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.

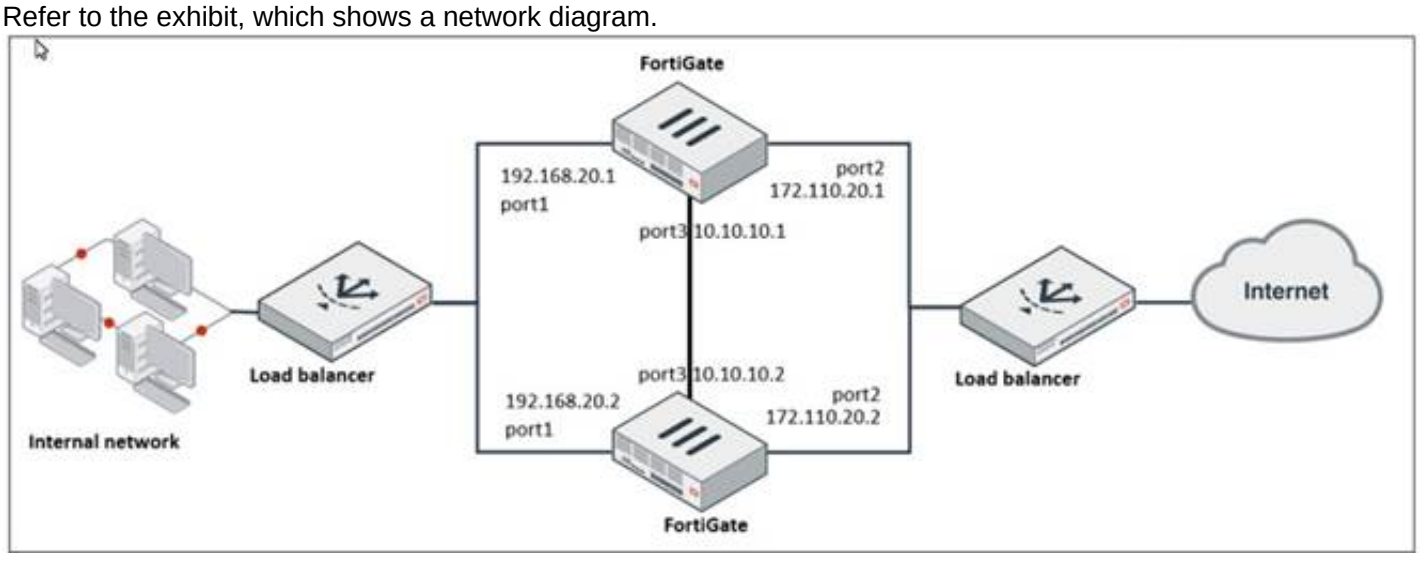
* 100% Pass Rate

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
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.

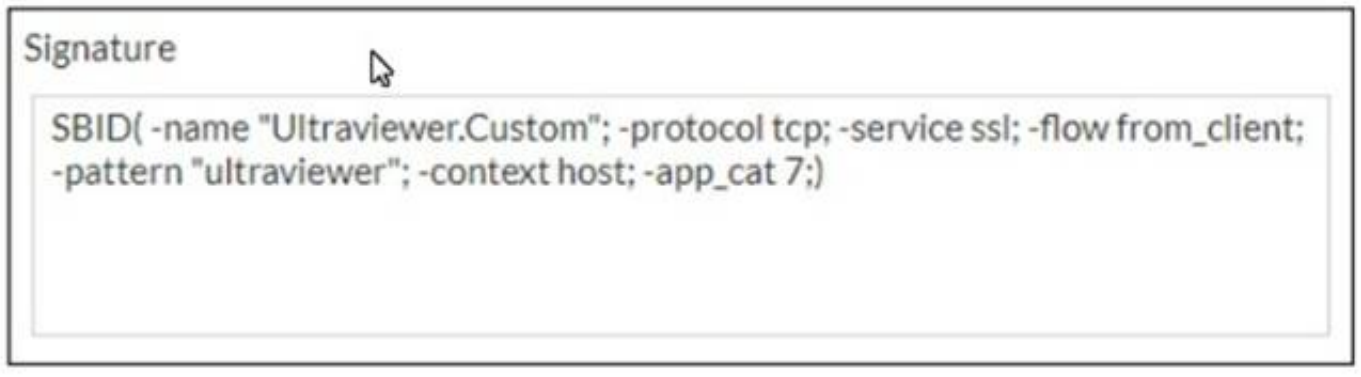
NEW QUESTION 2
Which two statements about bfd are true? (Choose two)

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 3
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 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
Refer to the exhibit, which shows an error in system fortiguard configuration.

```
NGFW-1 (fortiguard) # set protocol udp

command parse error before 'udp'
Command fail. Return code -61
```

What is the reason you cannot set the protocol to udp in config system fortiguard?

A. FortiManager provides FortiGuard.
B. fortiguard-anycast is set to enable.
C. You do not have the corresponding write access.
D. udp is not a protocol option.

