

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 shows a custom signature.



Which two modifications must you apply to the configuration of this custom signature so that you can save it on FortiGate? (Choose two.)

- A. Add severity.
- B. Add attack_id.
- C. Ensure that the header syntax is F-SBID.
- D. Start options with --.

Answer: AB

Explanation:

For a custom signature to be valid and savable on a FortiGate device, it must include certain mandatory fields. Severity is used to specify the level of threat that the signature represents, and attack_id is a unique identifier for the signature. Without these, the signature would not be complete and could not be correctly utilized by the FortiGate's Intrusion Prevention System (IPS).

NEW QUESTION 2

Which two statements about the neighbor-group command are true? (Choose two.)

- A. You can configure it on the GUI.
- B. It applies common settings in an OSPF area.
- C. It is combined with the neighbor-range parameter.
- D. You can apply it in Internal BGP (IBGP) and External BGP (EBGP).

Answer: BD

Explanation:

The neighbor-group command in FortiOS allows for the application of common settings to a group of neighbors in OSPF, and can also be used to simplify configuration by applying common settings to both IBGP and EBGP neighbors. This grouping functionality is a part of the FortiOS CLI and is documented in the Fortinet CLI reference.

NEW QUESTION 3

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

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 4

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 5

Exhibit.

```

FortiGate-A (port4) # show
config system interface
  edit "port4"
    set vdom "root"
    set ip 10.1.5.1 255.255.255.0
    set allowaccess ping https
    set type physical
    set vrrp-virtual-mac enable
    config vrrp
      edit 1
        set vrgrp 1
        set vrip 10.1.5.254
        set priority 255
        set preempt enable
        set vrdst 8.8.8.8
        set vrdst-priority 30
      next
    end
  set snmp-index 4
next
end

FortiGate-B (port4) # show
config system interface
  edit "port4"
    set vdom "root"
    set ip 10.1.5.2 255.255.255.0
    set allowaccess ping https
    set type physical
    set vrrp-virtual-mac enable
    config vrrp
      edit 1
        set vrgrp 1
        set vrip 10.1.5.254
        set priority 50
        set preempt enable
        set vrdst 8.8.8.8
        set vrdst-priority 40
      next
    end
  set snmp-index 4
next
end
  
```

Refer to the exhibit, which contains the partial interface configuration of two FortiGate devices.

Which two conclusions can you draw from this configuration? (Choose two)

- A. 10.1.5.254 is the default gateway of the internal network
- B. On failover new primary device uses the same MAC address as the old primary
- C. The VRRP domain uses the physical MAC address of the primary FortiGate
- D. By default FortiGate B is the primary virtual router

Answer: AB

Explanation:

The Virtual Router Redundancy Protocol (VRRP) configuration in the exhibit indicates that 10.1.5.254 is set as the virtual IP (VRIP), commonly serving as the default gateway for the internal network (A). With vrrp-virtual-mac enabled, both FortiGates would use the same virtual MAC address, ensuring a seamless transition during failover (B). The VRRP domain does not use the physical MAC address (C), and the priority settings indicate that FortiGate-A would be the primary router by default due to its higher priority (D).

NEW QUESTION 6

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 interface. What two conclusions can you draw from this command output? (Choose two.)

- A. The port3 network has more than 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:

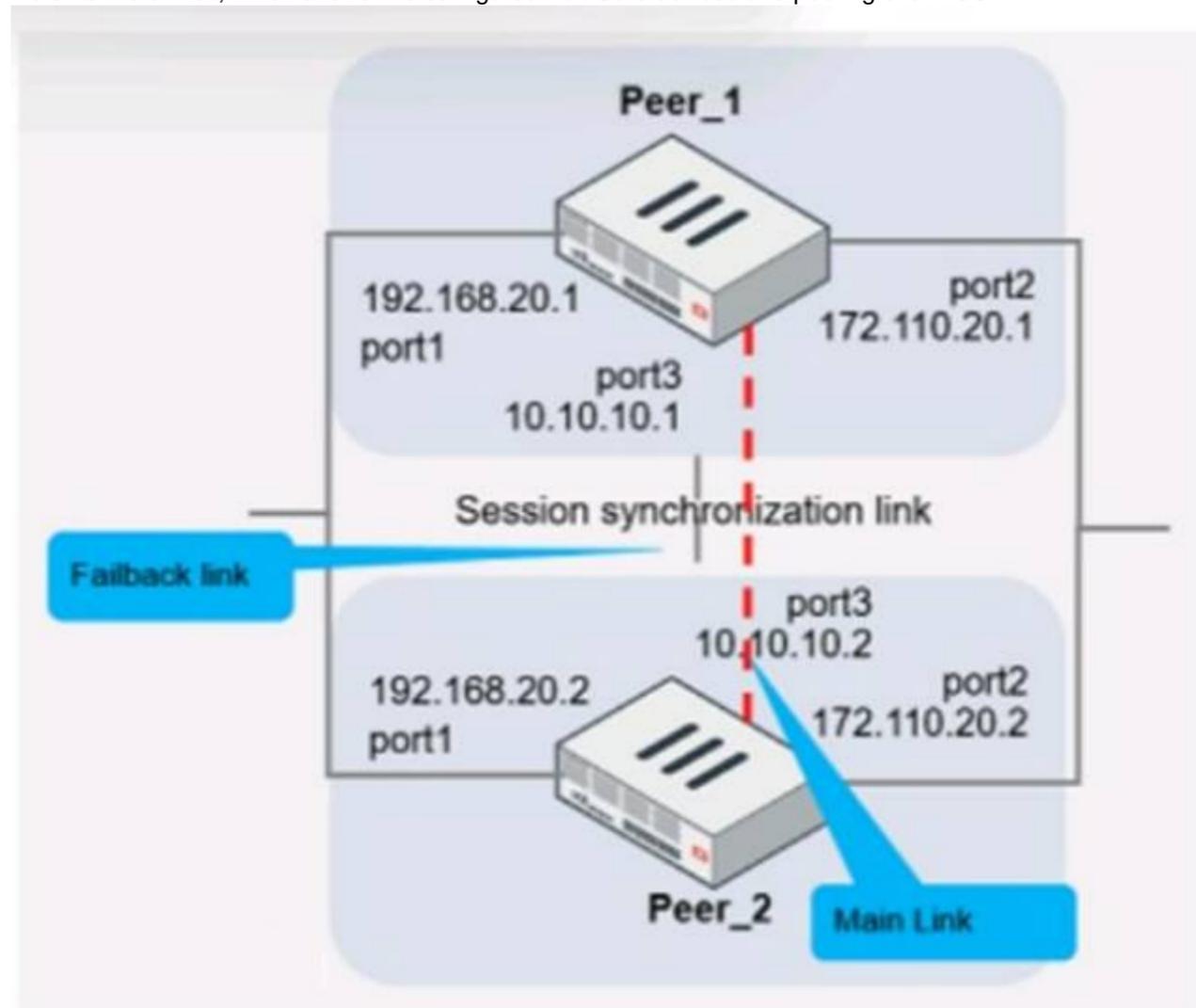
From the OSPF interface command output, we can conclude that the port3 network has more than one OSPF router because the Neighbor Count is 2, indicating the presence of another OSPF router besides NGFW-1. Additionally, we can deduce that the interfaces of the OSPF routers match the MTU value configured 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 7

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 8

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 9

Refer to the exhibit, which shows the output of a BGP summary.

```
FGT # get router info bgp summary
BGP router identifier 0.0.0.117, local AS number 65117
BGP table version is 104
3 BGP AS-PATH entries
0 BGP community entries

Neighbor      V    AS      MsgRcvd MsgSent  TblVer  InQ  OutQ  Up/Down  State/PfxRcd
10.125.0.60   4  65060    1698    1756    103    0    0    03:02:49    1
10.127.0.75   4  65075    2206    2250    102    0    0    02:45:55    1
100.64.3.1    4  65501     101     115     0      0    0    never       Active

Total number of neighbors 3
```

What two conclusions can you draw from this BGP summary? (Choose two.)

- A. External BGP (EBGP) exchanges routing information.
- B. The BGP session with peer 10. 127. 0. 75 is established.
- C. The router 100. 64. 3. 1 has the parameter bfd set to enable.
- D. The neighbors displayed are linked to a local router with the neighbor-range set to a value of 4.

Answer: AB

Explanation:

The output of the BGP (Border Gateway Protocol) summary shows details about the BGP neighbors of a router, their Autonomous System (AS) numbers, the state of the BGP session, and other metrics like messages received and sent.

From the BGP summary provided:

- * A.External BGP (EBGP) exchanges routing information.This conclusion can be inferred because the AS numbers for the neighbors are different from the local AS number (65117), which suggests that these are external connections.
- * B.The BGP session with peer 10.127.0.75 is established.This is indicated by the state/prefix received column showing a numeric value (1), which typically means that the session is established and a number of prefixes has been received.
- * C.The router 100.64.3.1 has the parameter bfd set to enable.This cannot be concluded directly from the summary without additional context or commands specifically showing BFD (Bidirectional Forwarding Detection) configuration.
- * D.The neighbors displayed are linked to a local router with the neighbor-range set to a value of 4.The neighbor-range concept does not apply here; the value 4 in the 'V' column stands for the BGP version number, which is typically 4.

NEW QUESTION 10

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 10

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 configur
- D. FortiGate automatically generates the interfaces after you configure the required settings
- E. 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. References:

- ? Creating IPsec VPN communities
- ? VPN | FortiGate / FortiOS 7.2.0

NEW QUESTION 11

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 filter 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 14

Which, three conditions are required for two FortiGate devices to form an OSPF adjacency? (Choose three.)

- A. OSPF interface network types match
- B. OSPF router IDs are unique
- C. OSPF interface priority settings are unique
- D. OSPF link costs match
- E. Authentication settings match

Answer: ABE

Explanation:

? Option A is correct because the OSPF interface network types determine how the routers form adjacencies and exchange LSAs on a network segment. The network types must match for the routers to become neighbors1.
 ? Option B is correct because the OSPF router IDs are used to identify each router in the OSPF domain and to establish adjacencies. The router IDs must be unique for the routers to become neighbors2.
 ? Option E is correct because the authentication settings control how the routers authenticate each other before exchanging OSPF packets. The authentication settings must match for the routers to become neighbors3.
 ? Option C is incorrect because the OSPF interface priority settings are used to elect the designated router (DR) and the backup designated router (BDR) on a broadcast or non-broadcast multi-access network. The priority settings do not have to be unique for the routers to become neighbors, but they affect the DR/BDR election process4.
 ? Option D is incorrect because the OSPF link costs are used to calculate the shortest path to a destination network based on the bandwidth of the links. The link costs do not have to match for the routers to become neighbors, but they affect the routing decisions5. References: =
 ? 1: OSPF network types
 ? 2: OSPF router ID
 ? 3: OSPF authentication
 ? 4: OSPF interface priority
 ? 5: OSPF link cost

