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

Correct Answer: *BC*

Currently there are no comments in this discussion, be the first to comment!

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

Suggested Answer: *AD*

jackcarter1992 5 months ago

Selected Answer: AD

A and D is correct

upvoted 1 times

lol1000 8 months, 3 weeks ago

AD is correct

upvoted 3 times

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

Correct Answer: *B*

Community vote distribution

B (100%)

Currently there are no comments in this discussion, be the first to comment!

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

Correct Answer: *B*

Community vote distribution

B (100%)

Currently there are no comments in this discussion, be the first to comment!

Question #5 *Topic 1*

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

A. Host containers

B. Source applications

C. Containers

D. Pods

Suggested Answer: *D*

Redrum702 Highly Voted 1 year, 3 months ago

Answer is C: CN-Series firewall with PAN-OS 10.1 version supports CN-Series firewall deployment on Alicloud ACK platform with Terway CNI to secure traffic between containers within the same cluster, as well as between containers and other workload types such as virtual machines and bare-metal servers.

upvoted 7 times

javim 1 year, 2 months ago

Your are right! Correct answer is C

upvoted 3 times

Merlin0o Most Recent 2 months ago

Selected Answer: C

Agree C

upvoted 1 times

oshkosh82 11 months ago

C) Containers (CN stands for Container Native)

upvoted 1 times

92060c1 1 year, 2 months ago

CN-Series offers threat protection for inbound, outbound, and east-west traffic between container trust zones and other workload types, without slowing the speed of development.

upvoted 2 times

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

Suggested Answer: *A*

Community vote distribution

A (100%)

2533eed Highly Voted 1 year, 2 months ago

Selected Answer: A

Anything related to ML needs to have "Advanced" in its name.

upvoted 6 times

onaicul Most Recent 6 months, 2 weeks ago

Selected Answer: C

C - AURLF does not focus on the dynamic detection of new, unknown threats using machine learning techniques as seen in features like WildFire or DNS Security.

AURLF does not leverage machine learning for real-time detection

upvoted 1 times

Questionario 11 months ago

Selected Answer: A

A is the answer, has been linked already... it offers ML

B is not even topic of the exam

C has no machine learning, only inline cloud analysis

D is just wrong

upvoted 1 times

lol1000 1 year, 2 months ago

I think it's A. D could also work since Palo is all about AI on all of the subs...

upvoted 1 times

scn_lewisk 1 year, 2 months ago

Selected Answer: A

A is the correct answer

upvoted 4 times

SyedHussain 1 year, 3 months ago

A is the correct answer

upvoted 3 times

Redrum702 1 year, 3 months ago

Answer is A: in addition to the protection offered by PAN-DB, Advanced URL Filtering provides real-time analysis using machine learning (ML) to defend against new and unknown threats.

upvoted 3 times

symph0ny 1 year, 6 months ago

A is the correct answer

upvoted 4 times

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

Correct Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #8 *Topic 1*

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.

Suggested Answer: *BC*

Community vote distribution

BC (100%)

onaicul 6 months, 2 weeks ago

Selected Answer: CD

The VM-Series plugin allows seamless integration and management of the VM-Series firewalls with public cloud platforms, such as AWS, Azure, and Google Cloud. It enables the management of cloud-specific interactions, including the configuration and monitoring of cloud-native features like security groups, load balancers, and virtual networks.
D. It can manage Panorama plugins.

The VM-Series plugin can work with Panorama, the centralized management system for Palo Alto Networks firewalls. Through the plugin, administrators can manage multiple VM-Series firewalls, including cloud-specific configurations and interactions, and it can also manage plugins related to Panorama.

upvoted 1 times

lol1000 8 months, 3 weeks ago

Selected Answer: BC

BC

upvoted 1 times

javim 9 months ago

Selected Answer: BC

Correct answers B & C

upvoted 1 times

Redrum702 9 months, 4 weeks ago

Answer is correct: B/C

upvoted 2 times

Question #9 *Topic 1*

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

Suggested Answer: *B*

Community vote distribution

B (100%)

