Number: PSE-PrismaCloud
Passing Score: 800
Time Limit: 120
File Version: 3.0

Exam Code: PSE-PrismaCloud

Exam Name: Palo Alto Networks System Engineer - Prisma Cloud

Exam A

QUESTION 1
Prisma Public Cloud enables compliance monitoring and reporting by mapping which configurations to compliance standards?

A. RQL queries
B. alert rules
C. notification templates
D. policies

Correct Answer: D
Section:

QUESTION 2
What configuration on AWS is required in order for VM-Series to forward traffic between its network interfaces?

A. Both Source and Destination Checks are disabled
B. Both Source and Destination Checks are enabled
C. Source Check is disabled and Destination Check is enabled
D. Source Check is enabled and Destination Check is disabled

Correct Answer: A
Section:
Explanation:
https://docs.paloaltonetworks.com/vm-series/9-0/vm-series-deployment/set-up-the-vm-series-firewall-on-aws/use-case-secure-the-ec2-instances-in-the-aws-cloud

QUESTION 3
Amazon Web Services WAF can be enabled on which two resources?(Choose two.)

A. AWS CDN
B. AWS NAT Gateway
C. AWS ALB
D. AWS NLB

Correct Answer: A, C
Section:

QUESTION 4
Which three methods can provide application-level security for a web server instance on Amazon Web Services? (Choose three.)

A. Traps
B. Prisma SaaS
C. Amazon Web Services WAF
D. VM-Series firewalls

E. Security Groups

Correct Answer: A, C, D
Section:

QUESTION 5
Which RQL string searches for all EBS volumes that do not have a 'DataClassification' tag?

A. config where api.name = 'aws-ec2-describe-volumes, AND json.rule = tags[*]key contains DataClassification
B. config where api.name = ,aws-ec2-describe-volumes' AND json.rule = tags[*]key != DataClassification
C. config where api.name = ,aws-ec2-describe-volumes' AND json.rule = tags[*].key exists
D. config where api.name = 'aws-ec2-describe-volumes' AND json.rule = tags[*].key = 1

Correct Answer: B
Section:

QUESTION 6
Which three services can Google Cloud Security Scanner assess? (Choose three.)

A. Google Kubernetes Engine
B. BigQuery
C. Compute Engine
D. App Engine
E. Google Virtual Private Cloud

Correct Answer: A, C, D
Section:

QUESTION 7
In which two ways does Palo Alto Networks VM orchestration help service providers automatically provision security instances and policies? (Choose two.)

A. fully instrumented API
B. Aperture Orchestration Engine
C. VM Orchestration Policy Editor
D. support for Dynamic Address Groups

Correct Answer: A, D
Section:

QUESTION 8
Which change represents a VM-Series NGFW license transfer?

A. VM-100 BYOL on Microsoft Azure to VM-100 BYOL on Amazon Web Services
B. VM-300 BYOL on Microsoft Azure to VM-300 PAY6 on Amazon Web Services
C. VM-100 BYOL on Microsoft Azure to VM-300 BYOL on Microsoft Azure
D. VM-100 BYOL on Microsoft Azure to VM-300 PAYG on Amazon Web Services

Correct Answer: C
Section:

QUESTION 9
The VM-Series integration with Amazon GuardDuty feeds malicious IP addresses to the VM-Series NGFW using XML API to populate a Dynamic Address Group within a Security policy that blocks traffic.
How does Amazon Web Services achieve this integration?

A. SNS
B. SQS
C. CodeDeploy
D. Lambda

Correct Answer: D
Section:

QUESTION 10
What are two examples of Amazon Web Services logging services? (Choose two.)

A. CloudLog
B. CloudEvent
C. CloudWatch
D. CloudTrail

Correct Answer: C, D
Section:

QUESTION 11
Which three anomaly policies are predefined in Prisma Public Cloud? (Choose three.)

A. Excessive login failures
B. Unusual user activity
C. Denial-of-service activity
D. Account hijacking attempts
E. Suspicious file activity

Correct Answer: A, B, D
Section:
Explanation:
Account hijacking attempts
---Detect potential account hijacking attempts discovered by identifying unusual login activities. These can happen if there are concurrent login attempts made in short duration from two different geographic locations, which is
impossible time travel
, or login from a previously unknown browser, operating system, or location.
Excessive login failures
---Detect potential account hijacking attempts discovered by identifying brute force login attempts. Excessive login failure attempts are evaluated dynamically based on the models observed with continuous learning.
Unusual user activity
---Discover insider threat and an account compromise using advanced data science. The Prisma Cloud machine learning algorithm profiles a user's activities on the console, as well as the usage of access keys based on the location and the type of cloud resources.

https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/prisma-cloud-policies/anomaly-policies.html

QUESTION 12
Which two data sources are ingested by Prisma Cloud? (Choose two.)

A. network flow logs
B. list of all database instances' tables
C. metadata about compute resources' configuration
D. Cortex Data Lake

Correct Answer: A, C
Section:

QUESTION 13
Which pillar of the Prisma Cloud platform can secure outbound traffic, stop lateral attack movement, and block inbound threats?

A. Cloud Workload Protection (CWP)
B. Cloud Code Security
C. Cloud Network Security
D. Cloud Identity Security

Correct Answer: C
Section:

QUESTION 14
Which statement applies to vulnerability management policies?

A. Host and serverless rules support blocking, whereas container rules do not.
B. Rules explain the necessary actions when vulnerabilities are found in the resources of a customer environment.
C. Policies for containers, hosts, and serverless functions are not separate.
D. Rules are evaluated in an undefined order.

Correct Answer: B
Section:

QUESTION 15
An administrator deploys a VM-Series firewall into Amazon Web Services. Which attribute must be disabled on the data-plane elastic network interface for the instance to handle traffic that is not destined to its own IP address?

A. security group
B. tags
C. elastic ip address
D. source/destination checking

Correct Answer: D
Section:
Explanation:

https://docs.paloaltonetworks.com/vm-series/8-1/vm-series-deployment/set-up-the-vm-series-firewall-on-aws/deploy-the-vm-series-firewall-on-aws/launch-the-vm-series-firewall-on-aws.html

QUESTION 16
Which Google Cloud Platform project shares its VPC networks with other projects?

A. Service project
B. Host project
C. Admin project
D. Subscribing project

Correct Answer: B
Section:
Explanation:
Create a shared VPC using the Trust VPC created when you deployed the firewall template.
Set up a shared VPC for the host (firewall) project:
gcloud compute shared-vpc enable HOST_PROJECT_ID
https://docs.paloaltonetworks.com/vm-series/9-1/vm-series-deployment/set-up-the-vm-series-firewall-on-google-cloud-platform/autoscaling-on-google-cloud-platform/deploy-autoscaling-on-google-cloud.html

QUESTION 17
An administrator has deployed an AWS transit gateway and used multiple VPC spokes to segregate a multi-tier application. The administrator also created a security VPC with multiple VM-Series NGFWs in an active/active deployment model via ECMP using Amazon Web Services VPN-based attachments.
What must be configured on the firewall to avoid asymmetric routing?

A. source address translation
B. destination address translation
C. port address translation
D. source and destination address translation

Correct Answer: A
Section:

QUESTION 18
Which two items are required when a VM-100 BYOL instance is upgraded to a VM-300 BYOL instance? (Choose two.)

A. UUID
B. new Auth Code
C. CPU ID
D. API Key

Correct Answer: B, D
Section:
Explanation:
In a public cloud deployment, if your firewall is licensed with the BYOL option, you mustDeactivate VMbefore you change the instance type or VM type and apply the license again on the firewall after you complete the model or instance upgrade. When you change the instance type, because the firewall has a new UUID and CPU ID, the existing license will no longer be valid.
https://docs.paloaltonetworks.com/vm-series/9-0/vm-series-deployment/about-the-vm-series-firewall/upgrade-the-vm-series-firewall/upgrade-the-vm-series-model

QUESTION 19
can you create a custom compliance standard in Prisma Public Cloud?

A. Generate a new Compliance Report.
B. Create compliance framework in a spreadsheet then import into Prisma Public Cloud.
C. From Compliance tab, clone a default framework and customize.
D. From Compliance tab > Compliance Standards, click 'Add New.'

Correct Answer: D
Section:
Explanation:
https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/prisma-cloud-compliance/create-a-custom-compliance-standard

QUESTION 20
Which three types of security checks can Prisma Public Cloud perform? (Choose three.)

A. compliance where
B. network where
C. user where
D. config where
E. event where

Correct Answer: B, D, E
Section:

QUESTION 21
What are two ways to initially deploy a VM-Series NGFW in Microsoft Azure? (Choose two.)

