

## Topic 1 - Exam A

### Question #1

Topic 1

Which two subscriptions should be recommended to a customer who is deploying VM-Series firewalls to a private data center but is concerned about protecting data-center resources from malware and lateral movement? (Choose two.)

- A. Intelligent Traffic Offload
- B. Threat Prevention
- C. WildFire
- D. SD-WAN

### Question #2

Topic 1

Which two mechanisms could trigger a high availability (HA) failover event? (Choose two.)

- A. Heartbeat polling
- B. Ping monitoring
- C. Session polling
- D. Link monitoring

### Question #3

Topic 1

Which technology allows for granular control of east-west traffic in a software-defined network?

- A. Routing
- B. Microsegmentation
- C. MAC Access Control List
- D. Virtualization

Question #4

Topic 1

Which solution is best for securing an EKS environment?

- A. VM-Series single host
- B. CN-Series high availability (HA) pair
- C. PA-Series using load sharing
- D. API orchestration

Question #5

Topic 1

A CN-Series firewall can secure traffic between which elements?

- A. Host containers
- B. Source applications
- C. Containers
- D. Pods

Question #6

Topic 1

Which feature provides real-time analysis using machine learning (ML) to defend against new and unknown threats?

- A. Advanced URL Filtering (AURLF)
- B. Cortex Data Lake
- C. DNS Security
- D. Panorama VM-Series plugin

Question #7

Topic 1

Which of the following can provide application-level security for a web-server instance on Amazon Web Services (AWS)?

- A. VM-Series firewalls
- B. Hardware firewalls
- C. Terraform templates
- D. Security groups

Which two statements apply to the VM-Series plugin? (Choose two.)

- A. It can manage capabilities common to both VM-Series firewalls and hardware firewalls.
- B. It can be upgraded independently of PAN-OS.
- C. It enables management of cloud-specific interactions between VM-Series firewalls and supported public cloud platforms.
- D. It can manage Panorama plugins.

What can software next-generation firewall (NGFW) credits be used to provision?

- A. Remote browser isolation
- B. Virtual Panorama appliances
- C. Migrating NGFWs from hardware to VMs
- D. Enablement of DNS security

How is traffic directed to a Palo Alto Networks firewall integrated with Cisco ACI?

- A. By using contracts between endpoint groups that send traffic to the firewall using a shared policy
- B. Through a virtual machine (VM) monitor domain
- C. Through a policy-based redirect (PBR)
- D. By creating an access policy

Which protocol is used for communicating between VM-Series firewalls and a gateway load balancer in Amazon Web Services (AWS)?

- A. VRLAN
- B. Geneve
- C. GRE
- D. VMLAN

Which two elements of the Palo Alto Networks platform architecture enable security orchestration in a software-defined network (SDN)? (Choose two.)

- A. Full set of APIs enabling programmatic control of policy and configuration
- B. VXLAN support for network-layer abstraction
- C. Dynamic Address Groups to adapt Security policies dynamically
- D. NVGRE support for advanced VLAN integration

Which component scans for threats in allowed traffic?

- A. Intelligent Traffic Offload
- B. TLS decryption
- C. Security profiles
- D. NAT

Which two deployment modes of VM-Series firewalls are supported across NSX-T? (Choose two.)

- A. Prism Central
- B. Bootstrap
- C. Service Cluster
- D. Host-based

A customer in a VMware ESXi environment wants to add a VM-Series firewall and partition an existing group of virtual machines (VMs) in the same subnet into two groups. One group requires no additional security, but the second group requires substantially more security. How can this partition be accomplished without editing the IP addresses or the default gateways of any of the guest VMs?

- A. Edit the IP address of all of the affected VMs.
- B. Create a new virtual switch and use the VM-Series firewall to separate virtual switches using virtual wire mode. Then move the guests that require more security into the new virtual switch.
- C. Create a Layer 3 interface in the same subnet as the VMs and then configure proxy Address Resolution Protocol (ARP).
- D. Send the VLAN out of the virtual environment into a hardware Palo Alto Networks firewall in Layer 3 mode. Use the same IP address as the old default gateway, then delete it.