TheIronSheik 12 months ago

this should be a mulitple choice question. The PSE study guide indicates credits can be used for PANO

upvoted 1 times

ChrjSM0512 1 year, 1 month ago

This is a tricky question as you might get confuse between answer B and C, however parsing the answer C make me realize that the right answer must be the B. https://docs.paloaltonetworks.com/vm-series/9-1/vm-series-deployment/license-the-vm-series-firewall/software-ngfw/provision-panorama (anser C is not correct as you might have an on-prem PAN-OS already license and you'll not have the option to transfer that license to a new deployed VM using those credits) therefore the right answer is B

upvoted 1 times

29fb203 1 year, 1 month ago

Yes the correct answer is B

https://docs.paloaltonetworks.com/vm-series/9-1/vm-series-deployment/license-the-vm-series-firewall/software-ngfw

upvoted 2 times

javim 1 year, 2 months ago

Selected Answer: B

The correct answer is B

Software NGFW credits can be used to fund Software NGFWs (VM-Series and CN-Series), Cloud-Delivered Security Services (CDSS), or virtual Panorama appliances in networks with or without internet access (air-gapped networks, for example).

https://docs.paloaltonetworks.com/vm-series/9-1/vm-series-deployment/license-the-vm-series-firewall/software-ngfw

upvoted 4 times

Question #10 *Topic 1*

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

Suggested Answer: *C*

Community vote distribution

A (67%) C (33%)

Merlin0o 2 months, 1 week ago

Selected Answer: C

Should be C:
The Question is asking how the traffic is send to the PA FW not how to configure it.
You may configure it with contracts but the traffic is directed to the PA FW with a PBR.

"traffic is sent to the firewall with a policy-based redirect (PBR)"
"For east-west traffic, define a bridge domain and subnet in the ACI fabric for the firewall. Configure contracts between EPGs that send traffic to the firewall using a PBR. The PBR forwards traffic to the firewall based on policy containg the firewall's IP and MAC address."

Src: https://docs.paloaltonetworks.com/vm-series/11-1/vm-series-deployment/set-up-a-firewall-in-cisco-aci/palo-alto-firewall-integration-with-cisco-aci-overview

upvoted 1 times

kafka1 8 months, 1 week ago

This is one of those purposly missleading questions.
"ON" PA FW you use PBR, but here is "TO" PA so I would go for A

upvoted 2 times

Zalthoz 8 months, 2 weeks ago

Selected Answer: A

Cisco ACI uses contract to tie in external security appliances

upvoted 1 times

hifire 9 months, 1 week ago

Selected Answer: A

Answer A is correct. Cisco ACI is using descriptiv language via UI and API. Contracts can utilize Proxy ARP and PBR as techniques for traffic routing, but it isn't the way to configure.
https://www.cisco.com/c/en/us/solutions/collateral/data-center-virtualization/application-centric-infrastructure/white-paper-c11-743951.html#Howcontractswork

upvoted 1 times

Doobiedoo 1 year, 2 months ago

Selected Answer: C

https://www.cisco.com/c/en/us/solutions/collateral/data-center-virtualization/application-centric-infrastructure/white-paper-c11-739971.html

upvoted 1 times

Question #11 *Topic 1*

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

Suggested Answer: *B*

Community vote distribution

B (100%)

onaicul 6 months, 2 weeks ago

Selected Answer: B

B - In Amazon Web Services (AWS), the protocol used for communication between VM-Series firewalls and a Gateway Load Balancer (GLB) is Geneve.

Geneve (Generic Network Virtualization Encapsulation) is a tunneling protocol that allows for efficient and flexible communication between network appliances, such as firewalls, and the Gateway Load Balancer. Geneve is used to encapsulate traffic between the load balancer and the VM-Series firewalls, enabling proper traffic inspection and scaling.

upvoted 1 times

d3b8198 1 year ago

B is correct

upvoted 1 times

javim 1 year, 3 months ago

Selected Answer: B

B is the correct answer

upvoted 2 times

Question #12 *Topic 1*

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

Suggested Answer: *AC*

⊟ **ChrjSM0512** 7 months ago

A and C are correct

upvoted 3 times

Question #13 *Topic 1*

Which component scans for threats in allowed traffic?

