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.leads4pass.com/nse7_efw-7-2.html

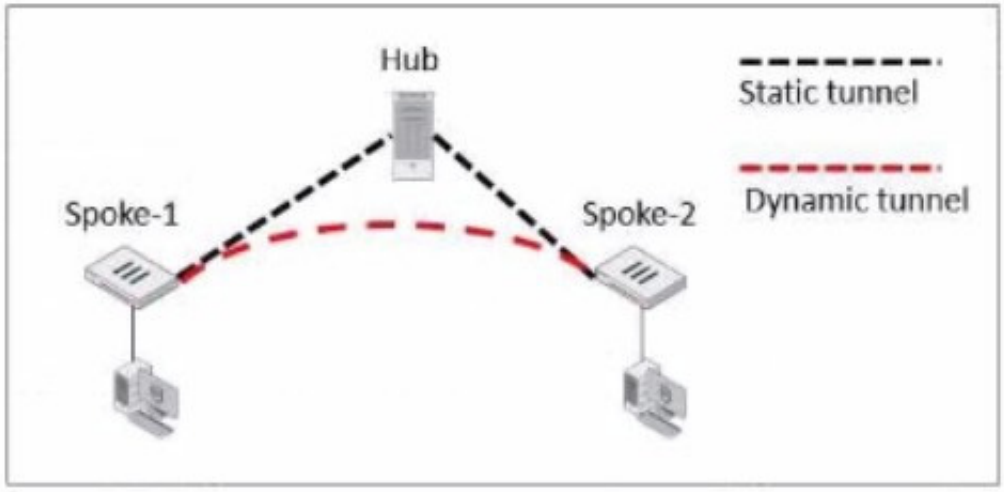
100% Passing Guarantee
100% Money Back Assurance

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

Exhibit.



Refer to the exhibit, which shows an ADVPN network.

The client behind Spoke-1 generates traffic to the device located behind Spoke-2.

Which first message floes the hub send to Spoke-110 bring up the dynamic tunnel?

A. Shortcut query

B. Shortcut reply

C. Shortcut offer

D. Shortcut forward

Correct Answer: A

In an ADVPN scenario, when traffic is initiated from a client behind one spoke to another spoke, the hub sends a shortcut query to the initiating spoke. This query is used to determine if there is a more direct path for the traffic, which can then trigger the establishment of a dynamic tunnel between the spokes.

QUESTION 2

Which ADVPN configuration must be configured using a script on fortiManager, when using VPN Manager to manage fortiGate VPN tunnels?

A. Enable AD-VPN in IPsec phase 1

B. Disable add-route on hub

C. Configure IP addresses on IPsec virtual interlaces

D. Set protected network to all

Correct Answer: A

To enable AD-VPN, you need to edit an SD-WAN overlay template and enable the Auto-Discovery VPN toggle. This will automatically add the required settings to the IPsec template and the BGP template. You cannot enable AD-VPN directly in the IPsec phase 1 settings using VPN Manager. References := ADVPN | FortiManager 7.2.0 - Fortinet Documentation

QUESTION 3

Exhibit.

```
config system central-management
    set type fortimanager
    set fmg "10.0.1.242"
    config server-list
        edit 1
            set server-type rating
            set addr-type ipv4
            set server-address 10.0.1.240
        next
        edit 2
            set server-type update
            set addr-type ipv4
            set server-address 10.0.1.243
        next
        edit 3
            set server-type rating
            set addr-type ipv4
            set server-address 10.0.1.244
        next
    end
    set include-default-servers enable
end
```

Refer to exhibit, which shows a central management configuration

Which server will FortiGate choose for web filler rating requests if 10.0.1.240 is experiencing an outage?

A. Public FortiGuard servers

B. 10.0.1.242

C. 10.0.1.244

D. 10.0.1.243

Correct Answer: C

In the event of an outage at 10.0.1.240, the FortiGate will choose the next server in the sequence for web filter rating requests, which is 10.0.1.244 according to the configuration shown in the exhibit. This is because the server list is ordered by priority, and the server with the lowest priority number is chosen first. If that server is unavailable, the next server with the next lowest priority number is chosen, and so on. The public FortiGuard servers are only used if the

include-defaultservers option is enabled and all the custom servers are unavailable. References := Fortinet Enterprise Firewall Study Guide for FortiOS 7.2, page 132.

QUESTION 4

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".

QUESTION 5

Which two statements about IKE version 2 fragmentation are true? (Choose two.)

A. Only some IKE version 2 packets are considered fragmentable.

B. The reassembly timeout default value is 30 seconds.

C. It is performed at the IP layer.

D. The maximum number of IKE version 2 fragments is 128.

Correct Answer: AD

In IKE version 2, not all packets are fragmentable. Only certain messages within the IKE negotiation process can be fragmented. Additionally, there is a limit to the number of fragments that IKE version 2 can handle, which is 128. This is specified in the Fortinet documentation and ensures that the IKE negotiation process can proceed even in networks that have issues with large packets. The reassembly timeout and the layer at which fragmentation occurs are not specified in this context within Fortinet documentation.