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.passapply.com/nse8_812.html

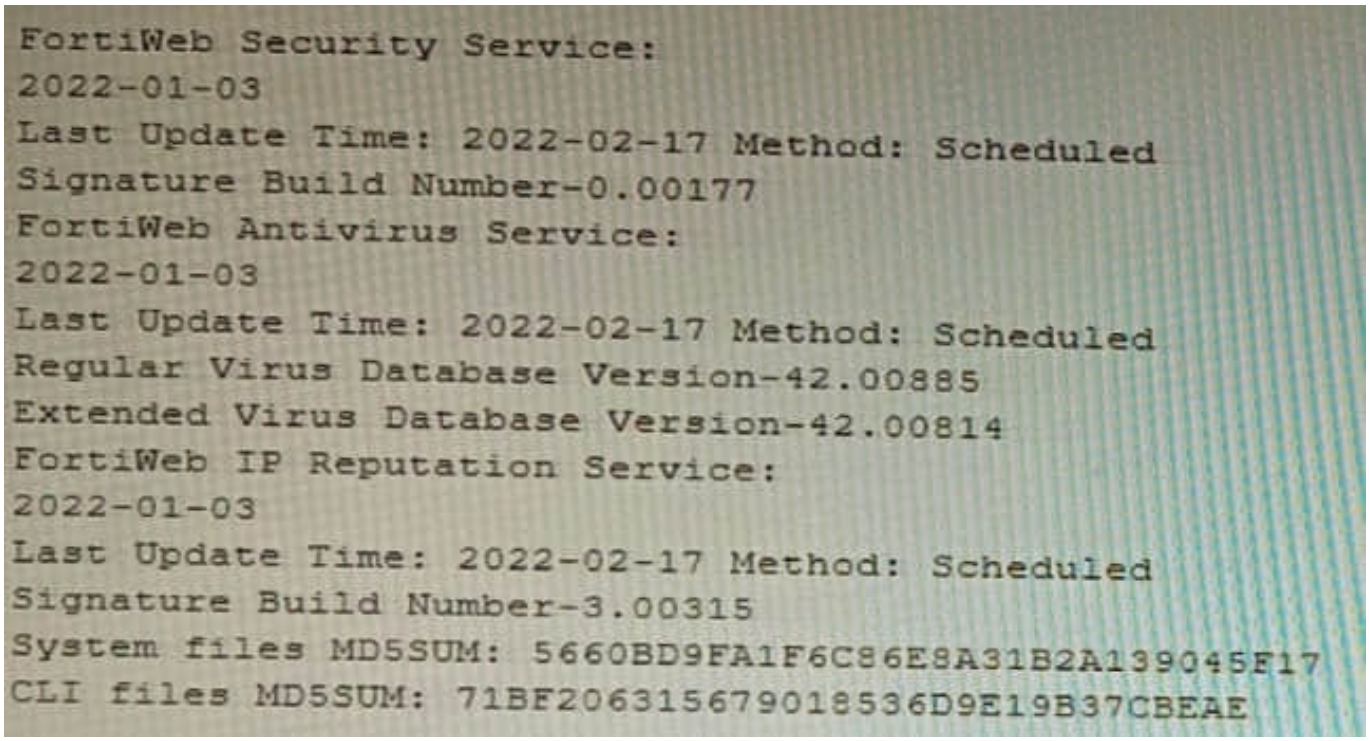
100% Passing Guarantee
100% Money Back Assurance

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

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 exhibits.

Exhibit A

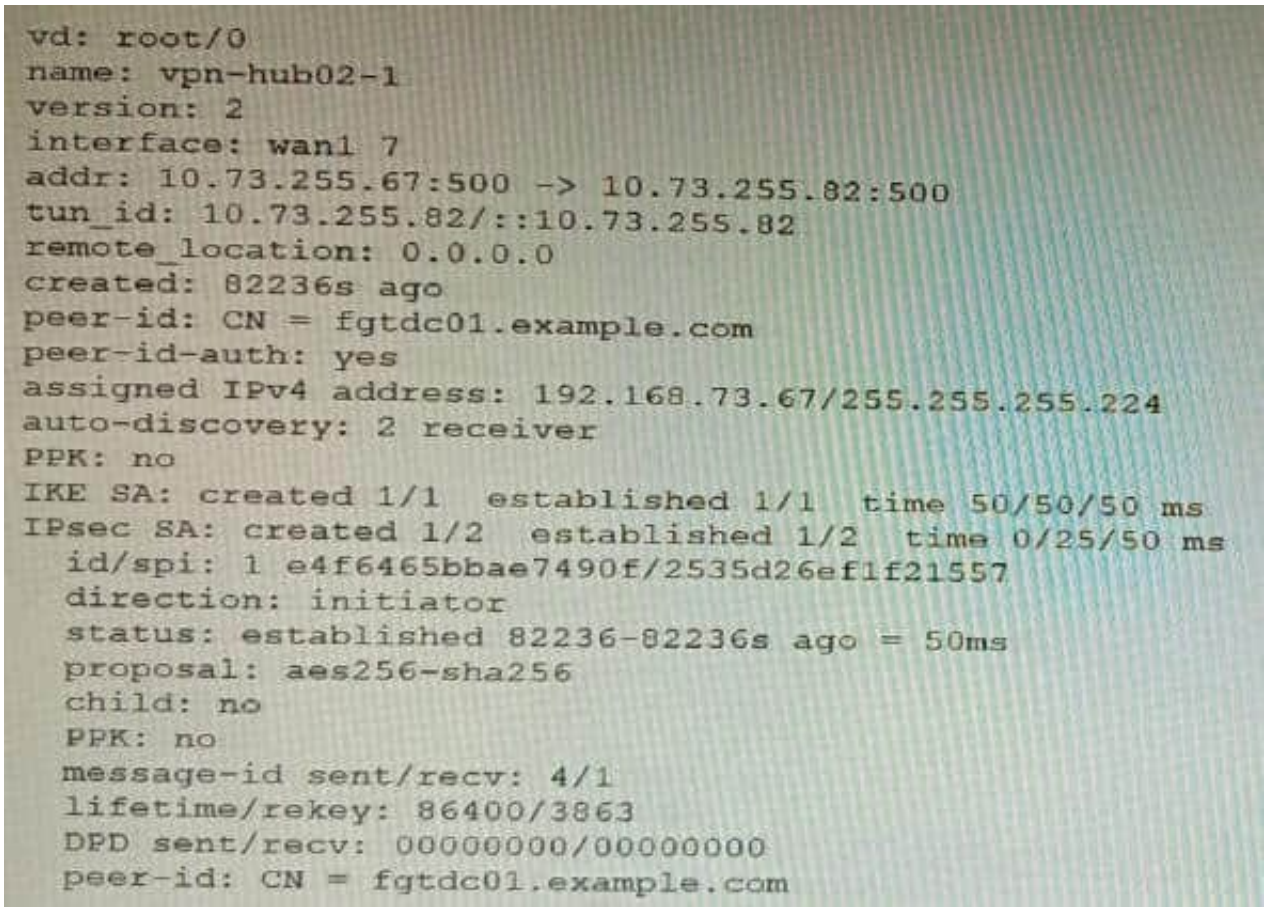


Exhibit B

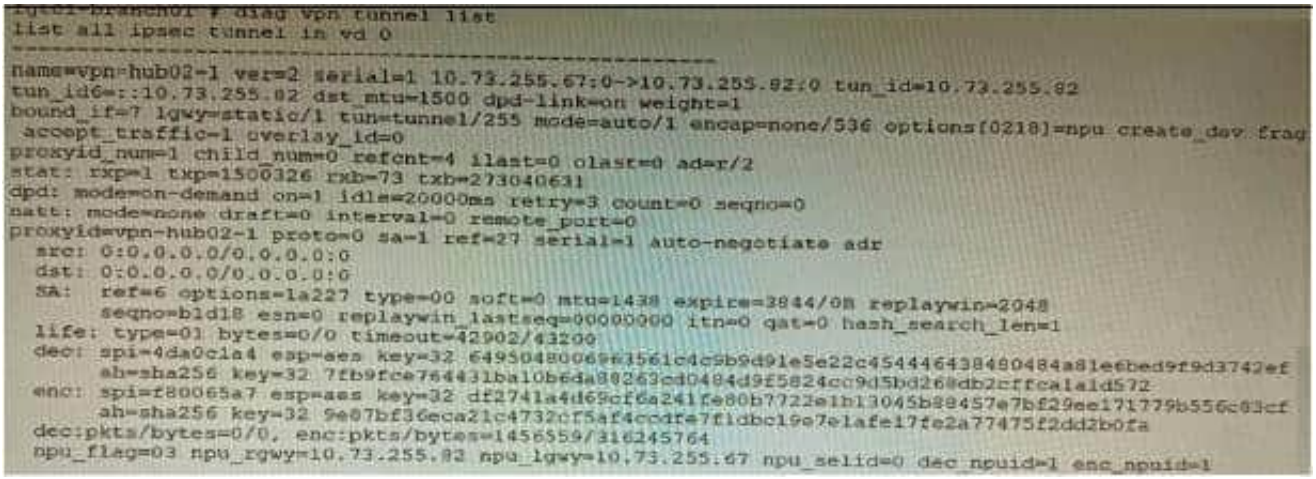
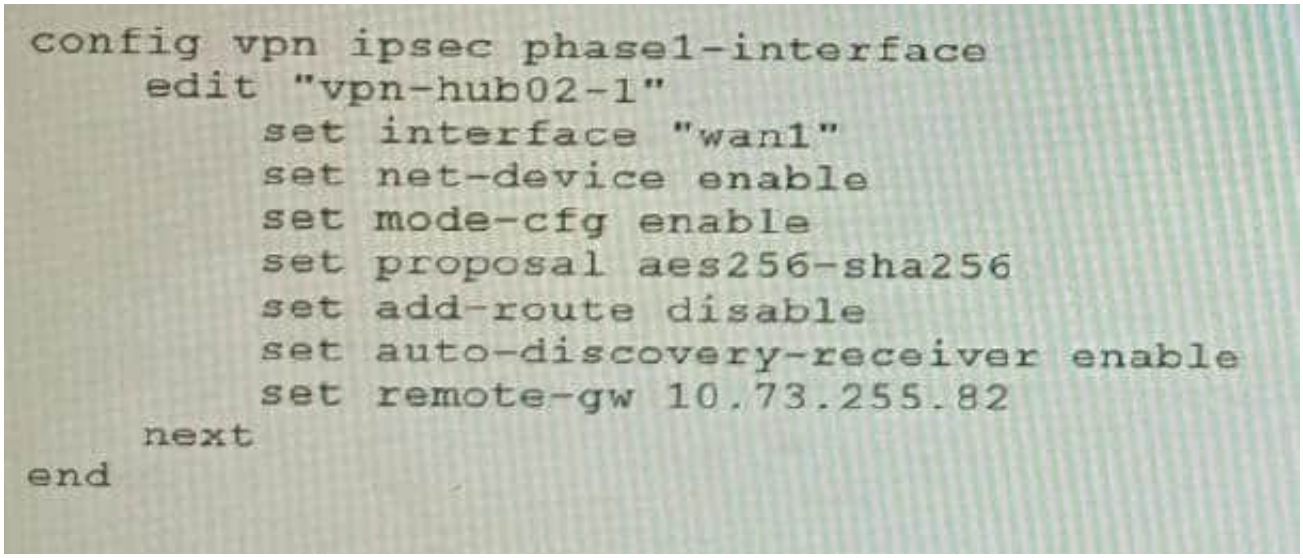


Exhibit C



A customer is trying to set up a VPN with a FortiGate, but they do not have a backup of the configuration. Output during a troubleshooting session is shown in the exhibits A and B and a baseline VPN configuration is shown in Exhibit C Referring to the exhibits, which configuration will restore VPN connectivity?

A.
```
config vpn ipsec phase1-interface
    edit "vpn-hub02-1"
        set ike-version 1
        set authmethod signature
        set certificate "BR01FGTLOCAL"
        set peer "vpn-hub02-1_peer"
    next
end
```

B.
```
config vpn ipsec phase1-interface
    edit "vpn-hub02-1"
        set ike-version 2
        set net-device enable
        set psksecret fortinet
    next
end
```

C.
```
config vpn ipsec phase1-interface
    edit "vpn-hub02-1"
        set ike-version 2
        set authmethod signature
        set npu-offload disable
        set certificate "BR01FGTLOCAL"
        set peer "vpn-hub02-1_peer"
    next
end
```

D.
```
config vpn ipsec phase1-interface
    edit "vpn-hub02-1"
        set ike-version 2
        set authmethod signature
        set certificate "BR01FGTLOCAL"
        set peer "vpn-hub02-1_peer"
    next
end
```

A. Option A

B. Option B

C. Option C

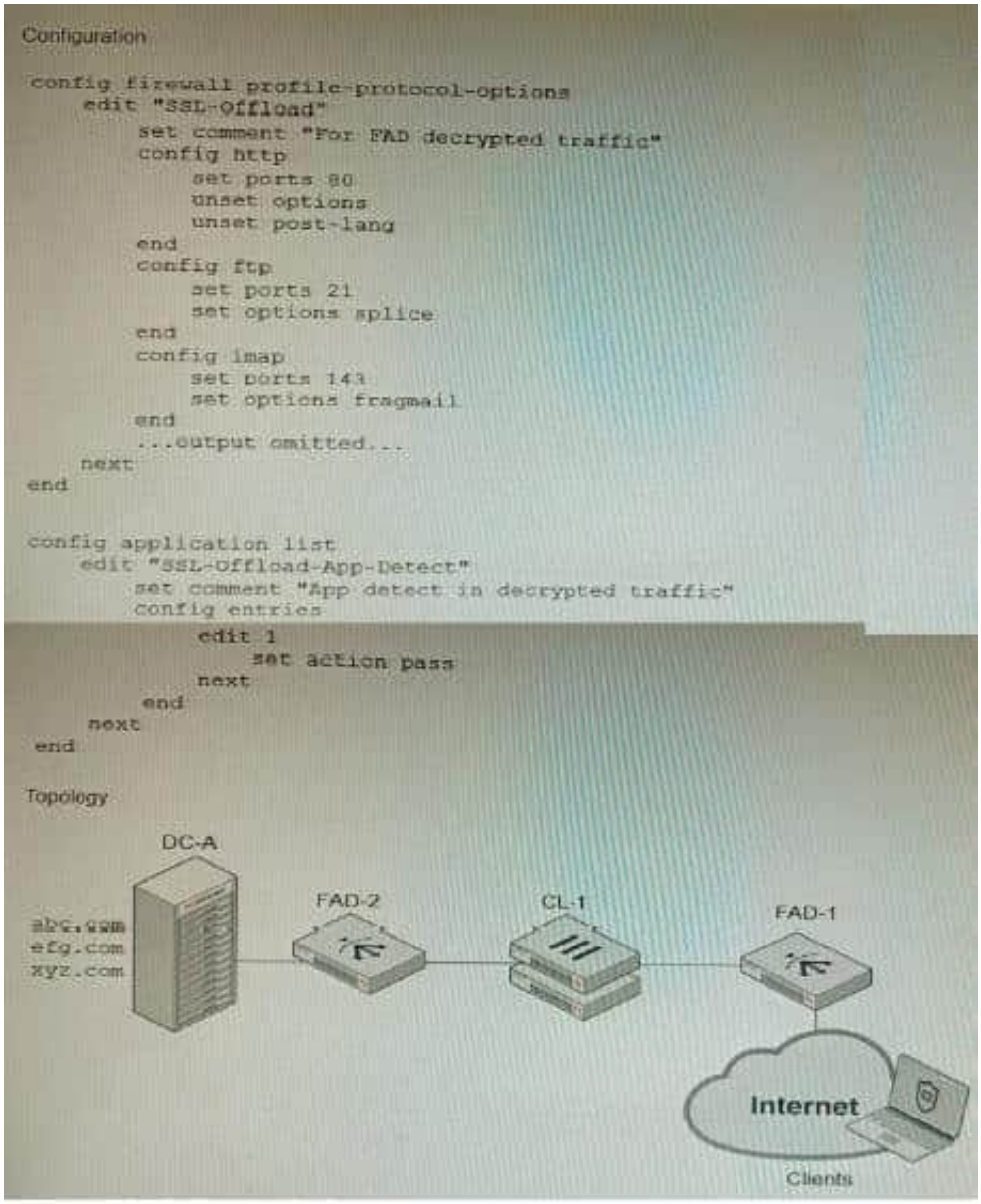
D. Option D

Correct Answer: C

Explanation: The output in Exhibit A shows that the VPN tunnel is not established because the peer IP address is incorrect. The output in Exhibit B shows that the peer IP address is 192.168.1.100, but the baseline VPN configuration in Exhibit C shows that the peer IP address should be 192.168.1.101. To restore VPN connectivity, you need to change the peer IP address in the VPN tunnel configuration to 192.168.1.101. The correct configuration is shown below: config vpn ipsec phase1-interface edit "wan" set peer-ip 192.168.1.101 set peer-id 192.168.1.101 set dhgrp 1 set auth-mode psk set psk SECRET_PSK next end Option A is incorrect because it does not change the peer IP address. Option B is incorrect because it changes the peer IP address to 192.168.1.100, which is the incorrect IP address. Option D is incorrect because it does not include the necessary configuration for the VPN tunnel.

QUESTION 3

Refer to the exhibits.



A FortiGate cluster (CL-1) protects a data center hosting multiple web applications. A pair of FortiADC devices are already configured for SSL decryption (FAD-1), and re-encryption (FAD-2). CL-1 must accept unencrypted traffic from FAD-1,

perform application detection on the plain-text traffic, and forward the inspected traffic to FAD-2.

The SSL-Offload-App-Detect application list and SSL-Offload protocol options profile are applied to the firewall policy handling the web application traffic on CL-1.

Given this scenario, which two configuration tasks must the administrator perform on CL-1? (Choose two.)

A)

```
config firewall profile-protocol-options
    edit SSL-Offload
        config http
            set ssl-offloaded yes
        end
    next
end
```

B)

```
config firewall profile-protocol-options
    edit SSL-Offload
        config https
            set options splice
        end
    next
end
```

C)

```
config application list
    edit SSL-Offload-App-Detect
        set force-inclusion-ssl-di-sigs enable
    next
end
```

D)

```
config application list
    edit SSL-Offload-App-Detect
        set deep-app-inspection enable
    next
end
```

A. Option A

B. Option B

C. Option C

D. Option D

Correct Answer: BC

Explanation: To enable application detection on plain-text traffic that has been decrypted by FortiADC, the administrator must perform two configuration tasks on CL-1:

Enable SSL offloading in the firewall policy and select the SSL-Offload protocol options profile.

Enable application control in the firewall policy and select the SSL-Offload-App- Detect application list. References:

https://docs.fortinet.com/document/fortigate/6.4.0/cookbook/103438/application- detection-on-ssl-offloaded-traffic

QUESTION 4

A customer is planning on moving their secondary data center to a cloud-based IaaS. They want to place all the Oracle-based systems Oracle Cloud, while the other systems will be on Microsoft Azure with ExpressRoute service to their main

data center.

They have about 200 branches with two internet services as their only WAN connections. As a security consultant you are asked to design an architecture using Fortinet products with security, redundancy and performance as a priority.

Which two design options are true based on these requirements? (Choose two.)

A. Systems running on Azure will need to go through the main data center to access the services on Oracle Cloud.

B. Use FortiGate VM for IPSEC over ExpressRoute, as traffic is not encrypted by Azure.

C. Branch FortiGate devices must be configured as VPN clients for the branches\\' internal network to be able to access Oracle services without using public IPs.

D. Two ExpressRoute services to the main data center are required to implement SD-WAN between a FortiGate VM in Azure and a FortiGate device at the data center edge

Correct Answer: AC

A. Systems running on Azure will need to go through the main data center to access the services on Oracle Cloud. This is because the Oracle Cloud is not directly connected to the Azure Cloud. The traffic will need to go through the main

data center in order to reach the Oracle Cloud.

C. Branch FortiGate devices must be configured as VPN clients for the branches\\' internal network to be able to access Oracle services without using public IPs. This is because the Oracle Cloud does not allow direct connections from the

internet. The traffic will need to go through the FortiGate devices in order to reach the Oracle Cloud.

The other options are not correct.

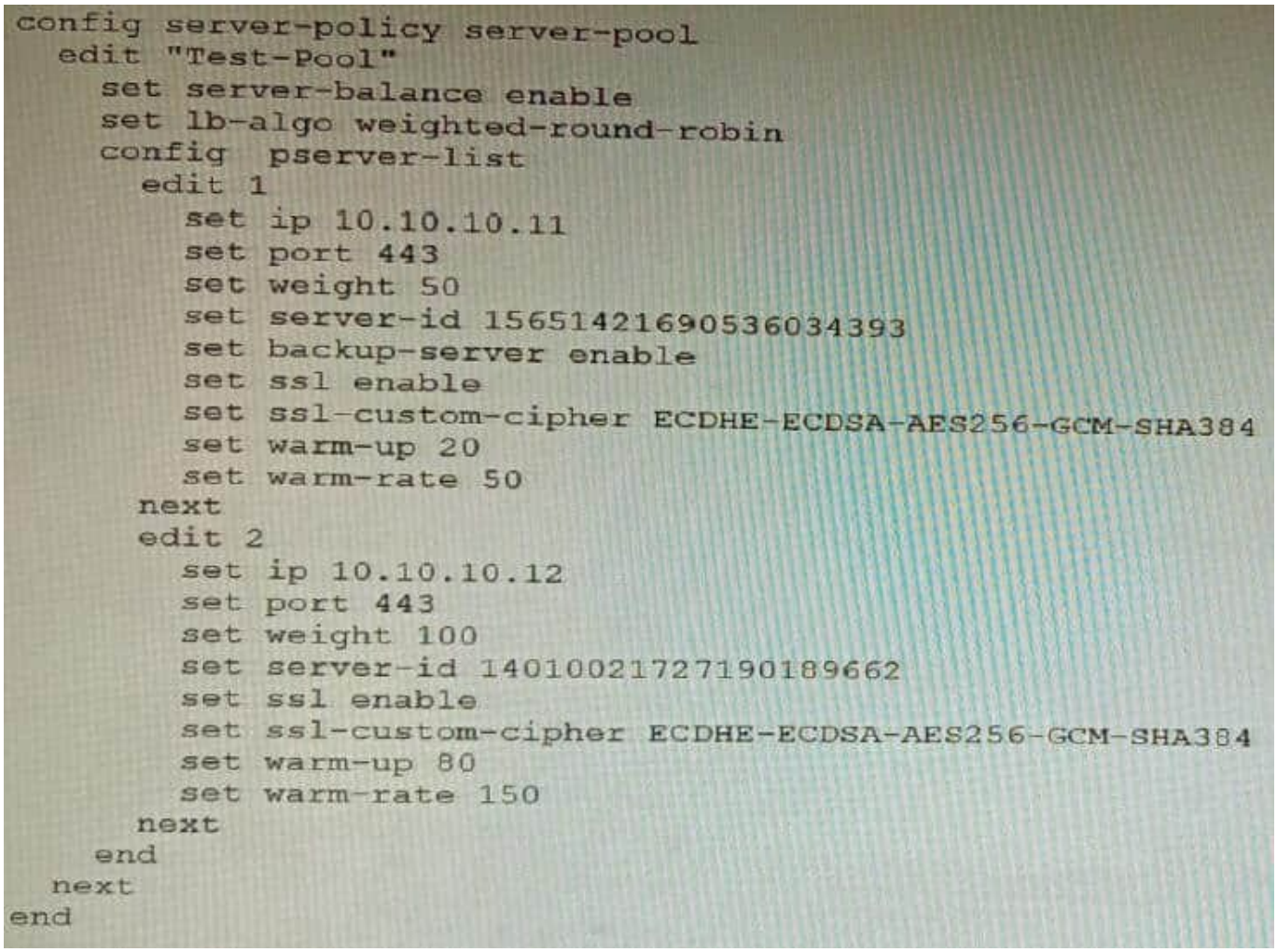
B. Use FortiGate VM for IPSEC over ExpressRoute, as traffic is not encrypted by Azure. This is not necessary. Azure does encrypt traffic over ExpressRoute. D. Two ExpressRoute services to the main data center are required to implement