NEW QUESTION 17

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

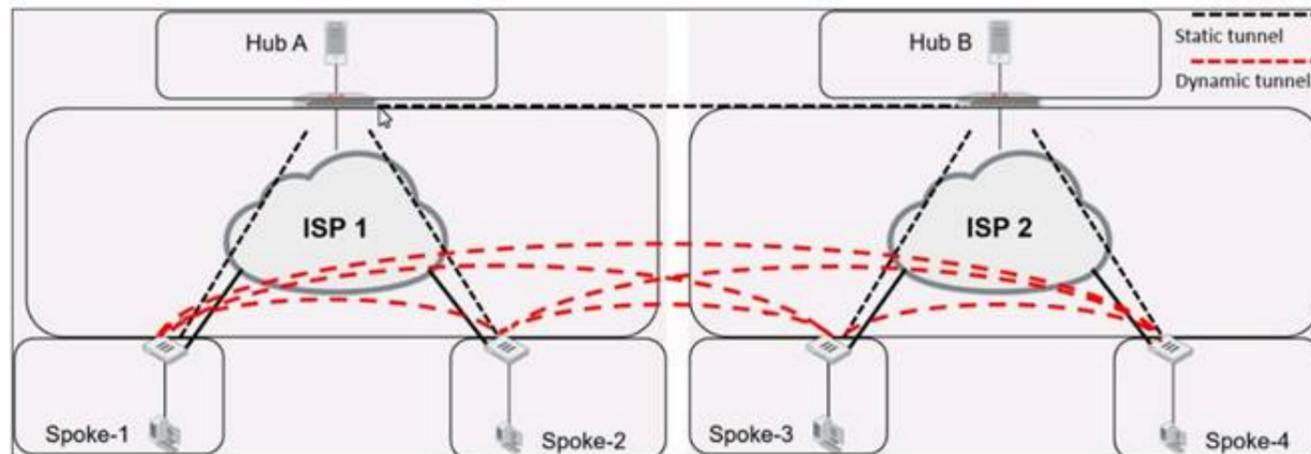
? 2: Services

? 3: Protocol options profiles

? 4: Application control

NEW QUESTION 18

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 22

Exhibit.

Script Name	Static Route
Comments	<div style="border: 1px solid gray; height: 40px; width: 100%;"></div> 0/255 0/255
Type	CLI Script
Run script on	Remote FortiGate Directly (...)
Script details	<pre># conf rout stat # edit 0 # set gateway 10.20.121.2 # set priority 20 # set device "wan1" # next # end</pre>

Refer to the exhibit, which contains a CLI script configuration on FortiManager. An administrator configured the CLI script on FortiManager but the script failed 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 26

Refer to the exhibit, which contains a partial OSPF configuration.

```
config router ospf
  set router-id 0.0.0.3
  set restart-mode graceful-restart
  set restart-period 30
  set restart-on-topology-change enable
  ...
end
```

What can you conclude from this output?

- A. Neighbors maintain communication with the restarting router.
- B. The router sends grace LSAs before it restarts.
- C. FortiGate restarts if the topology changes.
- D. The restarting router sends gratuitous ARP for 30 seconds.

Answer: B

Explanation:

From the partial OSPF (Open Shortest Path First) configuration output:

* B. The router sends grace LSAs before it restarts: This is implied by the command 'set restart-mode graceful-restart'. When OSPF is configured with graceful restart, the router sends grace LSAs (Link State Advertisements) to inform its neighbors that it is restarting, allowing for a seamless transition without recalculating routes.

Fortinet documentation on OSPF configuration clearly states that enabling graceful restart mode allows the router to maintain its adjacencies and routes during a brief restart period.

NEW QUESTION 31

You want to improve reliability over a lossy IPsec tunnel.

Which combination of IPsec phase 1 parameters should you configure?

- A. fec-ingress and fec-egress
- B. Odpd and dpd-retryinterval
- C. fragmentation and fragmentation-mtu
- D. keepalive and keylive