A. Intelligent Traffic Offload

B. TLS decryption

C. Security profiles

D. NAT

Suggested Answer: *C*

onaicul 6 months, 2 weeks ago

Selected Answer: C

Security profiles (C) are the components that scan for threats in allowed traffic, providing essential protection by applying various security checks and controls.

upvoted 1 times

djedeen 9 months, 1 week ago

Security Profiles are not used in the match criteria of a traffic flow. The Security Profile is applied to scan traffic after the application or category is allowed by the Security policy rule.

upvoted 1 times

Question #14 *Topic 1*

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

Suggested Answer: *CD*

Community vote distribution

CD (100%)

⊟ **Ac1d_** **Highly Voted** 👍 1 year, 1 month ago

Selected Answer: CD

https://docs.paloaltonetworks.com/vm-series/9-1/vm-series-deployment/set-up-the-vm-series-firewall-on-nsx/set-up-the-vm-series-firewall-on-nsx-t-east-west/supported-deployments-of-the-vm-series-firewall-on-vmware-nsx-t-ew

upvoted 7 times

⊟ **SyedHussain** **Most Recent** 🕓 9 months, 2 weeks ago

Answer is C and D

upvoted 4 times

Question #15 *Topic 1*

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.

Suggested Answer: *B*

Community vote distribution

B (100%)

Questionario 11 months ago

Selected Answer: B

B is how it is explained in beacon content

upvoted 1 times

Doobiedoo 1 year, 2 months ago

Selected Answer: B

B is the best way. This is kind of what virtual switches were actually made for. Same VLAN-IDs but different broadcast domains.

upvoted 1 times

djedeen 1 year, 3 months ago

It is B

upvoted 2 times

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.

Suggested Answer: *B*

Community vote distribution

B (100%)

Questionario 11 months ago

Selected Answer: B

correct

upvoted 2 times

YifanZhan 1 year, 6 months ago

correct see reference: https://docs.paloaltonetworks.com/vm-series/11-0/vm-series-deployment/set-up-a-firewall-in-cisco-aci/palo-alto-firewall-integration-with-cisco-aci-overview

upvoted 2 times

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

Suggested Answer: *D*

Community vote distribution

D (100%)

Questionario 11 months ago

Selected Answer: D

I agree with artic...

both work on software firewalls, EDLs are not available on CN series (yet?)

upvoted 2 times

articpolarbear 1 year ago

This could be both B and D. both answers seem correct but D seems more alligned with the goals of the exam (and the features of the VMs, CNs and CNGFW)

upvoted 1 times

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

Suggested Answer: *D*

29fb203 7 months, 2 weeks ago

D is the answer.

https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/policy/monitor-changes-in-the-virtual-environment/use-dynamic-address-groups-in-policy

upvoted 2 times

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

Suggested Answer: *AC*

⊟ **onaicul** 6 months, 2 weeks ago

Selected Answer: BC

B and C

The two main factors that lead to improved ROI when deploying Palo Alto Networks virtualized NGFWs are reduced operational expenditures (B) and reduced time to deploy (C), as both directly impact cost efficiency and operational agility

upvoted 1 times

⊟ **commit666** 7 months, 3 weeks ago

A; C

https://www.paloaltonetworks.com/blog/2023/12/research-shows-roi-with-software-firewalls/

upvoted 1 times

Question #20 *Topic 1*

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

Suggested Answer: *D*

Redrum702 9 months, 4 weeks ago

Answer D: https://docs.paloaltonetworks.com/vm-series/10-2/vm-series-deployment/set-up-the-vm-series-firewall-on-aws/auto-scale-vm-series-firewalls-with-the-amazon-elb/vm-series-auto-scale-template-for-aws-version-v21

upvoted 2 times

Question #21 *Topic 1*

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

Suggested Answer: *B*

Community vote distribution

B (100%)

Doobiedoo 8 months, 2 weeks ago

Selected Answer: B

B is correct. https://www.paloaltonetworks.com/engage/cloud-ngfw/next-generation-firewall-for-aws

upvoted 4 times

Question #22 *Topic 1*

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.

