

Free Questions for FCP_WCS_AD-7.4

Shared by Head on 04-10-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

An administrator is adding a web application to be protected by FortiWeb Cloud.

Which two steps are necessary to successfully onboard the application? (Choose two.)

An administrator is adding a web application to be protected by FortiWeb Cloud.

Which two steps are necessary to successfully onboard the application? (Choose two.)

Options:

- A- Wait for the EC2 instance to be created.
- B- Provide a web application name.
- C- Create DNS records in the domain server that hosts the application.
- D- Enable a content delivery network (CDN) in the same region where your application is located.

Answer:

B, C

Explanation:

Web Application Name:

When onboarding a web application to be protected by FortiWeb Cloud, you need to provide a name for the web application. This helps in identifying and managing the application within the FortiWeb Cloud console (Option B).

DNS Records:

To ensure that traffic to your web application is correctly routed through FortiWeb Cloud, you must create DNS records in the domain server that hosts your application. This ensures that requests are directed to FortiWeb Cloud for inspection and protection (Option C).

Other Considerations:

Option A (Waiting for the EC2 instance) is incorrect as it is not a necessary step for onboarding a web application to FortiWeb Cloud.

Option D (Enabling a CDN) is not a mandatory step for onboarding but can be part of a broader strategy for improving performance and protection.

FortiWeb Cloud Documentation: [FortiWeb Cloud](#)

Question 2

Question Type: MultipleChoice

Which three statements are correct about VPC flow logs? (Choose three.)

Options:

- A- Flow logs do not capture traffic to and from 169.254.169.254 for instance metadata.
- B- Flow logs do not capture DHCP traffic.
- C- Flow logs can capture traffic to the reserved IP address for the default VPC router.
- D- Flow logs can be used as a security tool to monitor the traffic that is reaching the instance.
- E- Flow logs can capture real-time log streams for the network interfaces.

Answer:

A, B, D

Explanation:

Instance Metadata Traffic:

VPC flow logs do not capture traffic to and from the link-local address 169.254.169.254, which is used for accessing instance metadata (Option A).

DHCP Traffic:

DHCP traffic is not captured by VPC flow logs. This is because DHCP relies on broadcast and multicast traffic, which is excluded from flow logs (Option B).

Security Monitoring:

VPC flow logs can be used as a security tool to monitor the traffic that is reaching the instances. By analyzing the flow logs, administrators can detect suspicious activities and troubleshoot connectivity issues (Option D).

Other Considerations:

Option C is incorrect because flow logs do capture traffic to the reserved IP address of the default VPC router.

Option E is incorrect as VPC flow logs do not provide real-time log streams but rather capture data at intervals and deliver them to CloudWatch or S3.

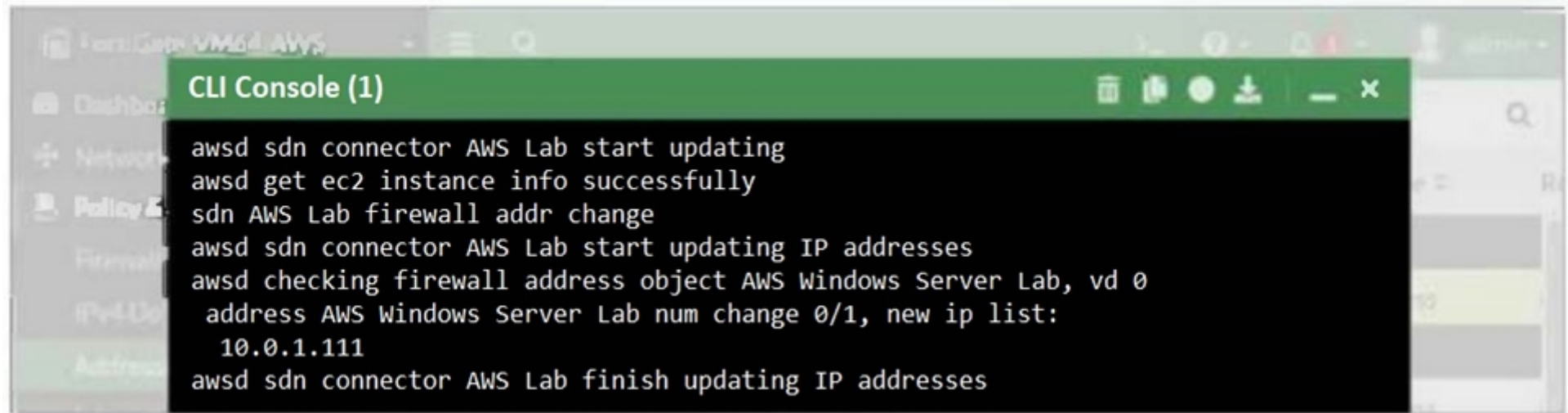
[AWS VPC Flow Logs Documentation: VPC Flow Logs](#)

[AWS Networking and Security: AWS Security Monitoring](#)

Question 3

Question Type: MultipleChoice

Refer to the exhibit.

A screenshot of a FortiGate CLI console window titled "CLI Console (1)". The window shows a series of log messages from an SDN connector. The messages indicate that the connector successfully updated IP addresses for a dynamic address object named "AWS Windows Server Lab". The new IP address listed is 10.0.1.111. The console output is as follows:

```
awsd sdn connector AWS Lab start updating
awsd get ec2 instance info successfully
sdn AWS Lab firewall addr change
awsd sdn connector AWS Lab start updating IP addresses
awsd checking firewall address object AWS Windows Server Lab, vd 0
address AWS Windows Server Lab num change 0/1, new ip list:
10.0.1.111
awsd sdn connector AWS Lab finish updating IP addresses
```

What two conclusions can you draw from the FortiGate debug output? (Choose two.)

Options:

- A-** The dynamic address object is automatically updated if the IP changes.
- B-** The address object AWS Windows Server Lab can be manually changed on FortiGate.
- C-** The SDN connector is correctly configured and authorized.
- D-** The AWS user account used for software-defined network (SDN) integration must have full administrative rights.

Answer:

A, C

Explanation:

Dynamic Address Object Update:

The debug output shows that the IP address of the AWS Windows Server Lab has been updated automatically, indicating that the dynamic address object feature is working as intended. This allows FortiGate to adapt to changes in the IP addresses of AWS instances dynamically (Option A).

SDN Connector Configuration:

The messages in the debug output confirm that the SDN connector is able to retrieve instance information and update the firewall address objects successfully. This implies that the SDN connector is correctly configured and has the necessary permissions (Option C).

Manual Change and Permissions:

Option B is incorrect because while the address object could theoretically be changed manually, this is not inferred from the debug output.

Option D is incorrect because the debug output does not indicate that the AWS user account must have full administrative rights. The required permissions are typically more scoped to specific actions related to SDN.

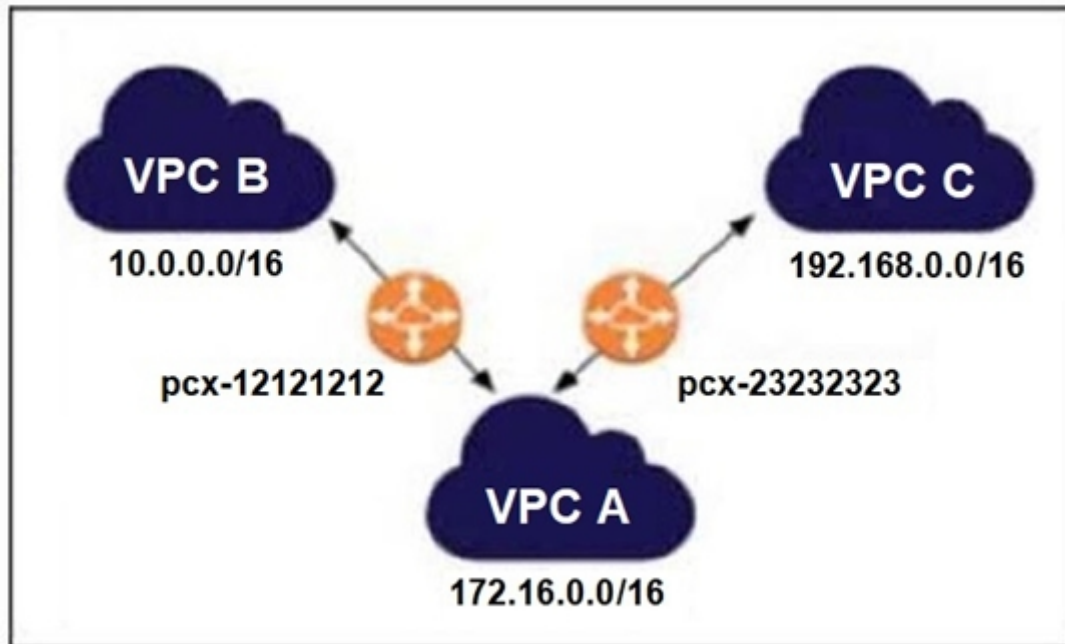
FortiGate AWS Integration Guide: FortiGate on AWS

[AWS IAM Policies for SDN: AWS IAM Policies](#)

Question 4

Question Type: MultipleChoice

Refer to the exhibit.



Which statement is correct about the VPC peering connections shown in the exhibit?

Options:

- A-** To route packets directly from VPC B to VPC C through VPC A, you must add a route for network 192.168.0.0/16 in the VPC A routing table.
- B-** You cannot route packets directly from VPC B to VPC C through VPC A.
- C-** You can associate VPC ID pcx-23232323 with VPC B to form a VPC peering connection between VPC B and VPC C.
- D-** You cannot create a separate VPC peering connection between VPC B and VPC C to route packets directly.

Answer:

B

Explanation:

Understanding VPC Peering:

VPC peering connections allow instances in one VPC to communicate with instances in another VPC. Peering is a one-to-one relationship between two VPCs.

Transit Routing Limitation:

AWS VPC peering connections do not support transitive peering. This means that a packet originating in VPC B cannot be routed through VPC A to reach VPC C. Each pair of VPCs must have its own peering connection.

Routing Table Configuration:

Even if you add a route in the VPC A routing table for the 192.168.0.0/16 network, it won't allow VPC B to communicate with VPC C because of the non-transitive nature of VPC peering.

Comparison with Other Options:

Option A is incorrect because adding a route in VPC A does not overcome the limitation of non-transitive peering.

Option C is incorrect because associating pcx-23232323 with VPC B is not how VPC peering works.

Option D is incorrect because you can create a separate peering connection between VPC B and VPC C, which is the required approach for communication between these VPCs.

[AWS VPC Peering Guide: VPC Peering](#)

[Limitations of VPC Peering: AWS VPC Peering Limitations](#)

Question 5

Question Type: MultipleChoice

Your organization is deciding between deploying an active-active (A-A) or active-passive (A-P) FortiGate high availability (HA) cluster in AWS cloud.

Which two statements are true about A-A clusters compared to A-P clusters? (Choose two.)

Options:

- A-** For A-A clusters, FortiGate must perform SNAT inbound to ensure symmetric traffic flow.
- B-** A-A clusters rely on API calls for sfailovers.
- C-** A-A clusters always require a load balancer.
- D-** A-A clusters can use a software-defined network (SDN) to perform a failover.

Answer:

A, C

Explanation:

Symmetric Traffic Flow with SNAT:

In active-active (A-A) clusters, symmetric traffic flow is essential for maintaining session integrity across multiple instances. Source Network Address Translation (SNAT) is performed inbound to ensure that return traffic is routed correctly (Option A).

Load Balancer Requirement:

A-A clusters require a load balancer to distribute incoming traffic evenly across the active instances. This is crucial for balancing the load and providing high availability (Option C).

API Calls and Failovers:

Option B is incorrect because failovers in A-A clusters do not typically rely on API calls but are managed by the load balancer and the clustering mechanism itself.

Software-Defined Network (SDN) Failover:

Option D is incorrect as SDN is not specifically required for performing failovers in A-A clusters. The failover mechanism is typically managed by the load balancer and FortiGate's clustering technology.

FortiGate High Availability on AWS: FortiGate HA

[AWS Elastic Load Balancing: AWS ELB](#)

Question 6

Question Type: MultipleChoice

AWS native network services offer vast functionality and inter-connectivity between the cloud and on-premises networks.

Which three additional functions can FortiGate for AWS offer to complement the native services offered by AWS? (Choose three.)