Answer: C

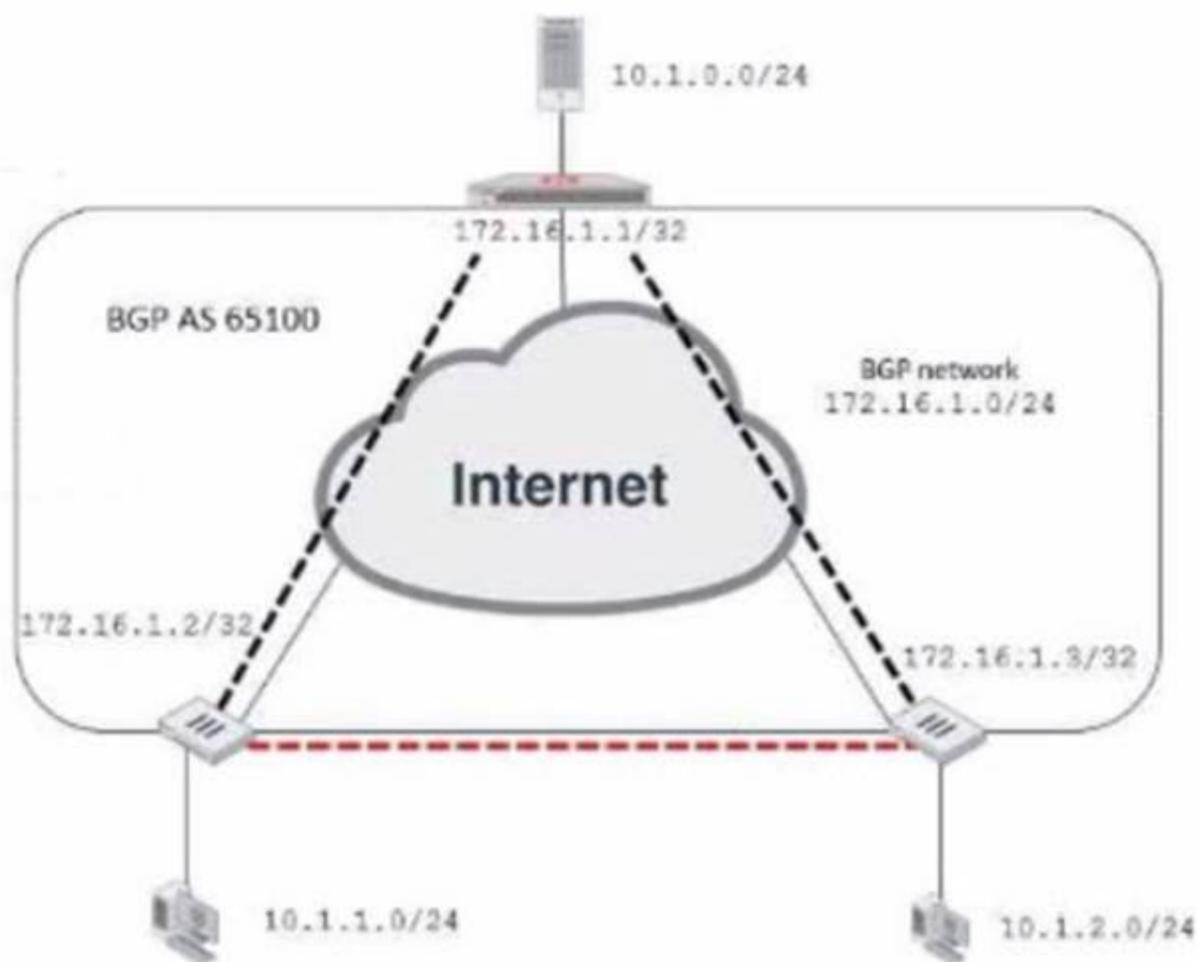
Explanation:

For improving reliability over a lossy IPsec tunnel, the fragmentation and fragmentation-mtu parameters should be configured. In scenarios where there might be issues with packet size or an unreliable network, setting the IPsec phase 1 to allow for fragmentation will enable large packets to be broken down, preventing them from being dropped due to size or poor network quality. The fragmentation-mtu specifies the size of the fragments. This is aligned with Fortinet's recommendations for handling IPsec VPN over networks with potential packet loss or size limitations.

NEW QUESTION 35

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 10.1.0.0 255.255.255.0

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 38

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 39

.....

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