ATMIC NETWORKS
YOUR GUIDE TO GLOBAL CERTIFICATION

"Please note that these files may not be up to date. However, the questions will help you understand the exam format and typical question patterns."

www.atmicnetworks .com

Warning: Keep connected with our support team for latest updates

Question: 1

An administrator would like to use FortiCNP to keep track of sensitive data files located in the Amazon Web Services (AWS) S3 bucket and protect it from malware. Which FortiCNP feature should the administrator use?

A. FortiCNP Threat Detection policies

B. FortiCNP Risk Management policies

C. FortiCNP Data Scan policies

D. FortiCNP Compliance policies

Answer: C

Explanation:

https://docs.fortinet.com/document/forticnp/22.4.a/online-help/359537/anti-virus-scan-policy

Question: 2

You are using Ansible to modify the configuration of several FortiGate VMs. What is the minimum number of files you need to create, and in which file should you configure the target FortiGate IP addresses?

A. One playbook file for each target and the required tasks, and one inventory file.

B. One .yaml file with the targets IP addresses, and one playbook file with the tasks.

C. One inventory file for each target device, and one playbook file.

D. One text file for all target devices, and one playbook file.

Answer: D

Explanation:

Comprehensive and Detailed Explanation From FortiOS 7.6, FortiWeb 7.4 Exact Extract study guide:

Based on the FortiOS 7.6 Automation Guide and the provided documentation for Ansible workflows, the following structure is required for managing multiple FortiGate nodes:

Inventory File (The Target List): The inventory is a single file that defines the list of managed nodes. It specifies critical information such as hostnames, connection details, and specifically the IP addresses of the target devices. According to the study guide, this inventory is a text file that lists all the systems you want to manage.

Playbook File (The Task List): You create and edit a separate file that acts as the playbook. This file is written in YAML format and contains the series of tasks that Ansible performs on the managed nodes to reach a desired state.

Minimum File Count: A basic Ansible workflow consists of exactly two files: one inventory file (text) and one playbook file (YAML). By listing the target IP address (e.g., 10.0.206.131) within the inventory text file, the administrator can manage the FortiGate device without needing individual files for every target.

Why other options are incorrect:

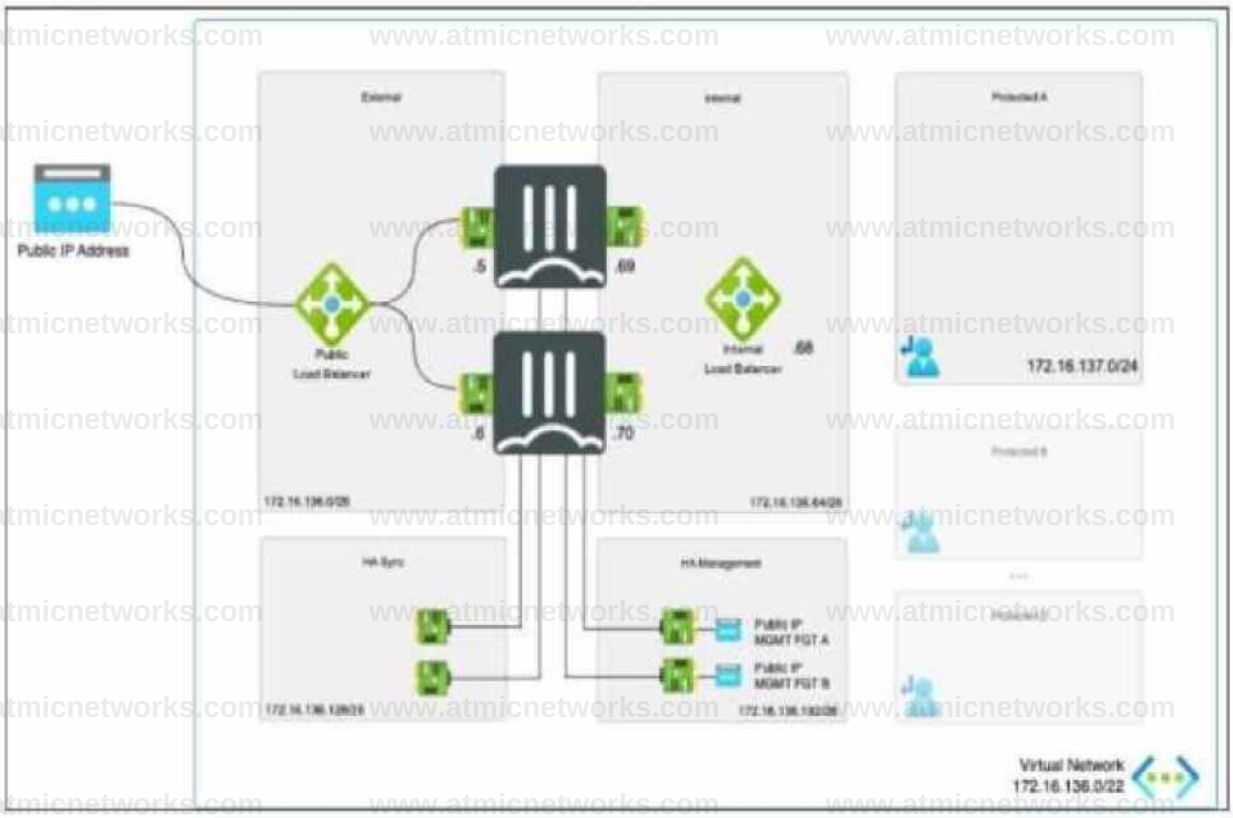
Option A & C: Creating a separate playbook or inventory file for each target is inefficient and contradicts the core Ansible workflow, which uses a single inventory to manage multiple hosts.

Option B: While the playbook is a .yaml file, the study guide specifically defines the inventory (where IP addresses are configured) as a text file in the context of the basic workflow.

Question: 3

Refer to the exhibit.

HA Topology



The exhibit shows an active-passive high availability FortiGate pair with external and internal Azure load balancers There is no SDN connector used in this solution.

Which configuration must the administrator implement on each FortiGate?

A. Single BGP route to Azure probe IP address.

B. One static route to Azure Lambda IP address.

C. Two static routes to Azure probe IP address.

D. Two BGP routes lo Azure probe IP address.

Answer: C

Explanation:

Question: 4

Your DevOps team is evaluating different Infrastructure as Code (IaC) solutions for deploying complex Azure environments.

What is an advantage of choosing Azure Bicep over other IaC tools available?

A. Azure Bicep generates deployment logs that are optimized to improve error handling.

B. Azure Bicep provides immediate support for all Azure services, including those in preview.

C. Azure Bicep requires less frequent schema updates than Azure Resource Manager (ARM) templates.

D. Azure Bicep can reduce deployment costs by limiting resource utilization during testing.

Answer: B

Explanation:

Question: 5

You must add an Amazon Web Services (AWS) network access list (NACL) rule to allow SSH traffic to a subnet for temporary testing purposes. When you review the current inbound and outbound NACL rules, you notice that the rules with number 5 deny SSH and telnet traffic to the subnet.

What can you do to allow SSH traffic?

A. You do not have to create any NACL rules because the default security group rule automatically allows SSH traffic to the subnet.

B. You must create a new allow SSH rule anywhere in the network ACL rule base to allow SSH traffic.

C. You must create two new allow SSH rules, each with a number bigger than 5.

D. You must create two new allow SSH rules, each with a number smaller than 5.

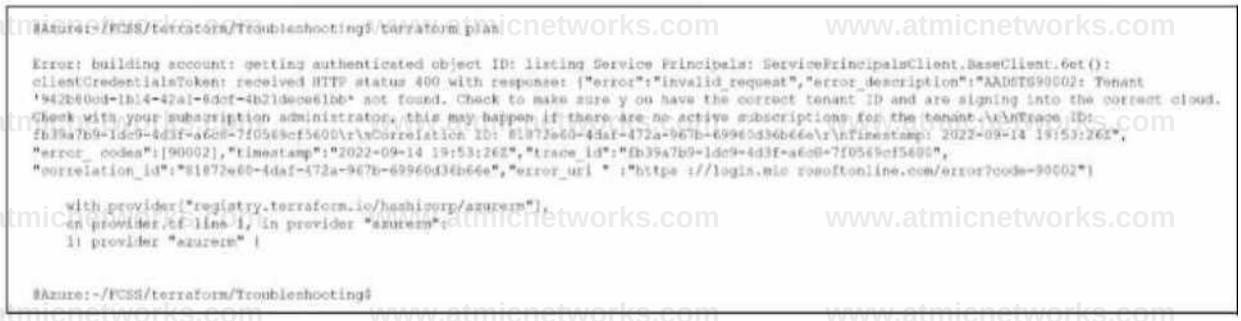
Answer: D

Explanation:

Question: 6

Refer to the exhibit.

Terraform configuration



After the initial Terraform configuration in Microsoft Azure, the terraform plan command is run.

Which two statements about running the terraform plan command are true? (Choose two.)

A. The terraform plan command will deploy the rest of the resources except the service principle details.

B. You cannot run the terraform apply command before the terraform plan command.

C. The terraform plan command makes terraform do a dry run.

D. You must run the terraform init command once, before the terraform plan command.

Answer: C, D

Explanation:

Question: 7

A Network security administrator is searching for a solution to secure traffic going in and out of the container infrastructure.

In which two ways can Fortinet container security help secure container infrastructures? (Choose two.)

A. FortiGate NGFW can inspect north-south container traffic with label aware policies.

B. FortiGate NGFW and FortiWeb can be used to secure container traffic.

C. FortiGate NGFW can connect to the worker nodes and protect the containers.

D. FortiGate NGFW can be placed between each application container for north-south traffic inspection.

Answer: A, B

Explanation:

Question: 8

An organization is deploying FortiDevSec to enhance security for containerized applications, and they need to ensure containers are monitored for suspicious behavior at runtime.

Which FortiDevSec feature is best for detecting runtime threats?

A. FortiDevSec software composition analysis (SCA)

B. FortiDevSec static application security testing (SAST)

C. FortiDevSec dynamic application security testing (DAST)

D. FortiDevSec container scanner

Answer: D

Explanation:

Question: 9

Refer to the exhibit.

You are troubleshooting a Microsoft Azure SDN connector issue on your FortiGate VM in Azure.

Which command can you use to examine details about API calls sent by the connector?

A. diag debug application cloud-connector -1

B. diag test application azd 1

C. diag debug application azd -1

D. get system sdn-connector

Answer: C

Explanation:

Question: 10

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:

Question: 11

Refer to the exhibit.

Change set configuration

```
"Changes": [

    "Type": "Resource", "ResourceChange": {
        "ResourceType": "AWS::EC2;:Instance", "LogicalResourccId":
        "FGT_A_HA", "PhysicalResourceId": "i0cbl020adrlb308b",
        "Action": "Modify", "Replacement": "True",

    "ResourceChange": {
        "ResourceType": "AWS::EC2::Instance", "LogicalResourceId":
        "FGTBHA", "PhysicalResourceId": "i0559e20adrlb3ba3",
        "Action": "Modify", "Replacement": "False",
```

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?

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.

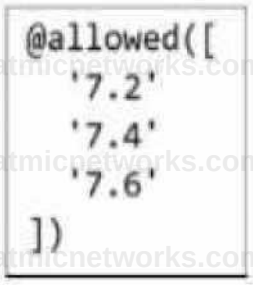
D. CloudFormation checks if you will surpass your account quota.

Answer: B

Explanation:

Question: 12

Refer to the exhibit.



```
@allowed([
  '7.2'
  '7.4'
  '7.6'
])
```

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

Explanation:

Question: 13

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: A, D, E

Explanation:

Comprehensive and Detailed Explanation From FortiOS 7.6, FortiWeb 7.4 Exact Extract study guide:

In an AWS SD-WAN Transit Gateway (TGW) Connect topology, traffic flow must be meticulously orchestrated through VPC route tables to ensure that the FortiGate-VM (Security VPC) can inspect traffic transitioning between spokes.

Spoke to TGW Redirection (Option E): For traffic to leave a Spoke VPC and reach the inspection hub, the Spoke VPC internal routing table must be configured to send all non-local traffic (0.0.0.0/0) to the Transit Gateway (TGW). This is the first step in the traffic chain.

TGW to FortiGate Redirection (Option A): Once the traffic arrives at the TGW and is forwarded to the Security VPC via a TGW attachment, it lands in the TGW subnet (or attachment subnet). To ensure this traffic is inspected, the Security VPC TGW subnet routing table must point the default route (0.0.0.0/0) to the FortiGate's internal network interface (ENI).

FortiGate Return/Egress Path (Option D): After the FortiGate processes the packet, it must be sent back to the TGW to reach its final destination in a different spoke or to exit via a different gateway. Therefore, the Security VPC FortiGate internal subnet routing table (the subnet where the FortiGate's internal leg resides) must have a default route (0.0.0.0/0) pointing back to the TGW.

Why other options are incorrect:

Option B: If the Security VPC TGW subnet routing table points to the TGW as the next hop, it creates a routing loop where traffic arrives from the TGW and is immediately sent back without being inspected by the FortiGate.

Option C: Pointing all traffic to an Internet Gateway (IGW) would bypass the Transit Gateway entirely and send traffic to the public internet rather than through the internal security fabric.

Question: 14

An AWS administrator must ensure that each member of the cloud deployment team has the correct permissions to deploy and manage resources using CloudFormation. The administrator is researching which tasks must be executed with CloudFormation and therefore require CloudFormation permissions.

Which task is run using CloudFormation?

A. Deploying a new pod with a service in an Elastic Kubernetes Service (EKS) cluster using the kubectl command

B. Installing a Helm chart to deploy a FortiWeb ingress controller in an EKS cluster

C. Creating an EKS cluster with the eksctl create cluster command

D. Changing the number of nodes in a EKS cluster from AWS CloudShell

Answer: C

Explanation:

Comprehensive and Detailed Explanation From FortiOS 7.6, FortiWeb 7.4 Exact Extract study guide:

Based on the Fortinet NSE 7 - Public Cloud Security 7.4/7.6 study materials and the FortiOS 7.6 AWS Administration Guide, understanding the underlying mechanisms of AWS deployment tools is essential for permission management.

Infrastructure as Code and eksctl (Option C): In the context of Amazon EKS, the eksctl command-line tool is the official CLI for creating and managing clusters on EKS. When an administrator executes the eksctl create cluster command, eksctl does not interact with the EKS API directly to provision infrastructure; instead, it generates and executes AWS CloudFormation stacks to provision the necessary VPC, IAM roles, and the EKS control plane. Therefore, users running this command must have explicit permissions to create and manage CloudFormation stacks.

Resource Provisioning via Stacks: CloudFormation is AWS's native service for Infrastructure as Code (IaC), allowing users to define resources in JSON or YAML templates. Commands like eksctl leverage these templates to ensure repeatable and organized deployments of complex architectures, such as those required for a FortiGate or FortiWeb cloud integration.

Why other options are incorrect:

Option A: The kubectl command interacts directly with the Kubernetes API server inside the cluster to manage pods and services; it does not trigger AWS CloudFormation processes.

Option B: Helm is a package manager for Kubernetes. While it manages "releases" within the EKS cluster, the installation of a Helm chart for a FortiWeb ingress controller happens at the Kubernetes software layer and does not utilize AWS CloudFormation stacks.

Option D: Changing the node count via CloudShell using the AWS CLI or kubectl typically modifies an Auto Scaling Group or a Kubernetes Deployment/DaemonSet directly, rather than initiating a new CloudFormation stack execution.

Question: 15

An administrator decides to use the Use managed identity option on the FortiGate SDN connector with Microsoft Azure. However, the SDN connector is failing on the connection.

What must the administrator do to correct this issue?

A. Make sure to add the Client secret on FortiGate side of the configuration.

B. Make sure to add the Tenant ID on FortiGate side of the configuration.

C. Make sure to enable the system assigned managed identity on Azure.

D. Make sure to set the type to system managed identity on FortiGate SDN connector settings.

Answer: C

Explanation:

Question: 16

Refer to the exhibit.

'Troubleshooting command

```
azadmin@Azure:~J a? feature show -namespace Microsoft.Network - name EnabieHlghAvallabrtityMode
{
  "id": '/subschptons/2t100b64-cedc-19cc-a00b-017ec43S92ac/pros'iders/Microsoft.Features/providera/M>crosoft.Network/features/EnableHignAvailabil>tyMode'
  "name": 'Microsoft Nctwork/EnablcHigtiAvuilabiUtyModc".
  "properties": {
    state': 'Unregistered'
  ).
  "type": "Microsoft.FeeturoafproviderB/fBaturea'
```

A managed security service provider (MSSP) administration team is trying to deploy a new HA cluster in Azure to filter traffic to and from a client that is also using Azure. However, every deployment attempt fails, and only some of the resources are deployed successfully. While troubleshooting this issue, the team runs the command shown in the exhibit.

What are the implications of the output of the command?

A. The teamwill not be able to deploy an A-P FortiGate HA cluster with Azure gateway load balancer.

B. The teamwill not be able to deploy an A-P FortiGate HA cluster with Azure load balancer.

C. The teamwill not be able to deploy an active-passive (A-P) FortiGate high availability (HA) cluster with SDN connector.

D. The team will not be able to deploy an active-active (A-P) FortiGate HA cluster with Azure load balancer.

Answer: D

Explanation:

Question: 17

Refer to the exhibit.

FortiGate HA configuration

```
config system sdn-connector edit 'azure oiofcalsdn am ha' set status enable set type azure set use-metadata
ram enable set ha status enable set subscriptaxi-id * set resource-group ' set azure-region global config nrc
        edit "fgta ap port!" config ip
            edit "ipconfig 1"
                set public ip "fgt ap Chisler
                set resource-group "forbgate ha training" nest end
    next end conftg route-able edit 'ezspokelusexstweb'
        set subscription-id "bcOe73Ob-2345-4c66-9a74-etdfc1xxxxxxx set resource-group 'forttgate-he-
        tnuning'
        config route
            edit 'defeuit spoltei ereb' set next-bop '10.60.5.4'
            next
            edit 'ai spoXel usexsi_app" set next-hop *10.60.5.4'
            next end next end
    set update-interval 40 next
end
```

You deployed a FortiGate HA active-passive cluster in Microsoft Azure.

Which two statements regarding this particular deployment are true? (Choose two.)

A. You can use the vdom-exception command to synchronize the configuration.

B. During a failover, all existing sessions are transferred to the new active FortiGate.

C. The configuration does not synchronize between the primary and secondary devices.

D. There is no SLA for API calls from Microsoft Azure.

Answer: B, D

Explanation:

Question: 18

Exhibit.

|eo2-iu»r!lp-10-0-0-200 *|$ sudo yum -y install unzip Last metadata expiration check: 0:02:31 ago on Sun Jul 21 22:12:44 2024. Package unzip-6.0-57.amzn2023.0.2. x86_64 is already installed.
Dependencies resolved Nothing to do.
Complete[1]
[ec2-user#ip-10-0-0-200 -]$ unzip terrafoim_$(TERRAFORM_VER|_linux_amd64. zip Archive: terraform 1.5.3 Linux amd64.zip inflating: terraform (eo2-user#ip-10-0-0-200 -1$ terraform version - bash: terraform: command not found [ec2-user?ip-10-0-0-200 -1$

You are tasked with deploying FortiGate using Terraform. When you run the terraform version command during the Terraform installation, you get an error message.

What could you do to resolve the command not found error?

A. You must move the binary file to the bin directory.

B. You must reinstall Terraform.

C. You must change the directory location to the root directory.

D. You must assign correct permissions to the ec2-user.

Answer: A

Explanation:

https://github.com/fortinet/fortigate-terraform-deploy

According to the Terraform documentation for installing Terraform on Linux, you need to download a zip archive that contains a single binary file called terraform. You need to unzip the archive and move the binary file to a directory that is included in your system's PATH environment variable, such as /usr/local/bin. This way, you can run the terraform command from any directory without specifying the full path.

If you do not move the binary file to the bin directory, you will get a command not found error when you try to run the terraform version command, as shown in the screenshot. To fix this error, you need to move the binary file to

the bin directory or specify the full path of the binary file when running the command.

Question: 19

Refer to the exhibit.

what-if tool

Resource and property changes are indicated with these symbols:

- ♦ Delete
- ♦ Create
- ♦ Modify

The deployment will update the following scope:

Scope: /subscription.[1]!/,/resourceGroups/DemoGroup

* Microsoft,Network/virtua1Networks/ServerApps vnet [2023-11-01]

- tags.Owner: "Apt-Ainms"

* properties.addressSpace.addressPrefIxes: [- 0: *10.0.0.0/16*

* 0: “' 92.1• '■. 0.0? 24“

J

- properties.subnets: [

- 0s

* properties.addressPrefix: *10.0.1.0/24* -> "Ji .0.2. <

Resource changes: 1 to modify.

An administrator used the what-if tool to preview changes to an Azure Bicep file.

What will happen if the administrator decides to apply these changes in Azure?

A. Subnet 10.0.1.0/24 will replace subnet 10.0.2.0/24.

B. This deployment will fail and no changes will be applied.

C. A new subnet will be added to ServerApps.

D. The ServerApps VNet will be renamed.

Answer: B

Explanation:

Based on the Fortinet NSE 7 - Public Cloud Security 7.4/7.6 curriculum and Azure Resource Manager (ARM) deployment logic, the what-if tool provides a predictive analysis of infrastructure changes.

Analyzing the Modification Symbols (Option B): The exhibit shows several critical changes being attempted simultaneously on the ServerApps_vnet.

VNet Address Space Change: The symbol - (Delete) is next to the address space 10.0.0.0/16, and + (Create) is next to 192.168.0.0/24.

Subnet Modification: Further down, the symbol ~ (Modify) indicates an attempt to change the prefix of an existing subnet from 10.0.1.0/24 to 10.0.2.0/24.

Azure Deployment Constraints: According to the FortiOS 7.6 Azure Administration Guide, Azure networking has strict dependencies. You cannot delete or modify an address space that contains active subnets or resources.

Why the deployment fails: The what-if output shows the administrator is trying to remove the 10.0.0.0/16 address range. However, the existing subnet 10.0.1.0/24 is still "resident" within that range during the transaction. Because the subnet is currently attached to the address space being deleted, Azure Resource Manager will reject the deployment as an invalid operation. The attempt to add a new 192.168.0.0/24 range does not resolve the conflict of removing the active range.

Why other options are incorrect:

Option A: The tool shows that 10.0.1.0/24 is being changed to 10.0.2.0/24, not that one is replacing the other as a new entity.

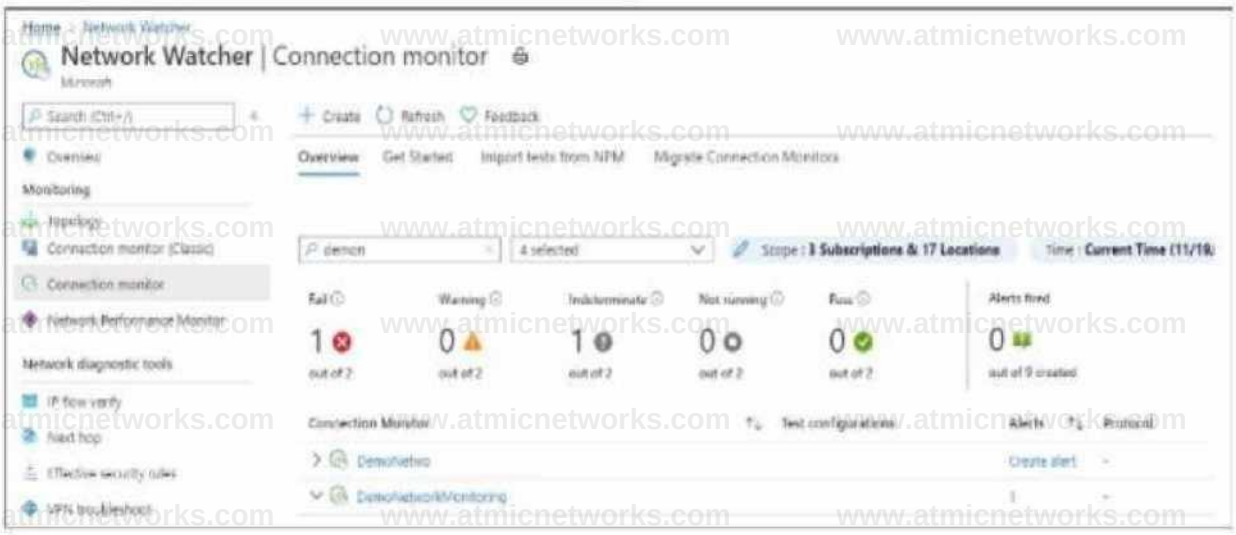
Option C: The symbols show a modification (~) of an existing subnet (index 0:), not the creation (+) of an entirely new subnet.

Option D: The VNet name ServerApps_vnet is not being changed; only its internal properties (tags, address space, and subnets) are being modified.

Question: 20

Refer to the exhibit.

Azure monitoring



After analyzing the native monitoring tools available in Azure, an administrator decides to use the tool displayed in the exhibit.

Why would an administrator choose this tool?

A. To view details about Azure resources and their relationships across multiple regions.

B. To obtain, and later examine, traffic flow data with a visualization tool.

C. To help debug issues affecting virtual network gateways.

D. To compare the latency of an on-premises site with the latency of an Azure application.

Answer: D

Explanation:

Question: 21

An administrator implements FortiWeb ingress controller to protect containerized web applications in an AWS Elastic Kubernetes Service (EKS) cluster.

What can you conclude about the topology shown in FortiView?

A. The FortiWeb VM gets the latest cluster information through an SDN connector.

B. This topology has two services and two ingress controllers deployed.

C. Both services will be load balanced among the two nodes and the four pods.

D. Adding a new service will update the FortiWeb configuration automatically.

Answer: A

Explanation:

Question: 22

What would be the impact of confirming to delete all the resources in Terraform?

Do you really want to destroy all resources?
Terraform will destroy all your managed infrastructure, as shown above.
There is no undo. Only 'yes' will be accepted to confirm.
Enter a value: [yeaJ

aws network interface sg attachment.publicattachment: Destroying... [id=sg-07| a»s_routs.#««rMlrovte: Destroying. .. [id*r-rtb-07301S20eflfd3c5cl080289494] aws_route_table_associatlon.publlclassociate: Destroying... [ld=rtbassoc-0142 aws_network_interface_sg_attachnent.internalattachment Destroying... [ld-ag-| awseip.FGTPublicIP Destroying . [id=eipalloc-089e0464dl8c2324dj
aws route table association.internalassociate: Destroying... [id-rtbassoc-020 aws_route.internal route. Destroying... (ld>r-rtb~0a3dl0220e4ed7b221080289494] aws route table association.publiclassociate: Destruction complete after os aws route table association.internalassociate: Destruction complete after os

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 .tfstate file.

D. It destroys all the resources in the .tfvars file.

Answer: C

Explanation:

Question: 23

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:

Question: 24

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:

According to the FortiOS 7.6 AWS Administration Guide and the Fortinet Public Cloud Security 7.4 training materials regarding centralized security inspection:

Multiple Route Tables (Option B): A single AWS Transit Gateway is designed to support multiple TGW route tables. By default, there is a soft limit of 20 route tables per Transit Gateway, which allows administrators to implement sophisticated network segmentation and granular routing policies. In a FortiGate-centric "Security Hub" or "Transit VPC" architecture, multiple route tables are used to separate "Spoke" traffic from "Security" traffic, ensuring all inter-VPC traffic is forced through the FortiGate-VM for inspection.

Associations and Propagations: * Association: Each individual TGW attachment (VPC, VPN, or Direct Connect) can be associated with exactly one TGW route table at any given time. This table dictates where packets coming from that attachment will be sent. Because of this 1:1 relationship, Option C is incorrect.

Propagation: An attachment can propagate its routes to one or many TGW route tables. This flexibility allows a VPC's prefix to be known in multiple routing domains, meaning that association and propagation do not need to occur in the same table, making Option A incorrect.

Default Route Table Management: When creating an AWS Transit Gateway, the options for "Default route table association" and "Default route table propagation" are enabled by default, but they can be disabled during or after

creation. Disabling these is a security best practice when deploying FortiGate-VMs to prevent the TGW from automatically creating a "full-mesh" connectivity that bypasses the firewall, making Option D incorrect.

Question: 25

Refer to the exhibit.

HA configuration

```
contig system ha
        act session-pickup enable
        set sessinp-p- ■kup-c^nnection ess era
        set seasion-pickup-nat enable
        set scssion-pickup-oxpcctatior. enable set. ©verr"de disable
end

config systeir. standalone cluster
        ed i I. 0
                set peerip 10,0.1.x
                set synevd "root"
        next
end
```

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 peerip configuration?

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.

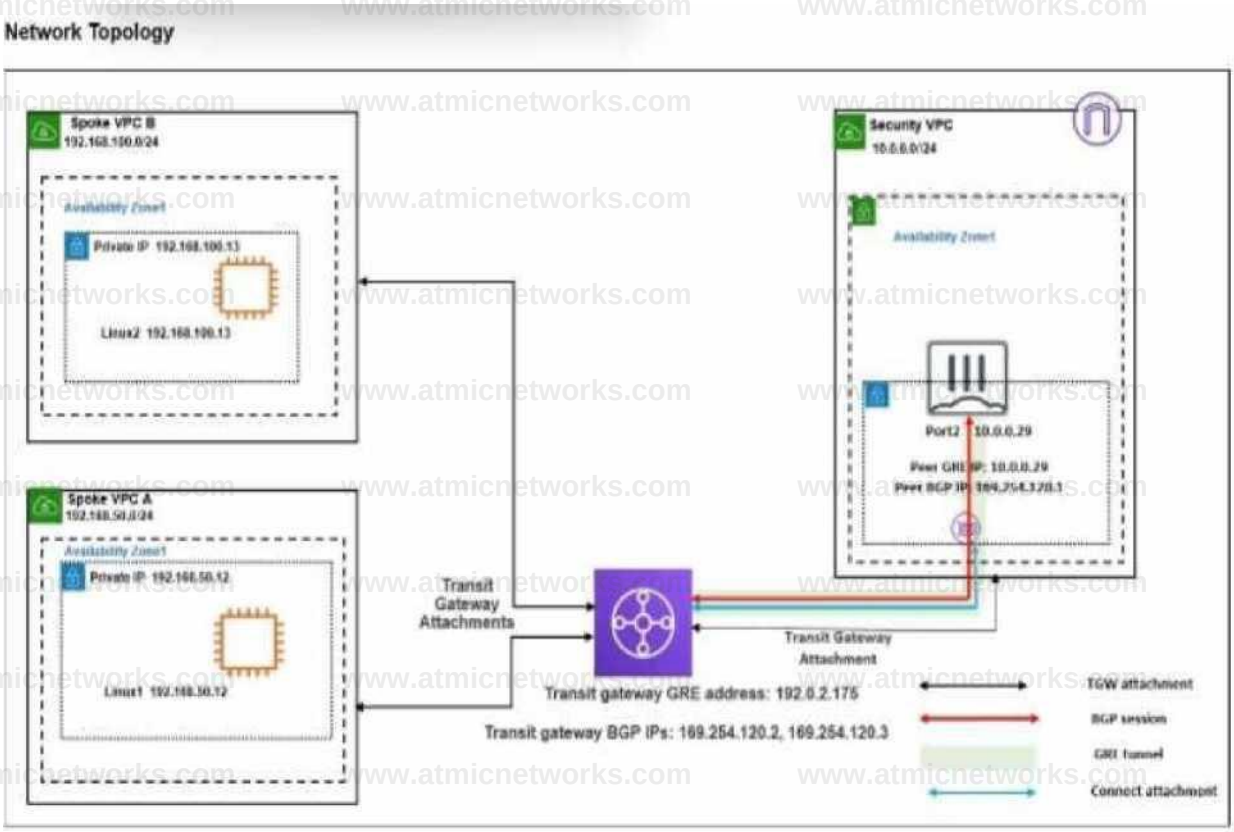
D. The opposite FortiGate port 1 IP address.

Answer: D

Explanation:

Question: 26

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 Fortinet documentation states: "An IGW in AWS is a VPC component that allows communication between instances in your VPC and the internet... AWS users with less experience may face connectivity issues if they create a new VPC, add EC2 instances to it, but forget that they need an IGW for internet connectivity."

Question: 27

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: B

Explanation:

Question: 28

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: C

Explanation:

Question: 29

Your monitoring team reports performance issues with a web application hosted in Azure. You suspect that the bottleneck might be due to unexpected inbound traffic spikes.

Which method should you use to identify and analyze the traffic pattern?

A. Deploy Azure Firewall to log traffic by IP address.

B. Enable Azure DDoS protection to prevent inbound traffic spikes.

C. Use Azure Traffic Manager to visualize all traffic to the application.

D. Enable NSG Flow Logs and analyze logs with Azure Monitor.

Answer: A

Explanation:

According to the FortiOS 7.6 Azure Administration Guide and the Fortinet 7.4 Public Cloud Security documentation regarding monitoring and troubleshooting in Microsoft Azure, administrators must utilize native diagnostic tools to gain visibility into network traffic patterns:

NSG Flow Logs (Option D): Network Security Group (NSG) flow logs are a feature of Azure Network Watcher that allows you to record information about IP traffic flowing through an NSG. These logs capture critical 5-tuple information (source/destination IP, port, and protocol) and whether the traffic was allowed or denied by specific security rules.

Traffic Pattern Analysis with Azure Monitor: To effectively analyze the "pattern" of a traffic spike, these logs are typically sent to a Log Analytics workspace within Azure Monitor. By using Traffic Analytics, the raw flow data is processed into rich visualizations and searchable datasets. This allows administrators to run Kusto Query Language (KQL) queries to identify "top talkers," visualize traffic spikes over time, and correlate the timing of these spikes with application performance degradation.

Identifying Bottlenecks: This method is preferred for identifying bottlenecks because it provides a granular view of every packet entering or leaving the subnets where the FortiGate-VM or application servers are hosted, revealing the exact nature of the inbound volume.

Why other options are incorrect:

Option A: While Azure Firewall provides logging, it is an additional security layer that may not be deployed in all environments. NSG Flow Logs are the primary and more ubiquitous method for monitoring all subnet-level traffic regardless of firewall placement.

Option B: DDoS Protection is a preventative measure; it does not provide the historical "identification and analysis" of traffic patterns required to diagnose a past performance bottleneck.

Option C: Azure Traffic Manager is a DNS-based load balancer. While it provides high-level metrics, it does not have visibility into the actual flow-level traffic data needed for a detailed pattern analysis of application bottlenecks.

Question: 30

The cloud administration team is reviewing an AWS deployment that was done using CloudFormation.

The deployment includes six FortiGate instances that required custom configuration changes after being deployed. The team notices that unwanted traffic is reaching some of the FortiGate instances because the template is missing a security group.

To resolve this issue, the team decides to update the JSON template with the missing security group and then apply the updated template directly, without using a change set.

What is the result of following this approach?

A. If new FortiGate instances are deployed later they will include the updated changes.

B. Some of the FortiGate instances may be deleted and replaced with new copies.

C. The update is applied, and the security group is added to all instances without interruption.

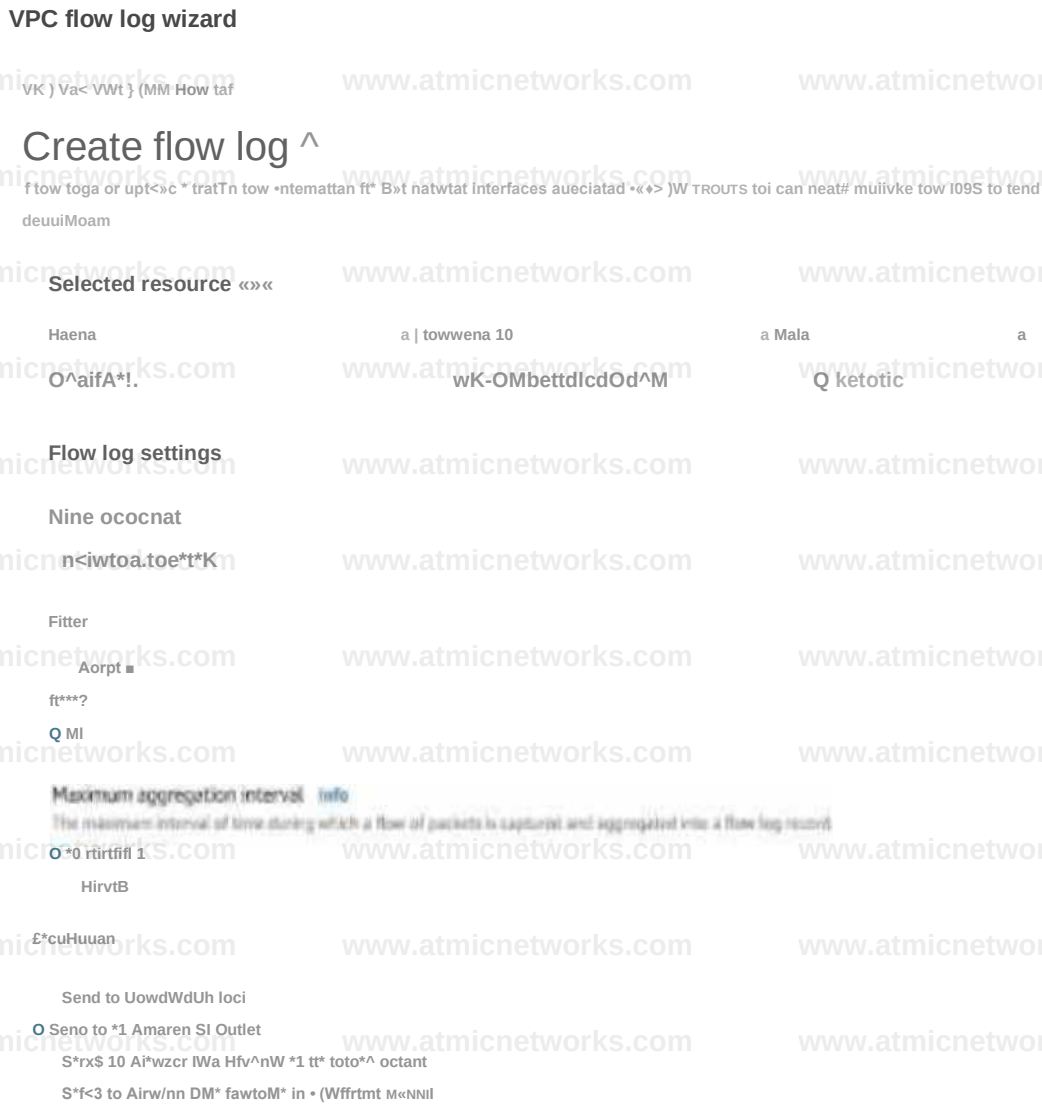
D. CloudFormation rejects the update and warns that a new full stack is required.

Answer: B

Explanation:

Question: 31

Refer to the exhibit.



An experienced AWS administrator is creating a new virtual public cloud (VPC) flow log with the settings shown in the exhibit.

What is the purpose of this configuration?

A. To maximize the number of logs saved

B. To monitor logs in real time

C. To retain logs for a long term

D. To troubleshoot a log flow issue

Answer: C

Explanation:

Question: 32

You need a solution to safeguard public cloud-hosted web applications from the OWASP Top 10 vulnerabilities. The solution must support the same region in which your applications reside, with minimum traffic cost.

Which solution meets the requirements?

A. Use FortiGate

B. Use FortiCNP

C. Use FortiWeb

D. Use FortiADC

Answer: C

Explanation:

Question: 33

An administrator is relying on an Azure Bicep linter to find possible issues in Bicep files.

Which problem can the administrator expect to find?

A. The resources to be deployed exceed the quota for a region.

B. Some resources are missing dependsOn statements.

C. There are output statements that contain passwords.

D. One or more modules are not using runtime values as parameters.

Answer: B

Explanation:

Question: 34

You have deployed a FortiGate HA cluster in Azure using a gateway load balancer for traffic inspection. However, traffic is not being routed correctly through the firewalls.

What can be the cause of the issue?

A. The FortiNet VMs have IP forwarding disabled, which is required for traffic inspection.

B. The health probes for the gateway load balancer are failing, which causes traffic to bypass the HA cluster.

C. The gateway load balancer is not associated with the correct network security group (NSG) rules, which

allow traffic to pass through.

D. The protected VMs are in a different Azure subscription, which prevents the gateway load balancer from forwarding traffic.

Answer: A

Explanation:

According to the FortiOS 7.6 Azure Administration Guide and the Cloud Security 7.4 Public Cloud Study Guide, the integration of FortiGate-VMs with an Azure Gateway Load Balancer (GWLB) requires specific network configurations to ensure packet transit:

IP Forwarding Requirement (Option A): By default, Azure Network Interfaces (NICs) drop any traffic that does not originate from or is not destined for the IP address assigned to that NIC. For a FortiGate to act as a "bump-in-the-wire" or transparent inspector, it must receive traffic destined for other IPs and forward it. This requires the IP Forwarding setting to be explicitly enabled on the FortiGate's network interfaces within the Azure portal. If this is disabled, the Azure fabric will discard the traffic being steered through the FortiGate HA cluster by the GWLB.

VXLAN Encapsulation: The Azure GWLB uses VXLAN to encapsulate traffic (adding a VXLAN header with a specific VNI) before sending it to the FortiGate. The FortiGate must terminate this VXLAN tunnel. While the VXLAN configuration is crucial, the underlying infrastructure check for IP Forwarding is the most common cause of traffic being blocked at the NIC level before the FortiOS stack can process the packet.

Why other options are incorrect:

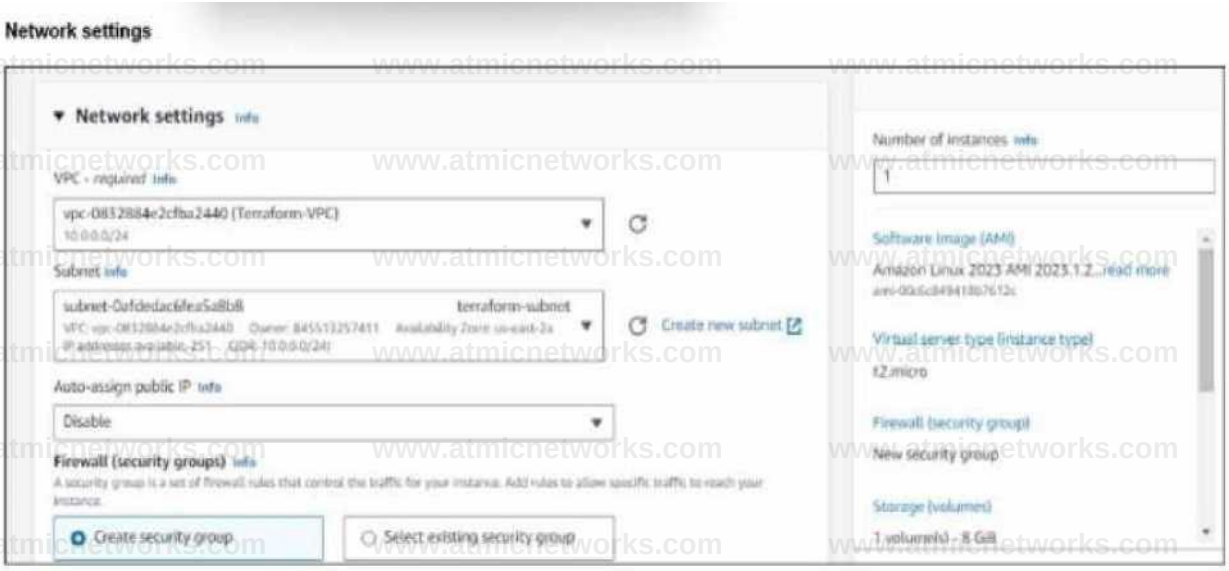
Option B: If health probes fail, the GWLB will typically stop sending traffic to that specific instance. While this affects the HA cluster's availability, the question states traffic is not being routed correctly through the firewalls (implying an active flow issue), and the primary mechanism for allowing a VM to process third-party traffic in Azure is IP Forwarding.