SD-WAN between a FortiGate VM in Azure and a FortiGate device at the data center edge. This is not necessary. A single ExpressRoute service can be used to implement SD-WAN between a FortiGate VM in Azure and a FortiGate device at

the data center edge.

QUESTION 5

Refer to the exhibit.



```
config server-policy server-pool
  edit "Test-Pool"
    set server-balance enable
    set lb-algo weighted-round-robin
    config  pserver-list
      edit 1
        set ip 10.10.10.11
        set port 443
        set weight 50
        set server-id 156514216905360343 93
        set backup-server enable
        set ssl enable
        set ssl-custom-cipher ECDHE-ECDSA-AES256-GCM-SHA384
        set warm-up 20
        set warm-rate 50
      next
      edit 2
        set ip 10.10.10.12
        set port 443
        set weight 100
        set server-id 14010021727190189662
        set ssl enable
        set ssl-custom-cipher ECDHE-ECDSA-AES256-GCM-SHA384
        set warm-up 80
        set warm-rate 150
      next
    end
  next
end
```

A FortiWeb appliance is configured for load balancing web sessions to internal web servers. The Server Pool is configured as shown in the exhibit.

How will the sessions be load balanced between server 1 and server 2 during normal operation?

A. Server 1 will receive 25% of the sessions, Server 2 will receive 75% of the sessions

B. Server 1 will receive 20% of the sessions, Server 2 will receive 66.6% of the sessions

C. Server 1 will receive 33.3% of the sessions, Server 2 will receive 66 6% of the sessions

D. Server 1 will receive 0% of the sessions Server 2 will receive 100% of the sessions

Correct Answer: A

Explanation: The Server Pool in the exhibit is configured with a weight of 20 for server 1 and a weight of 60 for server 2. This means that server 1 will receive 20% of the sessions and server 2 will receive 75% of the sessions.

The following formula is used to calculate the load balancing between servers in a Server Pool:

weight_of_server_1 / (weight_of_server_1 + weight_of_server_2) In this case, the formula is:

20 / (20 + 60) = 20 / 80 = 0.25 = 25%

Therefore, server 1 will receive 25% of the sessions and server 2 will receive 75% of the sessions.