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!

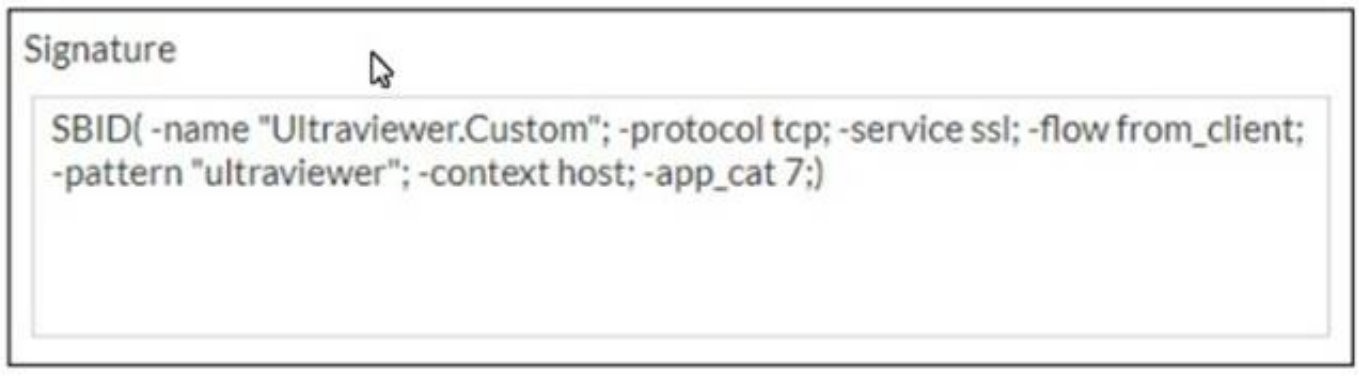
NEW QUESTION 1
Which two statements about bfd are true? (Choose two)

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: BC

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. References := BFD | FortiGate / FortiOS 7.2.0 - Fortinet Document Library, section “BFD”.

NEW QUESTION 2
Refer to the exhibit, which shows a custom signature.



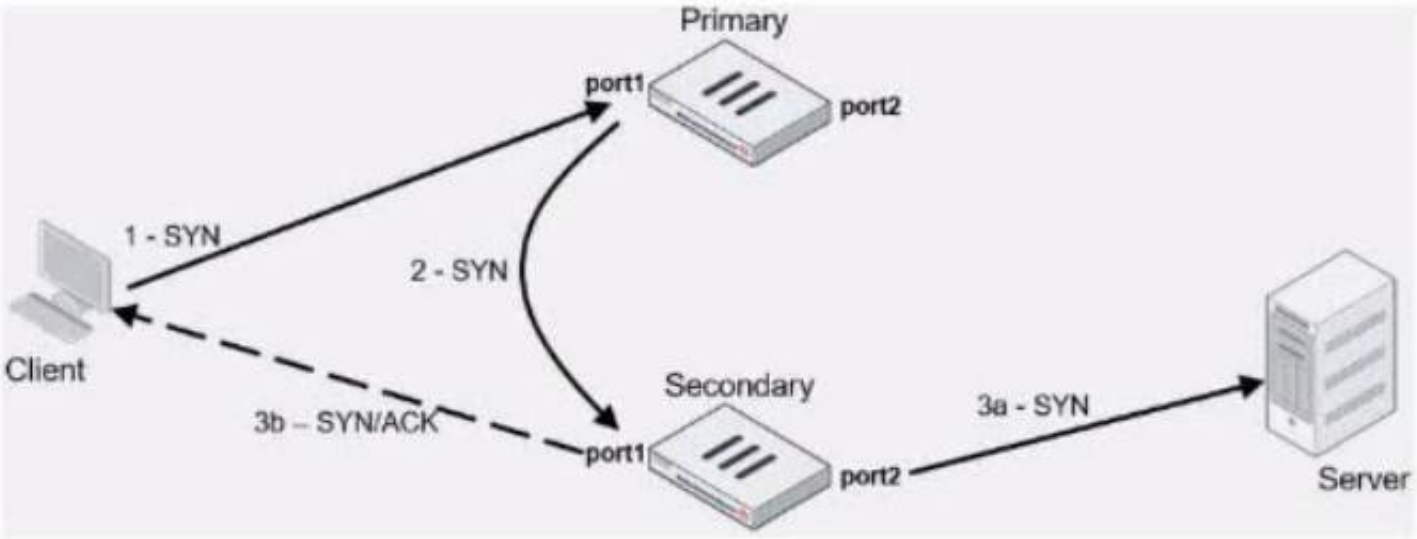
Which two modifications must you apply to the configuration of this custom signature so that you can save it on FortiGate? (Choose two.)

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
Exhibit.