Answer: D

Explanation:
The reason for the command failure when trying to set the protocol to UDP in theconfig system fortiguardis likely that UDP is not a protocol option in this context. The command syntax might be incorrect or the option to set a protocol for FortiGuard updates might not exist in this manner. So the correct answer is D. udp is not a protocol option.

NEW QUESTION 6
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
```

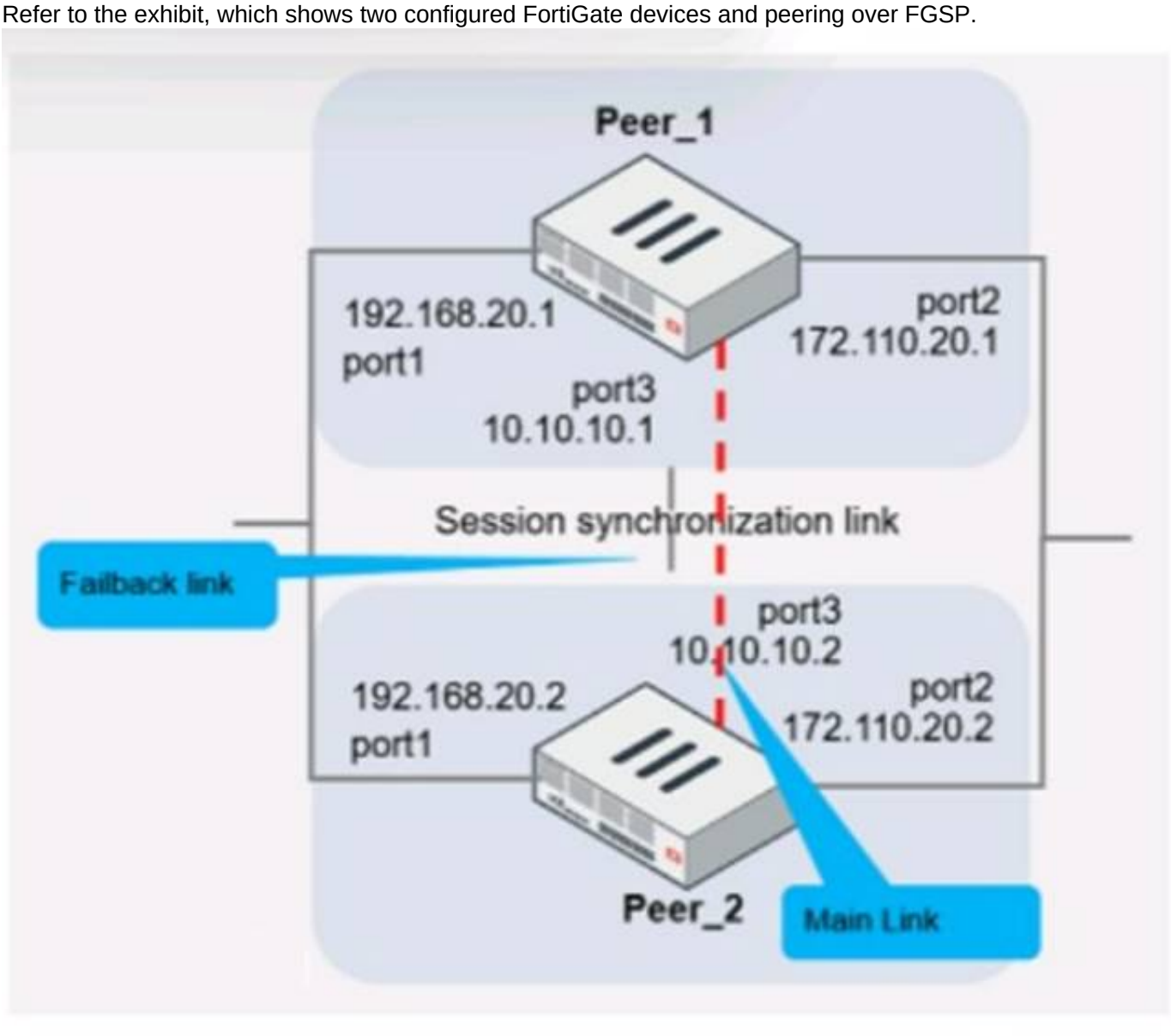
Refer to the exhibit, which contains the partial interface configuration of two FortiGate devices.
Which two conclusions can you draw from this con figuration? (Choose two)

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). Withvrrp-virtual-macenabled, 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 7
Refer to the exhibit, which shows two configured FortiGate devices and peering over FGSP.



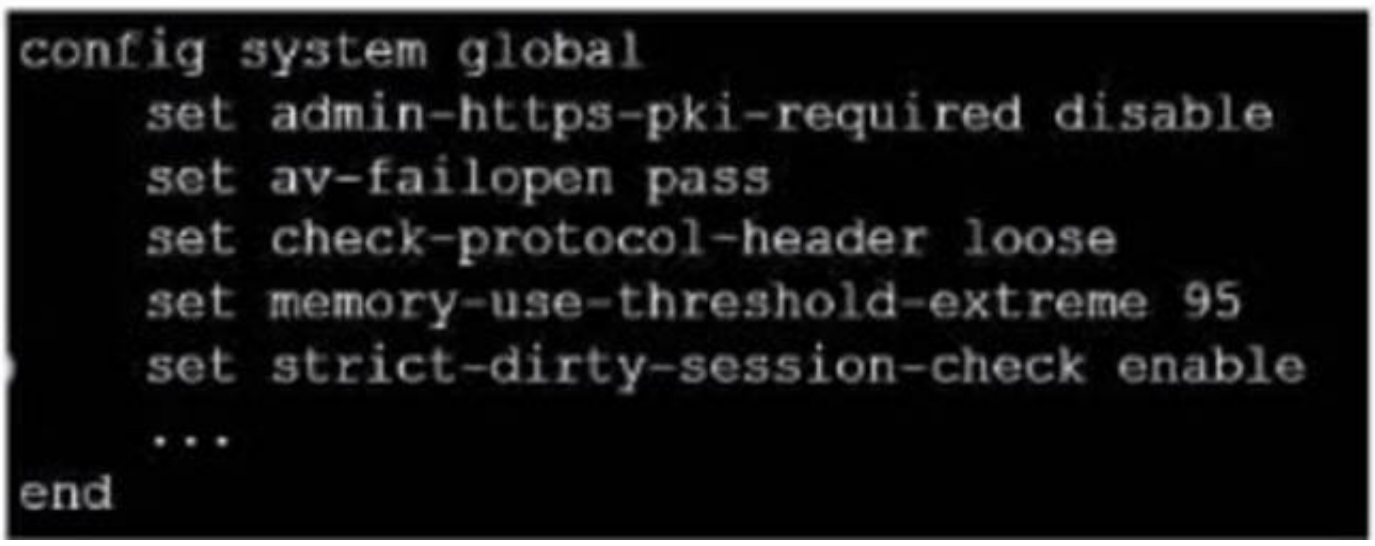
The main link directly connects the two FortiGate devices and is configured using the set session-syn-dev <interface> command.
What is the primary reason to configure the main link?

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
Refer to the exhibit.



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 9
Which two statements about IKE vision 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 toestablish 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 10
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, iffail-openis 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 10
Which two statements about metadata variables are true? (Choose two.)

A. You create them on FortiGate
B. They apply only to non-firewall objects.
C. The metadata format is $<metadata_variabie_name>.
D. They can be used as variables in scripts

Answer: AD

Explanation:
Metadata variables in FortiGate are created to store metadata associated
with different FortiGate features. These variables can be used in various configurations and scripts to dynamically replace the variable with its actual value during

processing. A: You create metadata variables on FortiGate. They are used to store metadata for FortiGate features and can be called upon in different configurations. D: They can be used as variables in scripts. Metadata variables are utilized within the scripts to dynamically insert values as per the context when the script runs.
Fortinet FortiOS Handbook: CLI Reference

NEW QUESTION 11
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	port2	0	Connected
172.16.100.0/24	0.0.0.0	port3	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 15
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 16
Which FortiGate in a Security I auric sends togs to FortiAnalyzer?

A. Only the root FortiGate.
B. Each FortiGate in the Security fabric.
C. The FortiGate devices performing network address translation (NAT) or unified threat management (UTM). if configured.
D. Only the last FortiGate that handled a session in the Security Fabric

Answer: B

Explanation:
? Option B is correct because each FortiGate in the Security Fabric can send logs to FortiAnalyzer for centralized logging and analysis12. This allows you to monitor and manage the entire Security Fabric from a single console and view aggregated reports and dashboards.
? Option A is incorrect because the root FortiGate is not the only device that can send logs to FortiAnalyzer. The root FortiGate is the device that initiates the Security Fabric and acts as the central point of contact for other FortiGate devices3. However, it does not have to be the only log source for FortiAnalyzer.
? Option C is incorrect because the FortiGate devices performing NAT or UTM are not the only devices that can send logs to FortiAnalyzer. These devices can perform additional security functions on the traffic that passes through them, such as firewall, antivirus, web filtering, etc4. However, they are not the only devices that generate logs in the Security Fabric.
? Option D is incorrect because the last FortiGate that handled a session in the Security Fabric is not the only device that can send logs to FortiAnalyzer. The last FortiGate is the device that terminates the session and applies the final security policy5. However, it does not have to be the only device that reports the session information to FortiAnalyzer. References: =
? 1: Security Fabric - Fortinet Documentation1

? 2: FortiAnalyzer Demo6
? 3: Security Fabric topology
? 4: Security Fabric UTM features
? 5: Security Fabric session handling

NEW QUESTION 19
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 21
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 25
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-senderenabled to send shortcut advertisement messages to the spokes. Also, the hub would need to haveauto-discovery-forwarderenabled 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. Theike-versiondoes not need to be reconfigured on the hub if it's already set to version 2 andauto-discovery-receiveris not necessary on the hub because it's the one sending the advertisements, not receiving.
References:
? FortiOS Handbook - ADVPN

NEW QUESTION 27
.....

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/