## Question #16

Topic 1

How must a Palo Alto Networks Next-Generation Firewall (NGFW) be configured in order to secure traffic in a Cisco ACI environment?

- A. It must be deployed as a member of a device cluster.
- B. It must use a Layer 3 underlay network.
- C. It must receive all forwarding lookups from the network controller.
- D. It must be identified as a default gateway.

## Question #17

Topic 1

Which component allows the flexibility to add network resources but does not require making changes to existing policies and rules?

- A. Content-ID
- B. External dynamic list (EDL)
- C. App-ID
- D. Dynamic address group

## Question #18

Topic 1

Which PAN-OS feature allows for automated updates to address objects when VM-Series firewalls are setup as part of an NSX deployment?

- A. Boundary automation
- B. Hypervisor integration
- C. Bootstrapping
- D. Dynamic Address Group

## Question #19

Topic 1

Which two factors lead to improved return on investment for prospects interested in Palo Alto Networks virtualized next-generation firewalls (NGFWs)? (Choose two.)

- A. Decreased likelihood of data breach
- B. Reduced operational expenditures
- C. Reduced time to deploy
- D. Reduced insurance premiums

Auto scaling templates for which type of firewall enable deployment of a single auto scaling group (ASG) of VM-Series firewalls to secure inbound traffic from the internet to Amazon Web Services (AWS) application workloads?

- A. HA-Series
- B. CN-Series
- C. PA-Series
- D. VM-Series

What Palo Alto Networks software firewall protects Amazon Web Services (AWS) deployments with network security delivered as a managed cloud service?

- A. VM-Series
- B. Cloud next-generation firewall (NGFW)
- C. CN-Series
- D. Ion-Series Ion-Series

What do tags allow a VM-Series firewall to do in a virtual environment?

- A. Enable machine learning (ML).
- B. Adapt Security policy rules dynamically.
- C. Integrate with security information and event management (SIEM) solutions.
- D. Provide adaptive reporting.

Which two methods of Zero Trust implementation can benefit an organization? (Choose two.)

- A. Compliance is validated.
- B. Boundaries are established.
- C. Security automation is seamlessly integrated.
- D. Access controls are enforced.

Which two actions can be performed for VM-Series firewall licensing by an orchestration system? (Choose two.)

- A. Creating a license
- B. Renewing a license
- C. Registering an authorization code
- D. Downloading a content update

What are two environments supported by the CN-Series firewall? (Choose two.)

- A. Positive K
- B. OpenShift
- C. OpenStack
- D. Native K8

Why are VM-Series firewalls and hardware firewalls that are external to the Kubernetes cluster problematic for protecting containerized workloads?

- A. They are located outside the cluster and have no visibility into application-level cluster traffic.
- B. They do not scale independently of the Kubernetes cluster.
- C. They are managed by another entity when located inside the cluster.
- D. They function differently based on whether they are located inside or outside of the cluster.

What is a benefit of network runtime security?

- A. It more narrowly focuses on one security area and requires careful customization, integration, and maintenance.
- B. It removes vulnerabilities that have been baked into containers.
- C. It is siloed to enhance workload security.
- D. It identifies unknown vulnerabilities that cannot be identified by known Common Vulnerability and Exposure (CVE) lists.

What is a design consideration for a prospect who wants to deploy VM-Series firewalls in an Amazon Web Services (AWS) environment?

- A. Special AWS plugins are needed for load balancing.
- B. Resources are shared within the cluster.
- C. Only active-passive high availability (HA) is supported.
- D. High availability (HA) clusters are limited to fewer than 8 virtual appliances.

Which three NSX features can be pushed from Panorama in PAN-OS? (Choose three.)