Option C: NSGs are typically applied to the NIC or Subnet. While incorrect NSG rules can block traffic, "IP Forwarding" is a specific requirement for the FortiGate to function as a network appliance (NVA) regardless of the NSG state.

Option D: Azure GWLB supports cross-subscription and cross-tenant chaining. The consumer (protected VMs) and the provider (FortiGate HA cluster) do not need to be in the same subscription, provided the GWLB endpoint is correctly mapped.

Question: 35

Refer to the exhibit.



You have deployed a Linux EC2 instance in Amazon Web Services (AWS) with the settings shown on the exhibit.

What next step must the administrator take to access this instance from the internet?

A. Allocate an Elastic IP address and assign it to the instance.

B. Create a VIP on FortiGate to allow access.

C. Enable SSH and allocate it to the device.

D. Configure the user name and password.

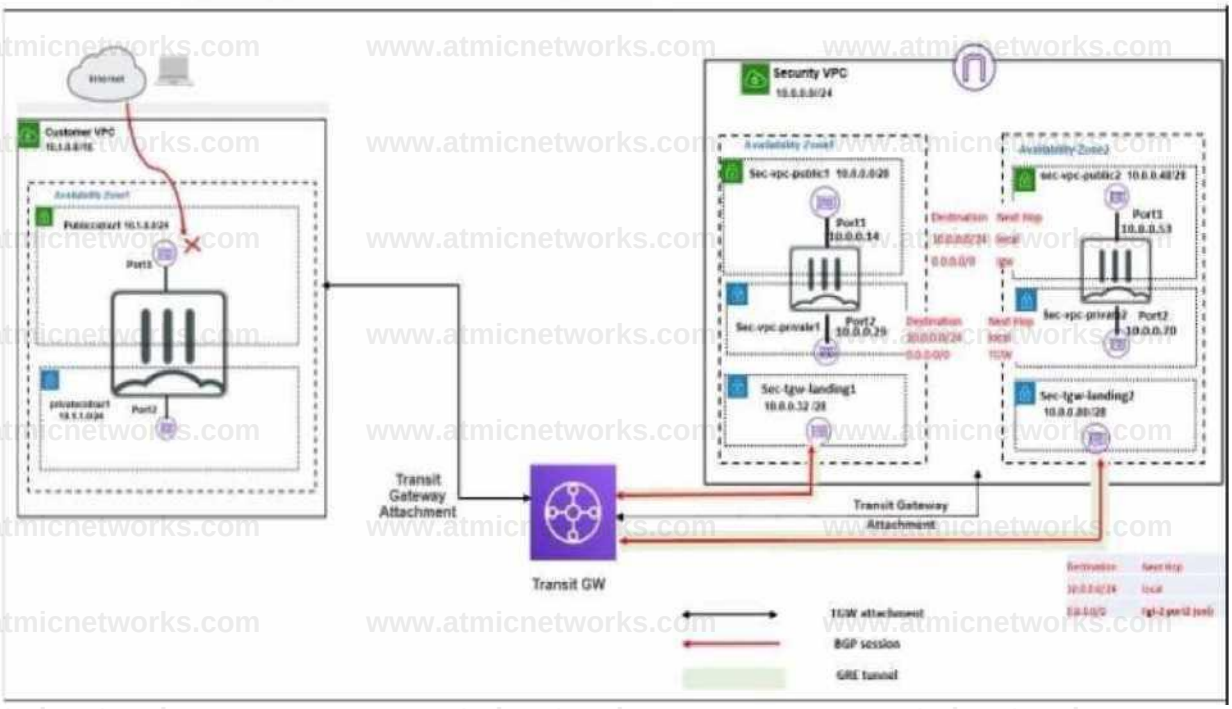
Answer: A

Explanation:

Question: 36

Refer to the exhibit.

Network Topology



In your Amazon Web Services (AWS), you must allow inbound HTTPS access to the Customer VPC FortiGate VM from the internet. However, your HTTPS connection to the FortiGate VM in the Customer VPC is not successful.

Also, you must ensure that the Customer VPC FortiGate VM sends all the outbound Internet traffic through the Security VPC.

How do you correct this issue with minimal configuration changes? (Choose three.)

A. Add a route with your local internet public IP address as the destination and the internet gateway as the target.

B. Add a route with your local internet public IP address as the destination and the transit gateway as the target.

C. Add a route to the destination 0.0.0.0/0 with the transit gateway as the target.

D. Deploy an internet gateway, associate an EIP with the Customer VPC private subnet, and then add a new route with destination 0.0.0.0/0 with the internet gateway as the target.

E. Deploy an internet gateway, attach it to the Customer VPC, and then associate an EIP with the port1 of the FortiGate in the Customer VPC.

Answer: B, C, E

Explanation:

Question: 37

Refer to the exhibit.

```
{
"AWSTemplateFcrmatVersion" : ”2010-09-09*
"Resources" : (
    "FGT-HQ-1” : {
      "Type" : "AKS::EC2::Instance”,
      "Properties" :{
      "imageid" : "ami-01bd410bcaa617f44",
      "InstanceType" : "t7.xlarge",
```

A senior administrator in a multinational organization needs to include a comment in the template shown in the exhibit to ensure that administrators from other regions change the Amazon Machine Image (AMI) ID to one that is valid in their location.

How can the administrator add the required comment in that section of the file?

A. The administrator can include the comment with the aws cloudformation update-stack command.

B. The administrator must convert the template file to YAML format to add a comment.

C. The administrator can add the comment starting with the # character next to the "Resources" section.

D. The administrator must update the AWSTemplateFormatVersion to the latest version.

Answer: B

Explanation:

According to the FortiOS 7.6 AWS Administration Guide and the Fortinet 7.4 Public Cloud Security study materials regarding infrastructure as code (IaC) for cloud deployments:

JSON Format Limitations (Option B): The exhibit shows an AWS CloudFormation template in JSON (JavaScript Object Notation) format. JSON, by its official specification, does not support comments. There is no native syntax (like // or /* */) to include remarks that are ignored by the CloudFormation parser.

YAML Support: To add descriptive comments—such as instructing other regional administrators to

update the AMI ID—the administrator must convert the template into YAML format. YAML is a superset of

JSON and specifically supports comments using the # character.

Best Practice for Multinational Deployments: For organizations operating across multiple AWS regions, using YAML is the recommended standard because it allows for inline documentation, making templates more maintainable and easier for different teams to understand regional requirements.

Why other options are incorrect:

Option A: Comments are part of the template file itself, not a parameter or flag within the aws cloudformation update-stack CLI command.

Option C: While # is the correct character for comments in YAML, it is invalid syntax in JSON and would cause the CloudFormation stack creation to fail with a parsing error.

Option D: The AWSTemplateFormatVersion "2010-09-09" is currently the only valid version for CloudFormation templates; updating it does not add JSON comment support.

Question: 38

What is the main advantage of using SD-WAN Transit Gateway Connect over traditional SD-WAN?

A. You can use BGP over IPsec for maximum throughput.

B. You can combine it with IPsec to achieve higher bandwidth.

C. It eliminates the use of ECMP.

D. You can use GRE-based tunnel attachments.

Answer: D

Explanation:

Question: 39

What are two main features in Amazon Web Services (AWS) network access control lists (NACLs)? (Choose two answers)

A. NACLs are stateless, and inbound and outbound rules are used for traffic filtering.

B. NACLs are tied to an instance.

C. The default NACL is configured to allow all traffic.

D. You cannot use NACLs and Security Groups at the same time.

Answer: A, C

Explanation:

Comprehensive and Detailed Explanation From FortiOS 7.6, FortiWeb 7.4 Exact Extract study guide:

As per the FortiOS 7.6 AWS Administration Guide and FortiWeb 7.4 cloud deployment documentation, understanding the AWS infrastructure layer is critical for integrating Fortinet virtual appliances. The two features that define AWS Network Access Control Lists (NACLs) are:

Stateless Nature (Option A): Unlike Security Groups, which are stateful (automatically allowing return traffic), NACLs are stateless. This means that if you allow inbound traffic on a specific port, you must also explicitly configure an outbound rule to allow the response traffic to leave the subnet. NACLs evaluate inbound and outbound traffic independently.

Default Configuration (Option C): Every VPC comes with a default NACL. By default, this NACL is configured to allow all inbound and outbound traffic. This is designed to ensure connectivity is not blocked until a custom security posture is defined. However, any custom NACL created manually starts by denying all traffic until rules are added.

Why other options are incorrect:

Option B: NACLs are associated at the subnet level, not the instance level. Security Groups are the components tied directly to an instance's Elastic Network Interface (ENI).

Option D: NACLs and Security Groups provide defense-in-depth and are designed to be used simultaneously. Traffic must pass through the NACL (subnet level) and then the Security Group (instance level) to reach its destination.

Question: 40

How does an administrator secure container environments in Amazon AWS from newly emerged security threats? (Choose one answer)

A. Using Docker-related application control signatures.

B. Using Amazon AWS-related application control signatures.

C. Using distributed network-related application control signatures.

D. Using Amazon AWS_S3-related application control signatures.

Answer: A

Explanation:

Comprehensive and Detailed Explanation From FortiOS 7.6, FortiWeb 7.4 Exact Extract study guide:

According to the FortiOS 7.6 Docker Administration Guide and the Public Cloud Security study materials, container

security is addressed through granular visibility into container-specific protocols.

Application Control for Containers (Option A): FortiOS includes a dedicated set of application control signatures specifically for Docker traffic. These signatures allow the FortiGate-VM to identify and control specific actions within a container environment, such as:

Docker_Pull.Blob / Docker_Pull.Manifest: Identifying when a container image is being pulled from a registry.

Docker_Push.Blob / Docker_Push.Manifest: Monitoring when images are uploaded to a registry.

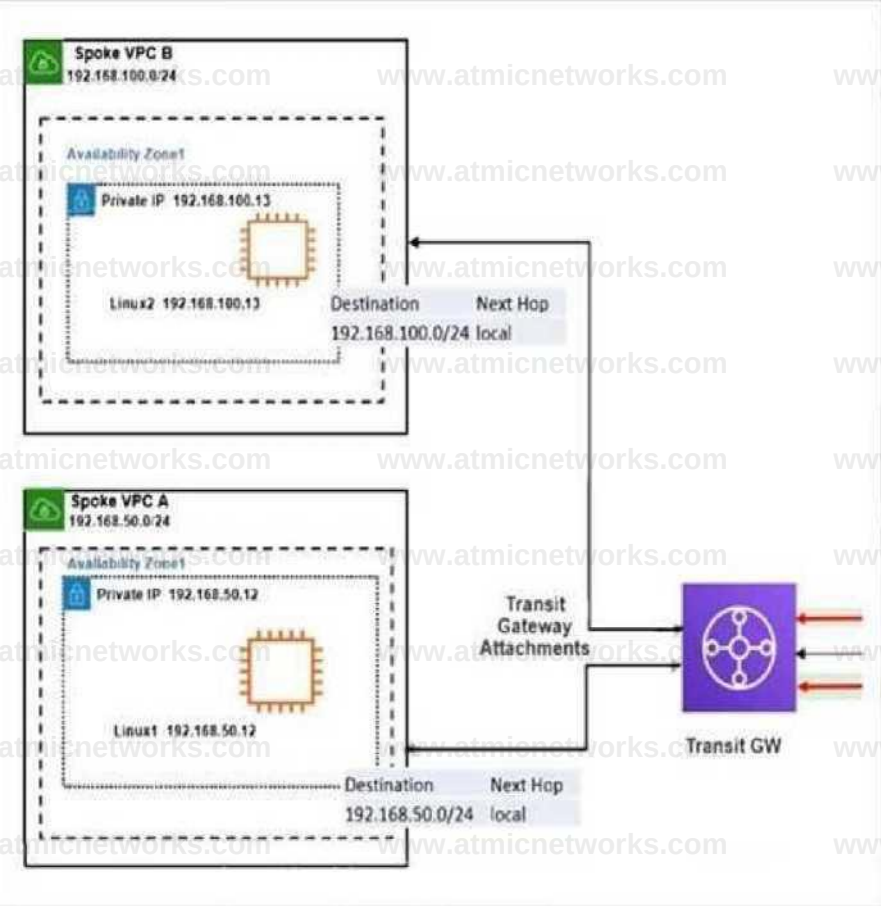
Enforcing Security Policies: By using these Docker-related signatures, an administrator can create firewall policies that only allow container pulls from known clean, private registries while blocking traffic from unauthorized or public registries that may contain vulnerable or malicious images.5

Defense-in-Depth: While traditional network-related signatures (Option C) or AWS-specific infrastructure signatures (Option B) protect the underlying network and cloud services, they do not provide the necessary visibility into the Docker API calls and manifest transfers required to secure the container lifecycle itself. FortiGate further enhances this by scanning the actual payload of these transfers using the Intrusion Prevention Service (IPS) and Advanced Malware Protection (AMP).

Question: 41

Refer to the exhibit.

Network Topology



The exhibit shows a customer deployment of two Linux instances and their main routing table in Amazon Web Services (AWS). The customer also created a Transit Gateway (TGW) and two attachments. Which two steps are required to route traffic from Linux instances to the TGW? (Choose two answers)

A. In the main subnet routing table in VPC A and B, add a new route with destination 0.0.0.0/0, next hop TGW.12

B. In the TGW route table, associate two attachments.34

C. In the TGW route table, add route propagation to 192.168.0.0/16.56

D. In the main subnet routing table in VPC A and B, add a new route with7 destination 0.0.0.0/0, next hop Internet 8gateway (IGW).

Answer: A, B

Explanation:

Comprehensive and Detailed Explanation From FortiOS 7.6, FortiWeb 7.4 Exact Extract study guide:

Based on the FortiOS 7.6 Cloud Security Study Guide regarding AWS Transit Gateway (TGW) integration and VPC routing, the following steps are mandatory to establish connectivity between Spoke VPCs via a TGW:

VPC Route Table Configuration (Option A): For traffic to leave a VPC and reach the Transit Gateway, the VPC's subnet route table must have a specific entry. While the exhibit shows local routes for internal VPC traffic (192.168.50.0/24 and 192.168.100.0/24), any traffic destined for "outside" the local VPC (such as the other Spoke VPC) must be directed to the TGW. Adding a default route (0.0.0.0/0) with the TGW ID as the next hop ensures that all non-local traffic is forwarded to the Transit Gateway for processing.

TGW Association (Option B): Within the Transit Gateway itself, connectivity is managed through Associations and Propagations. An "Association" links a specific VPC attachment to a TGW route table. Without associating the two attachments (for Spoke VPC A and Spoke VPC B) to a TGW route table, the TGW will not know which route table to use to make forwarding decisions for packets arriving from those VPCs.

Why Option C is incorrect: Route propagation is used to automatically populate the TGW route table with the CIDR blocks of the attached VPCs. While propagation is a valid step for dynamic routing, Option C specifically mentions propagating a static summary range (192.168.0.0/16) which is not the standard automated mechanism; usually, you propagate the specific VPC CIDRs. Furthermore, without the Association (Option B), propagation alone does not allow the TGW to process incoming traffic from the attachment.

Why Option D is incorrect: Directing traffic to an Internet Gateway (IGW) would send the traffic to the public internet. This would not facilitate internal routing between the two Spoke VPCs via the Transit Gateway.

Question: 42

Refer to the exhibit.

VPC flow log wizard

VPC) VOur WPG) Gtitr flaw log

Create flow log ^

Row logs can captun* IP ruffle Row mfornutlon for the network HMM Mees assocuied with your resources You can create multiple Row togs to send traffic to different destinations

Selected resources ate

Name	T Resource 10	» State	v
DefaultvPC	vpc 09d6e465Kd49d»J	©AniUMe	

Flow tog settings

Name ■ optional flo*toq..Pubti<VPC I

filer 0 Accept f Rei* t 0 All

Maximum aggregation interval info 11v nil I lfaun toumal nt i»w ckrvg wm n < Hoar of p* lrr< 4 cactusd and «»i noatrt «»I flow tog rttod O 10 minute Q 1 minute

Destination the deunauor- u -Two lo war he the to* log Hua C Sena to GoudWatth logs 0 Send to an Amazon $! bucket C Sena to Amat or Data re erose in the tame account Q Send to Amazon Data Feehote m a different account

Your team notices an unusually high volume of traffic sourced at one of the organizations FortiGate EC2 instances. They create a flow log to obtain and analyze detailed information

about this traffic. However, when they checked the log, they found that it included traffic that was not associated with the FortiGate instance in question.

What can they do to obtain the correct logs? (Choose one answer)

A. Create a new flow log at the interface level.

B. Change the maximum aggregation time to 1 minute.

C. Ensure that the flow log data is not mixed with the rest of the traffic.

D. Send the logs to Amazon Data Firehose instead to get more granular information.

Answer: A

Explanation:

Comprehensive and Detailed Explanation From FortiOS 7.6, FortiWeb 7.4 Exact Extract study guide:

According to the FortiOS 7.6 AWS Administration Guide and the Public Cloud Security documentation regarding AWS VPC Flow Logs, the level at which a flow log is created determines the scope of the data collected:

Flow Log Scope and Hierarchy (Option A): AWS VPC Flow Logs can be created at three different levels: VPC, Subnet, or Network Interface (ENI).

As seen in the exhibit (VPC flow log wizard), the flow log is being created for the resource vpc-09d6e4631cd49d2b3. When a flow log is created at the VPC level, it captures IP traffic for all network interfaces within that VPC.

To isolate traffic specifically for a single FortiGate EC2 instance and avoid seeing traffic from other instances in the same VPC or subnet, the administrator must create a flow log at the Network Interface level. This provides the most granular visibility and ensures the logs only contain traffic associated with the specific ENIs of that FortiGate instance.

Why other options are incorrect:

Option B: Changing the maximum aggregation interval from 10 minutes to 1 minute increases the frequency of log delivery and captures shorter-lived flows more accurately, but it does not change the scope of the resources being monitored.

Option C: This is a general troubleshooting statement and not a configuration action within the AWS Flow Log wizard that would filter the traffic by instance.

Option D: Changing the destination to Amazon Data Firehose changes how the logs are processed and delivered (e.g., for streaming to a SIEM), but the source data is still determined by the resource level selected (VPC vs. Interface).

Question: 43

Your administrator instructed you to deploy an Azure vWAN solution to create a connection between the main company site and branch sites to the other company VNETs. What is the best connection solution available between your company headquarters, branch sites, and the Azure vWAN hub? (Choose one answer)

A. An L2TP connection

B. SSL VPN connections

C. GRE tunnels

D. ExpressRoute

Answer: D

Explanation:

Comprehensive and Detailed Explanation From FortiOS 7.6, FortiWeb 7.4 Exact Extract study guide:

According to the FortiOS 7.6 Azure Administration Guide and the Fortinet 7.4 Public Cloud Security documentation regarding Azure Virtual WAN (vWAN) architectures, the choice of connectivity depends on the required performance, security, and scale:

ExpressRoute (Option D): For a large-scale enterprise deployment involving a company headquarters and multiple branch sites, ExpressRoute is the "best" and most robust solution. It provides a private, dedicated, and high-throughput connection (up to 100 Gbps) that bypasses the public internet entirely. This ensures predictable low latency and higher reliability compared to internet-based tunnels.

Virtual WAN Integration: Azure vWAN Standard SKU explicitly supports ExpressRoute gateways as a primary connectivity method for on-premises sites. This allows the vWAN hub to act as a global transit point, seamlessly connecting the ExpressRoute-linked headquarters to other branch sites and VNET spokes.

Scalability for Headquarters: While site-to-site IPsec VPNs are common for smaller branches, the "main company site" or headquarters typically requires the high bandwidth and SLA guarantees provided by ExpressRoute.

Why other options are incorrect:

Option A & B: L2TP and SSL VPN are primarily used for remote user access (Point-to-Site) rather than permanent site-to-hub infrastructure connections. vWAN uses OpenVPN or IKEv2 for user VPNs, not L2TP.

Option C: While GRE tunnels are used in some networking scenarios, they are not a native, primary gateway connectivity option for the Azure vWAN hub compared to the standardized Site-to-Site VPN (IPsec) and ExpressRoute.

Question: 44

Refer to the exhibit.

Which FortiCNP policy type generated the finding shown in the exhibit? (Choose one answer)

A. This finding was generated by a data scan policy.

B. This finding was generated by a threat detection policy.

C. This finding was generated by a risk management policy.

D. This finding was generated by a file collection policy.

Answer: B

Explanation:

Comprehensive and Detailed Explanation From FortiOS 7.6, FortiWeb 7.4 Exact Extract study guide:

Based on the FortiCNP 22.4/24.4 Administration Guide and the Fortinet Cloud Security Study Guide, findings in FortiCNP are categorized by the specific policy type that triggered the alert.

Threat Detection Policy (Option B): This policy category is designed to monitor and alert on anomalous User Activity and Network threats. Specifically, "Suspicious Location" is a predefined threat detection rule that triggers when a user performs an action (such as a Download File as seen in the exhibit) from a geographic location or IP address that is not on the organization's allow list or deviates from established behavioral baselines. The exhibit explicitly shows the "Activity Type" as "Download File" and the "Policy Name" as "Suspicious Location," both of which fall under the Threat Detection > User Activity policy tab.

Policy Hierarchy and Finding Types:

Threat Detection: Includes User Activity (Suspicious Location, Suspicious Time, Suspicious Movement) and Network findings.

Data Scan Policy (Option A): These policies are used for content-level inspection, such as searching for Malware or Data Loss Prevention (DLP) patterns like credit card numbers within files.

Risk Management Policy (Option C): These policies focus on Cloud Security Posture Management (CSPM), alerting

on misconfigurations such as unencrypted buckets or disabled logging (e.g., CloudTrail).

File Collection (Option D): While "File Collection" is a configuration object used to define a group of files for monitoring, it is not the policy type that generates a behavioral alert like "Suspicious Location".

Question: 45

Refer to the exhibit.

what-if tool

```
Resource and property changes are indicated with these symbols - Delete
    + Create
    * Modify
The deployment will update the following scope:
Scope: /subscriptions/./resourceGroups/ExampleGroup
* Microsoft.Network/virtualNetworks/vnet-002 [2018-10-01]
      - tags.Owner: "Production"
      * properties.subnets: (
        + 0:
              name: Brave-Dumps.com              "subnetOOl"
              properties.addressPrefix: "10.0.0.0/25"
Resource changes: 1 to modify.
```

An administrator used the what-if tool to preview the changes to an Azure Bicep file. What will happen if the administrator applies these changes in Azure? (Choose one answer)

A. A new subnet will be added to vnet-002.

B. The vnet-002 VNet will be renamed Production.

C. The resulting VNet will have a single subnet.

D. The VNet address space will be updated.

Answer: A

Explanation:

Comprehensive and Detailed Explanation From FortiOS 7.6, FortiWeb 7.4 Exact Extract study guide:

Based on the FortiOS 7.6 Azure Administration Guide and standard Azure Resource Manager (ARM) deployment practices, the what-if operation allows administrators to preview how a deployment will affect the current state of resources.

Interpreting the What-If Output (Option A): The exhibit shows the results of a change preview for a Virtual Network (vnet-002).

The symbol ~ (Modify) next to the VNet indicates that an existing resource is being updated rather than created or deleted.

The symbol - (Delete) next to tags.Owner: "Production" indicates that this specific tag will be removed from the VNet.

Crucially, the symbol + (Create) appearing inside the properties.subnets array next to index 0: indicates the addition of a new element. This confirms that a new subnet named subnet001 with the address prefix 10.0.0.0/25 will be added to the existing Virtual Network vnet-002.

Why other options are incorrect:

Option B: The text shows that the tag "Production" is being deleted (-), not that the VNet is being renamed to "Production."

Option C: The what-if tool only displays the changes. While one subnet is being added (+), the tool does not show the deletion of other existing subnets. Therefore, we cannot conclude the resulting VNet will have only a single subnet; it will have its existing subnets plus the new one.

Option D: There is no mention of addressSpace or addressPrefixes for the VNet itself being modified (~) or added (+) in the exhibit; only a subnet-level address prefix is shown.

Question: 46

An administrator is looking for a solution that can provide insight into users and data stored in major SaaS applications in the multicloud environment. Which product should the administrator deploy to have secure access to SaaS applications? (Choose one answer)

A. FortiSandbox

B. FortiCASB

C. FortiWeb

D. FortiSIEM

Answer: B

Explanation:

Comprehensive and Detailed Explanation From FortiOS 7.6, FortiWeb 7.4 Exact Extract study guide:

Based on the Fortinet Cloud Security 7.4 documentation and the FortiCASB Administration Guide, secur5ing a multi6cloud environment requires specialized tools for Software-as-a-Service (SaaS) visibility:

SaaS Visibility and Protection (Option B): FortiCASB (Cloud Access Security Broker) is a cloud-native service designed specifically to provide insight into users and data stored within major SaaS applications like Office 365, Google Drive, and Salesforce.

Key Capabilities:

Data Discovery: It allows administrators to scan and identify sensitive data (PII, PCI, etc.) stored within SaaS platforms to prevent data leakage.

User Behavior Monitoring: It tracks user activities and alerts on anomalous behavior, such as logins from suspicious locations or excessive file downloads, to ensure secure access.

Threat Protection: It integrates with FortiGuard to scan files within the cloud for malware, providing a layer of security that traditional network firewalls cannot reach once the data is inside the SaaS provider's infrastructure.

Why other options are incorrect:

Option A: FortiSandbox is used for advanced threat detection by executing suspicious files in a safe environment; it does not provide user/data management for SaaS applications.

Option C: FortiWeb is a Web Application Firewall (WAF) designed to protect web applications and APIs hosted on-premises or in the cloud from attacks like SQL injection; it is not a SaaS security broker.

Option D: FortiSIEM is a security information and event management solution used for crossinfrastructure logging and correlation; while it can ingest logs from SaaS, it does not provide the native data-level insights or direct access controls that FortiCASB offers.

Question: 47

Refer to the exhibit.

```
AWSTemplateFormatVersion: ”2010-09-09’’
Resources:
  FortiGateActive:
```

```
Type: "AWS::EC2::Instance"
Properties:
  ImageId: "ami-0lbd410bcaa617f44"
  InstanceType: t2.large
```

A senior administrator in a multinational organization needs to include a comment in the template shown in the exhibit to ensure that administrators from other regions change the EC2 instance size value to one that meets the requirements in their local deployments. How can the administrator add the comment in that section of the file? (Choose one answer)

A. The administrator can run the aws cloudformation update-stack and include the comment.

B. The administrator must update the AWSTemplateFormatVersion to a more current version.

C. The administrator must convert the template to JSON format before adding the comment.

D. The administrator can add the comment with the # character next to the InstanceType section.

Answer: D

Explanation:

Comprehensive and Detailed Explanation From FortiOS 7.6, FortiWeb 7.4 Exact Extract study guide:

According to the FortiOS 7.6 AWS Administration Guide and the Public Cloud Security documentation regarding AWS CloudFormation templates:

YAML Format and Comments (Option D): The exhibit provided (image_dce708.png) displays an AWS CloudFormation template in YAML (YAML Ain't Markup Language) format. Unlike JSON, YAML natively supports inline and block comments using the # character. An administrator can simply add # followed by the instruction next to the InstanceType line, and the CloudFormation parser will ignore it during stack creation.

Infrastructure as Code (IaC) Best Practices: In a multinational deployment environment, using comments in YAML templates is a critical best practice for documentation. It allows the lead administrator to provide context for regional teams (e.g., "Change t2.large to a supported instance type in your region") directly within the code.

Why other options are incorrect:

Option A: The aws cloudformation update-stack command is used to apply changes to an existing stack. While you can provide a "Description" for the stack, it does not allow you to inject comments into the source template file itself.

Option B: The AWSTemplateFormatVersion "2010-09-09" is the only currently supported version for

CloudFormation. Changing this would not impact comment functionality, as comment support is a property of the YAML file format, not the template version.

Option C: Converting the template to JSON would be counterproductive because the standard JSON specification does not support comments. If the template were in JSON, the administrator would actually need to convert it to YAML to add comments.

Question: 48

You are experiencing intermittent connectivity issues in a FortiGate HA cluster deployed with Azure gateway load balancer. Traffic is being dropped when it passes through the cluster. What is the cause of the issue? (Choose one answer)1

A. The FortiGate firewalls are using the default maximum transmission unit (M2TU) size supported by Azure.

B. The Azure gateway load balancer is configured with an incorrect health probe port.

C. The Azure gateway load balancer is blocking large packets, causing traffic failures.

D. The protected VMs are running an application that fragments packets.

Answer: A

Explanation:

Comprehensive and Detailed Explanation From FortiOS 7.6, FortiWeb 7.4 Exact Extract study guide:

According to the FortiOS 7.6 Azure Administration Guide and the Public Cloud Security documentation regarding Azure Gateway Load Balancer (GWLB) integration:

Encapsulation Overhead: Azure Gateway Load Balancer uses VXLAN (Virtual eXtensible LAN) to encapsulate the traffic before sending it to the FortiGate-VM HA cluster. This encapsulation adds a header that typically consists of 50 bytes for regular IPv4 traffic (Ethernet, IP, UDP, and VXLAN headers).

MTU Mismatch (Option A): The default maximum transmission unit (MTU) in Azure is 1500 bytes. If a protected VM sends a packet at the maximum default size (1500 bytes), and the GWLB then adds the 50-byte VXLAN header, the resulting encapsulated packet becomes 1550 bytes.

Packet Drops: If the FortiGate-VM's network interfaces are left at the default MTU of 1500 bytes, they will not be able to process the 1550-byte encapsulated frames without fragmentation. Because many network paths or configurations (including Azure's fabric for certain flows) may drop packets that require fragmentation or have the Don't Fragment (DF) flag set, this results in the observed intermittent connectivity issues and dropped traffic.

Required Resolution: To resolve this issue, administrators must increase the MTU on the FortiGate- VM interfaces (specifically the one receiving GWLB traffic) to at least 1570 bytes to accommodate both IPv4 and IPv6 VXLAN overhead.

Why other options are incorrect:

Option B: While an incorrect health probe port would cause the GWLB to mark the FortiGate as down, it would typically lead to a complete loss of traffic flow through that instance rather than intermittent packet drops within an active flow.

Option C: The GWLB itself is the component adding the overhead; it is the FortiGate's inability to receive the larger resulting frame (due to its own default MTU setting) that causes the failure.

Option D: Packet fragmentation by the application is a secondary effect. The primary "intermittent" issue described in GWLB deployments is almost always related to the tunneling overhead exceeding the receiving interface's MTU.

Question: 49

Refer to the exhibit.

variable configuration

```
variable access key ()
variable secret key {)

variable "region" (
  default = "eu-west-1"
}
// Availability zones for the region
variable "azl"(
  default = "eu west-la"
I

variable "vpccidr" (
  default = “10.2.0.0/16"
}
variable "publiccidrazl" {
  default = "10.1.0.0/24"
I

variable "privatecidrazl" { default = "10.1.1.0/24"
}

// License Type to create FortiGate-VM
// Provide the license type for FortiGate-VM Instances, either
byol or payg variable "license_type" {
  default = "byol" "8rave-0umps.com"
}

// AMIs are for FGTVM-AWS(PAYG) • 7.6 0 variable "fgtvmami" {
```

You are tasked to deploy a FortiGate VM with private and public subnets in Amazon Web Services (AWS). You examined the variables.tf file. Assume that all the other terraform files are in place. What will be the final result after running the terraform init and terraform apply commands? (Choose one answer)

A. Terraform will not deploy a FortiGate VM.

B. Terraform will deploy a FortiGate VM in the eu-West-1a availability zone without any subnets.

C. Terraform will deploy a FortiGate VM in the eu-West-1 region with private and public subnets.

D. Terraform will deploya FortiGate VM in the eu-West-1a availability zone with two subnets and BYOL license.

Answer: A

Explanation:

Comprehensive and Detailed Explanation From FortiOS 7.6, FortiWeb 7.4 Exact Extract study guide:

Based on the FortiOS 7.6 AWS Administration Guide and the Fortinet 7.4 Public Cloud Security documentation regarding Terraform deployments:

Variable Validation and Logic (Option A): The variables.tf file contains a logic error that prevents a successful deployment.

Specifically, the variable license_type has a default value defined as "byol" "Brave-Dumps.com".

In Terraform HCL (HashiCorp Configuration Language), a variable's default attribute can only hold a single value string (e.g., "byol"). The inclusion of the secondary string "Brave-Dumps.com" within the same default assignment is a syntax error.

Impact on Execution: When terraform apply is executed, the Terraform engine performs a validation check on all loaded files. Because of this syntax error in the variable definition, the validation will fail, and Terraform will stop execution with an error message before any resources—including the FortiGate VM—are created in AWS.

Network Mismatch: Additionally, the variable vpccidr is set to 10.2.0.0/16, while the public (10.1.0.0/24) and private (10.1.1.0/24) subnets are defined within a completely different address space (10.1.x.x). Even if the syntax error were fixed, the deployment would likely fail at the infrastructure level because subnets must reside within the CIDR block of their parent VPC.

Why other options are incorrect:

Option B, C, & D: None of these successful deployment outcomes can occur because the Terraform parser will identify the invalid syntax in the variables.tf file and abort the process entirely.

Question: 50

Refer to the exhibit.

An administrator installed a FortiWeb ingress controller to protect a containerized web application. What is the reason for the status shown in FortiView? (Choose one answer)

A. The SDN connector is not authenticated correctly.

B. The FortiWeb VM is missing a route to the node subnet.

C. The manifest file deployed is configured with the wrong node IP addresses.

D. The load balancing type is not set to round-robin.

Answer: B

Explanation:

Comprehensive and Detailed Explanation From FortiOS 7.6, FortiWeb 7.4 Exact Extract study guide:

According to the FortiWeb 7.4 Administration Guide and the FortiWeb Ingress Controller Installation Guide, the status of backend servers in the FortiView Topology dashboard is a direct reflection of the health check results.

Interpreting the Status Icon (Orange): In the FortiView Topology view, a green circle indicates that the server is up and responding to health checks, while an orange circle indicates that the server is not running or is unreachable.

Connectivity and Routing (Option B): For the FortiWeb ingress controller to accurately monitor and protect a containerized application, it must have a valid network path to the Kubernetes (K8s) worker nodes. If the FortiWeb VM is missing a route to the specific subnet where the K8s nodes reside, the health check packets will fail to reach their destination. As a result, FortiWeb identifies the backend servers (192.168.0.1, 192.168.0.2, and 192.168.0.3) as "Down," leading to the orange status shown in the exhibit.

Health Check Failures: When the status is orange, it implies that the Server Health Check (configured in the server pool) is detecting that the web servers are not responsive to connections. While this could be caused by an application-level failure, in a fresh cloud deployment of an ingress controller, the most common underlying cause is a network routing misconfiguration preventing the FortiWeb appliance from reaching the node IPs.12

Why other options are incorrect:34

Option A: If the SDN connector were not authenticated correctly, FortiWeb would likely fail to discover the containerized resources entirely, rather than discovering them and repor5ting them as "Down".6

Option C: While wron7g IP addresses would cause a failure, the Ingress Controller's job is to dynamically sync these addresses from the K8s API; a manual configuration error in a manifest file regarding IP addresses is less likely in an automated ingress environment.

Option D: The load balancing algorithm (Round Robin, Least Connections, etc.) affects how traffic is distributed, but it does not influence the up/down health status of the individual backend servers.

Question: 51

You are investigating an attack path for a top risky host. You notice that the Common Vulnerability Scoring System (CVSS) and the vulnerability impact scores are very high. However, the attack path severity for the top risky host itself is low. Which two pieces of contextualized information can help you understand why? (Choose two answers)

A. The FortiCNAPP risk score

B. The package status

C. The vulnerability score

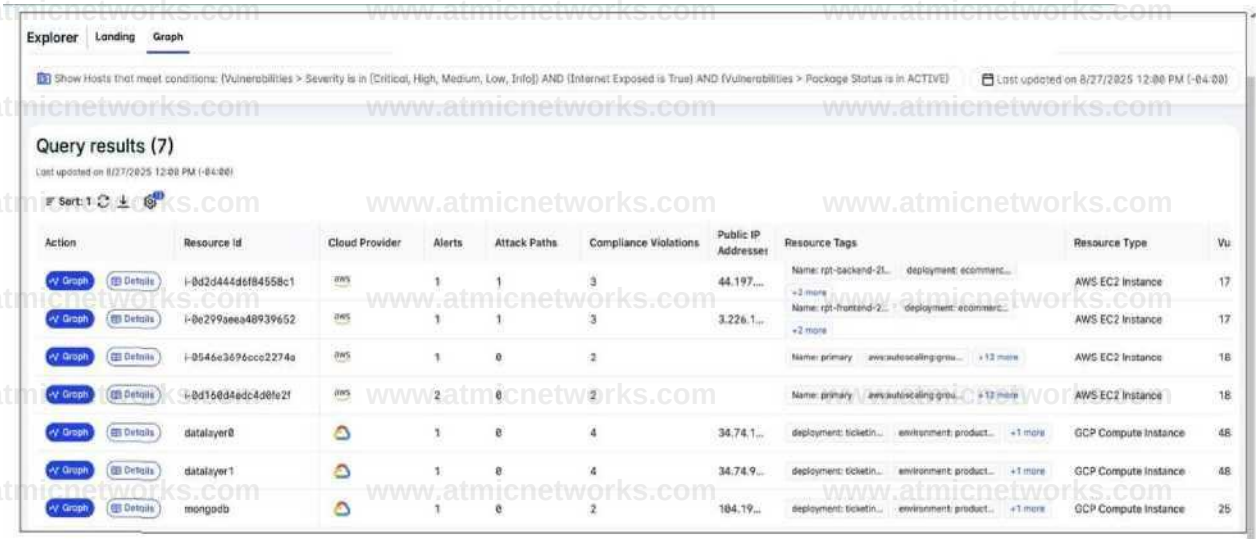
D. The fix version

Answer: AB

Explanation:

Question: 52

Refer to the exhibit.



A FortiCNAPP administrator used the FortiCNAPP Explorer to reveal all hosts exposed to the internet that are running active packages with vulnerabilities of all severity levels. Why do only the first two results have an attack path? (Choose one answer)

A. Attack paths areavailable only for AWS resources with public IP addresses.

B. Attack paths areavailable only for AWS resources with high impact scores.

C. Attack paths areavailable only for resources with potential multi-hop exposure.

D. Attack paths areavailable only for resources that have critical vulnerabilities.

Answer: A

Explanation:

Comprehensive and Detailed Explanation From FortiOS 7.6, FortiWeb 7.4 Exact Extract study guide:

Based on the FortiCNAPP (formerly Lacework) Cloud Security documentation regarding Attack Path Analysis and Explorer functionality:

Attack Path Generation (Option A): In FortiCNAPP, an "Attack Path" is a visualized sequence of potential exploit steps that an external attacker could take to reach a sensitive resource. For the platform to generate and display an attack path, the target resource must be externally reachable.

Evidence in the Exhibit: * The exhibit shows a list of EC2 and GCP instances.

The first two results (Resource IDs i-0d2d... and i-0e29...) have values populated in the Public IP Addresses column (44.197 ..... and 3.226). Consequently, these are the only two resources showing a value of 1 in the Attack Paths column.

The remaining resources in the list do not have public IP addresses listed in the exhibit's view, and as a result, their Attack Paths count is 0. This confirms that FortiCNAPP specifically calculates these

paths for resources that have a direct entry point from the internet via a public IP.

Contextual Risk Assessment: FortiCNAPP prioritizes attack path analysis for internet-exposed assets because they represent the highest immediate risk. While internal resources may have vulnerabilities, the lack of a public-facing network interface means there is no direct external "path" to visualize in this specific Explorer view.

Question: 53

You have onboarded the organization's Microsoft Azure account on FortiCNAPP using the automated configuration approach. However, FortiCNAPP does not appear to be receiving any workload scanning data. How can you remedy this? (Choose one answer)

A. Add a new Azure App Registration.

B. Add a service principal in the Azure Cloud Shell.

C. Add a FortiCNAPP threat policy to monitor Azure workloads.

D. Add the appropriate integration type using the guided configuration.

Answer: D

Explanation:

Comprehensive and Detailed Explanation From FortiOS 7.6, FortiWeb 7.4 Exact Extract study guide:

Based on the FortiCNAPP 24.x Administration Guide regarding Microsoft Azure onboarding and feature

activation:

Separation of Integration Types (Option D): In FortiCNAPP, onboarding a cloud account via the automated configuration approach often initializes the Cloud Security Posture Management (CSPM) and Cloud Infrastructure Entitlement Management (CIEM) features. However, Workload Scanning (specifically Agentless Scanning) is treated as a distinct integration type within the platform.

Guided Configuration Requirement: Even after the account is onboarded, the administrator must navigate to the Integrations or Onboarding section and specifically add the Workload Scanning integration for that Azure account. This "Guided Configuration" ensures that the necessary additional permissions (such as those required to create snapshots of disks and scan them) and resources (like the scanner VNet or regional scanners) are properly deployed within the Azure environment.

Why other options are incorrect:

Option A & B: Automated onboarding already handles the creation of necessary App Registrations and Service Principals. Manually adding more without following the specific integration workflow will not activate the workload scanning engine.

Option C: Threat policies are used to generate alerts based on existing data. If the raw workload scanning data is not being received from Azure, a policy will have no data to analyze; the issue is at the ingestion/integration layer, not the policy layer.

Question: 54

A customer would like to use FortiGate fabric integration with FortiCNP. When adding a FortiGate VM to FortiCNP, which three mandatory configuration steps must you follow on FortiGate? (Choose three answers)

A. Enable pre-shared key on both sides.

B. Import the FortiGate certificate into FortiCNP.

C. Configure FortiGate to send logs to FortiCNP.

D. Create an IPS sensor and a firewall policy.

E. Create an SSL/SSH inspection profile.

Answer: C, D, E

Explanation:

Comprehensive and Detailed Explanation From FortiOS 7.6, FortiWeb 7.4 Exact Extract study guide:

According to the FortiCNP 24.x Administration Guide and the FortiOS 7.6 Security Fabric Integration documentation, integrating a FortiGate-VM with FortiCNP requires specific local configurations on the FortiGate to ensure the cloud security platform can ingest and analyze traffic data.

Configuring Logging (Option C): Before adding the FortiGate VM to FortiCNP, the administrator must Enable Send Logs on the FortiGate. This allows the FortiGate to forward the necessary security telemetry and traffic logs to the FortiCNP cloud endpoint for threat correlation and risk analysis.

Policy and Inspection Setup (Option D): The integration relies on the FortiGate's ability to identify and block threats at the network layer. Specifically, the administrator must Create a FortiGate IPS Sensor and Create a FortiGate Firewall Policy. The IPS sensor detects malicious patterns, while the firewall policy dictates which traffic is subjected to this inspection.

Deep Packet Inspection (Option E): To provide visibility into encrypted traffic—which is critical for identifying threats hidden in HTTPS flows—the administrator must Create an SSL/SSH Inspection Profile on the FortiGate. Without this profile, FortiCNP would lose significant visibility into potential attack vectors utilizing encrypted channels.

Why other options are incorrect:

Option A: While pre-shared keys are used in VPN and some Fabric setups, they are not listed as one

of the specific mandatory steps for the initial FortiGate-to-FortiCNP fabric integration workflow.

Option B: While certificate exchange is part of the overall trust relationship, the primary "mandatory configuration steps on FortiGate" defined in the official setup guide focus on the logging and security profile components required to generate the data FortiCNP needs.