Suggested Answer: *B*

Redrum702 9 months, 4 weeks ago

Answer is B: https://docs.paloaltonetworks.com/pan-os/11-1/pan-os-admin/policy/use-tags-to-group-and-visually-distinguish-objects/create-and-apply-tags

upvoted 3 times

Question #23 *Topic 1*

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.

Suggested Answer: *BD*

Community vote distribution

BD (100%)

bbbb72f 11 months, 1 week ago

C & D is correct - Refecence: https://docs.paloaltonetworks.com/best-practices/zero-trust-best-practices/zero-trust-best-practices/what-is-zero-trust-and-why-do-i-need-it -- "The goal of Zero Trust is to eliminate implicit trust from the enterprise. Eliminating implicit trust helps prevent successful data breaches, simplifies operations through automation and a reduced rulebase, and simplifies regulatory compliance and audits because Zero Trust environments are designed for compliance and easy auditing."

upvoted 1 times

javim 1 year, 2 months ago

Selected Answer: BD

Correct answers are B & D

- Boundaries are established is a method of Zero Trust implementation that involves defining and segmenting the network into smaller zones based on data sensitivity, user identity, device type, or application function. Boundaries are established can benefit an organization by isolating and protecting critical assets from unauthorized access or lateral movement.

- Access controls are enforced can benefit an organization by preventing data exfiltration, malware propagation, or credential theft.

Compliance is validated and security automation is seamlessly integrated are not methods of Zero Trust implementation, but they may be potential outcomes or benefits of implementing Zero Trust.

upvoted 3 times

Question #24 *Topic 1*

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

Suggested Answer: *BC*

Community vote distribution

BC (75%) CD (25%)

glorki Highly Voted 1 year, 7 months ago

I think it should be: BC

"Use the licensing API to register auth codes, retrieve licenses attached to an auth code, renew licenses, or deactivate all licenses on a VM-Series firewall"

https://docs.paloaltonetworks.com/vm-series/10-2/vm-series-deployment/license-the-vm-series-firewall/vm-series-models/licensing-api

upvoted 5 times

Redrum702 1 year, 3 months ago

I would say you're correct after looking at the link you provided

upvoted 2 times

bbbb72f Most Recent 11 months, 1 week ago

C & D "This quickplay solution provides an Ansible playbook to license a VM-series NGFW using an activated authcode, provide content updates, and upgrade or downgrade to a user-inputted PAN-OS software version."

Reference: Ansible Playbook to Baseline the NGFW | Palo Alto Networks

upvoted 1 times

Questionario 11 months, 2 weeks ago

Selected Answer: CD

It should be CD

you cannot renew a license via any orchestration tool

you can however activate a license with an auth code via panorama and you can also download and install content updates via panorama

upvoted 1 times

1298ac2 1 year ago

Selected Answer: BC

I agree from the point that licenses are deployed on devices not created.

upvoted 1 times

lol1000 1 year, 2 months ago

Selected Answer: BC

Agree with glorki

B,C

upvoted 1 times

scn_lewisk 1 year, 2 months ago

Selected Answer: BC

Answer should be B and C

upvoted 1 times

Question #25 *Topic 1*

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

A. Positive K

B. OpenShift

C. OpenStack

D. Native K8

Suggested Answer: *BD*

Community vote distribution

BD (100%)

javim 9 months ago

Selected Answer: BD

You can deploy CN-Series on all private and public cloud flavors of Kubernetes, including AKS, EKS, GKE, OpenShift, Oracle, Rancher, native Kubernetes, and VMware Tanzu. Use either a manual process or program an automated combination of Helm charts and Terraform templates.

upvoted 4 times

Question #26 *Topic 1*

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.

Suggested Answer: *A*

Doobiedoo 8 months, 2 weeks ago

A is the correct answer. The VM-Series sits outside the cluster so it's unable to inspect intra-cluster containers. This is the main use case for deploying CN-Series firewalls.

upvoted 2 times

Question #27 *Topic 1*

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.

Suggested Answer: *D*

Community vote distribution

D (100%)

1298ac2 1 year ago

Selected Answer: D

Not B - as no IPS Solution will remove a vulnerability, it will just block the attack.

upvoted 1 times

commit666 1 year, 1 month ago

Selected Answer: D

https://www.paloaltonetworks.com/cyberpedia/runtime-security

Employ a runtime scanning solution that can detect unknown vulnerabilities and malicious code execution. Additionally, consider integrating threat intelligence feeds to stay updated on the latest threats and vulnerabilities affecting container environments.

upvoted 1 times

lol1000 1 year, 2 months ago

Selected Answer: D

Answers d.
Defo not a or c. B is misleading as it suggests that runtime security can fix a container?

upvoted 2 times

javim 1 year, 3 months ago

Selected Answer: D

https://www.paloaltonetworks.com/cyberpedia/what-is-container-security

upvoted 2 times

Question #28 *Topic 1*

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.

Suggested Answer: *C*

articpolarbear 1 year ago

C cannot be correct, you can deploy Load Balancers, ASG, HA in AWS.

upvoted 1 times

scn_lewisk 1 year, 2 months ago

C is correct.

https://docs.paloaltonetworks.com/vm-series/10-1/vm-series-deployment/set-up-the-vm-series-firewall-on-aws/high-availability-for-vm-series-firewall-on-aws

upvoted 1 times

djedeen 1 year, 3 months ago

C is the only answer that make sense, but Act/Pasv in this mode will function poorly (60 sec or more to switch).

https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClD9CAK

upvoted 3 times

Question #29 Topic 1

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

Suggested Answer: *ABC*

Community vote distribution

ABC (100%)

javim 9 months ago

Selected Answer: ABC

https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-web-interface-help/panorama-web-interface/panorama-vmware-nsx

upvoted 1 times

Question #30 *Topic 1*

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

Suggested Answer: *B*

Community vote distribution

A (100%)

Merlin0o 2 months ago

Selected Answer: B

Both A and B seem correct, But still I will go with B.
Floating IP Address, is specifically designed to allow the HA pair to share a single IP address that can be used as the network's gateway IP address. While ARP Load-Sharing does involve sharing an IP address, it is more focused on load balancing rather than serving as a single gateway IP address in an active-active HA configuration. The Floating IP Address is the feature that directly addresses the requirement of sharing a single IP address as the network's gateway. - Copilot.

Src:
https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/high-availability/ha-concepts/arp-load-sharing
https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/high-availability/set-up-activeactive-ha/determine-your-activeactive-use-case/use-case-configure-activeactive-ha-with-floating-ip-address-bound-to-active-primary-firewall#id93973f10-2001-4ae4-b475-faa7e70967c1

upvoted 1 times

1298ac2 1 year ago

Selected Answer: A

I think it is A (ARP Load Shareing), as you will need at least two floating IP to distribute the traffic over both fw and you will be using two default gw in your network.

upvoted 2 times

javim 1 year, 2 months ago

A & B are correct answers. The question doesn't specified if there is a L3 device between PA and end host (ARP load Sharing)
A -> https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/high-availability/ha-concepts/arp-load-sharing
B -> https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/high-availability/ha-concepts/floating-ip-address-and-virtual-mac-address

upvoted 1 times

djedeen 1 year, 3 months ago

A) In a Layer 3 interface deployment and active/active HA configuration, ARP load-sharing allows the firewalls to share an IP address and provide gateway services. Use ARP load-sharing only when no Layer 3 device exists between the firewall and end hosts, that is, when end hosts use the firewall as their default gateway.

upvoted 3 times

Question #31 *Topic 1*

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

Suggested Answer: *AB*

MalonJay 11 months, 2 weeks ago

AD

Keepalive on HA2 helps with split brain.

upvoted 1 times

Question #32 *Topic 1*

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

A. Panorama

B. Local installation

C. GitHub

D. Customer Support Portal

Suggested Answer: *A*

ChrjSM0512 6 months, 3 weeks ago

I was wrong, the right answer is A as CN-Series can not be deployed without the Panorama intervantion, and we have to configure the authentication and autorization key in the bootstraping file... etc...https://docs.paloaltonetworks.com/cn-series/getting-started/cn-series-deployment-prereq/install-the-kubernetes-plugin-for-cn-series

upvoted 1 times

ChrjSM0512 7 months ago

CN-Series devices obtain a VM-Series authorization key from the Customer Support Portal. This authorization key is required to activate and license the VM-Series firewall functionality on CN-Series platforms. Once obtained from the Customer Support Portal, the authorization key can be applied during the deployment or configuration process of the CN-Series device to enable the VM-Series firewall features. Authentication code is generated from Panorama, however the Authentication code is used to connect the CN to the Panorama only.

upvoted 1 times

commit666 7 months, 3 weeks ago

A

https://docs.paloaltonetworks.com/cn-series/getting-started/cn-series-deployment-prereq/license-the-cn-series-firewall#:~:text=CN%2DSeries%20firewall%20licensing%20is,vCPU%20used%20the%20CN%2DNGFW.

upvoted 1 times

djedeen 9 months ago

A - generated in Panorama

upvoted 1 times

Question #33 *Topic 1*

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

Correct Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #34 *Topic 1*

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

Correct Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #35 *Topic 1*

What is the appropriate file format for Kubernetes applications?

A. .yaml

B. .exe

C. .json

D. .xml

Correct Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #36 *Topic 1*

Which offering inspects encrypted outbound traffic?

A. WildFire

B. TLS decryption

C. Content-ID

D. Advanced URL Filtering (AURLF)

Correct Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #37

Topic 1

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

Correct Answer: *AD*

Currently there are no comments in this discussion, be the first to comment!

Question #38 *Topic 1*

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

A. DNS Security

B. NAT

C. URL Filtering

D. App-ID

Correct Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #39 *Topic 1*

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

Correct Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #40 *Topic 1*

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

A. DNS sinkholing

B. User-ID

C. App-ID

D. NAT

Correct Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #41 *Topic 1*

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

Suggested Answer: *D*

Redrum702 10 months ago

Answer D: Both VM-Series and CN-Series firewalls can be used to protect container environments. The major difference between the two is the granularity of visibility and control delivered by the CN-Series. VM-Series firewalls can enforce cluster-level security policies, which makes them good for basic perimeter security of an entire cluster.

upvoted 4 times

Question #42 *Topic 1*

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

Suggested Answer: *BD*

Community vote distribution

BD (100%)

javim 9 months ago

Selected Answer: BD

https://docs.paloaltonetworks.com/vm-series/9-1/vm-series-deployment/set-up-the-vm-series-firewall-on-openstack/components-of-the-vm-series-for-openstack-solution

upvoted 2 times

Question #43 *Topic 1*

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

Suggested Answer: *D*

Community vote distribution

A (100%)

⊟ **SyedHussain** Highly Voted 👍 9 months, 2 weeks ago

Answers is A

CN-Series is the container-native version of the ML-powered NGFW designed specifically for Kubernetes environments. The Palo Alto Networks CN-Series containerized firewall is the best-in-class next generation firewall purpose built to secure the Kubernetes environment from network based attacks. The CN-Series firewall enables network security teams to gain layer-7 visibility into Kubernetes environments, provide inline threat protection for containerized applications deployed anywhere, and dynamically scale security without compromising DevOps agility.

upvoted 6 times

⊟ **AnukaRavintha** Most Recent ⏲ 6 months, 3 weeks ago

Selected Answer: A

Answer is A

upvoted 2 times

⊟ **commit666** 7 months, 3 weeks ago

Answers is A

https://docs.paloaltonetworks.com/cn-series

upvoted 2 times

Question #44 *Topic 1*

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.

