NSE8_812^Q&As

Network Security Expert 8 Written Exam

QUESTION 1

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

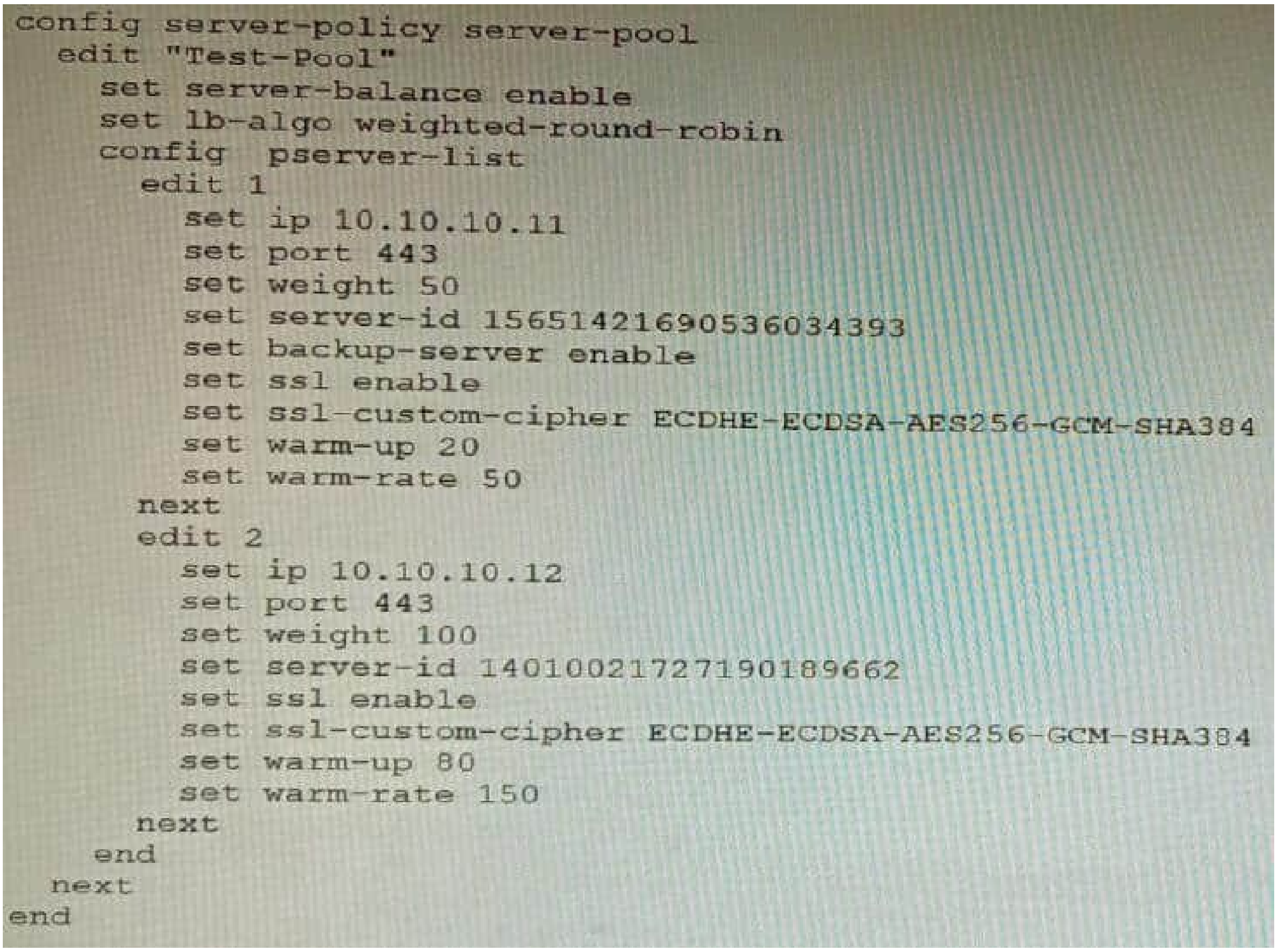
D. It allows for assignment of dynamic address objects matching NAC policy.