Options:

- A- Higher VPN throughput
- B- Web filtering
- C- OSPF over IPsec
- D- Advanced dynamic routing
- E- Secure SD-WAN with application visibility

Answer:

B, C, E

Explanation:

Web Filtering:

FortiGate for AWS offers advanced web filtering capabilities, which allow organizations to control and monitor web access. This feature complements AWS's native security services by providing granular control over web traffic (Option B).

OSPF over IPsec:

FortiGate for AWS can establish dynamic routing protocols such as OSPF (Open Shortest Path First) over IPsec tunnels. This capability enhances network routing flexibility and security, which is not natively provided by AWS (Option C).

Secure SD-WAN with Application Visibility:

FortiGate for AWS provides Secure SD-WAN functionality, offering enhanced application visibility and traffic management. This is a significant addition to AWS's networking services, optimizing application performance and security (Option E).

Comparison with Other Options:

Option A (Higher VPN throughput) is not specifically enhanced by FortiGate as compared to AWS native services.

Option D (Advanced dynamic routing) is partially covered under OSPF over IPsec but is not as specific as the other chosen options.

FortiGate for AWS Documentation: FortiGate on AWS

[AWS Networking and Content Delivery: AWS Networking](#)

Question 7

Question Type: MultipleChoice

Which three statements correctly describe FortiGate Cloud-Native Firewall (CNF)? (Choose three.)

Options:

- A-** It provides carrier-grade protection.
- B-** It scales seamlessly.
- C-** It uses AWS Elastic Load Balancing (ELB).
- D-** It is considered to be a Firewall-as-a-Service (FWaaS).
- E-** It can be managed by FortiManager and AWS firewall manager.

Answer:

B, D, E

Explanation:

Scalability:

FortiGate Cloud-Native Firewall (CNF) is designed to scale seamlessly with your cloud infrastructure, providing the necessary protection without requiring manual intervention for scaling (Option B).

Firewall-as-a-Service:

FortiGate CNF is offered as a Firewall-as-a-Service (FWaaS), which simplifies the deployment and management of firewall capabilities directly in the cloud environment (Option D).

Management:

FortiGate CNF can be managed using FortiManager and AWS Firewall Manager, providing comprehensive management capabilities both from Fortinet's platform and AWS's native management tools (Option E).

Other Considerations:

Option A (carrier-grade protection) is not specifically highlighted as a feature of FortiGate CNF.

Option C (uses AWS Elastic Load Balancing) is incorrect as FortiGate CNF operates independently of AWS ELB, although it can integrate with various AWS services.

FortiGate CNF Documentation: FortiGate CNF

[AWS Firewall Manager: AWS Firewall Manager](#)

Question 8

Question Type: MultipleChoice

Which two statements about the FortiCloud portal are true? (Choose two.)

Options:

- A-** You can gain remote access to your FortiGate VM directly from the portal.
- B-** To assign permissions in the identity and access management (IAM) portal, you must write a JSON script.
- C-** You can access the FortiFlex portal only after you purchase a FortiFlex license and register it on FortiCare.
- D-** You can access only cloud services that you have subscribed to on AWS marketplace.

Answer:

A, C

Explanation:

Remote Access to FortiGate VM:

The FortiCloud portal allows users to remotely access their FortiGate VM instances. This is particularly useful for managing and configuring instances without needing direct network access (Option A).

FortiFlex Portal Access:

The FortiFlex portal is a feature that becomes available only after purchasing a FortiFlex license and registering it on FortiCare. This portal provides additional functionalities and services related to FortiFlex (Option C).

IAM Permissions:

Option B is incorrect because the Identity and Access Management (IAM) permissions in the FortiCloud portal do not require writing JSON scripts; they can be managed through the portal interface.

Subscription to Cloud Services:

Option D is incorrect because FortiCloud provides access to services beyond those subscribed through the AWS marketplace, including services directly offered by Fortinet.

FortiCloud Documentation: FortiCloud

FortiFlex Portal: FortiFlex Licensing

To Get Premium Files for FCP_WCS_AD-7.4 Visit

https://www.p2pexams.com/products/fcp_wcs_ad-7.4

For More Free Questions Visit

<https://www.p2pexams.com/fortinet/pdf/fcp-wcs-ad-7.4>