- A. Security group assignment of virtual machines (VMs)
- B. Security groups
- C. Steering rules
- D. User IP mappings
- E. Multiple authorization codes

When implementing active-active high availability (HA), which feature must be configured to allow the HA pair to share a single IP address that may be used as the network's gateway IP address?

- A. ARP load sharing
- B. Floating IP address
- C. HSRP
- D. VRRP

Which two design options address split brain when configuring high availability (HA)? (Choose two.)

- A. Adding a backup HA1 interface
- B. Using the heartbeat backup
- C. Bundling multiple interfaces in an aggregated interface group and assigning HA2
- D. Sending heartbeats across the HA2 interfaces



Where do CN-Series devices obtain a VM-Series authorization key?

- A. Panorama
- B. Local installation
- C. GitHub
- D. Customer Support Portal

Which offering can gain visibility and prevent an attack by a malicious actor attempting to exploit a known web server vulnerability using encrypted communication?

- A. OCSP
- B. Secure Sockets Layer (SSL) Inbound Inspection
- C. Advanced URL Filtering (AURLF)
- D. WildFire

Which Palo Alto Networks firewall provides network security when deploying a microservices-based application?

- A. PA-Series
- B. CN-Series
- C. VM-Series
- D. HA-Series

What is the appropriate file format for Kubernetes applications?

- A. .yaml
- B. .exe
- C. .json
- D. .xml

Which offering inspects encrypted outbound traffic?

- A. WildFire
- B. TLS decryption
- C. Content-ID
- D. Advanced URL Filtering (AURLF)

Which two features of CN-Series firewalls protect east-west traffic between pods in different trust zones? (Choose two.)

- A. Intrusion prevention system (IPS)
- B. Communication with Panorama
- C. External load balancer (ELB)
- D. Layer 7 visibility

Which component can provide application-based segmentation and prevent lateral threat movement?

- A. DNS Security
- B. NAT
- C. URL Filtering
- D. App-ID

What does the number of required flex credits for a VM-Series firewall depend on?

- A. vCPU allocation
- B. IP address allocation
- C. Network interface allocation
- D. Memory allocation

Which element protects and hides an internal network in an outbound flow?

- A. DNS sinkholing
- B. User-ID
- C. App-ID
- D. NAT

Which software firewall would help a prospect interested in securing an environment with Kubernetes?

- A. KN-Series
- B. ML-Series
- C. VM-Series
- D. CN-Series

Which two valid components are used in installation of a VM-Series firewall in an OpenStack environment? (Choose two.)

- A. OpenStack heat template in JSON format
- B. OpenStack heat template in YAML Ain't Markup Language (YAML) format
- C. VM-Series VHD image
- D. VM-Series qcow2 image

Which software firewall would assist a prospect who is interested in securing extensive DevOps deployments?

- A. CN-Series
- B. Ion-Series
- C. Cloud next-generation firewall (NGFW)
- D. VM-Series

How does a CN-Series firewall prevent exfiltration?

- A. It employs custom-built signatures based on hash.
- B. It distributes incoming virtual private cloud (VPC) traffic across the pool of VM-Series firewalls.
- C. It provides a license deactivation API key.
- D. It inspects outbound traffic content and blocks suspicious activity.

What helps avoid split brain in active-passive high availability (HA) pair deployment?

- A. Using a standard traffic interface as the HA2 backup
- B. Enabling preemption on both firewalls in the HA pair
- C. Using the management interface as the HA1 backup link
- D. Using a standard traffic interface as the HA3 link

What must be enabled when using Terraform templates with a Cloud next-generation firewall (NGFW) for Amazon Web Services (AWS)?

- A. AWS CloudWatch logging
- B. Access to the Cloud NGFW for AWS console
- C. Access to the Palo Alto Networks Customer Support Portal
- D. AWS Firewall Manager console access

How does Prisma Cloud Compute offer workload security at runtime?

