Free Questions for NSE7_EFW-7.2 by actualtestdumps

Shared by Whitney on 24-05-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Refer to the exhibit, which contains information about an IPsec VPN tunnel.

```
FortiGate # diag vpn tunnel list
list all ipsec tunnel in vd 0
------------------------------------------------------
name=tunnel_0 ver=2 serial=1 100.64.3.1:0->100.64.1.1:0 tun_id=100.64.1.1 tun_id6=::100.64.1.1
bound_if=3 lgwy=static/1 tun=intf mode=auto/1 encap=none/552 options[0228]=npu frag-rfc  run_s

proxyid_num=1 child_num=0 refcnt=3 ilast=42949917 olast=42949917 ad=/0
stat: rxp=0 txp=0 rxb=0 txb=0
dpd: mode=off on=0 idle=20000ms retry=3 count=0 seqno=0
natt: mode=none draft=0 interval=0 remote_port=0
fec: egress=0 ingress=0
proxyid=tunnel_0_0 proto=0 sa=1 ref=2 serial=1
  src: 0:0.0.0.0-255.255.255.255:0
  dst: 0:0.0.0.0-255.255.255.255:0
  SA:  ref=3 options=30202 type=00 soft=0 mtu=1280 expire=1454/0B replaywin=2048
       seqno=1 esn=0 replaywin_lastseq=00000000 qat=192 rekey=0 hash_search_len=1
  life: type=01 bytes=0/0 timeout=1768/1800
  dec: spi=877d6590 esp=aes key=16 be308ec1fb054642057644 24bc40a76d
       ah=sha256 key=32 cc8894be3390983521a48b2e7a5c998e6b28a10a3ddd8e7bc7ecbe672dfe7cc5
  enc: spi=63d0f38a esp=aes key=16 d8d3343af2fed4ddd958a022cd656b06
       ah=sha256 key=32 264402ba8ad04a7e97732b52ec27c92ff86e0a97bb33e22887677336f1670c7d
  dec:pkts/bytes=0/0, enc:pkts/bytes=0/0
  npu_flag=00 npu_rgwy=100.64.1.1 npu_lgwy=100.64.3.1 npu_selid=0 dec_npuid=0 enc_npuid=0
run_tally=0
```

What two conclusions can you draw from the command output? (Choose two.)

Options:

A- Dead peer detection is set to enable.

B- The IKE version is 2.

C- Both IPsec SAs are loaded on the kernel.

D- Forward error correction in phase 2 is set to enable.

Answer:

B, C

Explanation:

From the command output shown in the exhibit:

B) The IKE version is 2: This can be deduced from the presence of 'ver=2' in the output, which indicates that IKEv2 is being used.

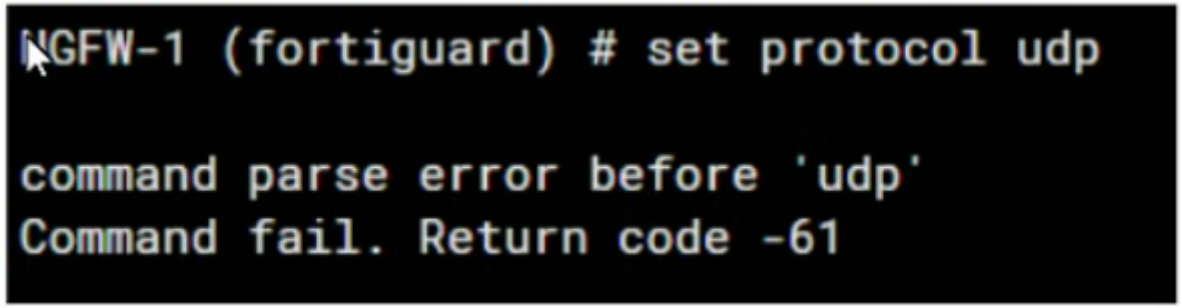
C) Both IPsec SAs are loaded on the kernel: This is indicated by the line 'npu flags=0x0/0', suggesting that no offload to NPU is occurring, and hence, both Security Associations are loaded onto the kernel for processing.

Fortinet documentation specifies that the version of IKE (Internet Key Exchange) used and the loading of IPsec Security Associations can be verified through the diagnostic commands related to VPN tunnels.

Question 2

Question Type: MultipleChoice

Refer to the exhibit, which shows an error in system fortiguard configuration.



What is the reason you cannot set the protocol to udp in config system fortiguard?

Options:

A- FortiManager provides FortiGuard.

B- fortiguard-anycast is set to enable.

