Passcert

Higher Quality, better service!

Q&A

Http://www.passcert.com

We offer free update service for one year.

Exam : **NSE7_PBC-7.2**

Title : Fortinet NSE 7 Public Cloud Security 7.2 (FCSS)

Version : DEMO

1.Refer to the exhibit

```
config system sdn-connector
    edit "azure-globalsdn-iam-ha"
        set status enable
        set type azure
        set use-metadata-iam enable
        set ha-status enable
        set subscription-id ''
        set resource-group ''
        set azure-region global
        config nic
            edit "fgta-ap-port1"
                config ip
                    edit "ipconfig1"
                        set public-ip "fgt-ap-cluster"
                        set resource-group "fortigate-ha-training"
                    next
                end
            next
        end
        config route-table
            edit "az_spoke1_useast_web"
                set subscription-id "bc0e730b-2345-4c66-9a74-efdfc1xxxxxxx"
                set resource-group "fortigate-ha-training"
                config route
                    edit "default_spoke1_web"
                        set next-hop "10.60.5.4"
                    next
                    edit "az_spoke1_useast_app"

                        set next-hop "10.60.5.4"
                    next
                end
            next
        end
        set update-interval 40
    next
end
```

You deployed an HA active-passive FortiGate VM in Microsoft Azure.
Which two statements regarding this particular deployment are true? (Choose two.)

A. During the failover, the passive FortiGate issues API calls to Azure
B. Use the vdom-excepticn command to synchronize the configuration.
C. There is no SLA for API calls from Microsoft Azure.
D. By default, the configuration does not synchromze between the primary and secondary devices.
Answer: A D
Explanation:
- A is correct because in this deployment, the passive FortiGate issues API calls to Azure to update the routing table and the public IP address of the active FortiGate123. This way, the traffic is redirected to the new active FortiGate after a failover.
- B is incorrect because the vdom-exception command is used to exclude specific VDOMs from being synchronized in an HA cluster.This command is not related to this deployment scenario.
- C is incorrect because Microsoft Azure does provide an SLA for API calls. According to the Azure Service Level Agreements, the API Management service has a monthly uptime percentage of at least 99.9% for the standard tier and higher.
- D is correct because by default, the configuration is not synchronized between the primary and secondary devices in this deployment. The administrator needs to manually enable configuration synchronization on both devices123. Alternatively, the administrator can use FortiManager to manage and synchronize the configuration of both devices4.

2.Which statement about Transit Gateway (TGW) in Amazon Web Services (AWS) is true?
A. TGW can have multiple TGW route tables.
B. Both the TGW attachment and propagation must be in the same TGW route table
C. A TGW attachment can be associated with multiple TGW route tables.
D. The TGW default route table cannot be disabled.
Answer: A
Explanation
According to the AWS documentation for Transit Gateway, a transit gateway is a network transit hub that connects VPCs and on-premises networks. A transit gateway route table is a set of rules that determines how traffic is routed among the attachments to the transit gateway1.
A transit gateway can have multiple route tables, and you can associate different attachments with different route tables. This allows you to control how traffic is routed between your VPCs and VPNs based on your network design and security requirements1.
The other options are incorrect because:
- Both the TGW attachment and propagation must be in the same TGW route table is not true. You can associate an attachment with one route table and enable propagation from another attachment to a different route table. This allows you to separate the routing domains for your attachments1.
- A TGW attachment can be associated with multiple TGW route tables is not true. You can only associate an attachment with one route table at a time. However, you can change the association at any time1.
- The TGW default route table cannot be disabled is not true. You can disable the default route table by deleting all associations and propagations from it. However, you cannot delete the default route table itself1.
1: Transit Gateways - Amazon Virtual Private Cloud

