

Exam : FCP_FGT_AD-7.4

**Title : FCP - FortiGate 7.4
Administrator**

Version : DEMO

1.Refer to the exhibit.

```

FGT1 # get router info routing-table all
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       V - BGP VPNv4
       * - candidate default

Routing table for VRF=0
S       0.0.0.0/0 [10/0] via 172.20.121.2, port1, [1/0]
C       172.20.121.0/24 is directly connected, port1
C       172.20.168.0/24 is directly connected, port2
C       172.20.167.0/24 is directly connected, port3
S       10.20.30.0/26 [10/0] via 172.20.168.254, port2, [1/0]
S       10.20.30.0/24 [10/0] via 172.20.167.254, port3, [1/0]
S       10.30.20.0/24 [10/0] via 172.20.121.2, port1, [1/0]

```

Which route will be selected when trying to reach 10.20.30.254?

- A. 10.20.30.0/24 [10/0] via 172.20.167.254, port3, [1/0]
- B. 10.30.20.0/24 [10/0] via 172.20.121.2, port1, [1/0]
- C. 10.20.30.0/26 [10/0] via 172.20.168.254, port2, [1/0]
- D. 0.0.0.0/0 [10/0] via 172.20.121.2, port1, [1/0]

Answer: A

Explanation:

The correct route to reach 10.20.30.254 would be:

- A. 10.20.30.0/24 [10/0] via 172.20.167.254, port3, [1/0]

This route is more specific (10.20.30.0/24) compared to the other routes (10.20.30.0/26 and 10.30.20.0/24) and would therefore be selected as the best match.

2.Which two IP pool types are useful for carrier-grade NAT deployments? (Choose two.)

- A. Port block allocation
- B. Fixed port range
- C. One-to-one
- D. Overload

Answer: A,B

Explanation:

The two IP pool types that are useful for carrier-grade NAT (CGNAT) deployments are:

- A. Port block allocation
- B. Fixed port range

A. Port block allocation: In this method, a range of ports is allocated to each internal IP address. This allows multiple internal devices to share the same public IP address but use different port ranges, enabling more efficient use of IP addresses.

B. Fixed port range: This method allocates a fixed range of ports to each internal IP address. It is similar to port block allocation but restricts the port range to a fixed set of ports for each internal IP address, which can be useful for certain applications or scenarios.

Both port block allocation and fixed port range allocation are commonly used in CGNAT deployments to manage the mapping of internal private IP addresses to public IP addresses and ports, allowing for efficient use of limited IPv4 addresses.

3.What is eXtended Authentication (XAuth)?

- A. It is an IPsec extension that forces remote VPN users to authenticate using their local ID.
- B. It is an IPsec extension that forces remote VPN users to authenticate using their credentials (username and password).
- C. It is an IPsec extension that authenticates remote VPN peers using a pre-shared key.
- D. It is an IPsec extension that authenticates remote VPN peers using digital certificates.

Answer: B

Explanation:

The correct answer is:

- B. It is an IPsec extension that forces remote VPN users to authenticate using their credentials (username and password).

eXtended Authentication (XAuth) is an IPsec extension that adds additional authentication for remote VPN users after the initial IPsec phase 1 and phase 2 negotiations. XAuth requires users to provide their credentials (username and password) in addition to the standard IPsec authentication, enhancing the security of the VPN connection.

4.What must you configure to enable proxy-based TCP session failover?

- A. You must configure ha-configuration-sync under configure system ha.
- B. You do not need to configure anything because all TCP sessions are automatically failed over.
- C. You must configure session-pickup-enable under configure system ha.
- D. You must configure session-pickup-connectionless enable under configure system ha.

Answer: C

Explanation:

The correct answer is:

- C. You must configure session-pickup-enable under configure system ha.

To enable proxy-based TCP session failover on a Fortinet FortiGate firewall, you must configure the session-pickup-enable setting under the high availability (HA) configuration. This setting allows the firewall to pick up and maintain TCP sessions after a failover event, ensuring continuity of service for established connections.

5.An administrator needs to inspect all web traffic (including Internet web traffic) coming from users connecting to the SSL-VPN.

How can this be achieved?

- A. Assigning public IP addresses to SSL-VPN users
- B. Configuring web bookmarks
- C. Disabling split tunneling
- D. Using web-only mode

Answer: C

Explanation:

The correct answer is: C. Disabling split tunneling

Split tunneling allows VPN users to access both local and remote networks simultaneously. However, if you want to inspect all web traffic, including Internet traffic, coming from users connecting to the SSL-VPN, you should disable split tunneling. Disabling split tunneling forces all user traffic through the VPN tunnel, allowing you to inspect and control the traffic more effectively.