

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

You created a VPN community using VPN Manager on FortiManager. You also added gateways to the VPN community. Now you are trying to create firewall policies to permit traffic over the tunnel however, the VPN interfaces do not appear as available options.

- A. Create interface mappings for the IPsec VPN interfaces before you use them in a policy.
- B. Refresh the device status using the Device Manager so that FortiGate populates the IPSec interfaces
- C. Configure the phase 1 settings in the VPN community that you didnt initially configure. FortiGate automatically generates the interfaces after you configure the required settings
- D. install the VPN community and gateway configuration on the fortiGate devices so that the VPN interfaces appear on the Policy Objects on fortiManager.

Correct Answer: D

To use the VPN interfaces in a policy, you need to install the VPN community and gateway configuration on the FortiGate devices first. This will create the VPN interfaces on the FortiGate and sync them with FortiManager.

References: Creating IPsec VPN communities VPN | FortiGate / FortiOS 7.2.0

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

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 3

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 server. fortiguard. net to the server list.
- B. Configure securewf.fortiguard. net on the default servers.
- C. Set update-server-location to automatic.
- D. Configure server-type with the rating option.

Correct Answer: D

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.

QUESTION 4

Exhibit.

```
config vpn ipsec phase1-interface
edit "tunnel"
    set interface "port1"
    set ike-version 2
    set keylife 28800
    set peertype any
    set net-device enable
    set proposal aes128gcm-prfsha256 aes256gcm-prfsha384
    set auto-discovery-receiver enable
    set remote-gw 100.64.1.1
    set psksecret fortinet
next
```

Refer to the exhibit, which contains the partial ADVPN configuration of a spoke.

Which two parameters must you configure on the corresponding single hub? (Choose two.)

- A. Set auto-discovery-sender enable
- B. Set ike-version 2
- C. Set auto-discovery-forwarder enable
- D. Set auto-discovery-receiver enable

Correct Answer: AC

For an ADVPN spoke configuration shown, the corresponding hub must have auto-discovery-sender enabled to send shortcut advertisement messages to the spokes. Also, the hub would need to have auto-discovery-forwarder enabled if it is to forward on those shortcut advertisements to other spokes. This allows the hub to inform all spokes about the best path to reach each other. The ike-version does not need to be reconfigured on the hub if it's already set to version 2 and auto-discovery-receiver is not necessary on the hub because it's the one sending the advertisements, not receiving. References: FortiOS Handbook - ADVPN

QUESTION 5

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

- A. auto-discovery receiver must be set to enable on the Spokes.
- B. Spoke to-spoke traffic never goes through the hub
- C. It supports NAI for on-demand tunnels
- D. Routing is configured by enabling add-advpn-route

Correct Answer: AC

ADVPN (Auto Discovery VPN) is a feature that allows to dynamically establish direct tunnels (called shortcuts) between the spokes of a traditional Hub and Spoke architecture. The auto-discovery receiver must be set to enable on the spokes to allow them to receive NHRP messages from the hub and other spokes. NHRP (Next Hop Resolution Protocol) is used for on-demand tunnels, which are established when there is traffic between spokes. Routing is

configured by enabling add-nhrp-route, not add-advpn- route. References := ADVPN | FortiGate / FortiOS 7.2.0 | Fortinet Document Library, Technical Tip: Fortinet Auto Discovery VPN (ADVPN)

[Latest NSE7_EFW-7.2 Dumps](#)

[NSE7_EFW-7.2 Study Guide](#)

[NSE7_EFW-7.2 Exam Questions](#)