3.What are two main features in Amazon Web Services (AWS) network access control lists (ACLs)? (Choose two.)
A. You cannot use Network ACL and Security Group at the same time.
B. The default network ACL is configured to allow all traffic
C. Network ACLs are stateless, and inbound and outbound rules are used for traffic filtering
D. Network ACLs are tied to an instance
Answer: B C
Explanation
B. The default network ACL is configured to allow all traffic. This means that when you create a VPC, AWS automatically creates a default network ACL for that VPC, and associates it with all the subnets in the VPC1. By default, the default network ACL allows all inbound and outbound IPv4 traffic and, if applicable, IPv6 traffic1. You can modify the default network ACL, but you cannot delete it1.
C. Network ACLs are stateless, and inbound and outbound rules are used for traffic filtering. This means that network ACLs do not keep track of the traffic that they allow or deny, and they evaluate each packet separately1. Therefore, you need to create both inbound and outbound rules for each type of traffic that you want to allow or deny1. For example, if you want to allow SSH traffic from a specific IP address to your subnet, you need to create an inbound rule to allow TCP port 22 from that IP address, and an outbound rule to allow TCP port 1024-65535 (the ephemeral ports) to that IP address2.
The other options are incorrect because:
- You can use network ACL and security group at the same time. Network ACL and security group are two different types of security layers for your VPC that can work together to control traffic3. Network ACLacts as a firewall for your subnets, while security group acts as a firewall for your instances3. You can use both of them to create a more granular and effective security policy for your VPC.
- Network ACLs are not tied to an instance. Network ACLs are associated with subnets, not instances1. This means that network ACLs apply to all the instances in the subnets that they are associated with1. You cannot associate a network ACL with a specific instance. However, you can associate a security group with a specific instance or multiple instances3.

4.You are adding more spoke VPCs to an existing hub and spoke topology Your goal is to finish this task in the minimum amount of time without making errors.
Which Amazon AWS services must you subscribe to accomplish your goal?
A. GuardDuty, CloudWatch
B. WAF, DynamoDB
C. Inspector, S3
D. CloudWatch, S3
Answer: D
Explanation
The correct answer is D. CloudWatch and S3.
According to the GitHub repository for the Fortinet aws-lambda-tgw script1, this function requires the following AWS services:
- CloudWatch: A monitoring and observability service that collects and processes events from various AWS resources, including Transit Gateway attachments and route tables.
- S3: A scalable object storage service that can store the configuration files and logs generated by the Lambda function.

By using the Fortinet aws-lambda-tgw script, you can automate the creation and configuration of Transit Gateway Connect attachments for your FortiGate devices.This can help you save time and avoid errors when adding more spoke VPCs to an existing hub and spoke topology1.
The other AWS services mentioned in the options are not required for this task. GuardDuty is a threat detection service that monitors for malicious and unauthorized behavior to help protect AWS accounts and workloads. WAF is a web application firewall that helps protect web applications from common web exploits. Inspector is a security assessment service that helps improve the security and compliance of applications deployed on AWS. DynamoDB is a fast and flexible NoSQL database service that can store various types of data.
1: GitHub - fortinet/aws-lambda-tgw

5.Which two Amazon Web Services (AWS) features support east-west traffic inspection within the AWS cloud by the FortiGate VM? (Choose two.)
A. A NAT gateway with an EIP
B. A transit gateway with an attachment
C. An Internet gateway with an EIP
D. A transit VPC
Answer: B D
Explanation
The correct answer is B and D. A transit gateway with an attachment and a transit VPC support east-west traffic inspection within the AWS cloud by the FortiGate VM.
According to the Fortinet documentation for Public Cloud Security, a transit gateway is a network transit hub that connects VPCs and on-premises networks. A transit gateway attachment is a resource that connects a VPC or VPN to a transit gateway. By using a transit gateway with an attachment, you can route traffic from your spoke VPCs to your security VPC, where the FortiGate VM can inspect the traffic1.
A transit VPC is a VPC that serves as a global network transit center for connecting multiple VPCs, remote networks, and virtual private networks (VPNs). By using a transit VPC, you can deploy the FortiGate VM as a virtual appliance that provides network security and threat prevention for your VPCs2.
The other options are incorrect because:
- A NAT gateway with an EIP is a service that enables instances in a private subnet to connect to the internet or other AWS services, but prevents the internet from initiating a connection with those instances. A NAT gateway with an EIP does not support east-west traffic inspection within the AWS cloud by the FortiGate VM3.
- An Internet gateway with an EIP is a horizontally scaled, redundant, and highly available VPC component that allows communication between instances in your VPC and the internet.An Internet gateway with an EIP does not support east-west traffic inspection within the AWS cloud by the FortiGate VM4.
1: Fortinet Documentation Library - Deploying FortiGate VMs on AWS
2: [Fortinet Documentation Library - Transit VPC on AWS]
3: [NAT Gateways - Amazon Virtual Private Cloud]
4: [Internet Gateways - Amazon Virtual Private Cloud]