Free Questions for PCNSA by braindumpscollection

Shared by Brady on 24-05-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

When a security rule is configured as Intrazone, which field cannot be changed?

Options:

A- Actions

B- Source Zone

C- Application

D- Destination Zone

Answer:

D

Explanation:

When a security rule is configured as Intrazone, the destination zone field cannot be changed. This is because an intrazone rule applies to traffic that originates and terminates in the same zone.The destination zone is automatically set to the same value as the source zone and cannot be modified1.An intrazone rule allows you to control and inspect traffic within a zone, such as applying security profiles or

logging options2.Reference:What are Universal, Intrazone and Interzone Rules?,Security Policy,Updated Certifications for PAN-OS 10.1,Palo Alto Networks Certified Network Security Administrator (PAN-OS 10.0)or [Palo Alto Networks Certified Network Security Administrator (PAN-OS 10.0)].

Question 2

Question Type: MultipleChoice

An administrator wants to enable access to www.paloaltonetworks.com while denying access to all other sites in the same category.

Which object should the administrator create to use as a match condition for the security policy rule that allows access to www.paloaltonetworks.com?

Options:

A- Application group

B- Address ab

C- URL category

D- Service

Answer:

C

Explanation:

A URL category object is the object that the administrator should create to use as a match condition for the security policy rule that allows access to www.paloaltonetworks.com while denying access to all other sites in the same category. A URL category object allows the administrator to define a custom list of URLs that belong to a specific category, such as Business and Economy.The administrator can then use this object in a security policy rule to allow or deny access to the URLs based on the category1. For example, the administrator can create a URL category object that contains www.paloaltonetworks.com and assign it to the Business and Economy category.Then, the administrator can create a security policy rule that allows access to this URL category object and denies access to the predefined Business and Economy category2.Reference:Create a Custom URL Category,Create a Security Policy Rule to Allow or Deny Access to a Custom URL Category,Certifications - Palo Alto Networks,Palo Alto Networks Certified Network Security Administrator (PAN-OS 10.0)or [Palo Alto Networks Certified Network Security Administrator (PAN-OS 10.0)].

Question 3

Question Type: MultipleChoice

Which path in PAN-OS 11.x would you follow to see how new and modified App-IDs impact a Security policy?

Options:

A- Objects > Dynamic Updates > Review App-IDs

B- Device > Dynamic Updates > Review Policies

C- Device > Dynamic Updates > Review App-IDs

D- Objects > Dynamic Updates > Review Policies

Answer:

C

Explanation:

To see how new and modified App-IDs impact your Security policy, you need to follow the path Device > Dynamic Updates > Review App-IDs on PAN-OS 11.x. This option allows you to perform a content update policy review for both downloaded and installed content. You can view the list of new and modified App-IDs and their descriptions, and see which Security policy rules are affected by them.You can also modify the rules or create new ones to adjust your Security policy as needed1.Reference:See How New and Modified App-IDs Impact Your Security Policy,Updated Certifications for PAN-OS 10.1,Palo Alto Networks Certified Network Security Administrator (PAN-OS 10.0)or [Palo Alto Networks Certified Network Security Administrator (PAN-OS 10.0)].

Question 4

Question Type: MultipleChoice

Which action can be performed when grouping rules by group tags?

Options:

A- Delete Tagged Rule(s)

B- Edit Selected Rule(s)

C- Apply Tag to the Selected Rule(s)

D- Tag Selected Rule(s)

Answer:

D

Explanation:

When grouping rules by group tags, the action that can be performed is to tag selected rule(s). This action allows you to assign one or more tags to the selected rules, which will group them together and display them under the corresponding tag group.You can use tags to organize and visually distinguish your rules based on different criteria, such as function, location, or priority1.Reference:View Rules by Tag Group,Use Tags to Group and Visually Distinguish Objects,Certifications - Palo Alto Networks,Palo Alto Networks Certified Network Security Administrator (PAN-OS 10.0)or [Palo Alto Networks Certified Network Security Administrator (PAN-OS 10.0)].

Question 5

Question Type: MultipleChoice

Which three Ethernet interface types are configurable on the Palo Alto Networks firewall? (Choose three.)

Options:

A- Virtual Wire

B- Tap

C- Dynamic

D- Layer 3

E- Static

Answer:

A, B, D

Explanation:

Palo Alto Networks firewalls support three types of Ethernet interfaces that can be configured on the firewall: virtual wire, tap, and layer 31. These interface types determine how the firewall processes traffic and applies security policies. Some of the characteristics of these interface types are:

Virtual Wire: A virtual wire interface allows the firewall to transparently pass traffic between two network segments without modifying the packets or affecting the routing.The firewall can still apply security policies and inspect the traffic based on the source and destination zones of the virtual wire2.

Tap: A tap interface allows the firewall to passively monitor traffic from a network switch or router without affecting the traffic flow. The firewall can only receive traffic from a tap interface and cannot send traffic out of it.The firewall can apply security policies and inspect the traffic based on the source and destination zones of the tap interface3.

Layer 3: A layer 3 interface allows the firewall to act as a router and participate in the network routing.The firewall can send and receive traffic from a layer 3 interface and apply security policies and inspect the traffic based on the source and destination IP addresses and zones of the interface4.

Question 6

Question Type: **MultipleChoice**

Which table for NAT and NPTv6 (IPv6-to-IPv6 Network Prefix Translation) settings is available only on Panorama?

Options:

A- NAT Target Tab

B- NAT Active/Active HA Binding Tab

C- NAT Translated Packet Tab

D- NAT Policies General Tab

Answer:

A

Explanation:

The NAT Target tab is a table that allows you to specify the target firewalls or device groups for each NAT policy rule on Panorama. This tab is available only on Panorama and not on individual firewalls. The NAT Target tab enables you to create a single NAT policy rulebase on Panorama and then selectively push the rules to the firewalls or device groups that require them.This reduces the complexity and duplication of managing NAT policies across multiple firewalls1.Reference:NAT Target Tab,NAT Policy Overview,NPTv6 Overview,Updated Certifications for PAN-OS 10.1.

Question 7

Question Type: **MultipleChoice**

What is a default setting for NAT Translated Packets when the destination NAT translation is selected as Dynamic IP (with session distribution)?

Options:

A- IP Hash

B- Source IP Hash

C- Round Robin

D- Least Sessions

Answer:

C

Explanation:

When the destination NAT translation is selected as Dynamic IP (with session distribution), the firewall uses a round-robin algorithm to distribute sessions among the available IP addresses that are resolved from the FQDN.This option allows you to load-balance traffic to multiple servers that have dynamic IP addresses1.Reference:Destination NAT,NAT,Getting Started: Network Address Translation (NAT).

Question 8

Question Type: MultipleChoice

What is used to monitor Security policy applications and usage?

Options:

A- Policy Optimizer

B- App-ID

C- Security profile

D- Policy-based forwarding

Answer:

A

Question 9

Question Type: MultipleChoice

A systems administrator momentarily loses track of which is the test environment firewall and which is the production firewall. The administrator makes changes to the candidate configuration of the production firewall, but does not commit the changes. In addition, the configuration was not saved prior to

making the changes.

Which action will allow the administrator to undo the changes?

Options:

A- Load configuration version, and choose the first item on the list.

B- Load named configuration snapshot, and choose the first item on the list.

C- Revert to last saved configuration.

D- Revert to running configuration.

Answer:

D

Explanation:

Reverting to the running configuration will undo the changes made to the candidate configuration since the last commit. This operation will replace the settings in the current candidate configuration with the settings from the running configuration.The firewall provides the

option to revert all the changes or only specific changes by administrator or location1.Reference:Revert Firewall Configuration Changes,How to Revert to a Previous Configuration,How to revert uncommitted changes on the firewall?.

Question 10

Question Type: **MultipleChoice**

Which two addresses should be reserved to enable DNS sinkholing? (Choose two.)

Options:

A- IPv6

B- Email

C- IPv4

D- MAC

Answer:

A, C

Explanation:

https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClGECA0