NSE8_812 Q&As

Network Security Expert 8 Written Exam

Pass Fortinet NSE8_812 Exam with 100% Guarantee

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

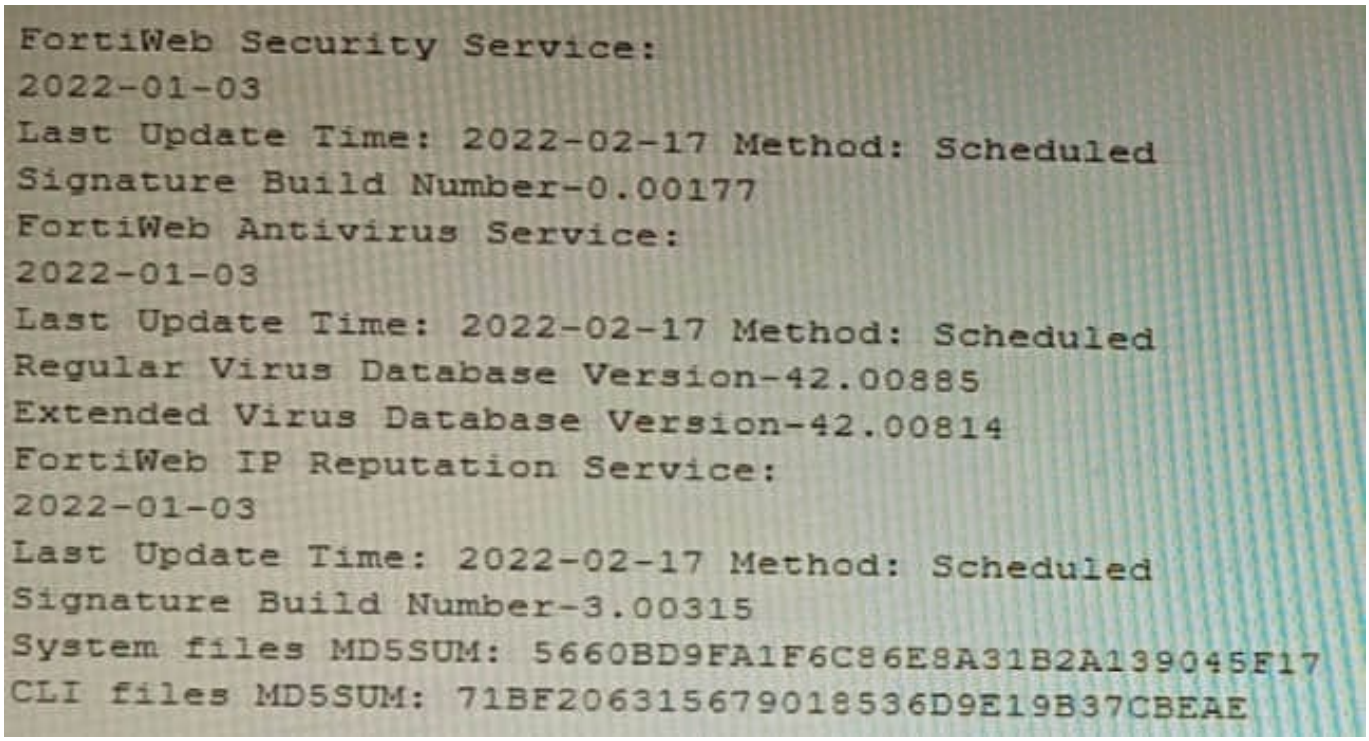
https://www.pass2lead.com/nse8_812.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

Refer to the CLI output:



Given the information shown in the output, which two statements are correct? (Choose two.)

