

Fortinet

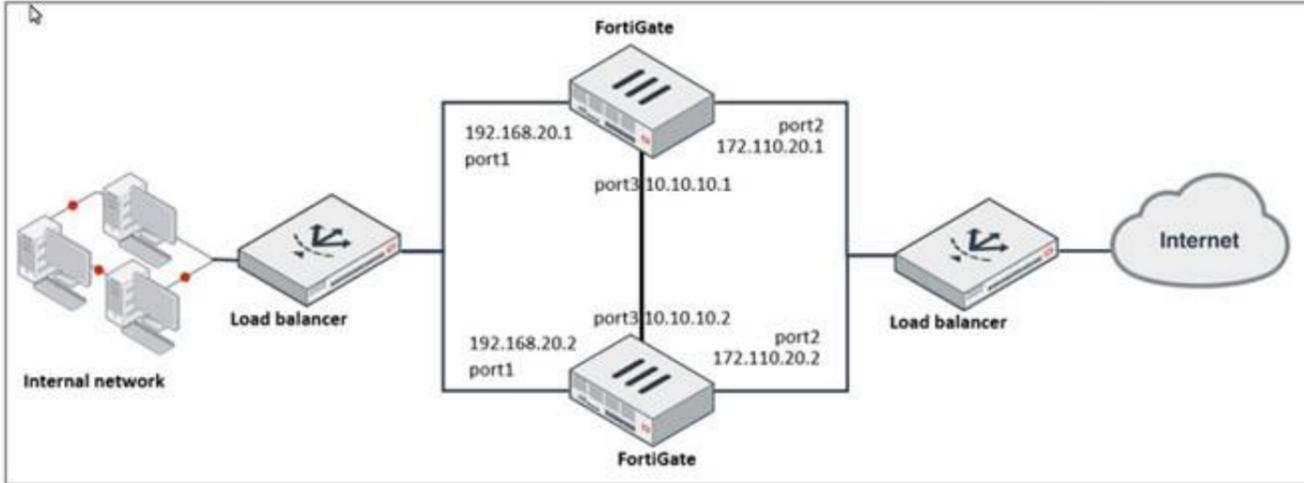
Exam Questions NSE7_EFW-7.2

Fortinet NSE 7 - Enterprise Firewall 7.2



NEW QUESTION 1

Refer to the exhibit, which shows a network diagram.



Which protocol should you use to configure the FortiGate cluster?

- A. FGCP in active-passive mode
- B. OFGSP
- C. VRRP
- D. FGCP in active-active mode

Answer: A

Explanation:

Given the network diagram and the presence of two FortiGate devices, the Fortinet Gate Clustering Protocol (FGCP) in active-passive mode is the most appropriate for setting up a FortiGate cluster. FGCP supports high availability configurations and is designed to allow one FortiGate to seamlessly take over if the other fails, providing continuous network availability. This is supported by Fortinet documentation for high availability configurations using FGCP.

NEW QUESTION 2

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 3

Refer to the exhibit, which contains information about an IPsec VPN tunnel.

```
FortiGate # diag vpn tunnel list
list all ipsec tunnel in vd 0
-----
name=tunnel_0 ver=2 serial=1 100.64.3.1:0->100.64.1.1:0 tun_id=100.64.1.1 tun_id6=:100.64.1.1
bound_if=3 lgwy=static/1 tun=intf mode=auto/1 encap=none/552 options[0228]=npu frag-rfc run_
proxyid_num=1 child_num=0 refcnt=3 ilast=42949917 olast=42949917 ad=/0
stat: rxp=0 txp=0 rxb=0 txb=0
dpd: mode=off on=0 idle=20000ms retry=3 count=0 seqno=0
natt: mode=none draft=0 interval=0 remote_port=0
fec: egress=0 ingress=0
proxyid=tunnel_0_0 proto=0 sa=1 ref=2 serial=1
src: 0:0.0.0.0-255.255.255.255:0
dst: 0:0.0.0.0-255.255.255.255:0
SA: ref=3 options=30202 type=00 soft=0 mtu=1280 expire=1454/0B replaywin=2048
seqno=1 esn=0 replaywin_lastseq=00000000 qat=192 rekey=0 hash_search_len=1
life: type=01 bytes=0/0 timeout=1768/1800
dec: spi=877d6590 esp=aes key=16 be308ec1fb05464205764424bc40a76d
ah=sha256 key=32 cc8894be3390983521a48b2e7a5c998e6b28a10a3ddd8e7bc7ecbe672dfe7cc5
enc: spi=63d0f38a esp=aes key=16 d8d3343af2fed4ddd958a022cd656b06
ah=sha256 key=32 264402ba8ad04a7e97732b52ec27c92ff86e0a97bb33e22887677336f1670c7d
dec:pkts/bytes=0/0, enc:pkts/bytes=0/0
npu_flag=00 npu_rgwy=100.64.1.1 npu_lgwy=100.64.3.1 npu_selid=0 dec_npuid=0 enc_npuid=0
run_tally=0
```

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

- A. Dead peer detection is set to enable.
- B. The IKE version is 2.
- C. Both IPsec SAs are loaded on the kernel.
- D. Forward error correction in phase 2 is set to enable.

Answer: BC

Explanation:

From the command output shown in the exhibit:

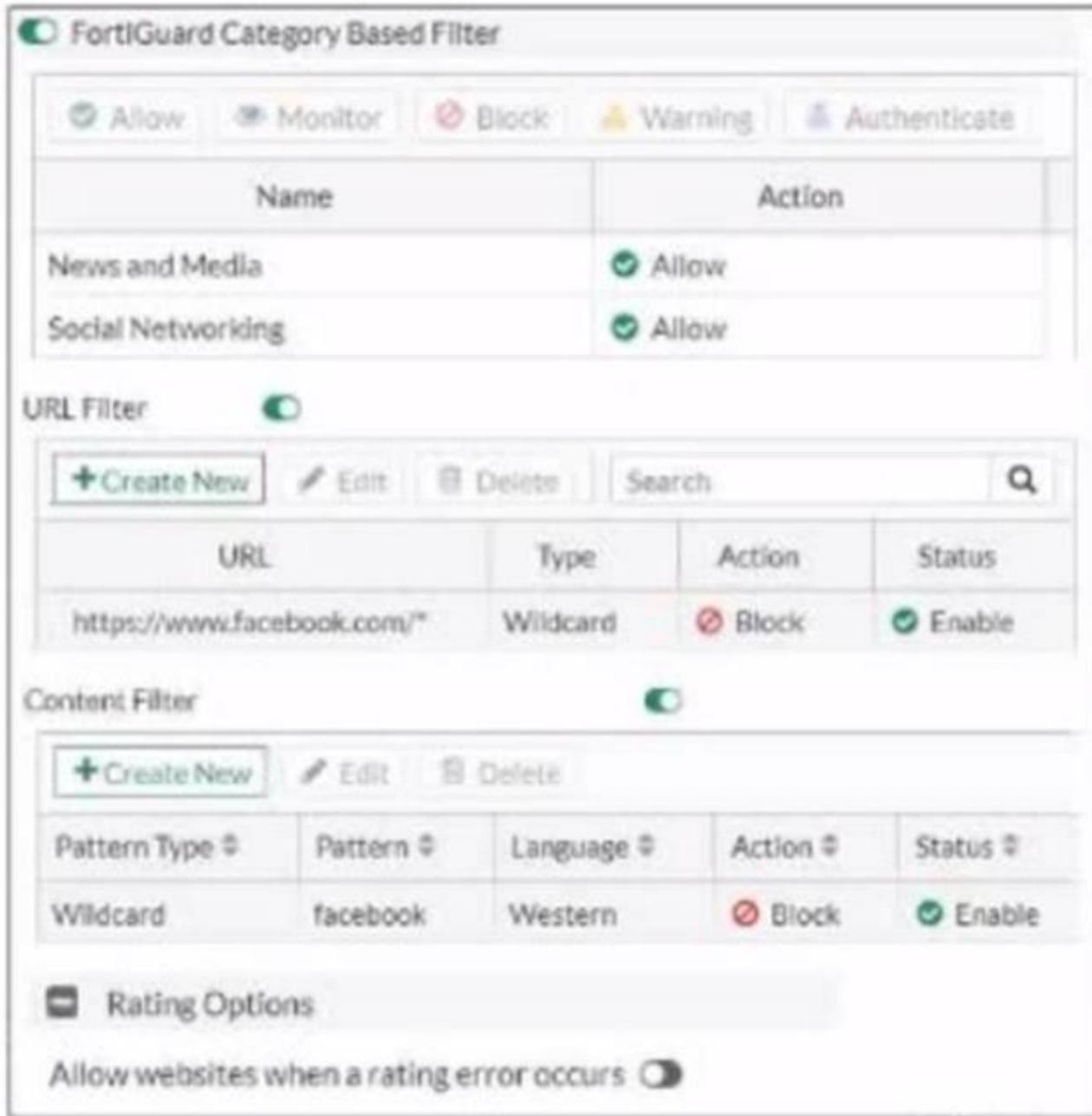
* B. The IKE version is 2: This can be deduced from the presence of 'ver=2' in the output, which indicates that IKEv2 is being used.

* C. Both IPsec SAs are loaded on the kernel: This is indicated by the line 'npu flags=0x0/0', suggesting that no offload to NPU is occurring, and hence, both Security Associations are loaded onto the kernel for processing.

Fortinet documentation specifies that the version of IKE (Internet Key Exchange) used and the loading of IPsec Security Associations can be verified through the diagnostic commands related to VPN tunnels.

NEW QUESTION 4

Exhibit.



Refer to the exhibit, which shows a partial web filter profile configuration. What can you conclude from this configuration about access to www.facebook.com, which is categorized as Social Networking?

- A. The access is blocked based on the Content Filter configuration
- B. The access is allowed based on the FortiGuard Category Based Filter configuration
- C. The access is blocked based on the URL Filter configuration
- D. The access is blocked if the local or the public FortiGuard server does not reply

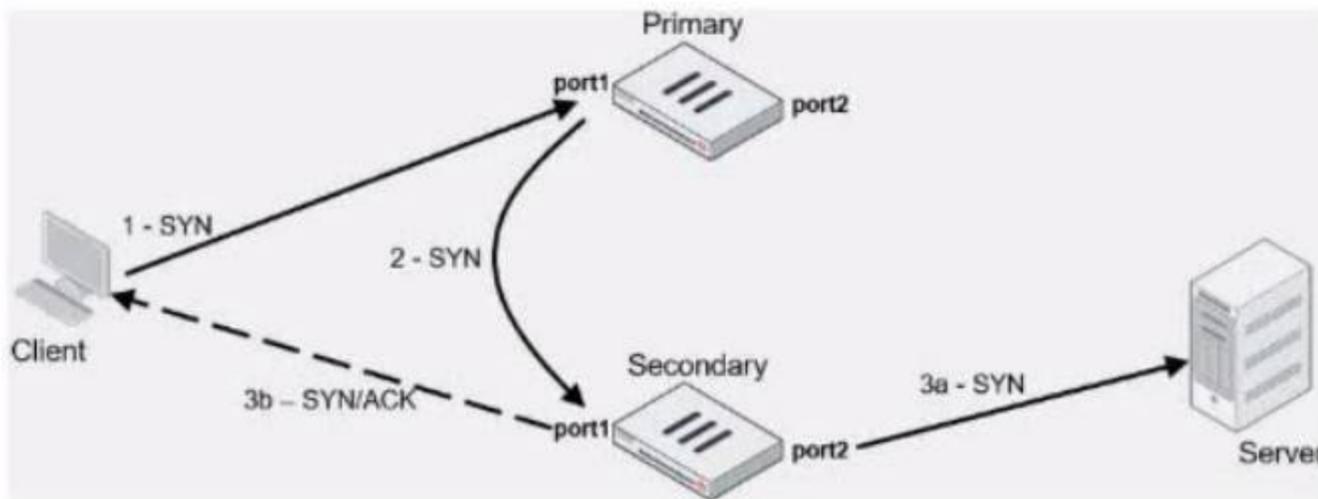
Answer: C

Explanation:

The access to www.facebook.com is blocked based on the URL Filter configuration. In the exhibit, it shows that the URL "www.facebook.com" is specifically set to "Block" under the URL Filter section. References := Fortigate: How to configure Web Filter function on Fortigate, Web filter | FortiGate / FortiOS 7.0.2 | Fortinet Document Library, FortiGate HTTPS web URL filtering ... - Fortinet ... - Fortinet Community

NEW QUESTION 5

Exhibit.



Refer to the exhibit, which contains an active-active load balancing scenario. During the traffic flow the primary FortiGate forwards the SYN packet to the secondary FortiGate. What is the destination MAC address or addresses when packets are forwarded from the primary FortiGate to the secondary FortiGate?

- A. Secondary physical MAC port1

- B. Secondary virtual MAC port1
- C. Secondary virtual MAC port1 then physical MAC port1
- D. Secondary physical MAC port2 then virtual MAC port2

Answer: A

Explanation:

In an active-active load balancing scenario, when the primary FortiGate forwards the SYN packet to the secondary FortiGate, the destination MAC address would be the secondary's physical MAC on port1, as the packet is being sent over the network and the physical MAC is used for layer 2 transmissions.

NEW QUESTION 6

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 7

Which two statements about the BFD parameter in BGP are true? (Choose two.)

- A. It allows failure detection in less than one second.
- B. The two routers must be connected to the same subnet.
- C. It is supported for neighbors over multiple hops.
- D. It detects only two-way failures.

Answer: AC

Explanation:

Bidirectional Forwarding Detection (BFD) is a rapid protocol for detecting failures in the forwarding path between two adjacent routers, including interfaces, data links, and forwarding planes. BFD is designed to detect forwarding path failures in a very short amount of time, often less than one second, which is significantly faster than traditional failure detection mechanisms like hold-down timers in routing protocols.
 Fortinet supports BFD for BGP, and it can be used over multiple hops, which allows the detection of failures even if the BGP peers are not directly connected. This functionality enhances the ability to maintain stable BGP sessions over a wider network topology and is documented in Fortinet's guides.

NEW QUESTION 8

Refer to the exhibits, which show the configurations of two address objects from the same FortiGate.

Engineering address object

Name	Engineering
Color	Change
Type	Subnet
IP/Netmask	192.168.0.0 255.255.255.0
Interface	<input type="checkbox"/> any
Static route configuration	<input type="checkbox"/>
Comments	Write a comment... 0/255
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

Finance address object

Name	Finance
Color	Change
Type	Subnet
IP/Netmask	192.168.1.0 255.255.255.0
Interface	<input type="checkbox"/> any
Static route configuration	<input type="checkbox"/>
Comments	Write a comment... 0/255
<input type="button" value="Return"/>	

Why can you modify the Engineering address object, but not the Finance address object?

- A. You have read-only access.
- B. FortiGate joined the Security Fabric and the Finance address object was configured on the root FortiGate.
- C. FortiGate is registered on FortiManager.
- D. Another user is editing the Finance address object in workspace mode.

Answer: B

Explanation:

The inability to modify the Finance address object while being able to modify the Engineering address object suggests that the Finance object is being managed by a higher authority in the Security Fabric, likely the root FortiGate. When a FortiGate is part of a Security Fabric, address objects and other configurations may be managed centrally.

This aligns with the Fortinet FortiGate documentation on Security Fabric and central management of address objects.

NEW QUESTION 9

Exhibit.

```
# get router info bgp neighbors
VRF 0 neighbor table:
BGP neighbor is 10.2.0.254, remote AS 65100, local AS 65200, external link
  BGP version 4, remote router ID 0.0.0.0
  BGP state = Idle
  Not directly connected EBGP
  last read 00:04:40, hold time is 180, keepalive interval is 60 seconds
  Configured hold time is 180, keepalive interval is 60 seconds
  Received 5 messages, 0 notifications, 0 in queue
  Sent 4 messages, 1 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  NLRI treated as withdraw: 0
  Minimum time between advertisement runs is 30 seconds...
```

Refer to the exhibit, which provides information on BGP neighbors. Which can you conclude from this command output?

- A. The router are in the number to match the remote peer.
- B. You must change the AS number to match the remote peer.
- C. BGP is attempting to establish a TCP connection with the BGP peer.
- D. The bfd configuration to set to enable.

Answer: C

Explanation:

The BGP state is "Idle", indicating that BGP is attempting to establish a TCP connection with the peer. This is the first state in the BGP finite state machine, and it means that no TCP connection has been established yet. If the TCP connection fails, the BGP state will reset to either active or idle, depending on the configuration. References: You can find more information about BGP states and troubleshooting in the following Fortinet Enterprise Firewall 7.2 documents:
 ? Troubleshooting BGP
 ? How BGP works

NEW QUESTION 10

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 interlaces
- D. Set protected network to all

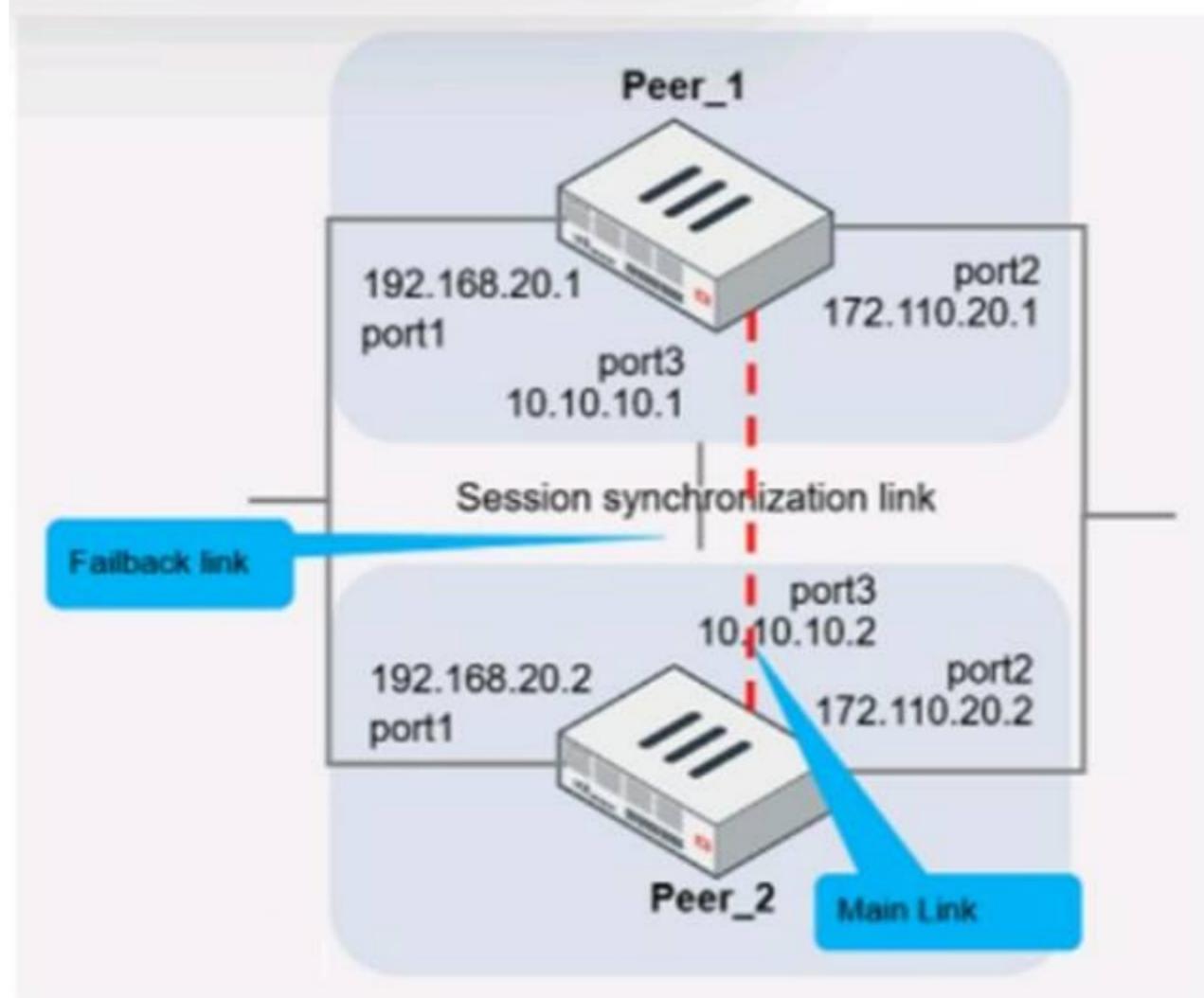
Answer: A

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 10

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 15

Refer to the exhibit.

```
config system global
  set admin-https-pki-required disable
  set av-failopen pass
  set check-protocol-header loose
  set memory-use-threshold-extreme 95
  set strict-dirty-session-check enable
  ...
end
```

which contains a partial configuration of the global system. What can you conclude from this output?

- A. NPs and CPs are enabled
- B. Only CPs are disabled
- C. Only NPs are disabled
- D. NPs and CPs are disabled

Answer: D

Explanation:

The configuration output shows various global settings for a FortiGate device. The terms NP (Network Processor) and CP (Content Processor) relate to FortiGate's hardware acceleration features. However, the provided configuration output does not directly mention the status (enabled or disabled) of NPs and CPs. Typically, the command to disable or enable hardware acceleration features would specifically mention NP or CP in the command syntax. Therefore, based on the output provided, we cannot conclusively determine the status of NPs and CPs, hence option D is the closest answer since the output does not confirm that they are enabled.

References:

? FortiOS Handbook - CLI Reference for FortiOS 5.2

NEW QUESTION 18

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 23

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 27

Which configuration can be used to reduce the number of BGP sessions in on IBGP network?

- A. Route-reflector-peer enable
- B. Route-reflector-client enable
- C. Route-reflector enable
- D. Route-reflector-server enable

Answer: B

Explanation:

To reduce the number of BGP sessions in an IBGP network, you can use a route reflector, which acts as a focal point for IBGP sessions and readvertises the prefixes to all other peers. To configure a route reflector, you need to enable the route-reflector-client option on the neighbor-group settings of the hub device. This will make the hub device act as a route reflector server and the other devices as route reflector clients. References := Route exchange | FortiGate / FortiOS 7.2.0 - Fortinet Documentation

NEW QUESTION 31

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

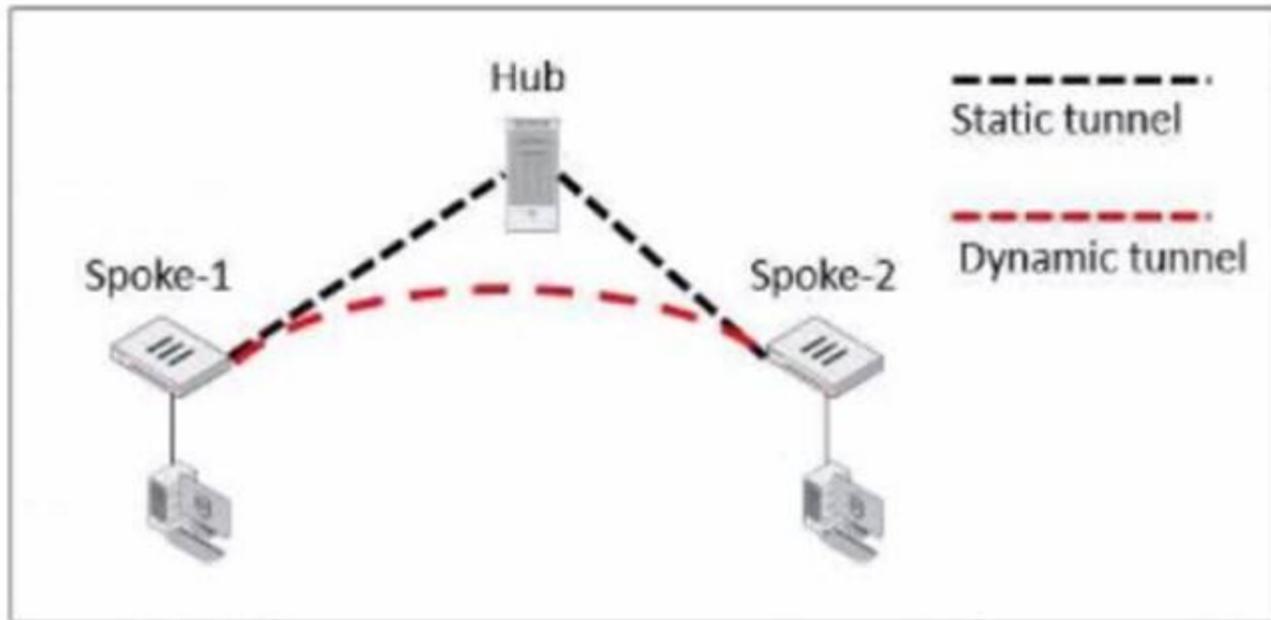
Answer: C

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 34

Exhibit.



Refer to the exhibit, which shows an ADVPN network.

The client behind Spoke-1 generates traffic to the device located behind Spoke-2. Which first message does the hub send to Spoke-1 to bring up the dynamic tunnel?

- A. Shortcut query
- B. Shortcut reply
- C. Shortcut offer
- D. Shortcut forward

Answer: A

Explanation:

In an ADVPN scenario, when traffic is initiated from a client behind one spoke to another spoke, the hub sends a shortcut query to the initiating spoke. This query is used to determine if there is a more direct path for the traffic, which can then trigger the establishment of a dynamic tunnel between the spokes.

NEW QUESTION 35

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 serve
- B. fortiguar
- C. net to the server list.
- D. Configure securewf.fortiguar
- E. net on the default servers.
- F. Set update-server-location to automatic.
- G. Configure server-type with the rating option.

Answer: D

Explanation:

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.

NEW QUESTION 37

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 40

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

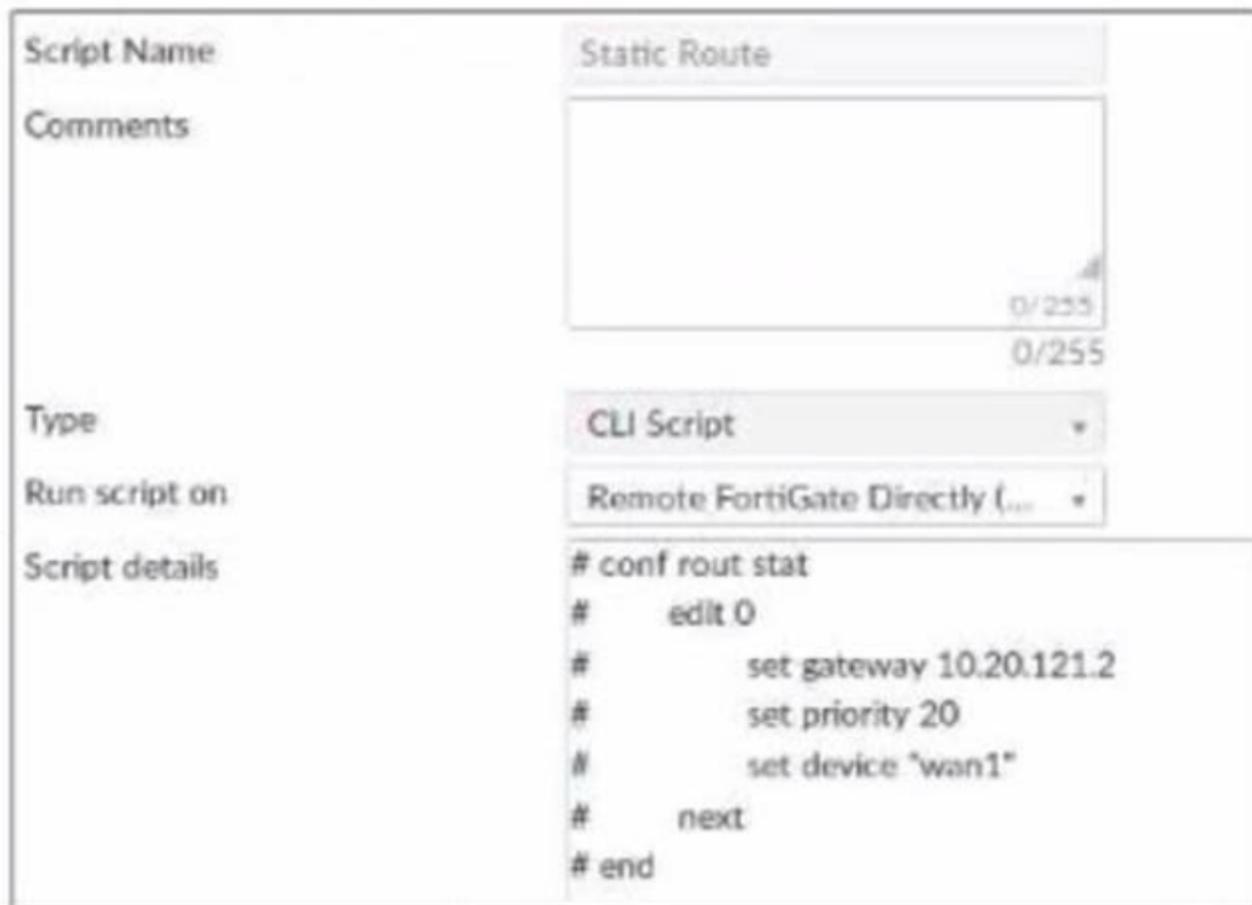
Answer: AB

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 42

Exhibit.



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 TCL 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 47

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 50

You configured 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)

- 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 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 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. 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 52

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 53

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

NSE7_EFW-7.2 Practice Exam Features:

- * NSE7_EFW-7.2 Questions and Answers Updated Frequently
- * NSE7_EFW-7.2 Practice Questions Verified by Expert Senior Certified Staff
- * NSE7_EFW-7.2 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * NSE7_EFW-7.2 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The NSE7_EFW-7.2 Practice Test Here](#)