

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

Winch 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

Answer: AC

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

NEW QUESTION 2

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

- A. FortiGate uses the FortiTelemetry protocol to communicate with FortiAnalyzer.
- B. Only the root FortiGate sends logs to FortiAnalyzer
- C. Only FortiGate devices with configuration-sync receive and synchronize global CMDB objects that the root FortiGate sends
- D. Only the root FortiGate collects network topology information and forwards it to FortiAnalyzer

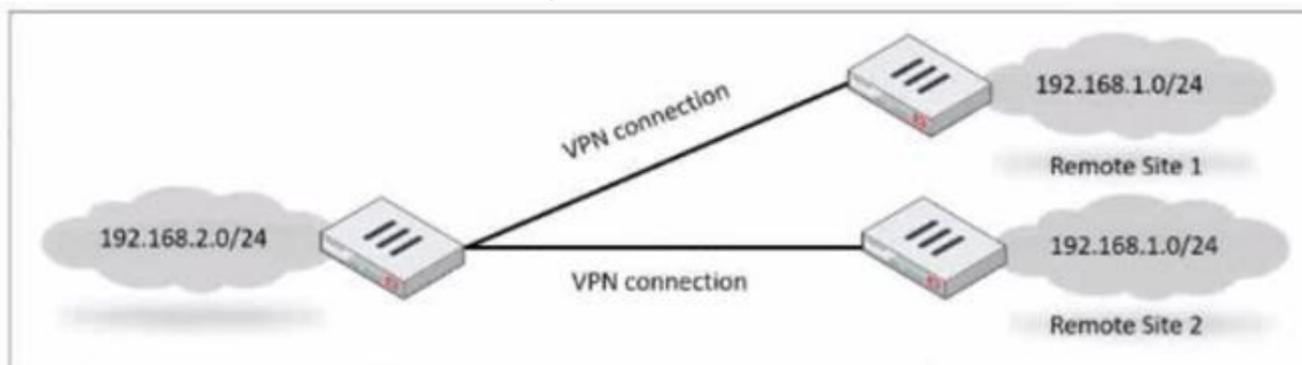
Answer: BC

Explanation:

In the Security Fabric, only the root FortiGate sends logs to FortiAnalyzer (B). Additionally, only FortiGate devices with configuration-sync enabled receive and synchronize global Central Management Database (CMDB) objects that the root FortiGate sends (C). FortiGate uses the FortiTelemetry protocol to communicate with other FortiGates, not FortiAnalyzer (A). The last option (D) is incorrect as all FortiGates can collect and forward network topology information to FortiAnalyzer. References: ? FortiOS Handbook - Security Fabric

NEW QUESTION 3

Refer to the exhibit, which shows a network diagram.



Which IPsec phase 2 configuration should you implement so that only one remote site is connected at any time?

- A. Set route-overlap to allow.
- B. Set single-source to enable
- C. Set route-overlap to either use—new or use-old
- D. Set net-device to enable

Answer: C

Explanation:

To ensure that only one remote site is connected at any given time in an IPsec VPN scenario, you should use route-overlap with the option to either use-new or use-old. This setting dictates which routes are preferred and how overlaps in routes are handled, allowing for one connection to take precedence over the other (C).

References:

? FortiOS Handbook - IPsec VPN

NEW QUESTION 4

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

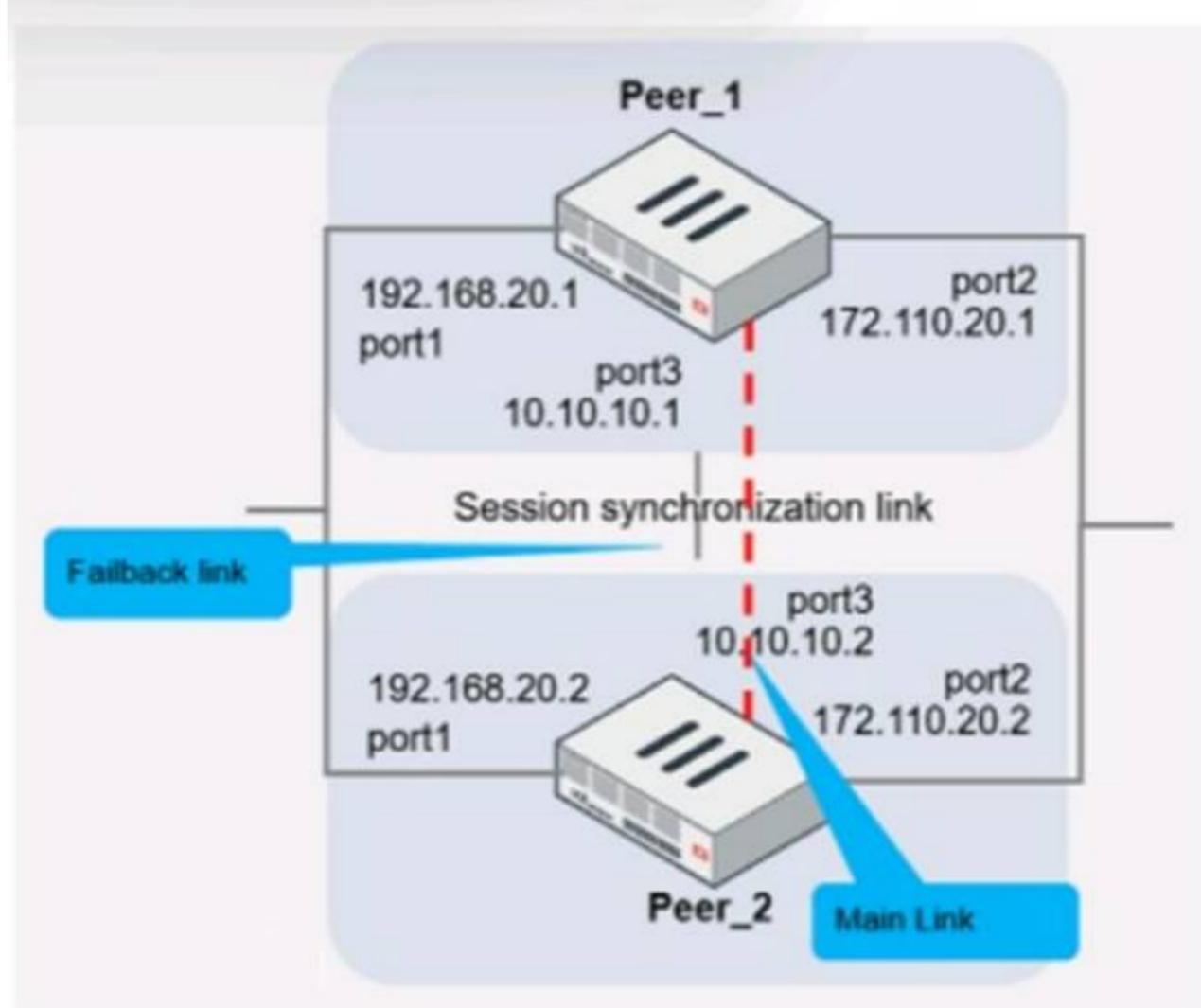
Explanation:

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 5

Refer to the exhibit, which shows two configured FortiGate devices and peering over FGSP.



The main link directly connects the two FortiGate devices and is configured using the set session-syn-dev <interface> command.

What is the primary reason to configure the main link?

- A. To have both sessions and configuration synchronization in layer 2
- B. To load balance both sessions and configuration synchronization between layer 2 and 3
- C. To have only configuration synchronization in layer 3
- D. To have both sessions and configuration synchronization in layer 3

Answer: D

Explanation:

The primary purpose of configuring a main link between the devices is to synchronize session information so that if one unit fails, the other can continue processing traffic without dropping active sessions.

* A.To have both sessions and configuration synchronization in layer 2.This is incorrect because FGSP is used for session synchronization, not configuration synchronization. B.To load balance both sessions and configuration synchronization between layer 2 and 3.FGSP does not perform load balancing and is not used for configuration synchronization.

* C.To have only configuration synchronization in layer 3.The main link is not used solely for configuration synchronization.

* D.To have both sessions and configuration synchronization in layer 3.The main link in an FGSP setup is indeed used to synchronize session information across the devices, and it operates at layer 3 since it uses IP addresses to establish the peering.

NEW QUESTION 6

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

- A. You must disable add-route in the hub.
- B. AllFortiGate 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 7

Exhibit.

Edit Policy

Name **Internet_Access**

Policy Mode **Standard** Learn Mode

Incoming Interface **port3**

Outgoing Interface **port1**

Source **all**

Destination **all**

Schedule **always**

Service **App Default** Specify

Application **DNS**, **FTP**, **LinkedIn**

URL Category

Action **ACCEPT** DENY

Firewall/Network Options

Protocol Options **default**

Security Profiles

Refer to the exhibit, which contains a partial policy configuration. Which setting must you configure to allow SSH?

- A. Specify SSH in the Service field
- B. Configure port 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. References: =

? 1: Firewall policies

? 2: Services

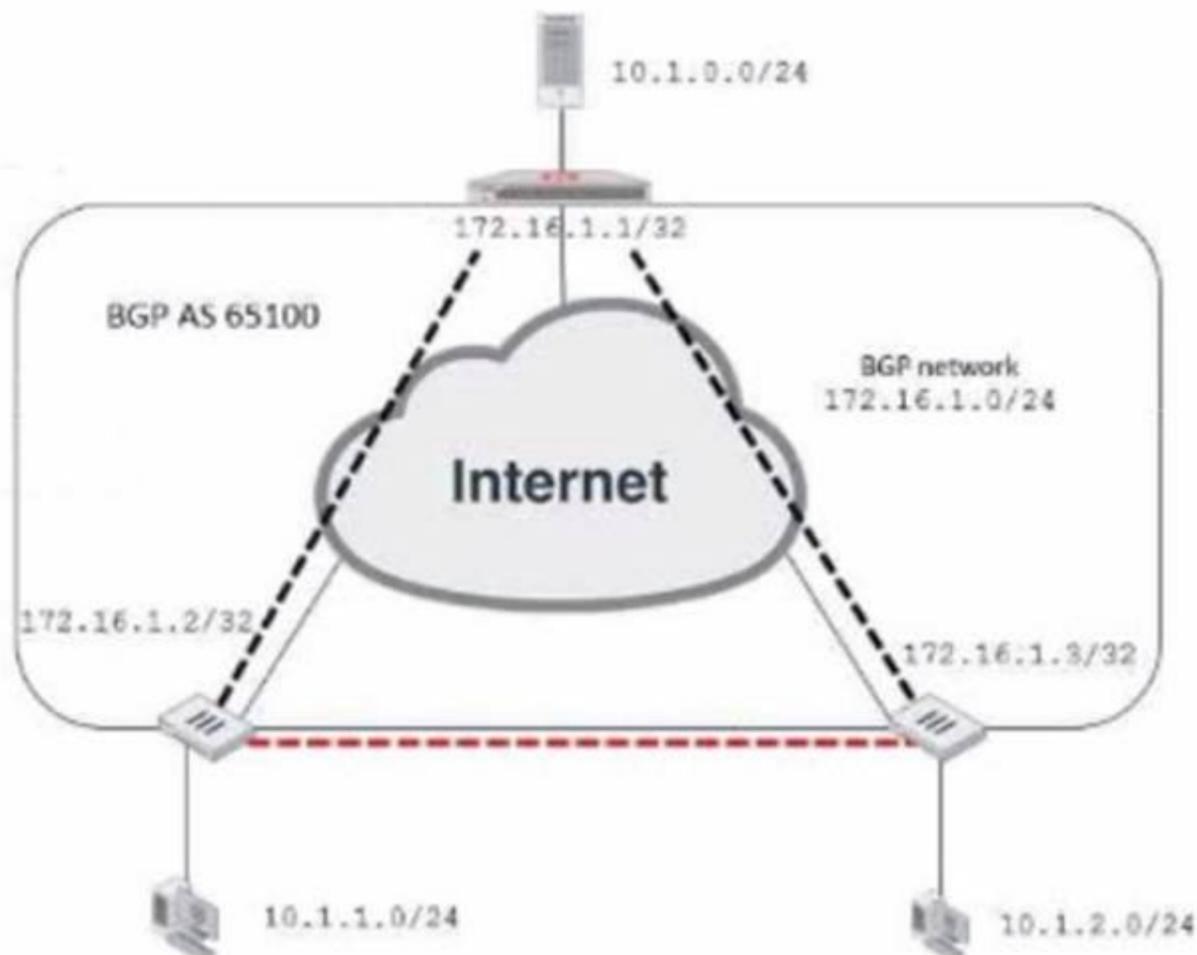
? 3: Protocol options profiles

? 4: Application control

NEW QUESTION 8

Exhibit.

Network diagram



Partial BGP configuration

```

Hub # show router bgp
config router bgp
  set as 65100
  set router-id 172.16.1.1
  config neighbor-group
    edit "advpn"
      set remote-as 65100
      ...
    next
  end
  ...
end

```

Refer to the exhibit, which contains an ADVPN network diagram and a partial BGP configuration. Which two parameters should you configure in config neighbor range? (Choose two.)

- A. set prefix 172.16.1.0 255.255.255.0
- B. set route reflector-client enable
- C. set neighbor-group advpn
- D. set prefix 10.1.0 255.255.255.0

Answer: AC

Explanation:

In the ADVPN configuration for BGP, you should specify the prefix that the neighbors can advertise. Option A is correct as you would configure the BGP network prefix that should be advertised to the neighbors, which matches the BGP network in the diagram. Option C is also correct since you should reference the neighbor group configured for the ADVPN setup within the BGP configuration.

NEW QUESTION 9

An administrator has configured two FortiGate devices for an HA cluster. While testing HA failover, the administrator notices that some of the switches in the network continue to send traffic to the former primary device. What can the administrator do to fix this problem?

- A. Verify that the speed and duplex settings match between the FortiGate interfaces and the connected switch ports
- B. Configure set link-failed-signal enable under-config system ha on both Cluster members
- C. Configure remote link monitoring to detect an issue in the forwarding path
- D. Configure set send-garp-on-failover enables under config system ha on both cluster members

Answer: B

Explanation:

Virtual MAC Address and Failover

- The new primary broadcasts Gratuitous ARP packets to notify the network that each virtual MAC is now reachable through a different switch port.
- Some high-end switches might not clear their MAC table correctly after a failover - Solution: Force former primary to shut down all its interfaces for one second when the failover happens (excluding heartbeat and reserved management interfaces):

```
#Config system ha
```

```
set link-failed-signal enable end
```

- This simulates a link failure that clears the related entries from MAC table of the switches.

NEW QUESTION 10

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 10

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 14

.....

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