A. Geographical IP policies are enabled and evaluated after local techniques.

B. Attackers can be blocked before they target the servers behind the FortiWeb.

C. The IP Reputation feature has been manually updated

D. An IP address that was previously used by an attacker will always be blocked

E. Reputation from blacklisted IP addresses from DHCP or PPPoE pools can be restored

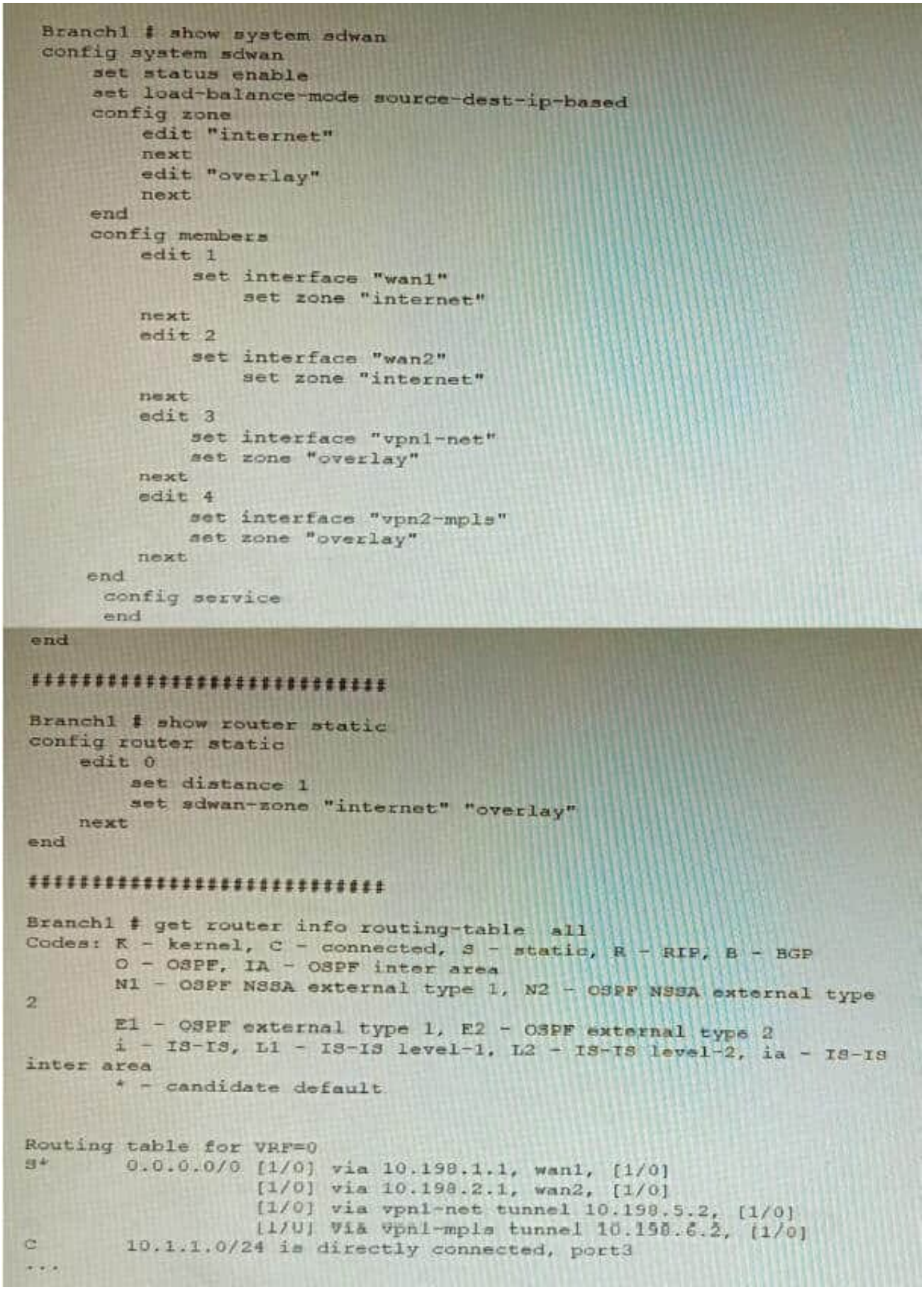
Correct Answer: BE

Explanation: The CLI output shown in the exhibit indicates that FortiWeb has enabled IP Reputation feature with local techniques enabled and geographical IP policies enabled after local techniques (set geoip-policy-order after-local). IP Reputation feature is a feature that allows FortiWeb to block or allow traffic based on the reputation score of IP addresses, which reflects their past malicious activities or behaviors. Local techniques are methods that FortiWeb uses to dynamically update its own blacklist based on its own detection of attacks or violations from IP addresses (such as signature matches, rate limiting, etc.). Geographical IP policies are rules that FortiWeb uses to block or allow traffic based on the geographical location of IP addresses (such as country, region, city, etc.). Therefore, based on the output, one correct statement is that attackers can be blocked before they target the servers behind the FortiWeb. This is because FortiWeb can use IP Reputation feature to block traffic from IP addresses that have a low reputation score or belongto a blacklisted location, which prevents them from reaching the servers and launching attacks. Another correct statement is that reputation from blacklisted IP addresses from DHCP or PPPoE pools can be restored. This is because FortiWeb can use local techniques to remove IP addresses from its own blacklist if they stop sending malicious traffic for a certain period of time (set local-techniques-expire-time), which allows them to regain their reputation and access the

servers. This is useful for IP addresses that are dynamically assigned by DHCP or PPPoE and may change frequently. References: https://docs.fortinet.com/document/fortiweb/6.4.0/administration-guide/19662/ip-reputationhttps://docs.fortinet.com/document/fortiweb/6.4.0/administration- guide/19662/geographical-ip-policies

QUESTION 2

Refer to the exhibit, which shows a Branch1 configuration and routing table. In the SD-WAN implicit rule, you do not want the traffic load balance for the overlay interface when all members are available.



```
Branch1 # show system sdwan
config system sdwan
    set status enable
    set load-balance-mode source-dest-ip-based
    config zone
        edit "internet"
        next
        edit "overlay"
        next
    end
    config members
        edit 1
            set interface "wan1"
                set zone "internet"
        next
        edit 2
            set interface "wan2"
                set zone "internet"
        next
        edit 3
            set interface "vpn1-net"
            set zone "overlay"
        next
        edit 4
            set interface "vpn2-mpls"
            set zone "overlay"
        next
    end
     config service
     end
end

##############################

Branch1 # show router static
config router static
    edit 0
        set distance 1
        set sdwan-zone "internet" "overlay"
    next
end

##############################

Branch1 # 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
       * - candidate default


Routing table for VRF=0
S*      0.0.0.0/0 [1/0] via 10.198.1.1, wan1, [1/0]
                  [1/0] via 10.198.2.1, wan2, [1/0]
                  [1/0] via vpn1-net tunnel 10.198.5.2, [1/0]
                  [1/0] via vpn1-mpls tunnel 10.198.6.2, [1/0]
C       10.1.1.0/24 is directly connected, port3
...
```

In this scenario, which configuration change will meet this requirement?

A. Change the load-balance-mode to source-ip-based.

B. Create a new static route with the internet sdwan-zone only

C. Configure the cost in each overlay member to 10.

D. Configure the priority in each overlay member to 10.

Correct Answer: D

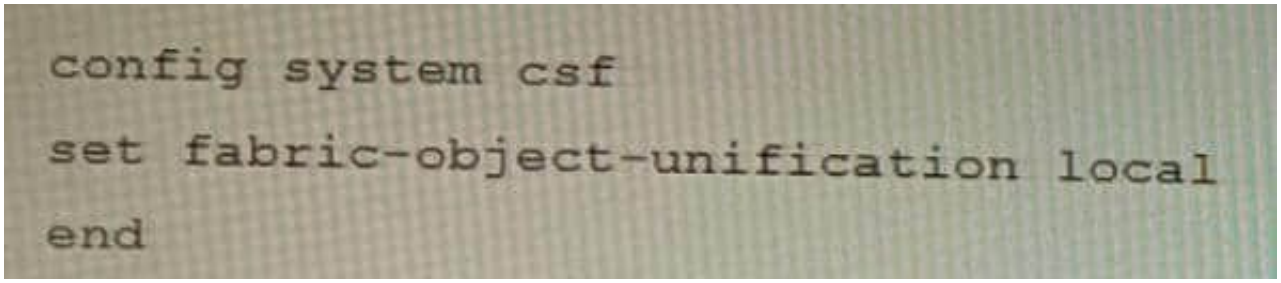
Explanation: The default load balancing mode for the SD-WAN implicit rule is source IP based. This means that traffic will be load balanced evenly between the overlay members, regardless of the member\\'s priority. To prevent traffic from being load balanced, you can configure the priority of each overlay member to 10. This will make the member ineligible for load balancing. The other options are not correct. Changing the load balancing mode to source-IP based will still result in traffic being load balanced. Creating a new static route with the internet sdwan-zone only will not affect the load balancing of the overlay interface. Configuring the cost in each overlay member to 10 will also not affect the load balancing, as the cost is only used when the implicit rule cannot find a match for the destination IP address.