Correct Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #45 *Topic 1*

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

Correct Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #46 *Topic 1*

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

Correct Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #47

Topic 1

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.

Suggested Answer: *A*

Redrum702 9 months, 3 weeks ago

Answer A is correct:

https://docs.prismacloud.io/en/classic/compute-admin-guide/runtime-defense/runtime-defense-containers

upvoted 3 times

Question #48 *Topic 1*

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)

Correct Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #49 *Topic 1*

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

Suggested Answer: *AC*

Redrum702 9 months, 4 weeks ago

Answer A/B:

upvoted 1 times

Redrum702 9 months, 4 weeks ago

CORRECTION: Answer A/C not B

upvoted 4 times

Question #50 *Topic 1*

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

Suggested Answer: *AB*

Community vote distribution

AB (80%) AD (20%)

1298ac2 1 year ago

Selected Answer: AD

I agree with ChrjSM0512, Cisco ACI is a SDN Solution, not a private Cloud Environment like NSX or Nutanix

upvoted 1 times

ChrjSM0512 1 year, 1 month ago

A and D, Cisco ACI is not a private cloud where you can deploy PA-VM

upvoted 2 times

Doobiedoo 1 year, 2 months ago

Selected Answer: AB

A and B have had deep integrations from the start of VM-Series. D is newer to the game. If you can only choose two, I would pick A and B.

upvoted 1 times

lol1000 1 year, 2 months ago

Selected Answer: AB

Seems AB has best integration.

upvoted 2 times

javim 1 year, 2 months ago

Selected Answer: AB

For me, the correct answer are A,B & D

https://live.paloaltonetworks.com/t5/private-cloud/ct-p/Private_Cloud

upvoted 1 times

Redrum702 1 year, 3 months ago

Answer is A/D:

upvoted 1 times

Question #51 *Topic 1*

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

Suggested Answer: *C*

Community vote distribution

B (100%)

davidtolo 12 months ago

according to chatgpt it is b

upvoted 1 times

commit666 1 year, 1 month ago

Selected Answer: B

I agree Doobiedoo.

https://github.com/PaloAltoNetworks/Kubernetes/tree/v3.0/pan-cn-k8s-daemonset/native

upvoted 1 times

Doobiedoo 1 year, 2 months ago

Selected Answer: B

B is the correct answer. Here is the github repo: https://github.com/PaloAltoNetworks/Kubernetes/tree/v3.0/pan-cn-k8s-daemonset/eks

List of deployment modes: https://docs.paloaltonetworks.com/cn-series/deployment/cn-deployment/deployment-modes-of-cn-series-firewalls

And the supported environments: https://docs.paloaltonetworks.com/compatibility-matrix/cn-series-firewalls/cn-series-supported-environments

upvoted 1 times

Redrum702 1 year, 3 months ago

Answer is C

upvoted 3 times

Question #52 *Topic 1*

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

Suggested Answer: *A*

Community vote distribution

A (100%)

1298ac2 1 year ago

Selected Answer: A

Need to correct, it's a

upvoted 1 times

javim 1 year, 2 months ago

Selected Answer: A

https://docs.vmware.com/en/VMware-NSX-Data-Center-for-vSphere/6.4/com.vmware.nsx.admin.doc/GUID-95600C1C-FE9A-4652-821B-5BCFE2FD8AFB.html

upvoted 2 times

Question #53 *Topic 1*

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

A. OSPF

B. RIP

C. BGP

D. IGRP

Suggested Answer: *AC*

Community vote distribution

AC (100%)

Doobiedoo 8 months, 2 weeks ago

Selected Answer: AC

A, B, and C are correct. Both RIP and IGRP are legacy protocols not used anymore in modern networks. IGRP is not at all supported on VM-Series, but RIP is still supported. However, if you need to only "Choose two", you will want to pick OSPF and BGP since they are the best and most supported options.

upvoted 1 times

Question #54 *Topic 1*

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.

Correct Answer: *BC*

Currently there are no comments in this discussion, be the first to comment!