Refer to the exhibit, which contains an active-active toad 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 4

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 5
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 interlace
What two conclusions can you draw from this command output? (Choose two.)

A. The port3 network has more man 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 6
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 7
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

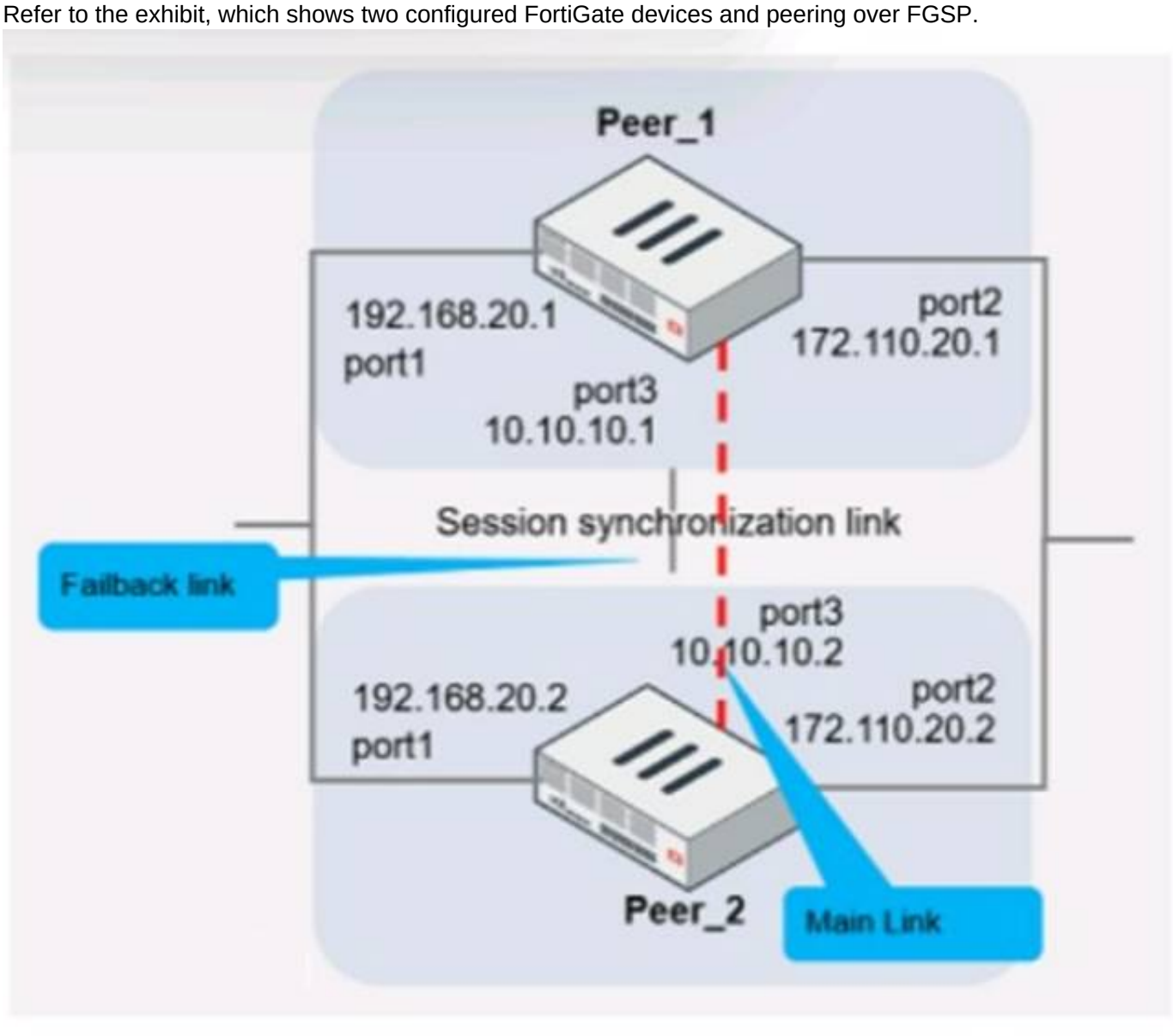
NEW QUESTION 8
Which ADVPN configuration must be configured using a script on fortiManager, when using VPN Manager to manage fortiGate VPN tunnels?

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 9
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 10
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 arc disabled
C. Only NPs are disabled
D. NPs and CPs arc 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 10
Which statement about network processor (NP) offloading is true?

A. For TCP traffic FortiGate CPU offloads the first packets of SYN/ACK and ACK of the three-way handshake to NP
B. The NP provides IPS signature matching
C. You can disable the NP for each firewall policy using the command np-acceleration st to loose.
D. The NP checks the session key or IPSec SA

Answer: B

Explanation:
Network processors (NPs) are specialized hardware within FortiGate devices that accelerate certain security functions. One of the primary functions of NPs is to provide IPS signature matching (B), allowing for high-speed inspection of traffic against a database of known threat signatures.

