Free Questions for PCNSA by certsinside

Shared by Porter on 12-12-2023

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

How are service routes used in PAN-OS?

Options:

A- By the OSPF protocol, as part of Dijkstra's algorithm, to give access to the various services offered in the network

B- To statically route subnets so they are joinable from, and have access to, the Palo Alto Networks external services

C- For routing, because they are the shortest path selected by the BGP routing protocol

D- To route management plane services through data interfaces rather than the management interface

Answer:

D

Explanation:

Service routes are a feature of PAN-OS that allows the administrator to customize the interface that the firewall uses to send requests to external services, such as DNS, email, Palo Alto Networks updates, User-ID agent, syslog, Panorama, dynamic updates, URL updates,

licenses, and AutoFocus1.

By default, the firewall uses the management interface for all service routes, unless the packet destination IP address matches the configured destination service route, in which case the source IP address is set to the source address configured for the destination1.

However, in some scenarios, the administrator may want to use a different interface for service routes, such as when the management interface does not have public internet access, or when the administrator wants to isolate or monitor the traffic for certain services23.

To configure service routes, the administrator can select Device > Setup > Services > Service Route Configuration and customize each service with a source interface and a source address.The administrator can also configure destination service routes to specify a destination IP address and a gateway for each service1.

Service routes are not related to routing protocols such as OSPF or BGP, which are used to exchange routing information between routers and determine the best path to reach a network destination. Service routes are only used to change the interface that the firewall uses to communicate with external services.

Therefore, service routes are used to route management plane services through data interfaces rather than the management interface.

References:

1:Configure Service Routes - Palo Alto Networks2:Setting a Service Route for Services to Use a Dataplane's Interface - Palo Alto Networks3:How to Perform Updates when Management Interface does not have Public Internet Access - Palo Alto Networks

Question 2

Question Type: MultipleChoice

How can a complete overview of the logs be displayed to an administrator who has permission in the system to view them?

Options:

A- Select the unified log entry in the side menu.

B- Modify the number of columns visible on the page

C- Modify the number of logs visible on each page.

D- Select the system logs entry in the side menu.

Answer:

A

Explanation:

The best way to view a complete overview of the logs is to select the unified log entry in the side menu.The unified log is a single view that displays all the logs generated by the firewall, such as traffic, threat, URL filtering, data filtering, and WildFire logs1.The unified log allows the administrator to filter, sort, and export the logs based on various criteria, such as time range, severity, source, destination, application, or action1.

Modifying the number of columns visible on the page or the number of logs visible on each page does not provide a complete overview of the logs, but only changes the display settings of the current log view.Selecting the system logs entry in the side menu does not show all the logs generated by the firewall, but only shows the logs related to system events, such as configuration changes, system alerts, or HA status2.

References:

1:View Logs - Palo Alto Networks2:View and Manage Logs - Palo Alto Networks

Question 3

Question Type: **MultipleChoice**

Which profile should be used to obtain a verdict regarding analyzed files?

Options:

A- WildFire analysis

B- Vulnerability profile

C- Content-ID

D- Advanced threat prevention

Answer:

A

Explanation:

A profile is a set of rules or settings that defines how the firewall performs a specific function, such as detecting and preventing threats, filtering URLs, or decrypting traffic1.

There are different types of profiles that can be applied to different types of traffic or scenarios, such as Antivirus, Anti-Spyware, Vulnerability Protection, URL Filtering, File Blocking, Data Filtering, Decryption, or WildFire Analysis1.

The WildFire Analysis profile is a profile that enables the firewall to submit unknown files or email links to the cloud-based WildFire service for analysis and verdict determination2.WildFire is the industry's most advanced analysis and prevention engine for highly evasive zero-day exploits and malware3.WildFire uses a variety of malware detection techniques, such as static analysis, dynamic analysis, machine learning, and intelligent run-time memory analysis, to identify and protect against unknown threats34.

The Vulnerability Protection profile is a profile that protects the network from exploits that target known software vulnerabilities.It allows the administrator to configure the actions and log settings for each vulnerability severity level, such as critical, high, medium, low, or informational5.

Content-ID is not a profile, but a feature of the firewall that performs multiple functions to identify and control applications, users, content, and threats on the network. Content-ID consists of four components: App-ID, User-ID, Content Inspection, and Threat Prevention.

Advanced Threat Prevention is not a profile, but a term that refers to the comprehensive approach of Palo Alto Networks to prevent sophisticated and unknown threats. Advanced Threat Prevention includes WildFire, but also other products and services, such as DNS Security, Cortex XDR, Cortex XSOAR, and AutoFocus.

Therefore, the profile that should be used to obtain a verdict regarding analyzed files is the WildFire Analysis profile.

References:

1:Security Profiles - Palo Alto Networks2:WildFire Analysis Profile - Palo Alto Networks3:WildFire - Palo Alto Networks4:Advanced Wildfire as an ICAP Alternative | Palo Alto Networks5:Vulnerability Protection Profile - Palo Alto Networks: [Content-ID - Palo Alto Networks] : [Advanced Threat Prevention - Palo Alto Networks]

Question 4

Question Type: **MultipleChoice**

Which two DNS policy actions in the anti-spyware security profile can prevent hacking attacks through DNS queries to malicious domains? (Choose two.)

Options:

A- Deny

B- Sinkhole

C- Override

D- Block

Answer:

B, D

Explanation:

A DNS policy action is a setting in an Anti-Spyware security profile that defines how the firewall handles DNS queries to malicious domains.A malicious domain is a domain name that is associated with a known threat, such as malware, phishing, or botnet1.

There are four possible DNS policy actions: alert, allow, block, and sinkhole1.

The alert action logs the DNS query and allows it to proceed to the intended destination.This action does not prevent hacking attacks, but only notifies the administrator of the potential threat1.

The allow action allows the DNS query to proceed to the intended destination without logging it.This action does not prevent hacking attacks, but only bypasses the DNS security inspection2.

The block action blocks the DNS query and sends a response to the client with an NXDOMAIN (non-existent domain) error code.This action prevents hacking attacks by preventing the client from resolving the malicious domain1.

The sinkhole action redirects the DNS query to a predefined IP address (the sinkhole IP address) that is under the control of the administrator.This action prevents hacking attacks by isolating the client from the malicious domain and allowing the administrator to monitor and remediate the infected host1.

The override action is not a valid DNS policy action, but a setting in an Anti-Spyware security profile that allows the administrator to create exceptions for specific spyware signatures that they want to override the default action or log settings3.

Therefore, the two DNS policy actions that can prevent hacking attacks through DNS queries to malicious domains are block and sinkhole.

References:

1:Enable DNS Security - Palo Alto Networks2:How To Disable the DNS Security Feature from an Anti-Spyware Profile - Palo Alto Networks3:Security Profile: Anti-Spyware - Palo Alto Networks

Question 5

Question Type: **MultipleChoice**

Within an Anti-Spyware security profile, which tab is used to enable machine learning based engines?

Options:

A- Inline Cloud Analysis

B- Signature Exceptions

C- Machine Learning Policies

D- Signature Policies

Answer:

A

Explanation:

An Anti-Spyware security profile is a set of rules that defines how the firewall detects and prevents spyware from compromising hosts on the network.Spyware is a type of malware that collects information from the infected system, such as keystrokes, browsing history, or personal data, and sends it to an external command-and-control (C2) server1.

An Anti-Spyware security profile consists of four tabs: Signature Policies, Signature Exceptions, Machine Learning Policies, and Inline Cloud Analysis1.

The Signature Policies tab allows you to configure the actions and log settings for each spyware signature category, such as adware, botnet, keylogger, phishing, or worm.You can also enable DNS Security to block malicious DNS queries and responses1.

The Signature Exceptions tab allows you to create exceptions for specific spyware signatures that you want to override the default action or log settings.For example, you can allow a signature that is normally blocked by the profile, or block a signature that is normally alerted by the profile1.

The Machine Learning Policies tab allows you to configure the actions and log settings for machine learning based signatures that detect unknown spyware variants.You can also enable WildFire Analysis to submit unknown files to the cloud for further analysis1.

The Inline Cloud Analysis tab allows you to enable machine learning based engines that detect unknown spyware variants in real time. These engines use cloud-based models to analyze the behavior and characteristics of network traffic and identify malicious patterns.You can enable inline cloud analysis for HTTP/HTTPS traffic, SMTP/SMTPS traffic, or IMAP/IMAPS traffic1.

Therefore, the tab that is used to enable machine learning based engines is the Inline Cloud Analysis tab.

References:

1:Security Profile: Anti-Spyware - Palo Alto Networks

Question 6

Question Type: **MultipleChoice**

By default, what is the maximum number of templates that can be added to a template stack?

Options:

A- 6

B- 8

C- 10

D- 12

Answer:

B

Explanation:

By default, the maximum number of templates that can be added to a template stack is 8. This is the recommended limit for performance reasons, as adding more templates may result in sluggish responses on the user interface. However, starting from PAN-OS 8.1.10 and 9.0.4, you can use a debug command to increase the maximum number of templates per stack to 16. This command requires a commit operation to take effect.

A template stack is a collection of templates that you can use to push common settings to multiple firewalls or Panorama managed collectors. A template contains the network and device settings that you want to share across devices, such as interfaces, zones, virtual routers, DNS, NTP, and login banners. You can create multiple templates for different device groups or locations and add them to a template stack in a hierarchical order. The settings in the lower templates override the settings in the higher templates if there are any conflicts. You can then assign a template stack to one or more devices and push the configuration changes.

Question 7

Question Type: MultipleChoice

In which section of the PAN-OS GUI does an administrator configure URL Filtering profiles?

Options:

A- Policies

B- Network

C- Objects

D- Device

Answer:

C

Explanation:

An administrator can configure URL Filtering profiles in the Objects section of the PAN-OS GUI.A URL Filtering profile is a collection of URL filtering controls that you can apply to individual Security policy rules that allow access to the internet1.You can set site access for URL categories, allow or disallow user credential submissions, enable safe search enforcement, and various other settings1.

To create a URL Filtering profile, go to Objects > Security Profiles > URL Filtering and click Add.You can then specify the profile name, description, and settings for each URL category and action2.You can also configure other options such as User Credential Detection, HTTP Header Insertion, and URL Filtering Inline ML2.After creating the profile, you can attach it to a Security policy rule that allows web traffic2.

Question 8

Question Type: **MultipleChoice**

Files are sent to the WildFire cloud service via the WildFire Analysis Profile. How are these files used?

Options:

A- WildFire signature updates

B- Malware analysis

C- Domain Generation Algorithm (DGA) learning

D- Spyware analysis

Answer:

B

Question 9

Question Type: MultipleChoice

What are three ways application characteristics are used? (Choose three.)

Options:

A- As an attribute to define an application group

B- As a setting to define a new custom application

C- As an Object to define Security policies

D- As an attribute to define an application filter

E- As a global filter in the Application Command Center (ACC)

Answer:

A, B, D

Question 10

Question Type: MultipleChoice

Which three filter columns are available when setting up an Application Filter? (Choose three.)

Options:

A- Parent App

B- Category

C- Risk

D- Standard Ports

E- Subcategory

Answer:

B, C, E

Explanation:

https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-web-interface-help/objects/objects-application-filters