Vendor: Fortinet

Exam Code: NSE7_CDS_AR-7.6

Exam Name: Fortinet NSE 7 - Public Cloud Security 7.6.4 Architect

Version: DEMO

QUESTION 1
As part of your organization's monitoring plan, you have been tasked with obtaining and analyzing detailed information about the traffic sourced at one of your FortiGate EC2 instances. What can you do to achieve this goal?

A. Use AWS CloudTrail to capture and then examine traffic from the EC2 instance.
B. Create a virtual public cloud (VPC) flow log at the network interface level for the EC2 instance.
C. Add the EC2 instance as a target in CloudWatch to collect its traffic logs.
D. Configure a network access analyzer scope with the EC2 instance as a match finding.

Answer: B
Explanation:
VPC Flow Logs are designed to capture metadata about IP traffic to and from network interfaces in a VPC, including those attached to EC2 instances such as FortiGate appliances.

Creating a flow log at the network interface level for the FortiGate EC2 instance lets you collect detailed information (source/destination IPs, ports, protocol, action, bytes, etc.) for all traffic sourced from and going to that instance, which you can then analyze in CloudWatch Logs or S3.

QUESTION 2
Refer to the exhibit. You are managing an active-passive FortiGate HA cluster in AWS that was deployed using CloudFormation. You have created a change set to examine the effects of some proposed changes to the current infrastructure. The exhibit shows some sections of the change set.
What will happen if you apply these changes?

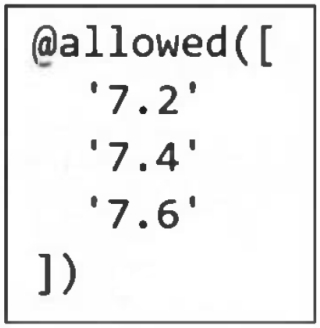
Change set configuration

```
"Changes": [
        {
         "Type": "Resource",
         "ResourceChange": {
               "ResourceType": "AWS::EC2::Instance",
               "LogicalResourceId": "FGT_A_HA",
               "PhysicalResourceId": "i0cb1020adr1b308b",
               "Action": "Modify",
               "Replacement": "True",
         :
         :
         "ResourceChange": {
               "ResourceType": "AWS::EC2::Instance",
               "LogicalResourceId": "FGT_B_HA",
               "PhysicalResourceId": "i0559e20adr1b3ba3",
               "Action": "Modify",
               "Replacement": "False",
```

A. This deployment can be done without any traffic interruption.
B. Both FortiGate VMs will get a new PhysicalResourceId.
C. The updated FortiGate VMs will not have the latest configuration changes.
D. CloudFormation checks if you will surpass your account quota.

Answer: B

QUESTION 3
Refer to the exhibit. What is the purpose of this section of an Azure Bicep file?



A. To restrict which FortiOS versions are accepted for deployment
B. To indicate the correct FortiOS upgrade path after deployment
C. To add a comment with the permitted FortiOS versions that can be deployed
D. To document the FortiOS versions in the resulting topology

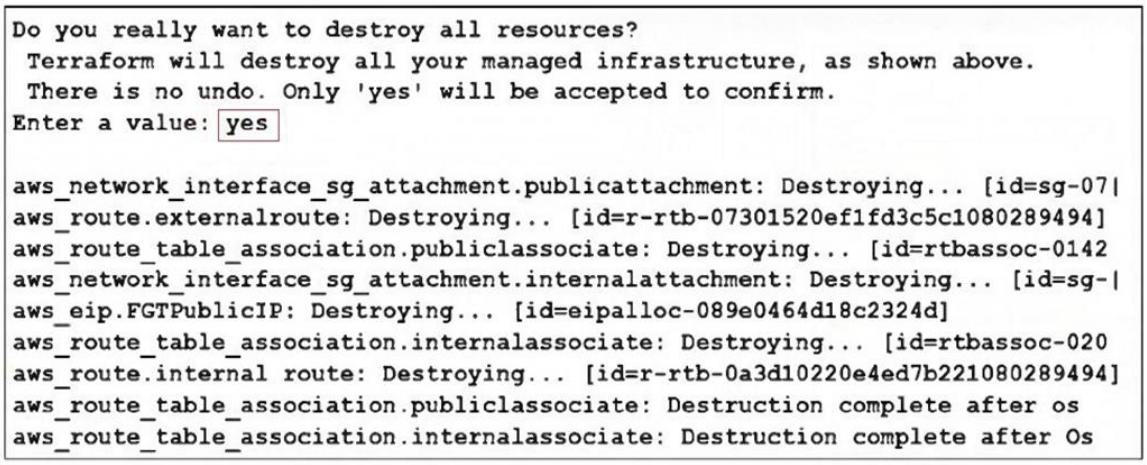
Answer: A

QUESTION 4
In an SD-WAN TGW Connect topology, which three initial steps are mandatory when routing traffic from a spoke VPC to a security VPC through a Transit Gateway? (Choose three.)

A. From the security VPC TGW subnet routing table, point 0.0.0.0/0 traffic to the FortiGate internal port.
B. From the security VPC TGW subnet routing table, point 0.0.0.0/0 traffic to the TGW.
C. From both spoke VPCs and the security VPC, point 0.0.0.0/0 traffic to the Internet Gateway.
D. From the security VPC FortiGate internal subnet routing table, point 0.0.0.0/0 traffic to the TGW.
E. From the spoke VPC internal routing table, point 0.0.0.0/0 traffic to the TGW.

Answer: ABE
Explanation:
In an SD-WAN TGW Connect topology, to route spoke VPC traffic through the Security VPC FortiGate via the Transit Gateway, the following are mandatory:
- The Security VPC TGW subnet route table must send 0.0.0.0/0 traffic to the TGW, so inbound spoke traffic can reach the FortiGate.
- The Security VPC FortiGate internal subnet route table must send 0.0.0.0/0 traffic to the FortiGate internal port, ensuring inspection.
- The Spoke VPC internal route table must point 0.0.0.0/0 to the TGW, so all spoke traffic is routed via the Transit Gateway toward the Security VPC.

QUESTION 5
Refer to the exhibit. What would be the impact of confirming to delete all the resources in Terraform?



A. It destroys all the resources tied to the AWS Identity and Access Management (IAM) user.
B. It destroys all the resources in the resource group.
C. It destroys all the resources in the state file.
D. It destroys all the resources in the .tfvars file.

Answer: C
Explanation:
When you confirm a terraform destroy, Terraform deletes all resources that are tracked in its state file. The state file represents the managed infrastructure, so only those resources defined and tracked there will be destroyed.

QUESTION 6
An administrator is configuring a software-defined network (SDN) connector in FortiWeb to dynamically obtain information about existing objects in an Amazon Elastic Kubernetes Service (EKS) cluster.
Which AWS policy should the administrator attach to a user to achieve this goal?

A. AmazonEKSConnectorServiceRolePolicy
B. AmazonEKSComputePolicy
C. AmazonEKSServicePolicy
D. AmazonEKSClusterPolicy

Answer: D
Explanation:
To allow FortiWeb to dynamically obtain information about objects in an Amazon EKS cluster, the required permission is provided by the AmazonEKSClusterPolicy. This policy grants read access to cluster resources, enabling FortiWeb's SDN connector to pull EKS object data.

QUESTION 7
Which statement about Transit Gateway (TGW) in Amazon Web Services (AWS) is true?

A. Both the TGW attachment and propagation must be in the same TGW route table.
B. TGW can have multiple TGW route tables.
C. A TGW attachment can be associated with multiple TGW route tables.
D. The TGW default route table cannot be disabled.

Answer: B
Explanation:
In AWS, a Transit Gateway (TGW) can indeed have multiple TGW route tables, allowing flexible routing policies for different VPCs and VPN attachments. Each attachment can be associated with only one route table, but TGW supports multiple route tables for segmentation and control.

