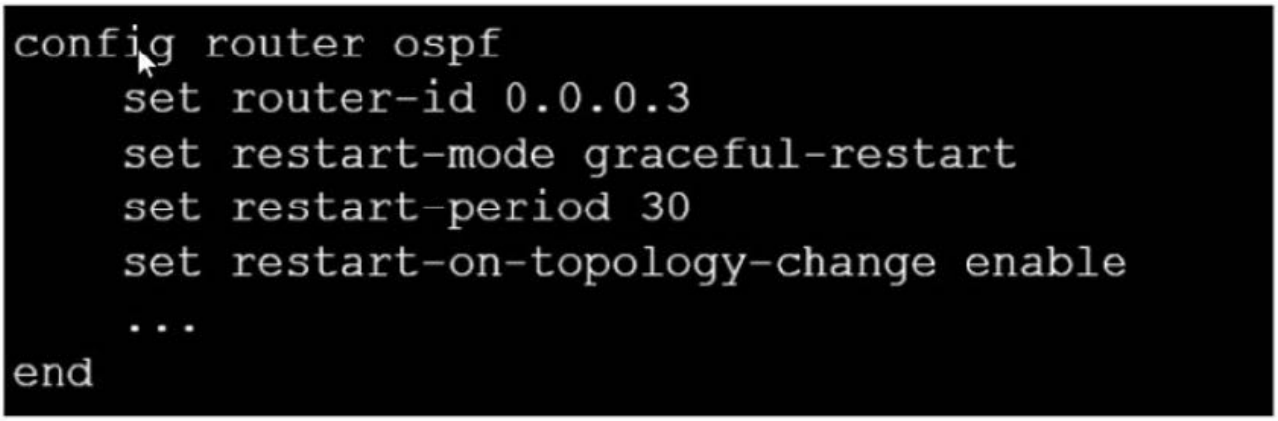
https://www.pass4itsure.com/nse7_efw-7-2.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Fortinet Official Exam Center

QUESTION 1

Refer to the exhibit, which contains a partial OSPF configuration.



What can you conclude from this output?

A. Neighbors maintain communication with the restarting router.

B. The router sends grace LSAs before it restarts.

C. FortiGate restarts if the topology changes.

D. The restarting router sends gratuitous ARP for 30 seconds.

Correct Answer: B

From the partial OSPF (Open Shortest Path First) configuration output:

B. The router sends grace LSAs before it restarts: This is implied by the command \\'set restart-mode graceful-restart\\'. When OSPF is configured with graceful restart, the router sends grace LSAs (Link State Advertisements) to inform its neighbors that it is restarting, allowing for a seamless transition without recalculating routes. Fortinet documentation on OSPF configuration clearly states that enabling graceful restart mode allows the router to maintain its adjacencies and routes during a brief restart period.

QUESTION 2

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

```
config router bgp
    set as 65200
    set router-id 172.16.1.254
    config neighbor
        edit 100.64.1.254
            set remote-as 65100
        next
    end
end
```

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

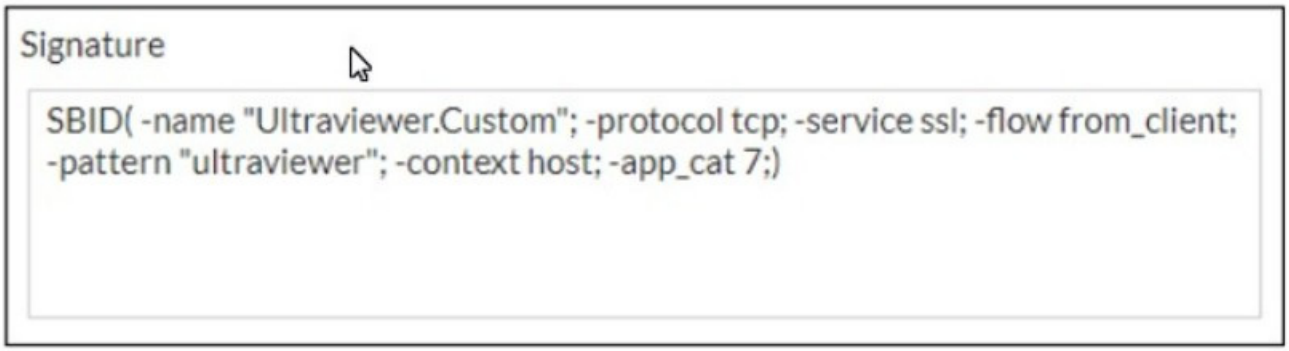
D. update-source

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 custom signature.



Which two modifications must you apply to the configuration of this custom signature so that you can save it on FortiGate? (Choose two.)

A. Add severity.

B. Add attack_id.

C. Ensure that the header syntax is F-SBID.

D. Start options with --.

Correct Answer: AB

For a custom signature to be valid and savable on a FortiGate device, it must include certain mandatory fields. Severity is used to specify the level of threat that the signature represents, and attack_id is a unique identifier for the signature. Without these, the signature would not be complete and could not be correctly utilized by the FortiGate\\'s Intrusion Prevention System (IPS).

QUESTION 4

Exhibit.

```
# diagnose webfilter fortiguard cache dump

Saving to file [/tmp/urcCache.txt]
Cache Contents:
---------------
Cache Mode:   TTL
Cache DB Ver: 23.6106

Domain   |IP        DB Ver   T URL
34000000|34000000 23.6106   P Bhttp://training.fortinet.com/
25000000|25000000 23.6106   E Bhttps://twitter.com/…

# get webfilter categories
…
g07 General Interest - Business:
     31 Finance and Banking
     …
     51 Government and Legal Organizations
     52 Information Technology
```

Refer to the exhibit, which shows the output from the webfilter fortiguard cache dump and webfilter categories commands.

Using the output, how can an administrator determine the category of the training.fortinet.comam website?

A. The administrator must convert the first three digits of the IP hex value to binary

B. The administrator can look up the hex value of 34 in the second command output.

C. The administrator must add both the Pima in and Iphex values of 34 to get the category number

D. The administrator must convert the first two digits of the Domain hex value to a decimal value

Correct Answer: B

Option B is correct because the administrator can determine the category of the training.fortinet.com website by looking

up the hex value of 34 in the second command output. This is because the first command output shows that the domain and the IP of the website are both in category (Hex) 34, which corresponds to Information Technology in the second command output1. Option A is incorrect because the administrator does not need to convert the first three digits of the IP hex value to binary. The IP hex value is already in the same format as the category hex value, so the administrator can simply compare them without any conversion2. Option C is incorrect because the administrator does not need to add both the Pima in and Iphex values of 34 to get the category number. The Pima in and Iphex values are not related to the category number, but to the cache TTL and the database version respectively3. Option D is incorrect because the administrator does not need to convert the first two digits of the Domain hex value to a decimal value. The Domain hex value is already in the same format as the category hex value, so the administrator can simply compare them without any conversion2. References: =

1: Technical Tip: Verify the webfilter cache content4

2: Hexadecimal to Decimal Converter5

3: FortiGate - Fortinet Community6 : Web filter | FortiGate / FortiOS 7.2.0 - Fortinet Documentation7

QUESTION 5

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.