A. through ARM Templates in the GitHub Repository
B. through Solution Templates in the Azure Marketplace
C. through Expedition in the Customer Success Portal
D. through Iron Skillets in the GitHub Repository

Correct Answer: A, B
Section:

QUESTION 22
Which two statements are true about CloudFormation? (Choose two.)

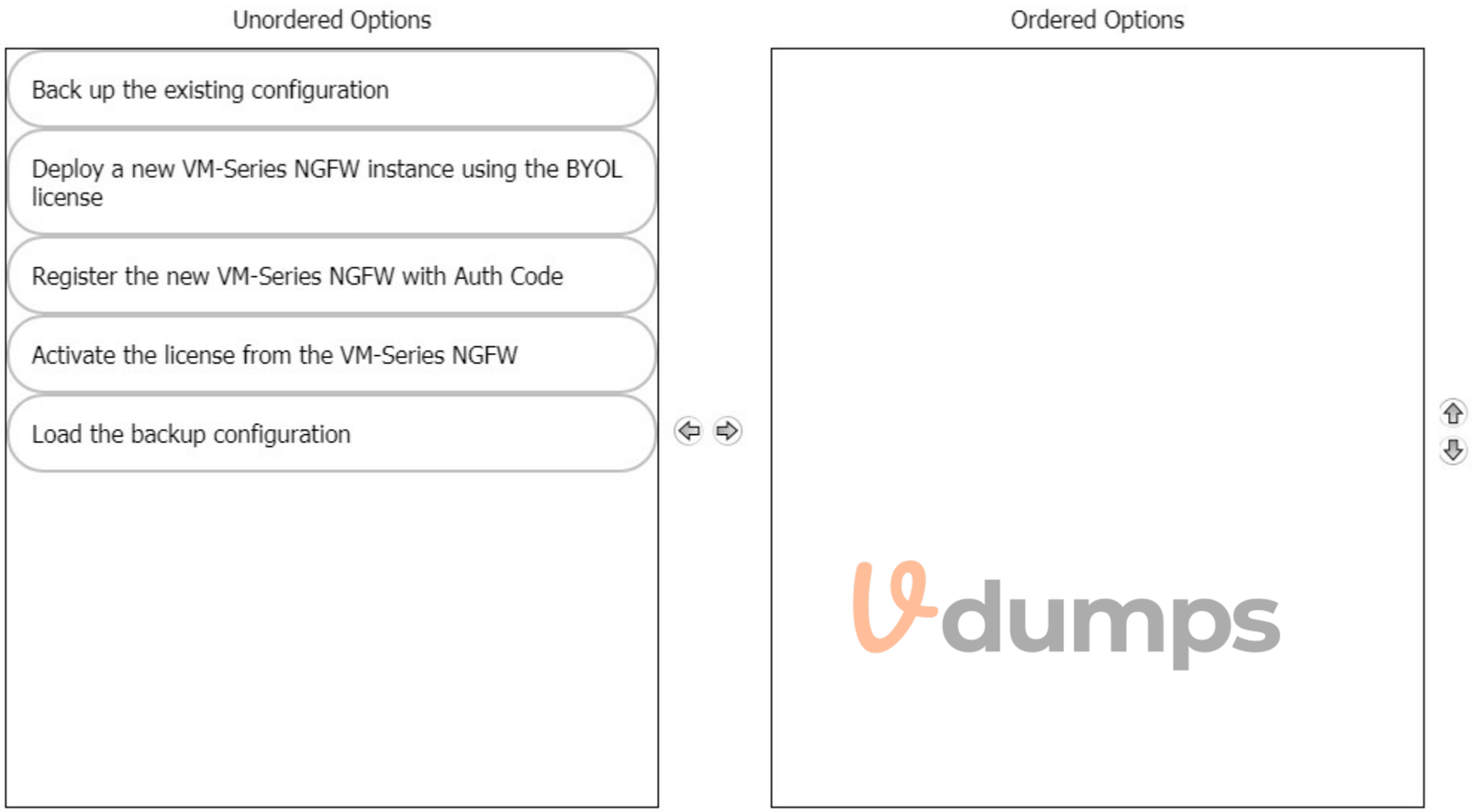
A. CloudFormation is a procedural configuration management tool.
B. CloudFormation templates can be used on both Amazon Web Services and Microsoft Azure
C. CloudFormation templates can be written in JSON or YAML
D. CloudFormation is a declarative orchestration tool.