QUESTION 8
Refer to the exhibit. You deployed an HA active-active load balance sandwich with two FortiGate VMs in Microsoft Azure. After the deployment, you prefer to use FGSP to synchronize sessions and allow asymmetric return traffic. In the environment, FortiGate port 1 and port 2 are facing external and internal load balancers respectively.
What IP address must you use in the peering configuration?

HA configuration

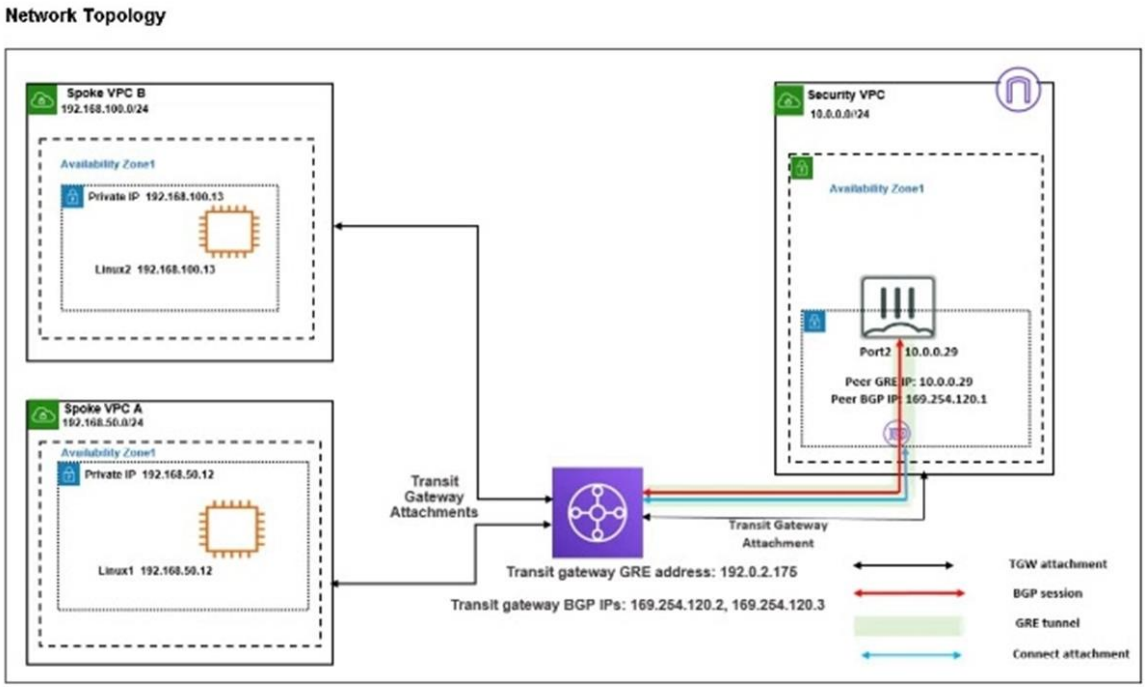
```
config system ha
    set session-pickup enable
    set session-pickup-connectionless enable
    set session-pickup-nat enable
    set session-pickup-expectation enable
    set override disable
end

config system standalone-cluster
    edit 0
        set peerip 10.0.1.x
        set syncvd "root"
    next
end
```

A. The opposite FortiGate port 2 IP address.
B. The public load balancer port 2 IP address.
C. The internal load balancer port 1 IP address.
D. The opposite FortiGate port 1 IP address.

Answer: A
Explanation:
In an FGSP (FortiGate Session Life Support Protocol) deployment with asymmetric traffic in Azure, the peerip must be set to the opposite FortiGate's internal interface (port2) IP address. This ensures session synchronization between FortiGates through the internal network (behind the internal load balancer), which is required for proper failover handling.

QUESTION 9
Refer to the exhibit. You attempted to access the Linux1 EC2 instance directly from the internet using its public IP address in AWS. However, your connection is not successful.
Given the network topology, what can be the issue?



A. There is no connection between VPC A and VPC B.
B. There is no Internet Gateway attached to the Spoke VPC A.
C. The Transit Gateway BGP IP address is incorrect.
D. There is no Elastic IP address attached to FortiGate in the Security VPC.

