

Fortinet

Exam Questions NSE7_EFW-7.2

Fortinet NSE 7 - Enterprise Firewall 7.2



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 --.

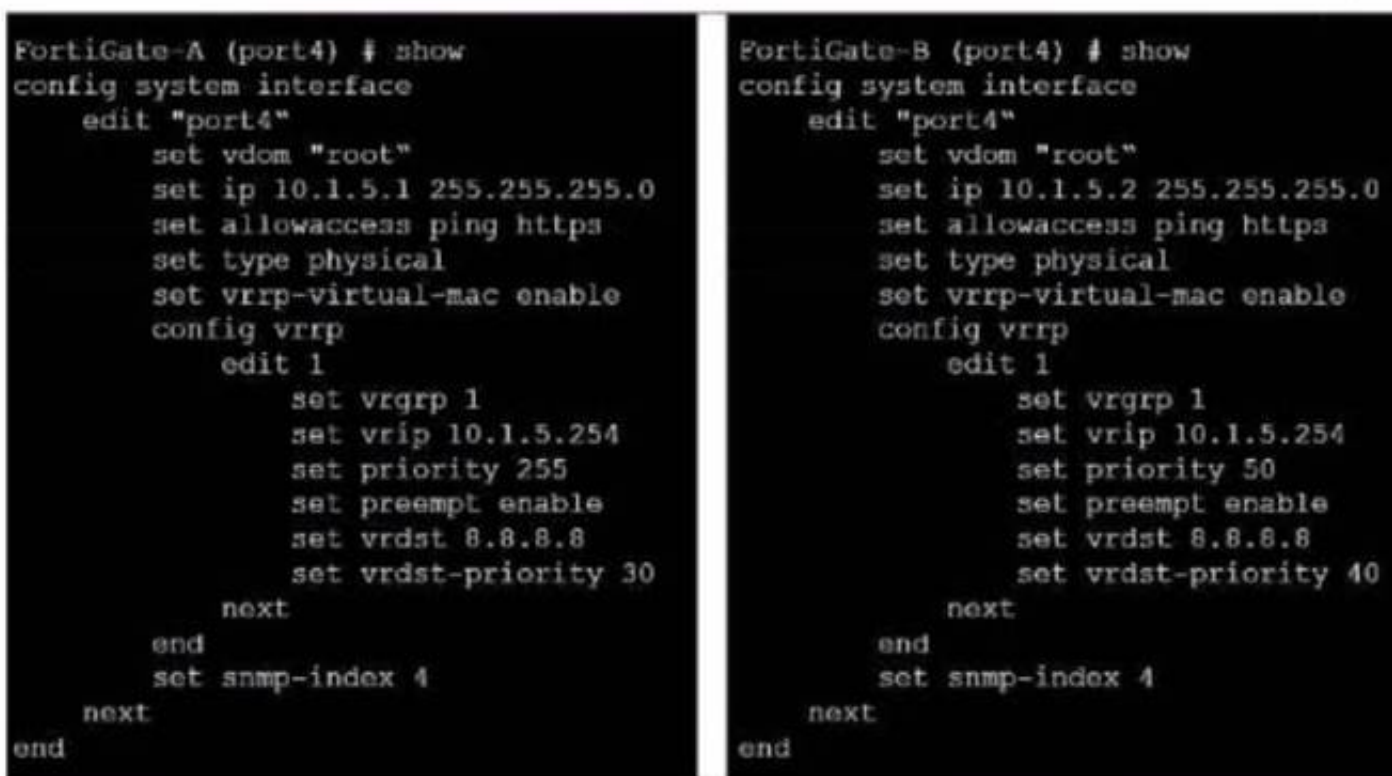
Answer: AB

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

Exhibit.



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 3

Which two statements about IKE version 2 fragmentation are true? (Choose two.)

- A. Only some IKE version 2 packets are considered fragmentable.
- B. The reassembly timeout default value is 30 seconds.
- C. It is performed at the IP layer.
- D. The maximum number of IKE version 2 fragments is 128.

Answer: AD

Explanation:

In IKE version 2, not all packets are fragmentable. Only certain messages within the IKE negotiation process can be fragmented. Additionally, there is a limit to the number of fragments that IKE version 2 can handle, which is 128. This is specified in the Fortinet documentation and ensures that the IKE negotiation process can proceed even in networks that have issues with large packets. The reassembly timeout and the layer at which fragmentation occurs are not specified in this context within Fortinet documentation.

NEW QUESTION 4

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 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 5

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

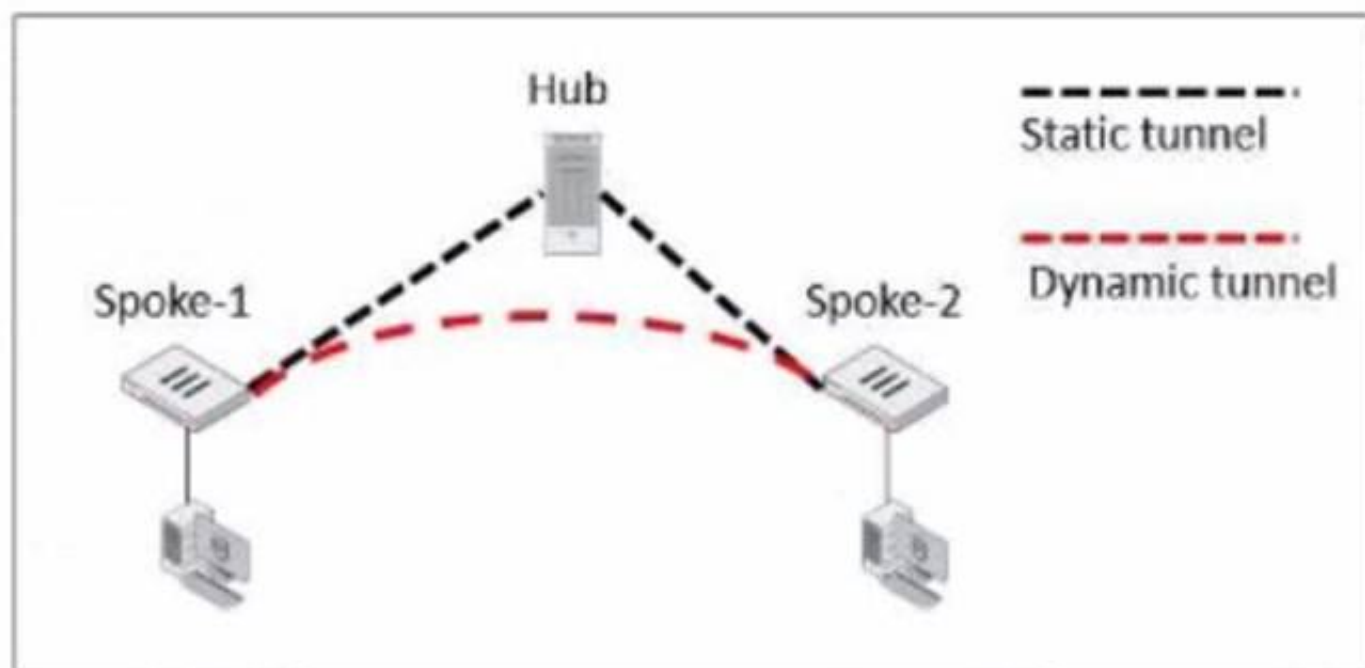
Answer: B

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 6

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 7

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 8

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 9

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

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

Answer: B

Explanation:

Virtual MAC Address and Failover

- The new primary broadcasts Gratuitous ARP packets to notify the network that each virtual MAC is now reachable through a different switch port.

- Some high-end switches might not clear their MAC table correctly after a failover - Solution: Force former primary to shut down all its interfaces for one second when the failover happens (excluding heartbeat and reserved management interfaces):

#Config system ha

set link-failed-signal enable end

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

NEW QUESTION 10

Exhibit.

```
# diagnose webfilter fortiguard cache dump

Saving to file [/tmp/urcCache.txt]
Cache Contents:
-----
Cache Mode:    TTL
Cache DB Ver:  23.6106

Domain |IP          DB Ver  T URL
34000000|34000000 23.6106 P Bhttp://training.fortinet.com/
25000000|25000000 23.6106 E Bhttps://twitter.com/...

# get webfilter categories
...
g07 General Interest - Business:
  31 Finance and Banking
...
  51 Government and Legal Organizations
  52 Information Technology
```

Refer to the exhibit, which shows the output from the webfilter fortiguard cache dump and webfilter categories commands. Using the output, how can an administrator determine the category of the training.fortinet.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 lphex values of 34 to get the category number
- D. The administrator must convert the first two digits of the Domain hex value to a decimal value

Answer: B

Explanation:

? Option B is correct because the administrator can determine the category of the training.fortinet.com website by looking up the hex value of 34 in the second command output. This is because the first command output shows that the domain and the IP of the website are both in category (Hex) 34, which corresponds to Information Technology in the second command output¹.

? Option A is incorrect because the administrator does not need to convert the first three digits of the IP hex value to binary. The IP hex value is already in the same format as the category hex value, so the administrator can simply compare them without any conversion².

? Option C is incorrect because the administrator does not need to add both the

Pima in and lphex values of 34 to get the category number. The Pima in and lphex values are not related to the category number, but to the cache TTL and the database version respectively³.

? Option D is incorrect because the administrator does not need to convert the first

two digits of the Domain hex value to a decimal value. The Domain hex value is already in the same format as the category hex value, so the administrator can simply compare them without any conversion². References: =

? 1: Technical Tip: Verify the webfilter cache content⁴

? 2: Hexadecimal to Decimal Converter⁵

? 3: FortiGate - Fortinet Community⁶

? : Web filter | FortiGate / FortiOS 7.2.0 - Fortinet Documentation⁷

NEW QUESTION 10

.....

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](#)