NEW QUESTION 13
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 filler 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 17
Refer to the exhibit, which contains a partial BGP combination.

```
config router bgp
    set as 65200
    set router-id 172.16.1.254
    config neighbor
        edit 100.64.1.254
            set remote-as 65100
        next
    end
end
```

You want to configure a loopback as the OGP source.
Which two parameters must you set in the BGP configuration? (Choose two)

A. ebgp-enforce-multihop
B. recursive-next-hop
C. ibgp-enfoce-multihop
D. update-source

Answer: AD

Explanation:
To configure a loopback as the BGP source, you need to set the “ebgp- enforce-multihop” and “update-source” parameters in the BGP configuration. The “ebgp-

enforce-multihop" allows EBGP connections to neighbor routers that are not directly connected, while "update-source" specifies the IP address that should be used for the BGP
session1. References := BGP on loopback, Loopback interface, Technical Tip: Configuring EBGP Multihop Load-Balancing, Technical Tip: BGP routes are not installed in routing
table with loopback as update source

NEW QUESTION 20
Refer to the exhibit, which shows a routing table.

Network	Gateway IP	Interfaces	Distance	Type
0.0.0.0/0	10.1.0.254	port1	10	Static
10.1.0.0/24	0.0.0.0	port1	0	Connected
10.1.4.0/24	10.1.0.100	port1	110	OSPF
10.1.10.0/24	0.0.0.0	port3	0	Connected
172.16.100.0/24	0.0.0.0	port8	0	Connected

What two options can you configure in OSPF to block the advertisement of the 10.1.10.0 prefix? (Choose two.)

A. Remove the 16.1.10.C prefix from the OSPF network
B. Configure a distribute-list-out
C. Configure a route-map out
D. Disable Redistribute Connected

Answer: BC

Explanation:
To block the advertisement of the 10.1.10.0 prefix in OSPF, you can configure a distribute-list-out or a route-map out. A distribute-list-out is used to filter outgoing routing updates from being advertised to OSPF neighbors1. A route-map out can also be used for filtering and is applied to outbound routing updates2. References := Technical Tip: Inbound route filtering in OSPF usi … - Fortinet Community, OSPF | FortiGate / FortiOS 7.2.2 - Fortinet Documentation

NEW QUESTION 23
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 28
Exhibit.

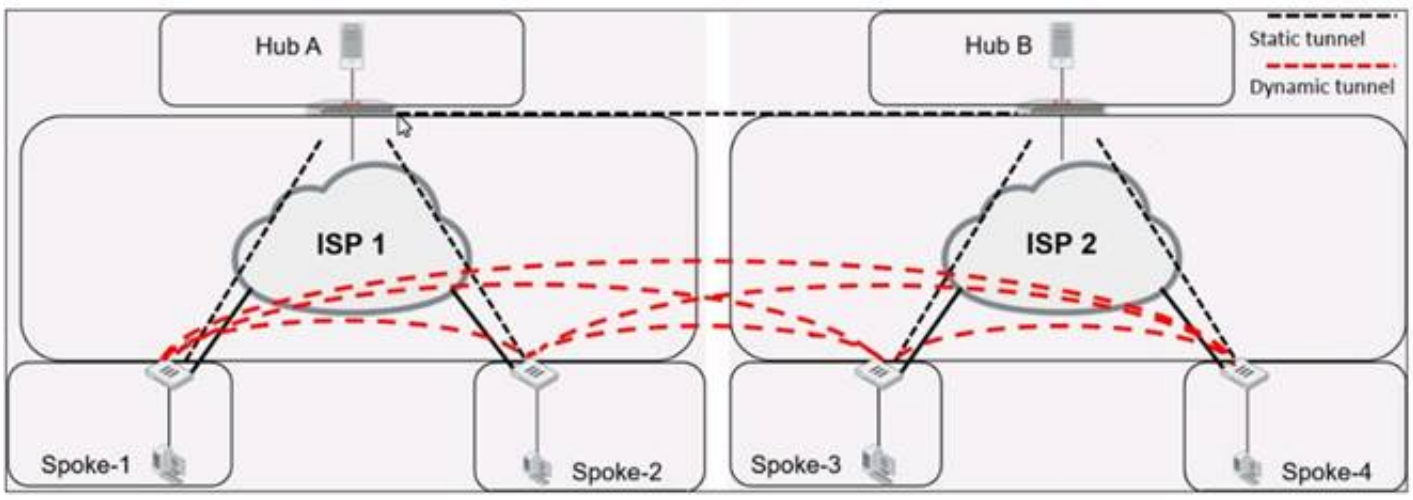
Refer to the exhibit, which contains a partial policy configuration. Which setting must you configure to allow SSH?

A. Specify SSH in the Service field
B. Configure pot 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 31
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 32
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 33
You want to improve reliability over a lossy IPSec tunnel.
Which combination of IPSec phase 1 parameters should you configure?

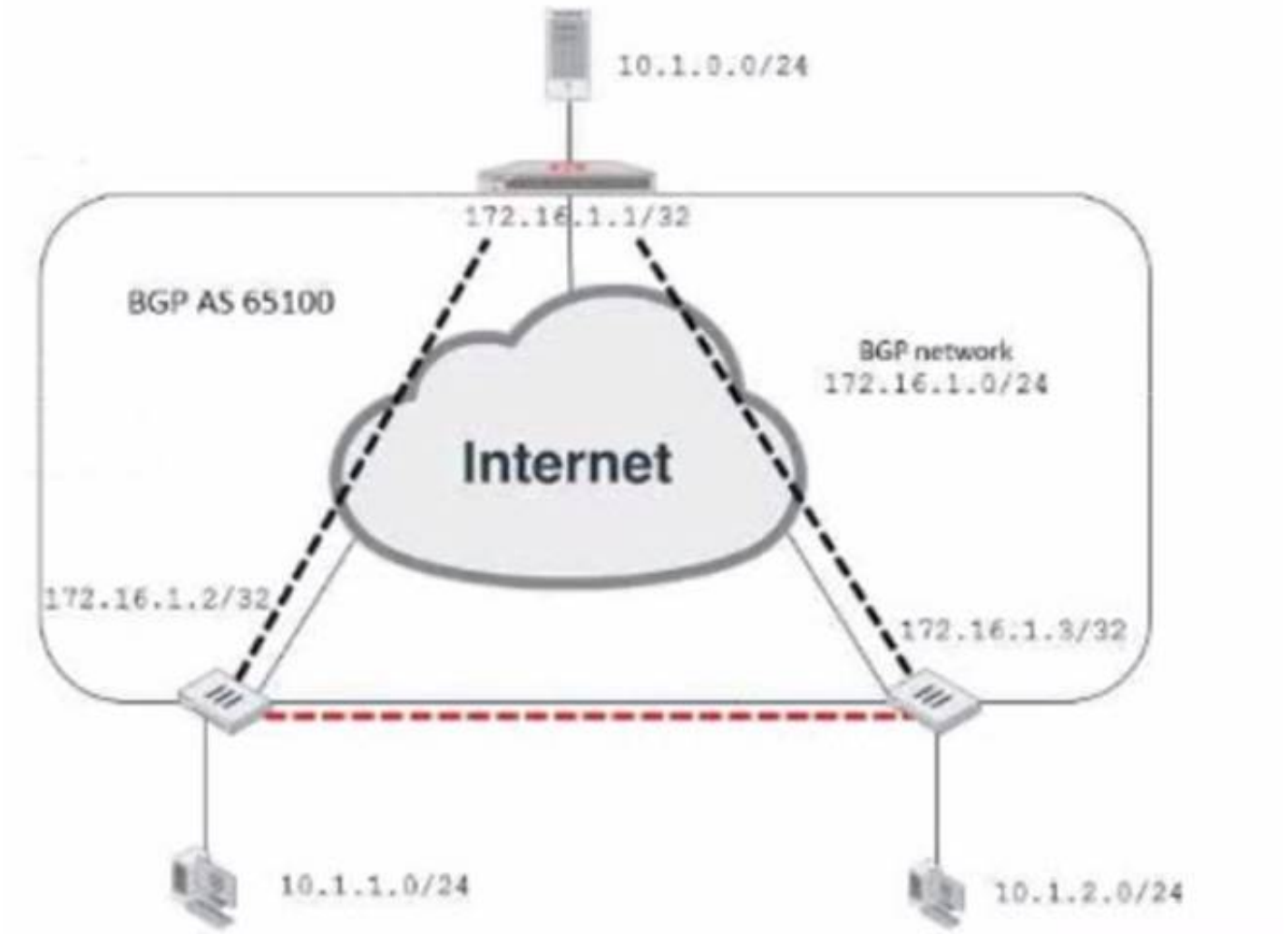
A. fec-ingress and fec-egress
B. Odpd and dpd-retryinterval
C. fragmentation and fragmentation-mtu
D. keepalive and keylive

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 37
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 con figuration 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 41
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 me FortiGate interfaces andthe 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 46
Exhibit.

```
# diagnose webfilter fortiguard cache dump

Saving to file [/tmp/urlCache.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.comam 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 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. 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 48
.....

Relate Links

100% Pass Your NSE7_EFW-7.2 Exam with Exambible 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/