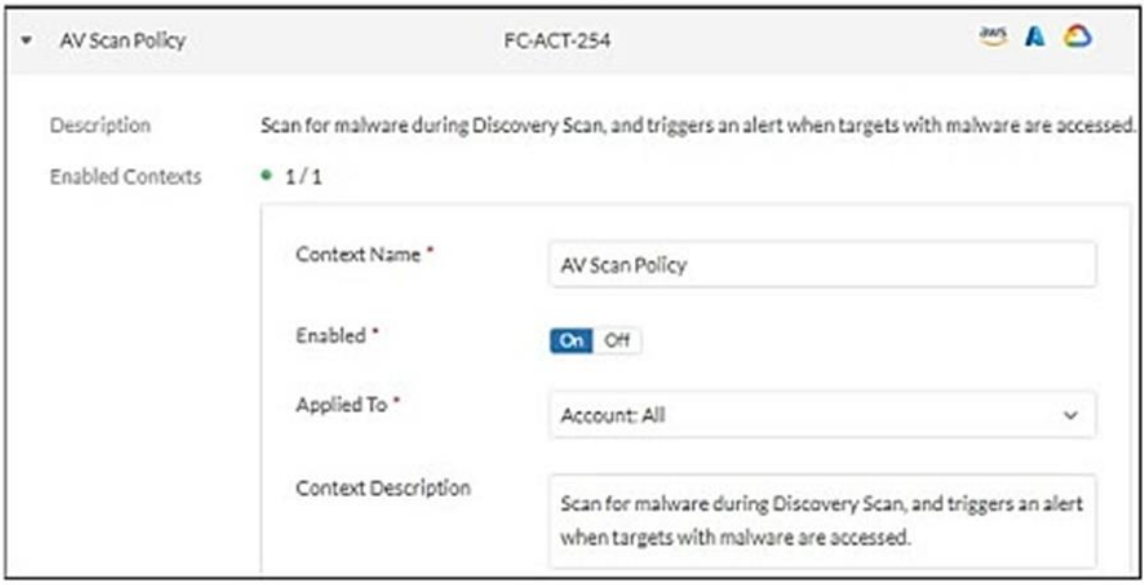
Answer: B
Explanation:
The instance is in Spoke VPC A, which (in this TGW Connect design) has no Internet Gateway attached. Without an IGW and corresponding routes, a public IP on the instance is not reachable from the internet.

QUESTION 10
An administrator is trying to implement FortiCNP with Microsoft Azure Security integration. However, FortiCNP is not able to extract any cloud integration data from Azure; therefore, real-time cloud security monitoring is not possible.
What is causing this issue?

A. The organization is using a free Azure AD license.
B. The Azure account doesn't have the Global Administrator role.
C. The administrator enabled the wrong Defender plan for servers.
D. The FortiCNP account in Azure has the Storage Blob Data Reader role.

Answer: D
Explanation:
For FortiCNP integration with Azure Security, the Azure account must have sufficient permissions to extract security and resource data. If the account only has the Storage Blob Data Reader role, it can read storage blobs but cannot access the required security or resource information, which prevents FortiCNP from performing real-time monitoring.

QUESTION 11
Refer to the exhibit. In which type of FortiCNP insights can an administrator examine the findings triggered by this policy?



A. Data
B. Threat
C. Risk
D. User activity

Answer: B
Explanation:
The policy shown is an AV Scan Policy that scans for malware during discovery and raises alerts when malicious targets are accessed. Findings from such policies are categorized under Threat insights in FortiCNP, since they deal with detection of malware and malicious activity.

Thank You for Trying Our Product

Lead2pass Certification Exam Features:

★ More than **99,900** Satisfied Customers Worldwide.

★ Average **99.9%** Success Rate.

★ **Free Update** to match latest and real exam scenarios.

★ **Instant Download** Access! No Setup required.

★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.

★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.

★ **100%** Guaranteed Success or **100%** Money Back Guarantee.

★ **Fast**, helpful support **24x7**.

View list of all certification exams: http://www.lead2pass.com/all-products.html

10% Discount Coupon Code: **ASTR14**