Free Questions for PCNSA by actualtestdumps

Shared by Lyons on 22-07-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Which path in PAN-OS 10.2 is used to schedule a content update to managed devices using Panorama?

Options:

A- Panorama > Device Deployment > Dynamic Updates > Schedules > Add

B- Panorama > Device Deployment > Content Updates > Schedules > Add

C- Panorama > Dynamic Updates > Device Deployment > Schedules > Add

D- Panorama > Content Updates > Device Deployment > Schedules > Add

Answer:

A

Explanation:

https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-upgrade/upgrade-panorama/deploy-updates-to-firewalls-log-collectors-and-wildfire-appliances-using-panorama/schedule-a-content-update-using-panorama

Question 2

Question Type: MultipleChoice

Which two actions are needed for an administrator to get real-time WildFire signatures? (Choose two.)

Options:

A- Obtain a Threat Prevention subscription.

B- Enable Dynamic Updates.

C- Move within the WildFire public cloud region.

D- Obtain a WildFire subscription.

Answer:

B, D

Explanation:

https://docs.paloaltonetworks.com/wildfire/u-v/wildfire-whats-new/wildfire-features-in-panos-100/wildfire-real-time-signature-updates

Question 3

Question Type: MultipleChoice

Which order of steps is the correct way to create a static route?

Options:

A- 1) Enter the route and netmask
2) Enter the IP address for the specific next hop
3) Specify the outgoing interface for packets to use to go to the next hop
4) Add an IPv4 or IPv6 route by name

B- 1) Enter the route and netmask
2) Specify the outgoing interface for packets to use to go to the next hop
3) Enter the IP address for the specific next hop
4) Add an IPv4 or IPv6 route by name

C- 1) Enter the IP address for the specific next hop
2) Enter the route and netmask
3) Add an IPv4 or IPv6 route by name
4) Specify the outgoing interface for packets to use to go to the next hop

D- 1) Enter the IP address for the specific next hop
2) Add an IPv4 or IPv6 route by name
3) Enter the route and netmask
4) Specify the outgoing interface for packets to use to go to the next hop

Answer:

A

Explanation:

Enter the route and netmask

Enter the IP address for the specific next hop

Specify the outgoing interface for packets to use to go to the next hop

Add an IPv4 or IPv6 route by nameComprehensive This is the correct order of steps to create a static route in a virtual router on the firewall. The first step is to enter the route and netmask for the destination network, such as 192.168.2.2/24 for an IPv4 address or 2001:db8:123:1::1/64 for an IPv6 address. The second step is to enter the IP address for the specific next hop, such as 192.168.56.1 or 2001:db8:49e:1::1. The third step is to specify the outgoing interface for packets to use to go to the next hop, such as ethernet1/1.The fourth step is to add an IPv4 or IPv6 route by name, such as route11.Reference:

Configure a Static Route - Palo Alto Networks

Question 4

Question Type: MultipleChoice

An organization has some applications that are restricted for access by the Human Resources Department only, and other applications that are available for any known user in the organization.

What object is best suited for this configuration?

Options:

A- Application Group

B- Tag

C- External Dynamic List

D- Application Filter

Answer:

A

Question 5

Question Type: MultipleChoice

A network administrator creates an intrazone security policy rule on a NGFW. The source zones are set to IT. Finance, and HR.

To which two types of traffic will the rule apply? (Choose two.)

Options:

A- Within zone HR

B- Within zone IT

C- Between zone IT and zone HR

D- Between zone IT and zone Finance

Answer:

A, B

Explanation:

https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClTHCA0

Question 6

Question Type: MultipleChoice

Which two features implement one-to-one translation of a source IP address while allowing the source port to change? (Choose two.)

Options:

A- Static IP

B- Dynamic IP / Port Fallback

C- Dynamic IP

D- Dynamic IP and Port (DIPP)

Answer:

A, D

Explanation:

Static IP and Dynamic IP and Port (DIPP) are two features that implement one-to-one translation of a source IP address while allowing the source port to change.Static IP translates a single source address to a specific public address, and allows the source port to change

dynamically1.Dynamic IP and Port (DIPP) translates the source IP address or range to a single IP address, and uses the source port to differentiate between multiple source IPs that share the same translated address2. Both of these features provide a one-to-one translation of IP addresses, but do not restrict the source port.Reference:

Static IP - Palo Alto Networks

Dynamic IP and Port - Palo Alto Networks

Question 7

Question Type: MultipleChoice

Where within the URL Filtering security profile must a user configure the action to prevent credential submissions?