- A. It automatically builds an allow-list security model for every container and service.
- B. It quarantines containers that demonstrate increased CPU and memory usage.
- C. It automatically patches vulnerabilities and compliance issues for every container and service.
- D. It works with the identity provider (IdP) to identify overprivileged containers and services, and it restricts network access.

What can be implemented in a CN-Series to protect communications between Dockers?

- A. Firewalling
- B. Runtime security
- C. Vulnerability management
- D. Data loss prevention (DLP)

Which two public cloud platforms does the VM-Series plugin support? (Choose two.)

- A. Azure
- B. IBM Cloud
- C. Amazon Web Services (AWS)
- D. OCI

With which two private cloud environments does Palo Alto Networks have deep integrations? (Choose two.)

- A. VMware NSX-T
- B. Cisco ACI
- C. Dell APEX
- D. Nutanix

What is the structure of the YAML Ain't Markup Language (YAML) file repository?

- A. Deployment\_Type/Kubernetes/Environment
- B. Kubernetes/Deployment\_Type/Environment
- C. Kubernetes/Environment/Deployment\_Type
- D. Environment/Kubernetes/Deployment\_Type

Which feature must be configured in an NSX environment to ensure proper operation of a VM-Series firewall in order to secure east-west traffic?

- A. Deployment of the NSX DFW
- B. VMware Information Sources
- C. User-ID agent on a Windows domain server
- D. Device groups within VMware Services Manager

Which two routing options are supported by VM-Series? (Choose two.)

- A. OSPF
- B. RIP
- C. BGP
- D. IGRP

What are two requirements for automating service deployment of a VM-Series firewall from an NSX Manager? (Choose two.)

- A. vCenter has been given Palo Alto Networks subscription licenses for VM-Series firewalls.
- B. Panorama has been configured to recognize both the NSX Manager and vCenter.
- C. The deployed VM-Series firewall can establish communications with Panorama.
- D. Panorama can establish communications to the public Palo Alto Networks update servers.

How are CN-Series firewalls licensed?

- A. Data-plane vCPU
- B. Service-plane vCPU
- C. Management-plane vCPU
- D. Control-plane vCPU

Regarding network segmentation, which two steps are involved in the configuration of a default route to an internet router? (Choose two.)

- A. Select the Static Routes tab, then click Add.
- B. Select Network > Interfaces.
- C. Select the Config tab, then select New Route from the Security Zone Route drop-down menu.
- D. Select Network > Virtual Router, then select the default link to open the Virtual Router dialog.

Why are containers uniquely suitable for runtime security based on allow lists?

- A. Containers have only a few defined processes that should ever be executed.
- B. Developers define the processes used in containers within the Dockerfile.
- C. Docker has a built-in runtime analysis capability to aid in allow listing.
- D. Operations teams know which processes are used within a container.

Which two steps are involved in deployment of a VM-Series firewall on NSX? (Choose two.)

- A. Create a virtual data center (vDC) and a vApp that includes the VM-Series firewall.
- B. Obtain the Amazon Machine Images (AMIs) from marketplace.
- C. Enable communication between Panorama and the NSX Manager.
- D. Register the VM-Series firewall as a service.

How are Palo Alto Networks Next-Generation Firewalls (NGFWs) deployed within a Cisco ACI architecture?

- A. SDN code hooks can help detonate malicious file samples designed to detect virtual environments.
- B. Traffic can be automatically redirected using static address objects.
- C. Service graphs are configured to allow their deployment.
- D. VXLAN or NVGRE traffic is terminated and inspected for translation to VLANs.

What is required to integrate a Palo Alto Networks VM-Series firewall with Azure Orchestration?

- A. Aperture orchestration engine
- B. Client-ID
- C. Dynamic Address Groups
- D. API Key

Which service, when enabled, provides inbound traffic protection?

- A. Advanced URL Filtering (AURLF)
- B. Threat Prevention
- C. Data loss prevention (DLP)
- D. DNS Security

Which two configuration options does Palo Alto Networks recommend for outbound high availability (HA) design in Amazon Web Services using a VM-Series firewall? (Choose two.)

- A. Transit VPC and Security VPC
- B. Traditional active-active HA
- C. Transit gateway and Security VPC
- D. Traditional active-passive HA

Which two criteria are required to deploy VM-Series firewalls in high availability (HA)? (Choose two.)

- A. Assignment of identical licenses and subscriptions
- B. Deployment on a different host
- C. Configuration of asymmetric routing
- D. Deployment on same type of hypervisor



What is a benefit of CN-Series firewalls securing traffic between pods and other workload types?

- A. It protects data center and internet gateway deployments.
- B. It allows for automatic deployment, provisioning, and immediate policy enforcement without any manual intervention.
- C. It ensures consistent security across the entire environment.
- D. It allows extension of Zero Trust Network Security to the most remote locations and smallest branches.

Which type of group allows sharing cloud-learned tags with on-premises firewalls?

- A. Device
- B. Notify
- C. Address
- D. Template

What needs to be configured to deploy VM-Series firewalls in Azure as an Active/Active High Availability (HA) pair?

- A. Active/Active HA is not supported in Azure
- B. HA3 Link
- C. Floating IP Address
- D. HA1 and HA2 Link

Organizations using multiple public and private cloud platforms can deploy and configure the VM-Series using which three toolsets? (Choose three.)

- A. Panorama
- B. Terraform
- C. Github
- D. Ansible
- E. CloudFormation

A data center experiences a power outage that results in the reboot of all ESXi servers, including the software firewall's virtual machine (VM). Subsequently, there is a notable decrease in performance. Most end users complain of being unable to access the internet. The system engineer is still able to log in to the firewall management console smoothly.

What is most likely causing this issue?

- A. The firewall license has expired.
- B. The dataplane disk partitions are unable to mount after the reboot.
- C. There is configuration file corruption on ESXi server.
- D. The last saved configuration did not save properly in the boot up partition.

Which type of Terraform code is commonly used to deploy infrastructure as code (IaC)?

- A. Library
- B. SDK
- C. Module
- D. Plugin

With the Panorama plugin for VM-Series installed. Panorama can collect a predefined set of attributes from which services in Amazon Web Services (AWS) as tags and populate it in the VM-Series firewall?

- A. Load balancers
- B. VPCs
- C. Transit gateways
- D. EC2 instances

Which two community-supported Palo Alto Networks templates will protect cloud workloads by using a CN-Series firewall on GKE? (Choose two.)

- A. Marketplace
- B. Ansible
- C. Helm
- D. Terraform

Which two licensing options provide the application visibility and control feature in a VM-Series deployment? (Choose two.)

- A. Palo Alto Networks Cloud Storage
- B. PAYG
- C. BYOL
- D. AWS Marketplace

A manager wants to enhance the performance of a Palo Alto Networks VM-Series firewall. How can the use of CLI increase the number of cores in the dataplane?

- A. Use init-cfg.txt with parameter "plugin-op-commands=dp-cores:<#-cores>".
- B. Use cfg.txt with parameter "plugin-op-commands=dp-cores:<#-cores>".
- C. Request vm\_series dp-cores <#-cores>.
- D. Request plugins vm\_series dp-cores <#-cores>.

What is created by the Panorama plugin as part of the infrastructure setup in Amazon Web Services (AWS) cloud?

- A. Route tables and Security VPC with GWLB Endpoints only
- B. AWS Transit Gateway, route tables, and NAT Gateway subnets
- C. NAT Gateway subnets, Security VPC with GWLB Endpoints, and route tables
- D. Security VPC with GWLB endpoints, NAT Gateway subnets, and AWS Transit Gateway

What is the valid command to setup the cluster for CN-series firewall HSF Deployment and to prepare the extend permissions for service account?

A. kubectl -n kube-system get secrets

```
kubectl -n kube-system get secrets (secrets-from-above-command) -o json >> cred.json  
kubectl apply -f plugin-deploy-serviceaccount.yaml  
kubectl apply -f pan-mgmt-serviceaccount.yaml
```

B. kubectl apply -f plugin-deploy-serviceaccount.yaml

```
kubectl apply -f pan-mgmt-serviceaccount.yaml  
kubectl -n kube-system get secrets  
kubectl -n kube-system get secrets (secrets-from-above-command) -o json >> cred.json
```

C. kubectl apply -f plugin-deploy-serviceaccount.yaml

```
kubectl -n kube-system get secrets  
kubectl apply -f pan-mgmt-serviceaccount.yaml  
kubectl -n kube-system get secrets (secrets-from-above-command) -o json >> cred.json
```

D. kubectl -n kube-system get secrets

```
kubectl -n kube-system get secrets (secrets-from-above-command) -o json >> cred.json  
kubectl apply -f pan-mgmt-serviceaccount.yaml  
kubectl apply -f plugin-deploy-serviceaccount.yaml
```

To list NGFW pods connected to a management plane, which Panorama CLI command should be used?

A. requests plugins kubernetes get-node-license-info

B. requests plugins kubernetes get-license-tokens

C. requests plugins vm-series list-dp-pods

D. requests tech-support dump

Which plugin is used to create and push device group-based policies to the Cloud NGFW?

A. Panorama AWS

B. Zero Touch Provisioning (ZTP)

C. Panorama Interconnect «•

D. Cloud Services

Using what two commands can an engineer confirm that the installation of the CN-series firewall as a K8S service on the production GKE cluster was successful after it was protected by the cloud workloads on GKE and YAML was downloaded to completed the setup? (Choose two.)

- A. `kubectl get pods -f app=pan-cn-mgmt -n kube-system`
- B. `kubectl get pods -l app=pan-mgmt -n kube-system`
- C. `kubectl get pods -n kube-system -l app=pan-ngfw -o wide`
- D. `kubectl get pods app=pan-cn-ngfw -o wide`

When deploying a firewall in Amazon Web Services (AWS) utilizing the orchestration through Panorama, which plugin is required?

- A. `vm_series-2.0.1` or later
- B. `cloud_services-3.2.0` or later
- C. `aws-3.0.1` or later
- D. `aws-5.0.1` or later

To get the current auth code applied to a CN-Series firewall, which Panorama CLI command should be used?

- A. `requests plugins kubernetes get-license-tokens`
- B. `requests plugins kubernetes get-node-license-info`
- C. `requests tech-support dump`
- D. `requests plugins vm-series list-dp-pods`

What are the three required ethernet interfaces to deploy the VM-Series in AWS as a centralized model? (Choose three.)

- A. Private interface for traffic to the GWLB
- B. Private interface for traffic from the GWLB
- C. Public interface for outbound traffic
- D. Public interface for inbound traffic
- E. Management interface

What is the minimum number of management interfaces created when the Google Cloud Platform (GCP) Marketplace deploys an instance of the VM-Series firewall?

- A. 1
- B. 2
- C. 3
- D. 4

What must be done in Panorama to enable the CN-MGMT to connect to Panorama?

- A. Auth Code activation on Kubernetes plugin
- B. Set Up Panorama in Management Only mode
- C. Reboot Panorama
- D. Set up High Availability (HA)

What is the default log destination for S3 bucket in the Cloud NGFW CloudFormation template (CFT) that is launched to set up the tenant?

- A. Cloud NGFW
- B. PaloAltoCloudNGFW
- C. PANWCloudNGFW
- D. Cortex Data Lake

After configuring a new software VM-Series firewall, the network team cannot detect any traffic being transmitted or received on the correct VLAN of the network switch. However, they are able to ping the management IP. Which two actions should be taken to troubleshoot this issue? (Choose two.)

- A. Use tcpdump.
- B. Debug flow create.
- C. Check the port groups and port mapping on the hypervisor.
- D. Show counter global filter.