NSE7_EFW-7.2 Q&As

Fortinet NSE 7 - Enterprise Firewall 7.2

Pass Fortinet NSE7_EFW-7.2 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.leads4pass.com/nse7_efw-7-2.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Fortinet Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

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.

Correct Answer: C

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

QUESTION 2

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_s

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.

Correct Answer: BC

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.

QUESTION 3

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

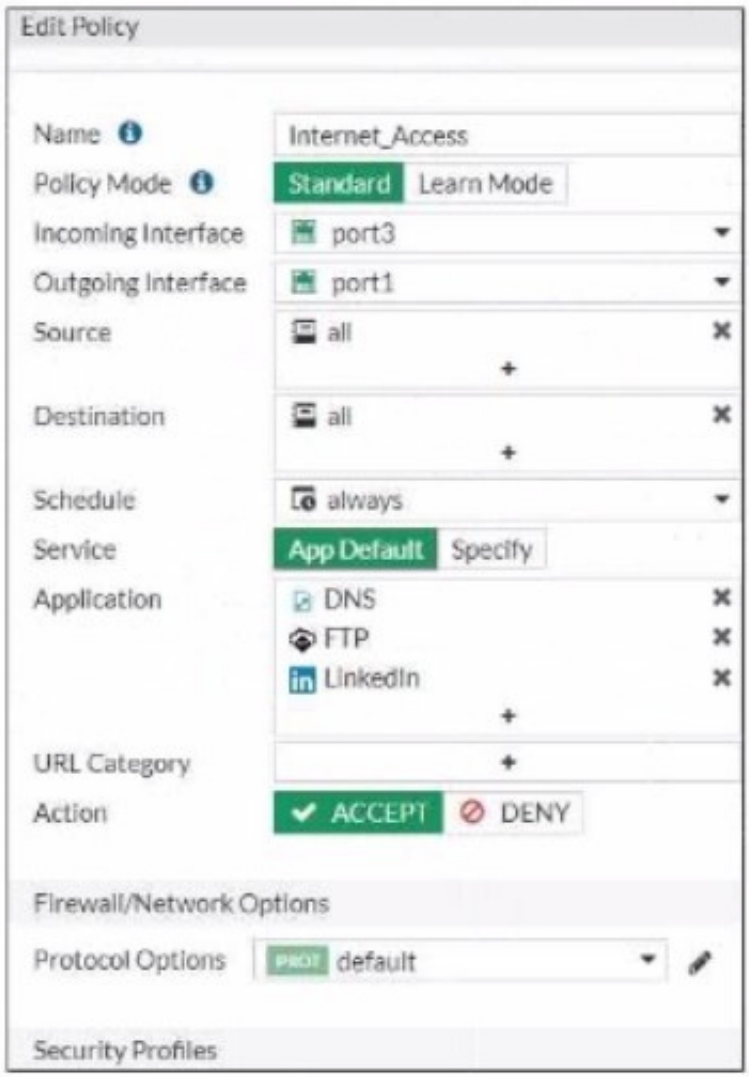
Correct Answer: B

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

QUESTION 4

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

Correct Answer: A

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

QUESTION 5

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 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

Correct Answer: B

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.