Options:

A- URL Filtering > Inline Categorization

B- URL Filtering > Categories

C- URL Filtering > URL Filtering Settings

D- URL Filtering > HTTP Header Insertion

Answer:

B

Explanation:

URL filtering technology protects users from web-based threats by providing granular control over user access and interaction with content on the Internet. You can develop a URL filtering policy that limits access to sites based on URL categories, users, and groups. For example, you can block access to sites known to host malware and prevent end users from entering corporate credentials to sites in certain categories.

Question 8

Question Type: MultipleChoice

Which situation is recorded as a system log?

Options:

A- An attempt to access a spoofed website has been blocked.

B- A connection with an authentication server has been dropped.

C- A file that has been analyzed is potentially dangerous for the system.

D- A new asset has been discovered on the network.

Answer:

B

Question 9

Question Type: MultipleChoice

Which System log severity level would be displayed as a result of a user password change?

Options:

A- High

B- Critical

C- Medium

D- Low

Answer:

D

Explanation:

System logs display entries for each system event on the firewall.

1. Critical - Hardware failures, including high availability (HA) failover and link failures.

2. High - Serious issues, including dropped connections with external devices, such as LDAP and RADIUS servers.

3. Medium - Mid-level notifications, such as antivirus package upgrades.

4. Low - Minor severity notifications, such as user password changes.

5. Informational - Log in/log off, administrator name or password change, any configuration change, and all other events not covered by the other severity levels.

https://docs.paloaltonetworks.com/pan-os/11-0/pan-os-admin/monitoring/view-and-manage-logs/log-types-and-severity-levels/system-logs#id8edbfdae-ed92-4d8e-ab76-6a38f96e8cb1

Question 10

Question Type: MultipleChoice

How does the Policy Optimizer policy view differ from the Security policy view?

Options:

A- It provides sorting options that do not affect rule order.

B- It displays rule utilization.

C- It details associated zones.

D- It specifies applications seen by rules.

Answer:

A

Explanation:

You can't filter or sort rules in PoliciesSecurity because that would change the order of the policy rules in the rulebase. Filtering and sorting PoliciesSecurityPolicy OptimizerNo App Specified, PoliciesSecurityPolicy OptimizerUnused Apps, and PoliciesSecurityPolicy OptimizerNew App Viewer (if you have a SaaS Inline Security subscription) does not change the order of the rules in the rulebase.

https://docs.paloaltonetworks.com/pan-os/11-0/pan-os-admin/app-id/security-policy-rule-optimization/policy-optimizer-concepts/sorting-and-filtering-security-policy-rules

Question 11

Question Type: MultipleChoice

What Policy Optimizer policy view differ from the Security policy do?

Options:

A- It shows rules that are missing Security profile configurations.

B- It indicates rules with App-ID that are not configured as port-based.

C- It shows rules with the same Source Zones and Destination Zones.

D- It indicates that a broader rule matching the criteria is configured above a more specific rule.

Answer:

B

Explanation:

Policy Optimizer policy view differs from the Security policy view in several ways. One of them is that it indicates rules with App-ID that are not configured as port-based. These are rules that have the application set to "any" instead of a specific application or group of applications. These rules are overly permissive and can introduce security gaps, as they allow any application traffic on the specified ports.Policy Optimizer helps you convert these rules to application-based rules that follow the principle of least privilege access12.You can use Policy Optimizer to discover and convert port-based rules to application-based rules, and also to remove unused applications, eliminate unused rules, and discover new applications that match your policy criteria3.Reference:

Policy Optimizer Best Practices - Palo Alto Networks

Manage: Policy Optimizer - Palo Alto Networks | TechDocs

Why use Security Policy Optimizer and what are the benefits?