Option	Description
Change the load-balance-mode to source-ip-based	Will still result in traffic being load balanced.
Create a new static route with the internet sdwan-zone only	Will not affect the load balancing of the overlay interface.
Configure the cost in each overlay member to 10	Will not affect the load balancing, as the cost is only used when the implicit rule cannot find a match for the destination IP address.
Configure the priority in each overlay member to 10	Will prevent traffic from being load balanced.

QUESTION 3

Refer to the exhibit.

You have deployed a security fabric with three FortiGate devices as shown in the exhibit. FGT_2 has the following configuration:



FGT_1 and FGT_3 are configured with the default setting. Which statement is true for the synchronization of fabric-objects?

A. Objects from the FortiGate FGT_2 will be synchronized to the upstream FortiGate.

B. Objects from the root FortiGate will only be synchronized to FGT__2.

C. Objects from the root FortiGate will not be synchronized to any downstream FortiGate.

D. Objects from the root FortiGate will only be synchronized to FGT_3.

Correct Answer: C

Explanation: The fabric-object-unification setting on FGT_2 is set to local, which means that objects will not be synchronized to any other FortiGate devices in the security fabric. The default setting for fabric-object-unification is default, which

means that objects will be synchronized from the root FortiGate to all downstream FortiGate devices. Since FGT_2 is not the root FortiGate and the fabric-object-unification setting is set to local, objects from the root FortiGate will not be

synchronized to FGT_2.

Reference:

Synchronizing objects across the Security Fabric:

https://docs.fortinet.com/document/fortigate/6.4.0/administration- guide/880913/synchronizing-objects-across-the-security-fabric

QUESTION 4

What is the benefit of using FortiGate NAC LAN Segments?

A. It provides support for multiple DHCP servers within the same VLAN.

B. It provides physical isolation without changing the IP address of hosts.

C. It provides support for IGMP snooping between hosts within the same VLAN

D. It allows for assignment of dynamic address objects matching NAC policy.

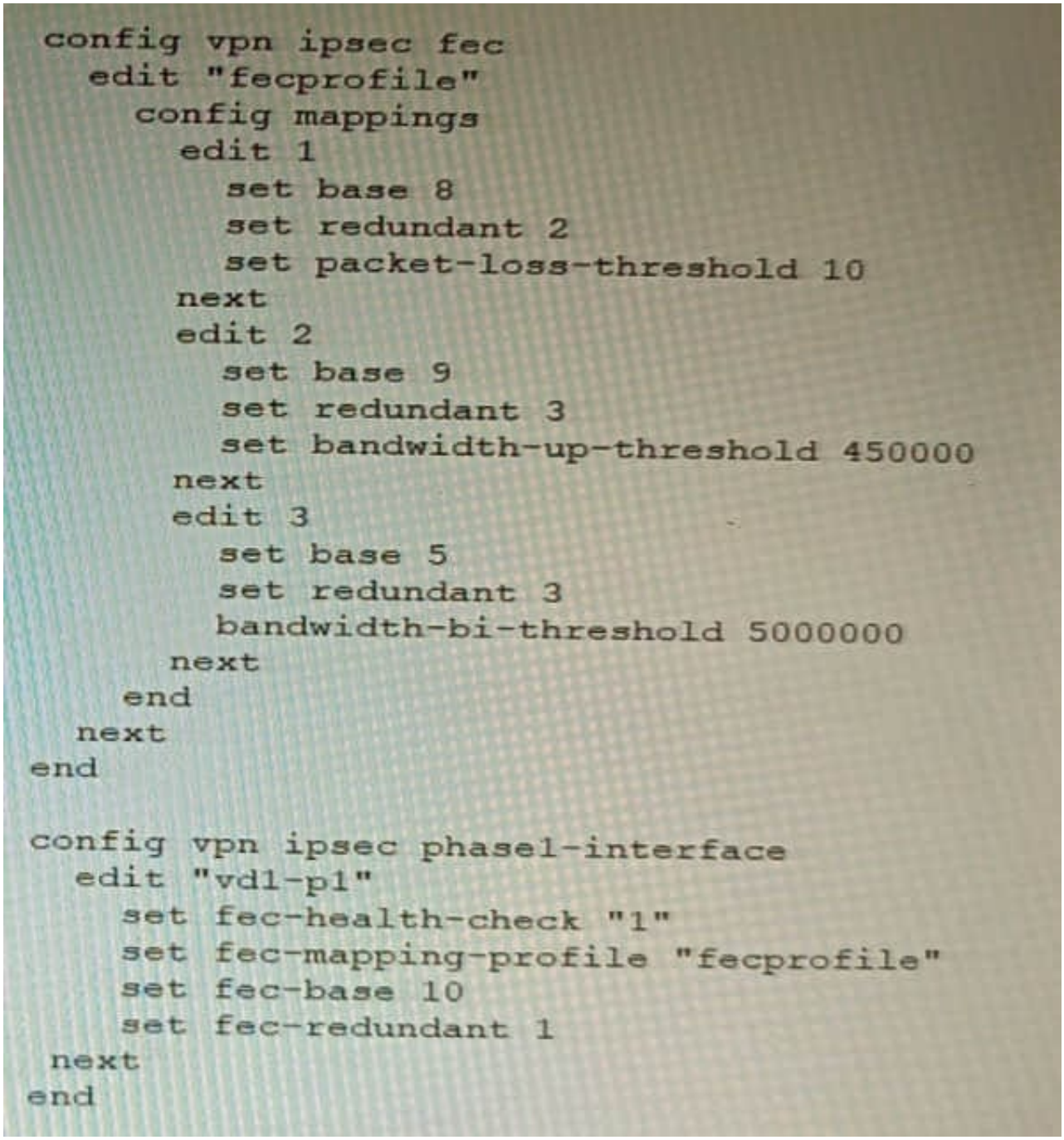
Correct Answer: D

Explanation: FortiGate NAC LAN Segments are a feature that allows users to assign different VLANs to different LAN segments without changing the IP address of hosts or bouncing the switch port. This provides physical isolation while

maintaining firewall sessions and avoiding DHCP issues. One benefit of using FortiGate NAC LAN Segments is that it allows for assignment of dynamic address objects matching NAC policy. This means that users can create firewall policies based on dynamic address objects that match the NAC policy criteria, such as device type, OS type, MAC address, etc. This simplifies firewall policy management and enhances security byapplying different security profiles to different types of devices. References: https://docs.fortinet.com/document/fortigate/7.0.0/new-features/856212/nac-lan-segments- 7-0-1

QUESTION 5

Review the VPN configuration shown in the exhibit.



```
config vpn ipsec fec
  edit "fecprofile"
    config mappings
      edit 1
        set base 8
        set redundant 2
        set packet-loss-threshold 10
      next
      edit 2
        set base 9
        set redundant 3
        set bandwidth-up-threshold 450000
      next
      edit 3
        set base 5
        set redundant 3
        bandwidth-bi-threshold 5000000
      next
    end
  next
end

config vpn ipsec phase1-interface
  edit "vd1-p1"
    set fec-health-check "1"
    set fec-mapping-profile "fecprofile"
    set fec-base 10
    set fec-redundant 1
 next
end
```

What is the Forward Error Correction behavior if the SD-WAN network traffic download is 500 Mbps and has 8% of packet loss in the environment?

A. 1 redundant packet for every 10 base packets

B. 3 redundant packet for every 5 base packets

C. 2 redundant packet for every 8 base packets

D. 3 redundant packet for every 9 base packets

Correct Answer: C

Explanation: The FEC configuration in the exhibit specifies that if the packet loss is greater than 10%, then the FEC mapping will be 8 base packets and 2 redundant packets. The download bandwidth of 500 Mbps is not greater than 950

Mbps, so the FEC mapping is not overridden by the bandwidth setting. Therefore, the FEC behavior will be 2 redundant packets for every 8 base packets.

Here is the explanation of the FEC mappings in the exhibit:

Packet loss greater than 10%: 8 base packets and 2 redundant packets. Upload bandwidth greater than 950 Mbps: 9 base packets and 3 redundant packets.

The mappings are matched from top to bottom, so the first mapping that matches the conditions will be used. In this case, the first mapping matches because the packet loss is greater than 10%. Therefore, the FEC behavior will be 2

redundant packets for every 8 base packets.

Reference: https://docs.fortinet.com/document/fortigate/7.0.0/new- features/169010/adaptive-forward-error-correction-7-0-2