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 2

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 15651421690536034393
        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:

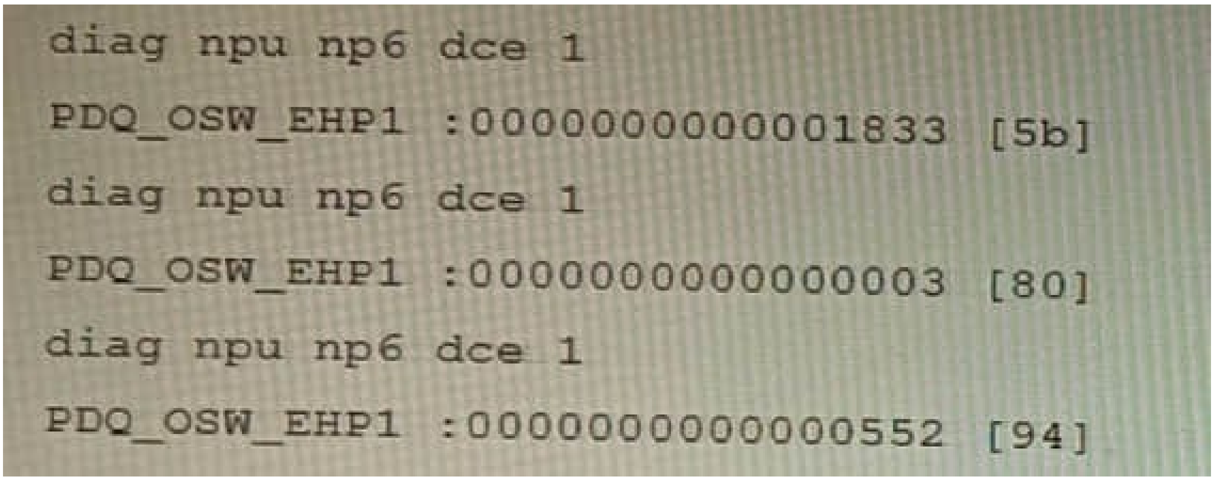
weight_of_server_1 / (weight_of_server_1 + weight_of_server_2) In this case, the formula is:

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.

QUESTION 3

You are running a diagnose command continuously as traffic flows through a platform with NP6 and you obtain the following output: Given the information shown in the output, which two statements are true? (Choose two.)



```
diag npu np6 dce 1
PDQ_OSW_EHP1  :0000000000001833  [5b]
diag npu np6 dce 1
PDQ_OSW_EHP1  :0000000000000003  [80]
diag npu np6 dce 1
PDQ_OSW_EHP1  :0000000000000552  [94]
```

A. Enabling bandwidth control between the ISF and the NP will change the output

B. The output is showing a packet descriptor queue accumulated counter

C. Enable HPE shaper for the NP6 will change the output

D. Host-shortcut mode is enabled.

E. There are packet drops at the XAUI.

Correct Answer: BE

Explanation: The diagnose command shown in the output is used to display information about NP6 packet descriptor queues. The output shows that there are 16 NP6 units in total, and each unit has four XAUI ports (XA0-XA3). The output also shows that there are some non-zero values in the columns PDQ ACCU (packet descriptor queue accumulated counter) and PDQ DROP (packet descriptor queue drop counter). These values indicate that there are some packet descriptor queues that have reached their maximum capacity and have dropped some packets at the XAUI ports. This could be caused by congestion or misconfiguration of the XAUI ports or the ISF (Internal Switch Fabric). References:https://docs.fortinet.com/document/fortigate/7.0.0/cli- reference/19662/diagnose-np6-pdq