Question #55 Topic 1

How are CN-Series firewalls licensed?

A. Data-plane vCPU

B. Service-plane vCPU

C. Management-plane vCPU

D. Control-plane vCPU

Suggested Answer: *A*

Community vote distribution

A (100%)

Doobiedoo 8 months, 2 weeks ago

Selected Answer: A

"A" is correct, it is based on vCPU of the Data Plane.

upvoted 1 times

javim 8 months, 3 weeks ago

Selected Answer: A

The correct answer is A, based in scn_lewik's documentation

upvoted 1 times

scn_lewisk 8 months, 4 weeks ago

Selected Answer: A

https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/datasheets/cn-series-container-firewall

Last page it mentions that CN-series are licensed based on data plane vCPU

"CN-Series licensing is similar to VM-Series licensing. Both
VM-Series and CN-Series Firewalls are licensed based on
Software NGFW Credits. CN-Series firewalls are licensed
based on the number of Data Plane vCPUs"

upvoted 2 times

Redrum702 9 months, 1 week ago

Answer C:

https://docs.paloaltonetworks.com/cn-series/getting-started/cn-series-firewall-for-kubernetes/cn-series-core-building-blocks#:~:text=%E2%80%94The%20management%20plane%20(CN%2D,manifest%20files%20with%20ConfigMap%20objects.

upvoted 1 times

Question #56 *Topic 1*

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.

Suggested Answer: *AD*

Community vote distribution

AD (100%)

TeachTrooper 6 months, 3 weeks ago

Selected Answer: AD

I would Say AD you set the default route in the VR under Static Routes and than add ...
C is Inccorect becouse you set the VR not in the zone setting.. so also B is is useless becouse there is nothing that you have to select something.

upvoted 1 times

commit666 7 months, 1 week ago

A&B

Only the two options make sense.
A - Add the default routes in the internet VR.
B - Selecting a VR for an interface.

upvoted 1 times

Question #57 Topic 1

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.

Suggested Answer: *B*

Community vote distribution

A (100%)

TopicNerd 10 months, 4 weeks ago

Selected Answer: A

A. Containers have only a few defined processes that should ever be executed.

upvoted 1 times

bbbb72f 11 months, 1 week ago

A. Containers have only a few defined processes that should ever be executed.

Reasons:
Nature of Containers:

Containers are designed to be lightweight and specialized, executing only a specific set of processes required by the application. This makes it easier to define and manage allow lists for runtime security.
Source: Docker Documentation - What is a Container?
Isolation and Immutability:

Containers are isolated from each other and from the underlying operating system, and are generally immutable after creation. This means that any additional or unexpected processes can be readily identified and blocked, enhancing security.
Source: Kubernetes Documentation - Containers

upvoted 2 times

Question #58 *Topic 1*

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.

Correct Answer: *CD*

Currently there are no comments in this discussion, be the first to comment!

Question #59 *Topic 1*

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.

Suggested Answer: *C*

Redrum702 9 months, 1 week ago

Answer C:

https://docs.paloaltonetworks.com/vm-series/10-2/vm-series-deployment/set-up-a-firewall-in-cisco-aci/palo-alto-firewall-integration-with-cisco-aci-overview/service-graph-templates#id12ea6e71-a2b2-4ac1-a61b-c7ece038d6d6

upvoted 2 times

Question #60 *Topic 1*

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

Suggested Answer: *D*

Redrum702 9 months, 1 week ago

Correct D

upvoted 3 times

Question #61 *Topic 1*

Which service, when enabled, provides inbound traffic protection?

A. Advanced URL Filtering (AURLF)

B. Threat Prevention

C. Data loss prevention (DLP)

D. DNS Security

Suggested Answer: *B*

Community vote distribution

B (100%)

Doobiedoo 8 months, 2 weeks ago

Selected Answer: B

"B" is correct. The rest are outbound-only.

upvoted 1 times

Question #62 *Topic 1*

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

Correct Answer: *AC*

Currently there are no comments in this discussion, be the first to comment!