NSE7_EFW-7.2 Dumps

Fortinet NSE 7 - Enterprise Firewall 7.2

https://www.certleader.com/NSE7_EFW-7.2-dumps.html

NEW QUESTION 1
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 be308ec1fb05464205764424bc40a76d
         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.)

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: BC

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.

NEW QUESTION 2
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

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

NEW QUESTION 3
Exhibit.

```
NGFW-1 # get router info ospf interface
port3 is up, line protocol is up
   Internet Address 10.1.0.254/24, Area 0.0.0.0, MTU 1500
   Process ID 0, VRF 0, Router ID 0.0.0.1, Network Type BROADCAST, Cost: 1
   Transmit Delay is 1 sec, State DROther, Priority 1
   Designated Router (ID) 0.0.0.3, Interface Address 10.1.0.1
   Backup Designated Router (ID) 0.0.0.2, Interface Address 10.1.0.100
   Timer intervals configured, Hello 10.000, Dead 40, Wait 40, Retransmit 5
      Hello due in 00:00:08
   Neighbor Count is 2, Adjacent neighbor count is 2
   Crypt Sequence Number is 21
   Hello received 412 sent 207, DD received 8 sent 8
   LS-Req received 2 sent 3, LS-Upd received 13 sent 6
   LS-Ack received 9 sent 7, Discarded 6
```

Refer to the exhibit, which shows information about an OSPF interlace
What two conclusions can you draw from this command output? (Choose two.)

A. The port3 network has more man one OSPF router
B. The OSPF routers are in the area ID of 0.0.0.1.
C. The interfaces of the OSPF routers match the MTU value that is configured as 1500.
D. NGFW-1 is the designated router

Answer: AC

Explanation:
From the OSPF interface command output, we can conclude that the port3 network has more than one OSPF router because the Neighbor Count is 2, indicating the presence of another OSPF router besides NGFW-1. Additionally, we can deduce that the interfaces of the OSPF routers match the MTU value configured as 1500, which is necessary for OSPF neighbors to form adjacencies. The MTU mismatch would prevent OSPF from forming a neighbor relationship.
References:
? Fortinet FortiOS Handbook: OSPF Configuration

NEW QUESTION 4
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

Answer: A

Explanation:
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

NEW QUESTION 5
Which two statements about IKE vision 2 are true? (Choose two.)

A. Phase 1 includes main mode
B. It supports the extensible authentication protocol (EAP)
C. It supports the XAuth protocol.
D. It exchanges a minimum of four messages to establish a secure tunnel

Answer: BD

Explanation:
IKE version 2 supports the extensible authentication protocol (EAP), which allows for more flexible and secure authentication methods1. IKE version 2 also exchanges a minimum of four messages to establish a secure tunnel, which is more efficient than IKE version 12. References: = IKE settings | FortiClient 7.2.2 - Fortinet
Documentation, Technical Tip: How to configure IKE version 1 or 2 … - Fortinet Community

NEW QUESTION 6
Which configuration can be used to reduce the number of BGP sessions in on IBGP network?

A. Route-reflector-peer enable
B. Route-reflector-client enable
C. Route-reflector enable
D. Route-reflector-server enable

Answer: B

Explanation:
To reduce the number of BGP sessions in an IBGP network, you can use a route reflector, which acts as a focal point for IBGP sessions and readvertises the prefixes to all other peers. To configure a route reflector, you need to enable the route-reflector- client option on the neighbor-group settings of the hub device. This will make the hub device act as a route reflector server and the other devices as route reflector clients. References := Route exchange | FortiGate / FortiOS 7.2.0 -

Fortinet Documentation

NEW QUESTION 7
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

Answer: C

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

NEW QUESTION 8
Refer to the exhibit, which shows config system central-management information.

```
config system central-management
    set type fortimanager
    set allow-push-firmware disable
    set allow-remote-firmware-upgrade disable
    set fmg "10.1.0.241"
    config server-list
        edit 1
            set server-type update
            set server-address 10.1.0.241
        next
    end
    set include-default-servers disable
end
```

Which setting must you configure for the web filtering feature to function?

A. Add serve
B. fortiguar
C. net to the server list.
D. Configure securewf.fortiguar
E. net on the default servers.
F. Set update-server-location to automatic.
G. Configure server-type with the rating option.

Answer: D

Explanation:
 For the web filtering feature to function effectively, the FortiGate device
needs to have a server configured for rating services. The rating option in the server-type setting specifies that the server is used for URL rating lookup, which is essential for web filtering. The displayed configuration does not list any FortiGuard web filtering servers, which would be necessary for web filtering. The setting set include-default-servers disable indicates that the default FortiGuard servers are not being used, and hence, a specific server for web filtering (like securewf.fortiguard.net) needs to be configured.

NEW QUESTION 9
Exhibit.
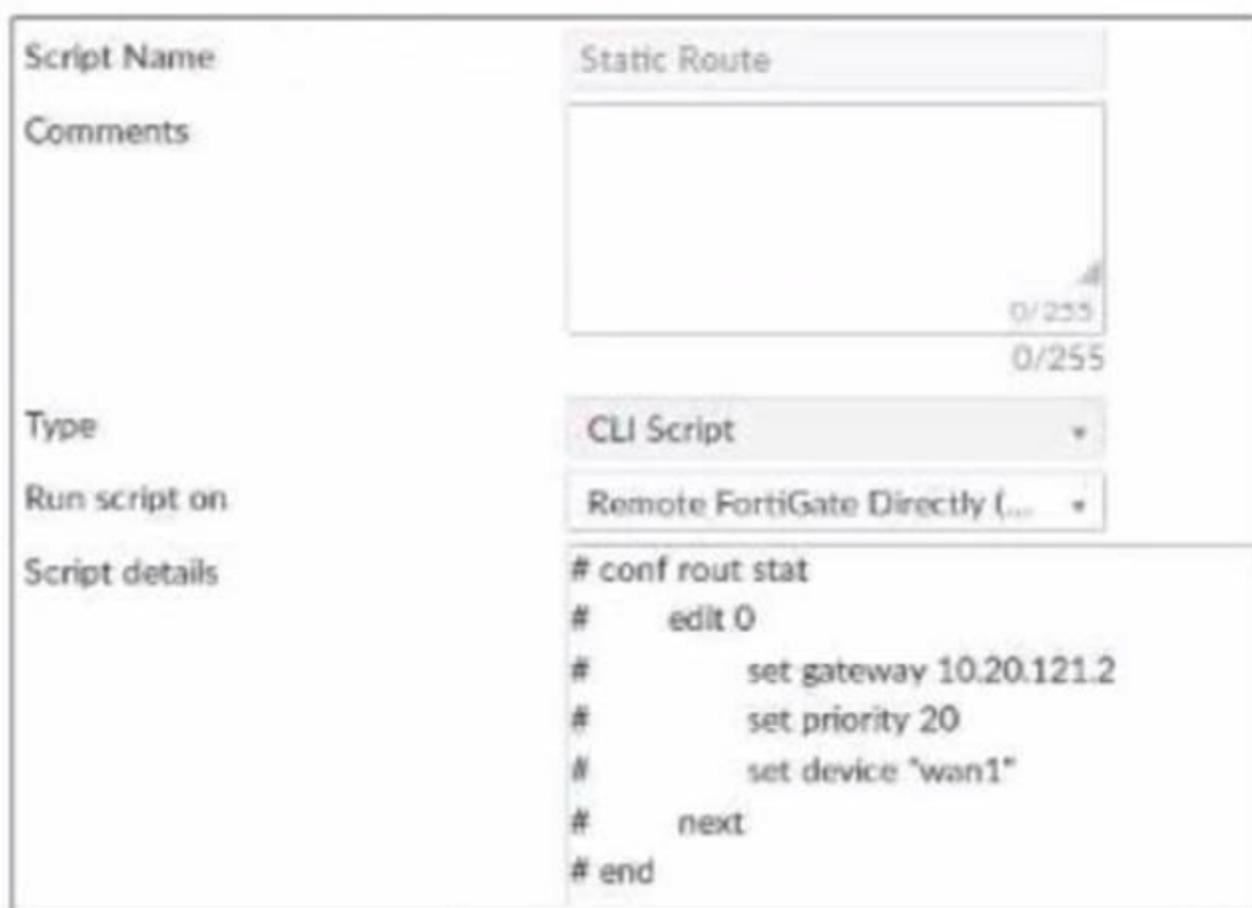
Refer to the exhibit, which contains a CLI script configuration on fortiManager. An administrator configured the CLI script on FortiManager rut the script tailed to apply any changes to the managed
device after being executed.
What are two reasons why the script did not make any changes to the managed device? (Choose two)

A. The commands that start with the # sign did not run.
B. Incomplete commands can cause CLI scripts to fail.
C. Static routes can be added using only TCI scripts.
D. CLI scripts must start with #!.

Answer: AB

Explanation:
 The commands that start with the # sign did not run because they are treated as comments in the CLI script. Incomplete commands can cause CLI scripts to fail because they are not recognized by the FortiGate device. The other options are incorrect because static routes can be added using CLI or GUI, and CLI scripts do not need to start with #!. References := Configuring custom scripts | FortiManager 7.2.0 - Fortinet Documentation, section "CLI script syntax".

NEW QUESTION 10
You contoured an address object on the tool fortiGate in a Security Fabric. This object is not synchronized with a downstream device. Which two reasons could be the cause? (Choose two)

A. The address object on the tool FortiGate has fabric-object set to disable
B. The root FortiGate has configuration-sync set to enable
C. The downstream TortiGate has fabric-object-unification set to local
D. The downstream FortiGate has configuration-sync set to local

Answer: AC

Explanation:
? Option A is correct because the address object on the tool FortiGate will not be synchronized with the downstream devices if it has fabric-object set to disable.
This option controls whether the address object is shared with other FortiGate devices in the Security Fabric or not1.

? Option C is correct because the downstream FortiGate will not receive the address object from the tool FortiGate if it has fabric-object-unification set to local. This option controls whether the downstream FortiGate uses the address objects from the root FortiGate or its own local address objects2.
? Option B is incorrect because the root FortiGate has configuration-sync set to enable by default, which means that it will synchronize the address objects with the downstream devices unless they are disabled by the fabric-object option3.
? Option D is incorrect because the downstream FortiGate has configuration-sync set to local by default, which means that it will receive the address objects from the root FortiGate unless they are overridden by the fabric-object-unification
option4. References: =
? 1: Group address objects synchronized from FortiManager5
? 2: Security Fabric address object unification6
? 3: Configuration synchronization7
? 4: Configuration synchronization7
? : Security Fabric - Fortinet Documentation

NEW QUESTION 10
......

Thank You for Trying Our Product

* 100% Pass or Money Back

    All our products come with a 90-day Money Back Guarantee.

* One year free update

    You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

    We currently serve more than 30,000,000 customers.

* Shop Securely

    All transactions are protected by VeriSign!

100% Pass Your NSE7_EFW-7.2 Exam with Our Prep Materials Via below:

https://www.certleader.com/NSE7_EFW-7.2-dumps.html