The output is showing a packet descriptor queue accumulated counter, which is a measure of the number of packets that have been dropped by the NP6 due to congestion. The counter will increase if there are more packets than the NP6 can handle, which can happen if the bandwidth between the ISF and the NP is not sufficient or if the HPE shaper is enabled. The output also shows that there are packet drops at the XAUI, which is the interface between the NP6 and the FortiGate\\'s backplane. This means that the NP6 is not able to keep up with the traffic and is dropping packets. The other statements are not true. Host-shortcut mode is not enabled, and enabling bandwidth control between the ISF and the NP will not change the output. HPE shaper is a feature that can be enabled to improve performance, but it will not change the output of the diagnose command. Reference: https://docs.fortinet.com/document/fortigate/7.4.0/hardware-acceleration/48875/diagnose-npu-np6-dce-np6-id-number-of-dropped-np6-packets

QUESTION 4

A remote worker requests access to an SSH server inside the network. You deployed a ZTNA Rule to their FortiClient. You need to follow the security requirements to inspect this traffic. Which two statements are true regarding the requirements? (Choose two.)

A. FortiGate can perform SSH access proxy host-key validation.

B. You need to configure a FortiClient SSL-VPN tunnel to inspect the SSH traffic.

C. SSH traffic is tunneled between the client and the access proxy over HTTPS

D. Traffic is discarded as ZTNA does not support SSH connection rules

Correct Answer: AC

Explanation: ZTNA supports SSH connection rules that allow remote workers to access SSH servers inside the network through an HTTPS tunnel between the client and the access proxy (FortiGate). The access proxy acts as an SSH client to connect to the real SSH server on behalf of the user, and performs host-key validation to verify the identity of the server. The user can use any SSH client that supports HTTPS proxy settings, such as PuTTY or OpenSSH. References:https://docs.fortinet.com/document/fortigate/7.0.0/ztna- deployment/899992/configuring-ztna-rules-to-control-access

QUESTION 5

A customer\\'s cybersecurity department needs to implement security for the traffic between two VPCs in AWS, but these belong to different departments within the company. The company uses a single region for all their VPCs.

Which two actions will achieve this requirement while keeping separate management of each department\\'s VPC? (Choose two.)

A. Create a transit VPC with a FortiGate HA cluster, connect to the other two using VPC peering, and use routing tables to force traffic through the FortiGate cluster.

B. Create an 1AM account for the cybersecurity department to manage both existing VPC, create a FortiGate HA Cluster on each VPC and IPSEC VPN to force traffic between the VPCs through the FortiGate clusters

C. Migrate all the instances to the same VPC and create 1AM accounts for each department, then implement a new subnet for a FortiGate auto-scaling group and use routing tables to force the traffic through the FortiGate cluster.

D. Create a VPC with a FortiGate auto-scaling group with a Transit Gateway attached to the three VPC to force routing through the FortiGate cluster

Correct Answer: AD

Explanation: To implement security for the traffic between two VPCs in AWS, while keeping separate management of each department\\'s VPC, two possible actions are: Create a transit VPC with a FortiGate HA cluster, connect to the other two using VPC peering, and use routing tables to force traffic through the FortiGate cluster. This option allows the cybersecurity department to manage the transit VPC and apply security policies on the FortiGate cluster, while the other departments can manage their own VPCs and instances. The VPC peering connections enable direct communication between the VPCs without using public IPs or gateways. The routing tables can be configured to direct all inter-VPC traffic to the transit VPC. Create a VPC with a FortiGate auto-scaling group with a Transit Gateway attached to the three VPCs to force routing through the FortiGate cluster. This option also allows the cybersecurity department to manage the security VPC and apply security policies on the FortiGate cluster, while the other departments can manage their own VPCs and instances. The Transit Gateway acts as a network hub that connects multiple VPCs and on-premises networks. The routing tables can be configured to direct all inter-VPC traffic to the security VPC. References: https://docs.fortinet.com/document/fortigate-public-cloud/7.2.0/aws-administration- guide/506140/connecting-a-local-fortigate-to-an-aws-vpc-vpn https://docs.fortinet.com/document/fortigate-public-cloud/7.0.0/sd-wan- architecture-forenterprise/166334/sd-wan-configuration