



Fortinet

Exam Questions NSE7_EFW-7.2

Fortinet NSE 7 - Enterprise Firewall 7.2

About ExamBible

Your Partner of IT Exam

Found in 1998

ExamBible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, ExamBible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

NEW QUESTION 1

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 2

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.

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. 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.

NEW QUESTION 3

You want to configure faster failure detection for BGP

Which parameter should you enable on both connected FortiGate devices?

- 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 command set bfd enable under the BGP configuration2. References: = Technical Tip :

FortiGate BFD implementation and examples ..., Configure BGP | FortiGate / FortiOS 7.0.2
- Fortinet Documentation

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 interfaces
- 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 version 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

After enabling IPS you receive feedback about traffic being dropped. What could be the reason?

- A. Np-accel-mode is set to enable
- B. Traffic-submit is set to disable
- C. IPS is configured to monitor
- D. Fail-open is set to disable

Answer: D

Explanation:

Fail-open is a feature that allows traffic to pass through the IPS sensor without inspection when the sensor fails or is overloaded. If fail-open is set to disable, traffic will be dropped in such scenarios¹. References: = IPS | FortiGate / FortiOS 7.2.3 - Fortinet Documentation
When IPS (Intrusion Prevention System) is configured, if fail-open is set to disable, it means that if the IPS engine fails, traffic will not be allowed to pass through, which can result in traffic being dropped (D). This is in contrast to a fail-open setting, which would allow traffic to bypass the IPS engine if it is not operational.

NEW QUESTION 7

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

- A. You must disable add-route in the hub.
- B. All FortiGate devices must be in the same autonomous system (AS).
- C. The hub adds routes based on IKE negotiations.
- D. You must configure phase 2 quick mode selectors to 0.0.0.0 0.0.0.0.

Answer: CD

Explanation:

C. The hub adds routes based on IKE negotiations: This is part of the ADVPN functionality where the hub learns about the networks behind the spokes and can add routes dynamically based on the IKE negotiations with the spokes.
* D. You must configure phase 2 quick mode selectors to 0.0.0.0 0.0.0.0: This wildcard setting in the phase 2 selectors allows any-to-any tunnel establishment, which is necessary for the dynamic creation of spoke-to-spoke tunnels. These configurations are outlined in Fortinet's documentation for setting up ADVPN, where the hub's role in route control and the use of wildcard selectors for phase 2 are emphasized to enable dynamic tunneling between spokes.

NEW QUESTION 8

Which FortiGate in a Security Fabric sends logs to FortiAnalyzer?

- A. Only the root FortiGate.
- B. Each FortiGate in the Security Fabric.
- C. The FortiGate devices performing network address translation (NAT) or unified threat management (UTM), if configured.
- D. Only the last FortiGate that handled a session in the Security Fabric

Answer: B

Explanation:

- ? Option B is correct because each FortiGate in the Security Fabric can send logs to FortiAnalyzer for centralized logging and analysis¹². This allows you to monitor and manage the entire Security Fabric from a single console and view aggregated reports and dashboards.
- ? Option A is incorrect because the root FortiGate is not the only device that can send logs to FortiAnalyzer. The root FortiGate is the device that initiates the Security Fabric and acts as the central point of contact for other FortiGate devices³. However, it does not have to be the only log source for FortiAnalyzer.
- ? Option C is incorrect because the FortiGate devices performing NAT or UTM are not the only devices that can send logs to FortiAnalyzer. These devices can perform additional security functions on the traffic that passes through them, such as firewall, antivirus, web filtering, etc⁴. However, they are not the only devices that generate logs in the Security Fabric.
- ? Option D is incorrect because the last FortiGate that handled a session in the Security Fabric is not the only device that can send logs to FortiAnalyzer. The last FortiGate is the device that terminates the session and applies the final security policy⁵. However, it does not have to be the only device that reports the session information to FortiAnalyzer. References: =
- ? 1: Security Fabric - Fortinet Documentation¹
- ? 2: FortiAnalyzer Demo⁶
- ? 3: Security Fabric topology
- ? 4: Security Fabric UTM features
- ? 5: Security Fabric session handling

NEW QUESTION 9

In which two ways does FortiManager function when it is deployed as a local FDS? (Choose two)

- A. It can be configured as an update server a rating server or both
- B. It provides VM license validation services
- C. It supports rating requests from non-FortiGate devices.
- D. It caches available firmware updates for unmanaged devices

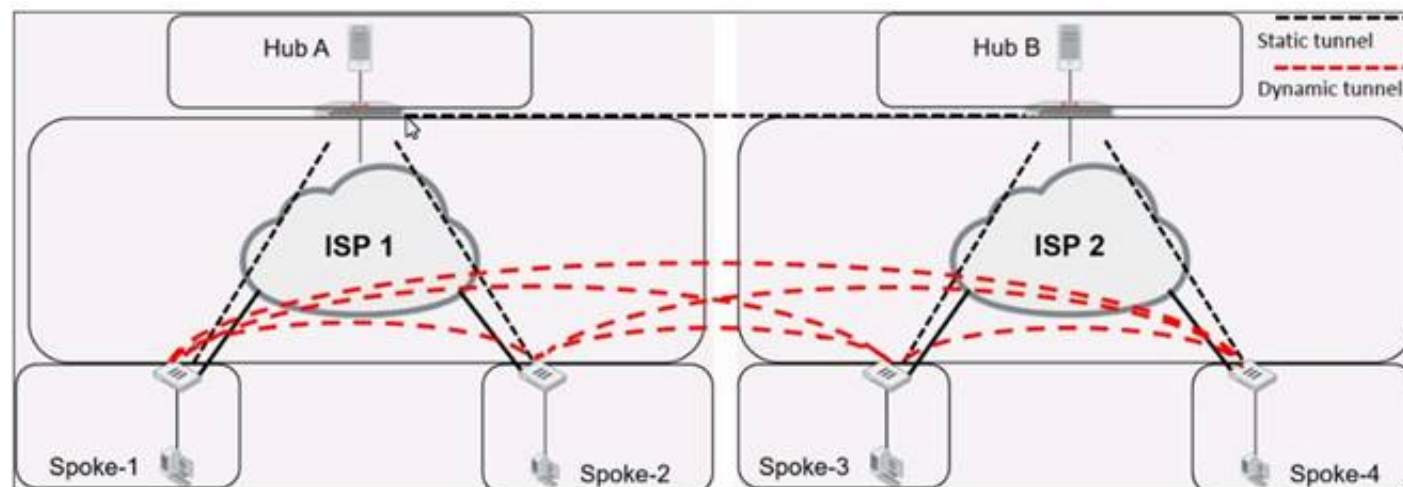
Answer: AB

Explanation:

When deployed as a local FortiGuard Distribution Server (FDS), FortiManager functions in several capacities. It can act as an update server, a rating server, or both, providing firmware updates and FortiGuard database updates. Additionally, it plays a crucial role in VM license validation services, ensuring that the connected FortiGate devices are operating with valid licenses. However, it does not support rating requests from non-FortiGate devices nor cache firmware updates for unmanaged devices. Fortinet FortiOS Handbook: FortiManager as a Local FDS Configuration

NEW QUESTION 10

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.)

- A. set auto-discovery-forwarder enable
- B. set add-route enable
- C. set auto-discovery-receiver enable
- D. set auto-discovery-sender enable

Answer: AC

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.

NEW QUESTION 10

You configured an address object on the root 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 root FortiGate has fabric-object set to disable
- B. The root FortiGate has configuration-sync set to enable
- C. The downstream FortiGate 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 root 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 14

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

Answer: AC

Explanation:

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

NEW QUESTION 17

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.com 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

Answer: B

Explanation:

- ? 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 lphex values of 34 to get the category number. The Pima in and lphex 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

NEW QUESTION 22

.....

Relate Links

100% Pass Your NSE7_EFW-7.2 Exam with Exam Bible Prep Materials

https://www.exambible.com/NSE7_EFW-7.2-exam/

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - <https://www.exambible.com/>