C- You do not have the corresponding write access.

D- udp is not a protocol option.

Answer:

D

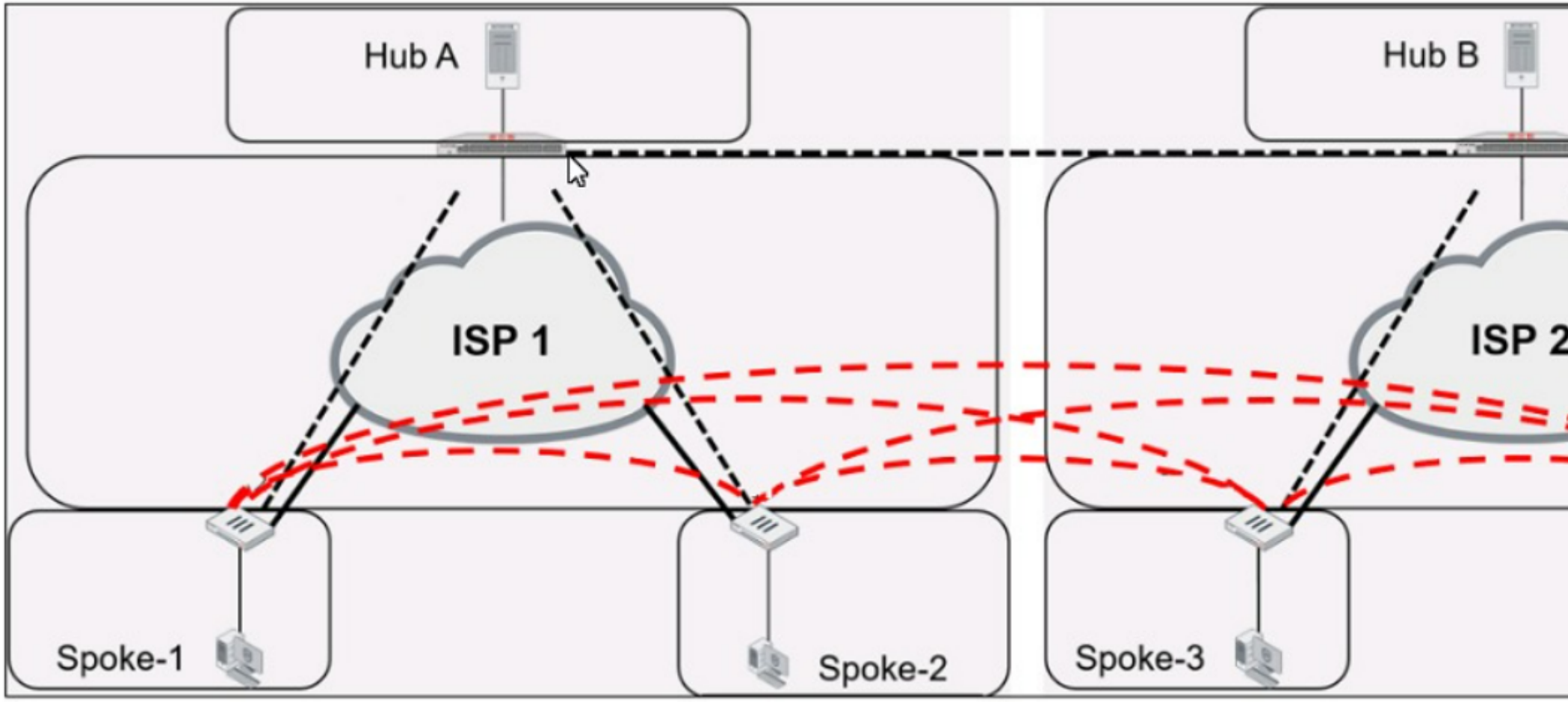
Explanation:

The reason for the command failure when trying to set the protocol to UDP in the config system fortiguard is likely that UDP is not a protocol option in this context. The command syntax might be incorrect or the option to set a protocol for FortiGuard updates might not exist in this manner. So the correct answer is D. udp is not a protocol option.

Question 3

Question Type: **MultipleChoice**

Refer to the exhibit, which shows an ADVPN network.



Which VPN phase 1 parameters must you configure on the hub for the ADVPN feature to function? (Choose two.)

Options:

A- set auto-discovery-forwarder enable

B- set add-route enable

C- set auto-discovery-receiver enable

D- set auto-discovery-sender enable

Answer:

A, C

Explanation:

For the ADVPN feature to function properly on the hub, the following phase 1 parameters must be configured:

A) set auto-discovery-forwarder enable: This enables the hub to forward shortcut information to the spokes, which is essential for them to establish direct tunnels.

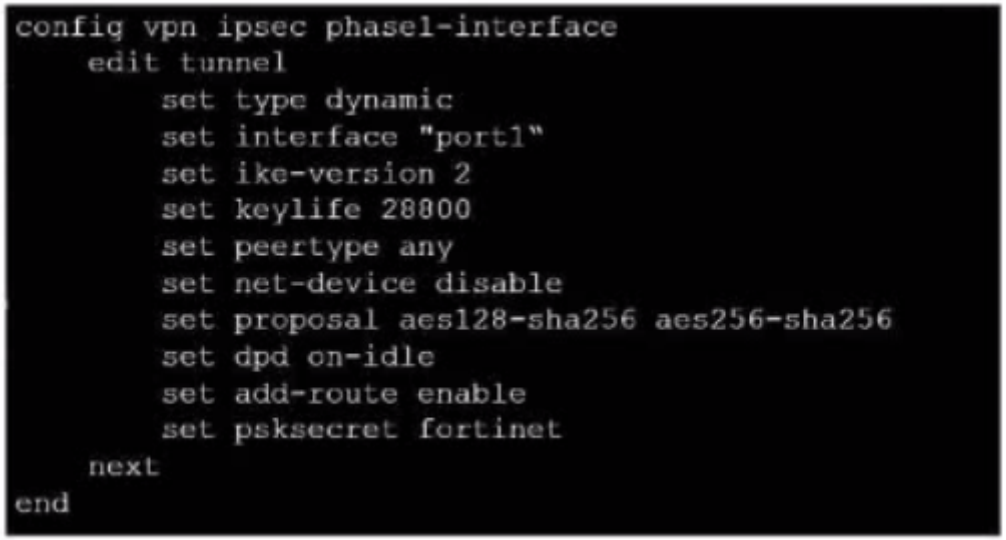
C) set auto-discovery-receiver enable: This allows the hub to receive shortcut offers from the spokes.

This information is corroborated by the Fortinet documentation, which explains that in an ADVPN setup, the hub must be able to both forward and receive shortcut information for dynamic tunnel creation between spokes.

Question 4

Question Type: MultipleChoice

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?

Options:

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.

Answer:

C

Explanation:

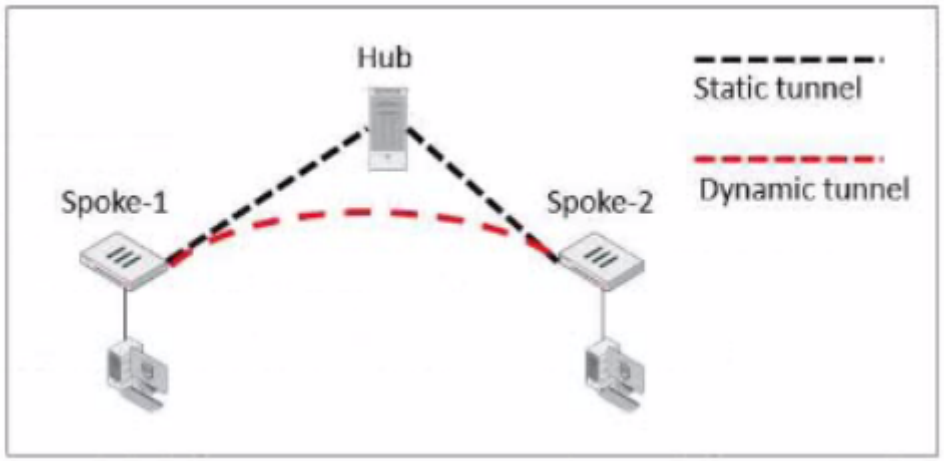
The configuration line "set dpd on-idle" indicates that dead peer detection (DPD) is set to trigger only when the tunnel is idle, not actively disabled1.Reference:FortiGate IPSec VPN User Guide - Fortinet Document Library

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 5

Question Type: MultipleChoice

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?

Options:

A- Shortcut query

B- Shortcut reply

C- Shortcut offer

D- Shortcut forward

Answer:

A

Explanation:

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 6

Question Type: **MultipleChoice**

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;)
```

Options:

A- Option A

B- Option B

C- Option C

D- Option D

Answer:

D

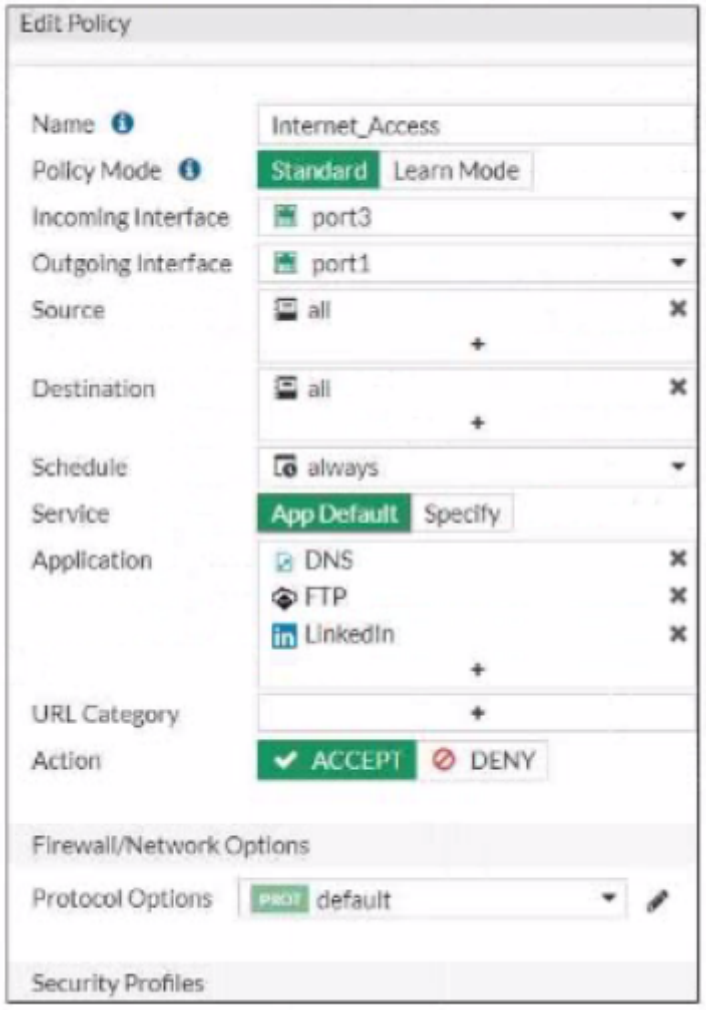
Explanation:

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").Reference:=Configuring custom signatures | FortiGate / FortiOS 7.4.0 - Fortinet Document Library, section "Signature to block access to example.com".

Question 7

Question Type: MultipleChoice

Exhibit.



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

Which setting must you configure to allow SSH?

Options:

A- Specify SSH in the Service field

B- Configure pot 22 in the Protocol Options field.

C- Include SSH in the Application field

D- Select an application control profile corresponding to SSH in the Security Profiles section

Answer:

A

Explanation:

Option A is correct because to allow SSH, you need to specify SSH in the Service field of the policy configuration.This is because the Service field determines which types of traffic are allowed by the policy1. By default, the Service field is set to App Default, which means that the policy will use the default ports defined by the applications.However, SSH is not one of the default applications, so you need to specify it manually or create a custom service for it2.

Option B is incorrect because configuring port 22 in the Protocol Options field is not enough to allow SSH.The Protocol Options field allows you to customize the protocol inspection and anomaly protection settings for the policy3. However, this field does not override the Service field, which still needs to match the traffic type.

Option C is incorrect because including SSH in the Application field is not enough to allow SSH.The Application field allows you to filter the traffic based on the application signatures and categories4. However, this field does not override the Service field, which still needs to match the traffic type.

Option D is incorrect because selecting an application control profile corresponding to SSH in the Security Profiles section is not enough to allow SSH. The Security Profiles section allows you to apply various security features to the traffic, such as antivirus, web filtering, IPS, etc. However, this section does not override the Service field, which still needs to match the traffic type.Reference: =

1: Firewall policies

2: Services

3: Protocol options profiles

4: Application control

Question 8

Question Type: **MultipleChoice**

You want to configure faster failure detection for BGP

Which parameter should you enable on both connected FortiGate devices?

Options:

A- Ebgp-enforce-multihop

B- bfd

C- Distribute-list-in

D- Graceful-restart

Answer:

B

Explanation:

BFD (Bidirectional Forwarding Detection) is a protocol that provides fast failure detection for BGP by sending periodic messages to verify the connectivity between two peers1.BFD can be enabled on both connected FortiGate devices by using the commandset bfd enableunder the BGP configuration2.Reference: =Technical Tip : FortiGate BFD implementation and examples ...,Configure BGP | FortiGate / FortiOS 7.0.2 - Fortinet Documentation