Free Questions for NSE7_EFW-7.2 by certsdeals

Shared by Avery on 01-01-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

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

Options:

A- auto-discovery receiver must be set to enable on the Spokes.

B- Spoke to-spoke traffic never goes through the hub

C- lt supports NAI for on-demand tunnels

D- Routing is configured by enabling add-advpn-route

Answer:

A, C

Explanation:

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.Reference:=ADVPN | FortiGate / FortiOS 7.2.0 | Fortinet Document Library,Technical Tip: Fortinet Auto Discovery VPN (ADVPN)

Question 2

Question Type: MultipleChoice

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

Options:

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

Answer:

B, C

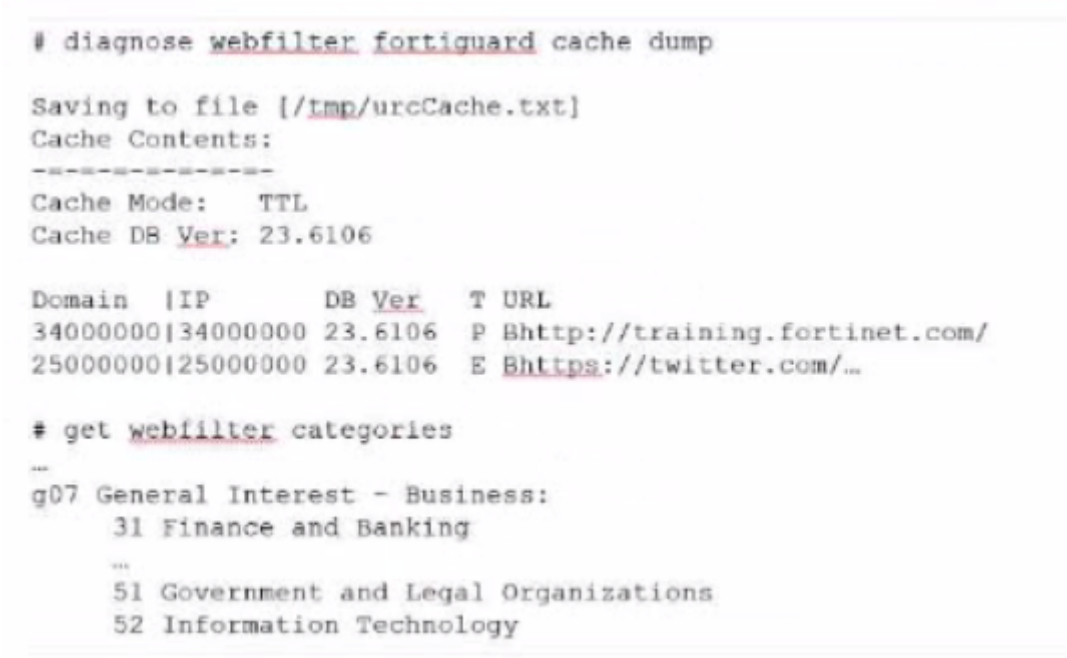
Explanation:

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.Reference:=BFD | FortiGate / FortiOS 7.2.0 - Fortinet Document Library, section "BFD".

Question 3

Question Type: MultipleChoice

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 am website?

Options:

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 Iphex values of 34 to get the category number.The Pima in and Iphex 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.Reference: =

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

Question 4

Question Type: **MultipleChoice**

Which two statements about the Security fabric are true? (Choose two.)

Options:

A- FortiGate uses the FortiTelemetry protocol to communicate with FortiAnatyzer.

B- Only the root FortiGate sends logs to FortiAnalyzer

C- Only FortiGate devices with configuration-sync receive and synchronize global CMDB objects that the toot FortiGate sends

D- Only the root FortiGate collects network topology information and forwards it to FortiAnalyzer

Answer:

A, D

Explanation:

FortiGate uses the FortiTelemetry protocol to communicate with FortiAnalyzer and other Security Fabric devices to exchange information such as device status, network topology, and security events1.Only the root FortiGate collects network topology information and forwards it to FortiAnalyzer, where it can be viewed and analyzed2.Reference: =Security Fabric - Fortinet Documentation,Fortinet Security Fabric for Securing Digital Innovations

Question 5

Question Type: MultipleChoice

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.

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.

Answer:

D

Explanation:

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.Reference:

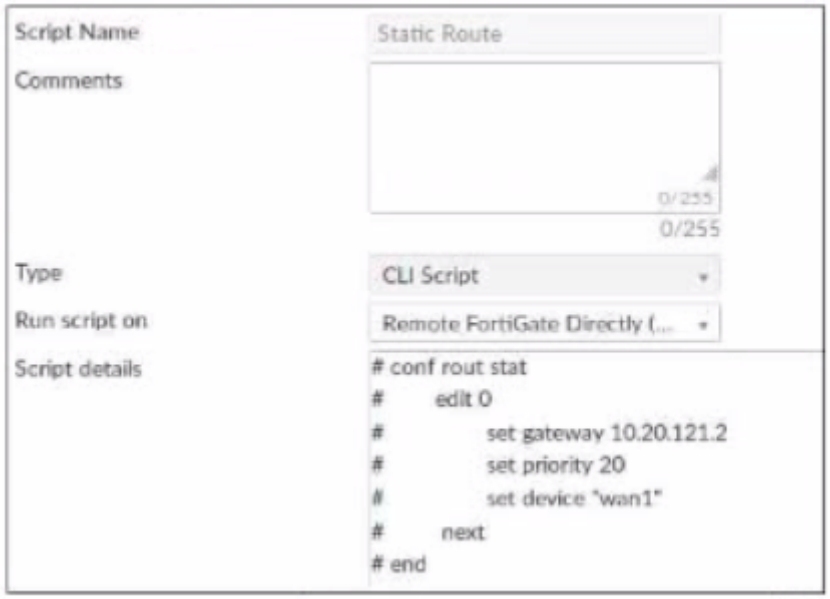
Creating IPsec VPN communities

VPN | FortiGate / FortiOS 7.2.0

Question 6

Question Type: **MultipleChoice**

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)

Options:

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:

A, B

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 #!.Reference:=Configuring custom scripts | FortiManager 7.2.0 - Fortinet Documentation, section "CLI script syntax".

Question 7

Question Type: MultipleChoice

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)

Options:

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:

A, C

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.Reference: =

1: Group address objects synchronized from FortiManager5

2: Security Fabric address object unification6

3: Configuration synchronization7

4: Configuration synchronization7

: Security Fabric - Fortinet Documentation