Free Questions for PCNSA by certsdeals

Shared by Preston on 15-04-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

In which two types of NAT can oversubscription be used? (Choose two.)

Options:

A- Static IP

B- Destination NAT

C- Dynamic IP and Port (DIPP)

D- Dynamic IP

Answer:

C, D

Explanation:

Oversubscription is a feature that allows you to use more private IP addresses than public IP addresses for NAT. This means that multiple private IP addresses can share the same public IP address, as long as they use different ports. Oversubscription can be used in two types of NAT: Dynamic IP and Port (DIPP) and Dynamic IP. DIPP NAT translates both the source IP address and the source port

number of the outgoing packets, and can have an oversubscription rate greater than 1. Dynamic IP NAT translates only the source IP address of the outgoing packets, and can have an oversubscription rate of 1 or less. Static IP and Destination NAT do not support oversubscription, as they require a one-to-one mapping between the private and public IP addresses.Reference:Source NAT,Configure NAT,NAT

Question 2

Question Type: MultipleChoice

Which policy set should be used to ensure that a policy is applied just before the default security rules?

Options:

A- Parent device-group post-rulebase

B- Child device-group post-rulebase

C- Local Firewall policy

D- Shared post-rulebase

Answer:

D

Explanation:

The policy set that should be used to ensure that a policy is applied just before the default security rules is the shared post-rulebase. The shared post-rulebase is a set of Security policy rules that are defined on Panorama and apply to all firewalls or device groups. The shared post-rulebase is evaluated after the local firewall policy and the child device-group post-rulebase, but before the default security rules.The shared post-rulebase can be used to enforce common security policies across multiple firewalls or device groups, such as blocking high-risk applications or traffic1.Reference:Security Policy Rule Hierarchy,Security Policy Rulebase,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

Where does a user assign a tag group to a policy rule in the policy creation window?

Options:

A- Application tab

B- General tab

C- Actions tab

D- Usage tab

Answer:

B

Explanation:

A user can assign a tag group to a policy rule in the policy creation window by selecting the General tab. A tag group is a collection of tags that can be used to identify and filter policy rules based on different criteria, such as function, location, or priority.A user can create a tag group on Panorama and assign it to a policy rule to apply the same set of tags to multiple firewalls or device groups1. To assign a tag group to a policy rule, the user needs to:

Select the General tab in the policy creation window.

Click the Tag Group drop-down menu and select the tag group that the user wants to assign to the policy rule.

Click OK to save the changes. The policy rule will inherit the tags from the tag group and display them in the Tag column.

Question 4

Question Type: MultipleChoice

What are three configurable interface types for a data-plane ethernet interface? (Choose three.)

Options:

A- Layer 3

B- HSCI

C- VWire

D- Layer 2

E- Management

Answer:

A, C, D

Explanation:

Three configurable interface types for a data-plane ethernet interface are Layer 3, VWire, and Layer 2. These interface types determine how the firewall processes traffic and applies security policies. Some of the characteristics of these interface types are:

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 interface1.

VWire: 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.

Layer 2: A layer 2 interface allows the firewall to act as a switch and forward traffic based on MAC addresses.The firewall can send and receive traffic from a layer 2 interface and apply security policies and inspect the traffic based on the source and destination zones of the interface3.

Question 5

Question Type: **MultipleChoice**

An administrator wants to reference the same address object in Security policies on 100 Panorama managed firewalls, across 10 device groups and five templates.

Which configuration action should the administrator take when creating the address object?

Options:

A- Ensure that the Shared option is checked.

B- Ensure that the Shared option is cleared.

C- Ensure that Disable Override is cleared.

D- Tag the address object with the Global tag.

Answer:

A

Explanation:

To reference the same address object in Security policies on 100 Panorama-managed firewalls, across 10 device groups and five templates, the administrator should ensure that the Shared option is checked when creating the address object. This option allows the administrator to create a shared address object that is available to all device groups and templates on Panorama.The shared address object can then be used in multiple firewall policy rules, filters, and other functions1.This reduces the complexity and duplication of managing address objects across multiple firewalls2.Reference:Address Objects,Create a Shared Address Object,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 6

Question Type: MultipleChoice

In which three places on the PAN-OS interface can the application characteristics be found? (Choose three.)

Options:

A- Objects tab > Application Filters

B- Policies tab > Security

C- ACC tab > Global Filters

D- Objects tab > Application Groups

E- Objects tab > Applications

Answer:

A, D, E

Explanation:

The application characteristics can be found in three places on the PAN-OS interface: Objects tab > Application Filters, Objects tab > Application Groups, and Objects tab > Applications. These places allow you to view and manage the applications and application groups

that are used in your Security policy rules.You can also create custom applications and application filters based on various attributes, such as category, subcategory, technology, risk, and behavior1. Some of the characteristics of these places are:

Objects tab > Application Filters: An application filter is a dynamic object that groups applications based on specific criteria. You can use an application filter to match multiple applications in a Security policy rule without having to list them individually. For example, you can create an application filter that includes all applications that have a high risk level or use peer-to-peer technology.

Objects tab > Application Groups: An application group is a static object that groups applications based on your custom requirements. You can use an application group to match multiple applications in a Security policy rule without having to list them individually. For example, you can create an application group that includes all applications that are related to a specific business function or project.

Objects tab > Applications: An application is an object that identifies and classifies network traffic based on App-ID, which is a technology that uses multiple attributes to identify applications. You can use an application to match a specific application in a Security policy rule and control its access and behavior. For example, you can use an application to allow web browsing but block file sharing or social networking.

Question 7

Question Type: **MultipleChoice**

What are three valid source or D=destination conditions available as Security policy qualifiers? (Choose three.)

Options:

A- Service

B- User

C- Application

D- Address

E- Zone ab

Answer:

B, C, E

Explanation:

Three valid source or destination conditions available as Security policy qualifiers are User, Application, and Zone. These qualifiers allow you to define the match criteria for a Security policy rule based on the identity of the user, the application used, and the zone where the traffic originates or terminates.You can use these qualifiers to enforce granular security policies that control access to network resources and prevent threats1. Some of the characteristics of these qualifiers are:

User: The User qualifier allows you to specify the source or destination user or user group for a Security policy rule. The firewall can identify users based on various methods, such as User-ID, Captive Portal, or GlobalProtect.You can use the User qualifier to apply different security policies for different users or user groups, such as allowing access to certain applications or resources based on user roles or privileges2.

Application: The Application qualifier allows you to specify the application or application group for a Security policy rule. The firewall can identify applications based on App-ID, which is a technology that classifies applications based on multiple attributes, such as signatures, protocol decoders, heuristics, and SSL decryption.You can use the Application qualifier to allow or deny access to specific applications or application groups, such as enabling web browsing but blocking social networking or file sharing3.

Zone: The Zone qualifier allows you to specify the source or destination zone for a Security policy rule. A zone is a logical grouping of one or more interfaces that have similar functions or security requirements. The firewall can apply security policies based on the zones where the traffic originates or terminates, such as intrazone, interzone, or universal.You can use the Zone qualifier to segment your network and isolate traffic based on different trust levels or network functions4.

Question 8

Question Type: MultipleChoice

In which two Security Profiles can an action equal to the block IP feature be configured? (Choose two.)

Options:

A- URL Filtering

B- Vulnerability Protection

C- Antivirus b

D- Anti-spyware

Answer:

B, D

Explanation:

The block IP feature can be configured in two Security Profiles: Vulnerability Protection and Anti-spyware. The block IP feature allows the firewall to block traffic from a source IP address for a specified period of time after detecting a threat.This feature can help prevent further attacks from the same source and reduce the load on the firewall1. The block IP feature can be enabled in the following Security Profiles:

Vulnerability Protection: A Vulnerability Protection profile defines the actions that the firewall takes to protect against exploits and vulnerabilities in applications and protocols.You can configure a rule in the Vulnerability Protection profile to block IP connections for a specific threat or a group of threats2.

Anti-spyware: An Anti-spyware profile defines the actions that the firewall takes to protect against spyware and command-and-control (C2) traffic. You can configure a rule in the Anti-spyware profile to block IP addresses for a specific spyware or C2 signature.