Correct Answer: C, D
Section:

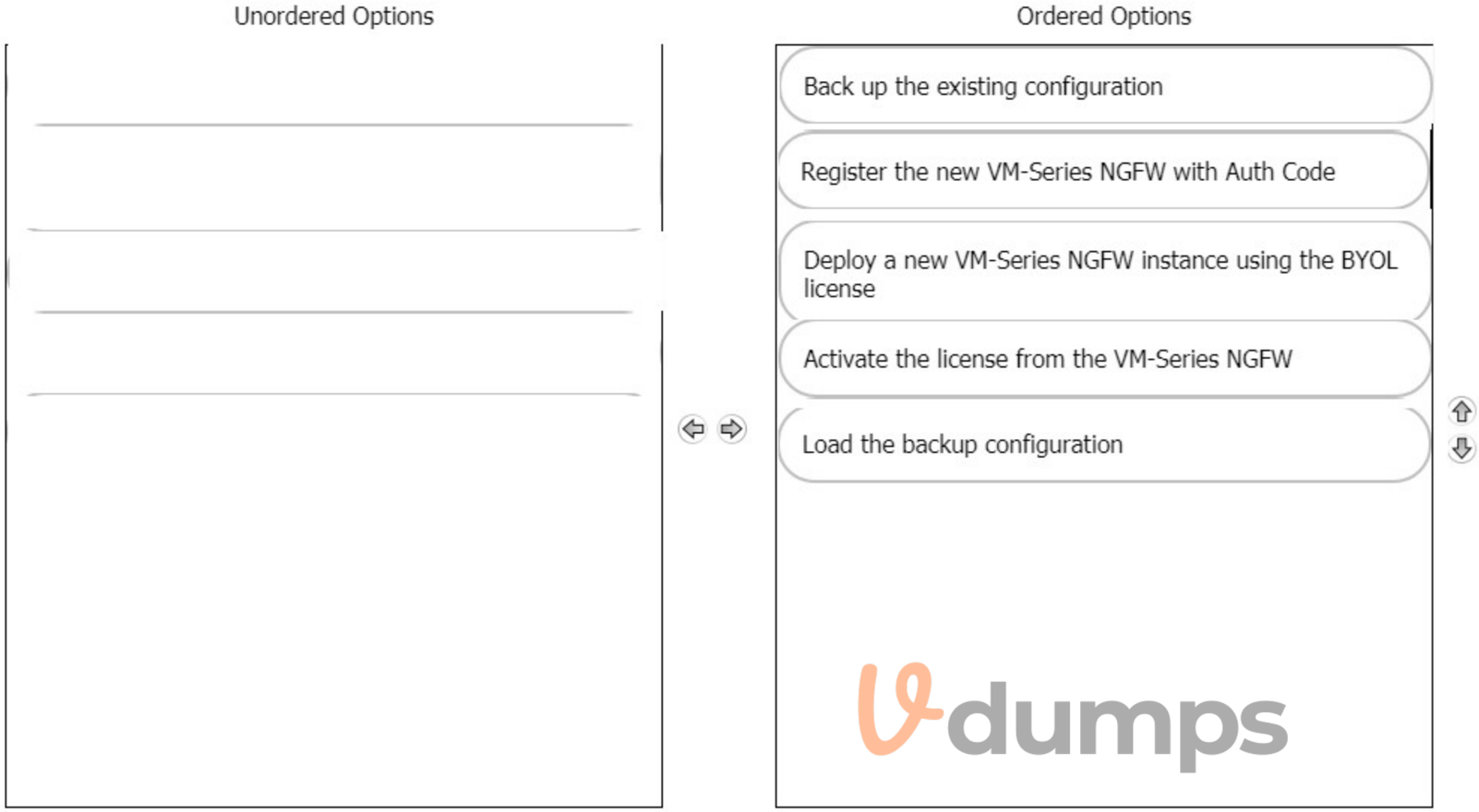
QUESTION 23
DRAG DROP

A customer has deployed a VM-Series NGFW on Amazon Web Services using a PAYG license. What is the sequence required by the customer to switch to a BYOL license?

Select and Place:

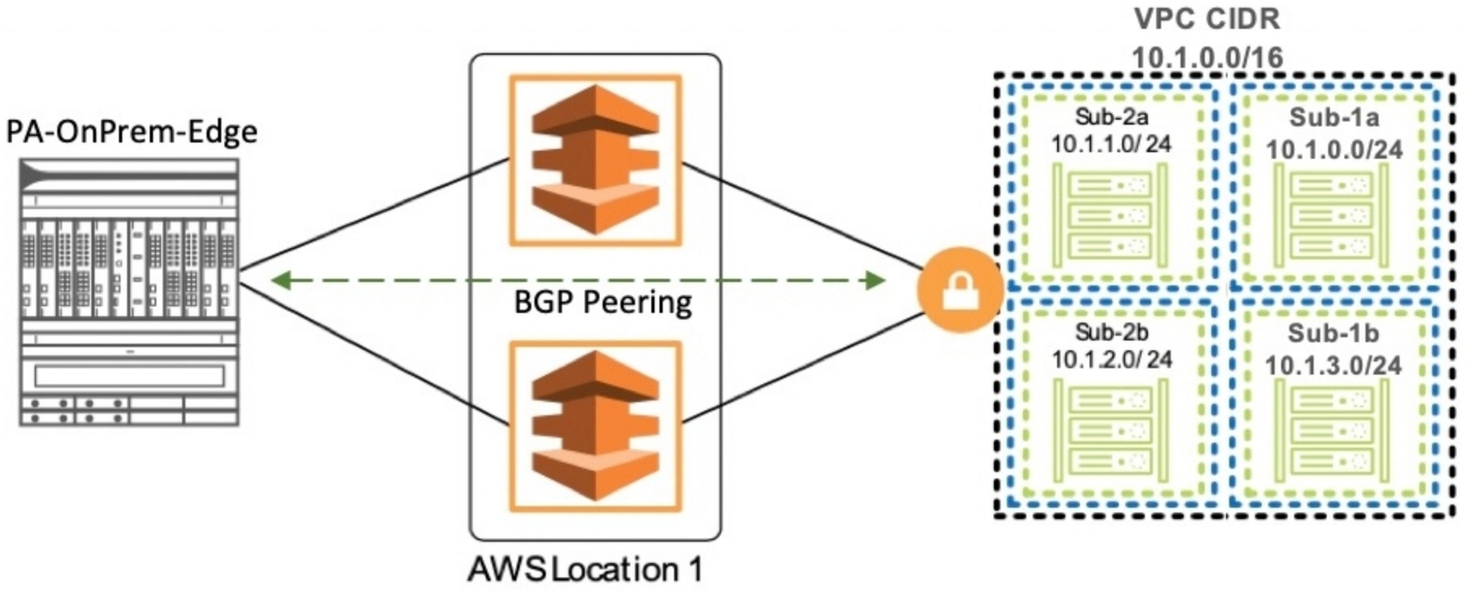


Correct Answer:



Section:
Explanation:

QUESTION 24
DRAG DROP
Based on the diagram, prioritize the order in which the Virtual Gateway evaluates the best route based on the deterministic B6P Path selection process.



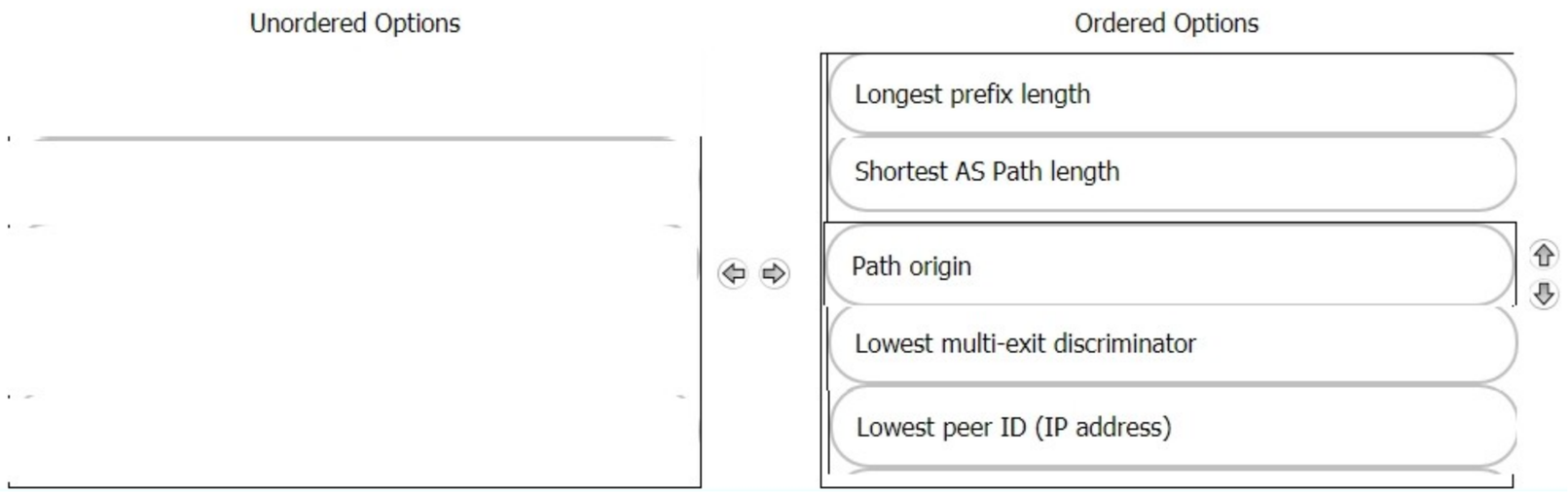
Select and Place:

Unordered Options

- Path origin
- Longest prefix length
- Lowest peer ID (IP address)
- Lowest multi-exit discriminator
- Shortest AS Path length

Ordered Options

Correct Answer:



Section:
Explanation:

QUESTION 25
What is required for an EC2 instance to access the internet directly from an AWS VPC?

A. Internet Gateway
B. Transit Gateway
C. Virtual Private Gateway
D. Customer Gateway

Correct Answer: A
Section:

QUESTION 26
What is a permanent public IP called on Amazon Web Services?

A. Reserved IP
B. PIP
C. EIP
D. Floating IP

Correct Answer: C
Section:

QUESTION 27
What are the two options to dynamically register tags used by Dynamic Address Groups that are referenced in policy? (Choose two.)

A. VM Monitoring
B. External Dynamic List
C. CFT Template

D. XML API

Correct Answer: A, D
Section:
Explanation:
https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/policy/monitor-changes-in-the-virtual-environment/use-dynamic-address-groups-in-policy

QUESTION 28
The Microsoft Azure virtual network gateway supports which two site-to-site connectivity options? (Choose two.)

A. Direct Connect
B. Fast Connect
C. IPsecVPN
D. ExpressRoute

Correct Answer: C, D
Section:
Explanation:
https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-howto-site-to-site-resource-manager-portal

QUESTION 29
Which Prisma Public Cloud policy alerts administrators to unusual user activity?

A. Anomaly
B. Audit Event
C. Network
D. Configuration

Correct Answer: A
Section:
Explanation:
https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/prisma-cloud-policies/anomaly-policies.html

QUESTION 30
Which RQL string monitors all traffic from the Internet and Suspicious IPs destined for your Amazon Web Services databases''

A. network where source.publicnetwork IN ('Suspicious IPs') and dest.resource IN (resource where role IN ('AWS RDS', 'Database'))
B. network where source.publicnetwork IN ('Suspicious IPs', 'Internet IPs') and dest.resource IN (resource where role IN ('LDAP'))
C. network where dest.resource IN (resource where role = 'Database'}
D. network where source.publicnetwork IN ('Suspicious IPs', 'Internet IPs') and dest resource IN (resource where role IN ('AWS RDS'. 'Database'))

Correct Answer: D
Section:

QUESTION 31
When protecting against attempts to exploit client-side and server-side vulnerabilities, what is the Palo Alto Networks best practice when using NGFW Vulnerability Protection Profiles?

A. Use the default Vulnerability Protection Profile to protect clients from all known critical, high, and medium-severity threats

B. Clone the predefined Strict Profile, with packet capture settings disabled
C. Use the default Vulnerability Protection Profile to protect servers from all known critical, high, and medium-severity threats
D. Clone the predefined Strict Profile, with packet capture settings enabled

Correct Answer: D
Section:

QUESTION 32
Which framework in Prisma Public Cloud can be used to provide general best practices when no specific legal requirements or regulatory standards need to be met?

A. HIPAA
B. CIS Benchmark
C. Payment Card Industry DSS V3
D. GDPR

Correct Answer: B
Section:

QUESTION 33
An Azure VNet has the IP network 10.0.0.0/16 with two subnets, 10.0.1.0/24 (used for web servers) and 10.0.2.0/24 (used for database servers). Which is a valid IP address to manage the VM-Series NGFW?

A. 10.0.1.254
B. 10.0.2.1
C. 10.0.3.255
D. 10.0.3.1

Correct Answer: D
Section:

QUESTION 34
Which Amazon Web Services security service can provide host vulnerability information to Prisma Public Cloud?

A. Shield
B. Inspector
C. GuardDuty
D. Amazon Web Services WAF

Correct Answer: B
Section: