PALO ALTO NETWORKS PCNSA Exam Questions

Total Questions: 350+
Demo Questions: 35
Version: Updated for 2025

Prepared and Verified by Cert Empire – Your Trusted IT Certification Partner

For Access to the full set of Updated Questions – Visit:
Palo Alto Networks PCNSA Exam Questions by Cert Empire

Question: 1

Which object would an administrator create to enable access to all applications in the office-programs subcategory?

A. application filter

B. URL category

C. HIP profile

D. application group

Answer:

A

Explanation:

An Application Filter is the correct object to create. It allows an administrator to dynamically group applications based on specific attributes, such as Category, Subcategory, and Technology. By creating a filter where the Subcategory is set to "office-programs," the firewall will automatically include all current and future applications that Palo Alto Networks classifies under that subcategory. This ensures the policy remains up-to-date without manual intervention and is the most efficient method for achieving the stated goal.

Why Incorrect Options are Wrong:

B. URL category: This object is used in URL Filtering profiles to control access to websites, not to identify and control applications via App-ID.
C. HIP profile: A Host Information Profile (HIP) is used by GlobalProtect to assess the security posture of an endpoint, not to group applications for policy enforcement.
D. application group: An application group is a static, manually-defined list of applications. It would require the administrator to add each application individually and would not automatically update.

References:

1. Palo Alto Networks. (2021). PAN-OS Administrator's Guide 10.2.
Section: Objects Application Filters.
Content: "Application filters enable you to dynamically group applications based on application attributes that you define... For example, you can create a filter for all low-risk, browser-based applications that are sanctioned by your IT department. When you use an application filter in a policy rule, the firewall dynamically evaluates the applications that match the filter and applies the rule to them." This directly supports using a filter based on an attribute like subcategory.
2. Palo Alto Networks. (2021). Palo Alto Networks Certified Network Security Administrator (PCNSA) Study Guide. Palo Alto Networks Press.

Chapter 4: App-IDTM.
Content: The guide explains that Application Filters are used to create dynamic groups of applications based on criteria such as category or subcategory. It contrasts this with Application Groups, which are described as static lists of applications that must be manually maintained. This distinction makes the filter the correct choice for including all applications in a subcategory.
3. Palo Alto Networks. (2023). Firewall 10.2 Essentials: Configuration and Management (EDU-210) Student Guide.
Module 6: App-ID.
Content: The official courseware for the PCNSA certification explicitly details the use of Application Filters for creating rules based on application characteristics. It emphasizes that filters are the preferred method for policies that need to adapt to new application definitions within a specific category or subcategory.

Question: 2

An administrator would like to create a URL Filtering log entry when users browse to any gambling website. What combination of Security policy and Security profile actions is correct?

A. Security policy = drop, Gambling category in URL profile = allow

B. Security policy = deny. Gambling category in URL profile = block

C. Security policy = allow, Gambling category in URL profile = alert

D. Security policy = allow. Gambling category in URL profile = allow

Answer:

C

Explanation:

For a Security Profile, such as URL Filtering, to inspect traffic, the corresponding Security policy rule must have an action of "allow". If the Security policy action is "drop" or "deny", the traffic is immediately blocked, and no further profile inspection occurs. The "alert" action within a URL Filtering profile is specifically designed to permit user access to a URL category while generating a log entry in the URL Filtering logs. This combination directly satisfies the administrator's requirement to log access to gambling websites without blocking the user.

Why Incorrect Options are Wrong:

A Security policy action of "drop" immediately discards the traffic, meaning the URL Filtering profile is never evaluated.
A Security policy action of "deny" immediately blocks the traffic, meaning the URL Filtering profile is never evaluated.
While the "allow" action also generates a log, the "alert" action is more specific for explicitly flagging and monitoring traffic for a category without blocking it.

References:

1. Palo Alto Networks PAN-OS Administrator's Guide 10.2, "URL Filtering" section: In the subsection "Configure URL Filtering," the guide details the available actions. It states for the alert action: "The firewall allows the user to access the site and generates a URL Filtering log." This confirms that the alert action fulfills the requirement.
2. Palo Alto Networks PAN-OS Administrator's Guide 10.2, "Security Policy" section: In the subsection "Security Policy Actions," it is explained that Security Profiles are only applied to traffic that is matched by a Security policy rule with an action of allow. This principle invalidates options A and B.
3. Palo Alto Networks PCNSA Study Guide, Chapter 6: "Securing Traffic with Security Profiles": This guide explains the relationship between Security Policies and Security Profiles. It clarifies

that a policy must first permit traffic before a profile can inspect it. It also describes the alert action in a URL Filtering profile as a method to log specific traffic categories while allowing access, distinguishing it from the simple allow action. (Reference: Palo Alto Networks: A Beginner's Guide to PCNSA, Chapter 6, Security Profiles section).

Question: 3

Which statement is true regarding NAT rules?

A. Static NAT rules have precedence over other forms of NAT.

B. Translation of the IP address and port occurs before security processing.

C. NAT rules are processed in order from top to bottom.

D. Firewall supports NAT on Layer 3 interfaces only.

Answer:

C

Explanation:

Palo Alto Networks firewalls evaluate Network Address Translation (NAT) policy rules sequentially from the top of the rulebase to the bottom. When a packet enters the firewall, it is compared against the criteria of the first NAT rule. If it matches, that rule is applied, and no subsequent NAT rules are evaluated for that specific session. This top-down, first-match logic is a fundamental principle for how ordered policies, including Security and NAT, are processed in PAN-OS.

Why Incorrect Options are Wrong:

A. Static NAT rules have precedence over other forms of NAT.
This is incorrect. Precedence is determined by the rule's position in the NAT policy rulebase (top-to-bottom), not by the type of NAT (e.g., Static, Dynamic).
B. Translation of the IP address and port occurs before security processing.
This is incorrect. The firewall performs the Security Policy lookup on the original, pre-NAT IP addresses. The actual IP address and port translation occurs later in the packet flow, after the session is established and allowed by the Security Policy.
D. Firewall supports NAT on Layer 3 interfaces only.
This is incorrect. While NAT is a Layer 3 function, PAN-OS also supports NAT on other interface types that operate at Layer 3, such as tunnel and aggregate interfaces, not just standard Layer 3 routed interfaces.

References:

1. Palo Alto Networks, "PAN-OS Administrator's Guide 10.2," NAT Policy Rules, Page 698.
"The firewall evaluates NAT policy rules in order from top to bottom and applies the first rule that matches the traffic." This directly supports the correct answer (C) and refutes option A by clarifying that order, not type, determines precedence.
2. Palo Alto Networks, "PAN-OS Administrator's Guide 10.2," Packet Flow Sequence in PAN-OS, Page 100.

The packet flow diagram shows that in the slow path, the "Security policy lookup" (Step 9) occurs using the original packet information before the "Forwarding lookup/NAT" (Step 11) where the translation is applied. This refutes option B.

3. Palo Alto Networks, "PAN-OS Administrator's Guide 10.2," NAT Concepts NAT Support on Interface Types, Page 697.

"You can configure NAT on Layer 3, tunnel, and aggregate interfaces. You cannot configure NAT on virtual wire, Layer 2, tap, or HA interfaces." This directly refutes option D, which incorrectly states NAT is supported on Layer 3 interfaces only.

4. Palo Alto Networks Education Services, "Firewall 10.2 Essentials: Configuration and Management (EDU-210)," Student Guide, Module 7: Network Address Translation.

This courseware reinforces that NAT rules are evaluated top-down and that Security policies are evaluated using pre-NAT addresses. It explicitly states, "NAT rules are evaluated in order from top to bottom. The first rule that matches the traffic is applied."

Question: 4

After making multiple changes to the candidate configuration of a firewall, the administrator would like to start over with a candidate configuration that matches the running configuration. Which command in Device Setup Operations would provide the most operationally efficient way to accomplish this?

A. Import named config snapshot

B. Load named configuration snapshot

C. Revert to running configuration

D. Revert to last saved configuration

Answer:

C

Explanation:

The "Revert to running configuration" command is the most efficient method to achieve the stated goal. This operation discards all uncommitted changes in the current candidate configuration and replaces it with a fresh copy of the active running configuration. This allows the administrator to start over with a clean slate that exactly matches what the firewall is currently using, without affecting the live traffic processing.

Why Incorrect Options are Wrong:

A. Import named config snapshot: This is used to load a configuration file from an external location (e.g., an administrator's computer) onto the firewall, not to revert to the active configuration.
B. Load named configuration snapshot: This loads a previously saved configuration version from the firewall's local storage into the candidate config. This is less direct and requires knowing which snapshot matches the running config.
D. Revert to last saved configuration: This loads the configuration that was last explicitly saved, which is not guaranteed to be the same as the current running configuration if changes were committed but not saved.

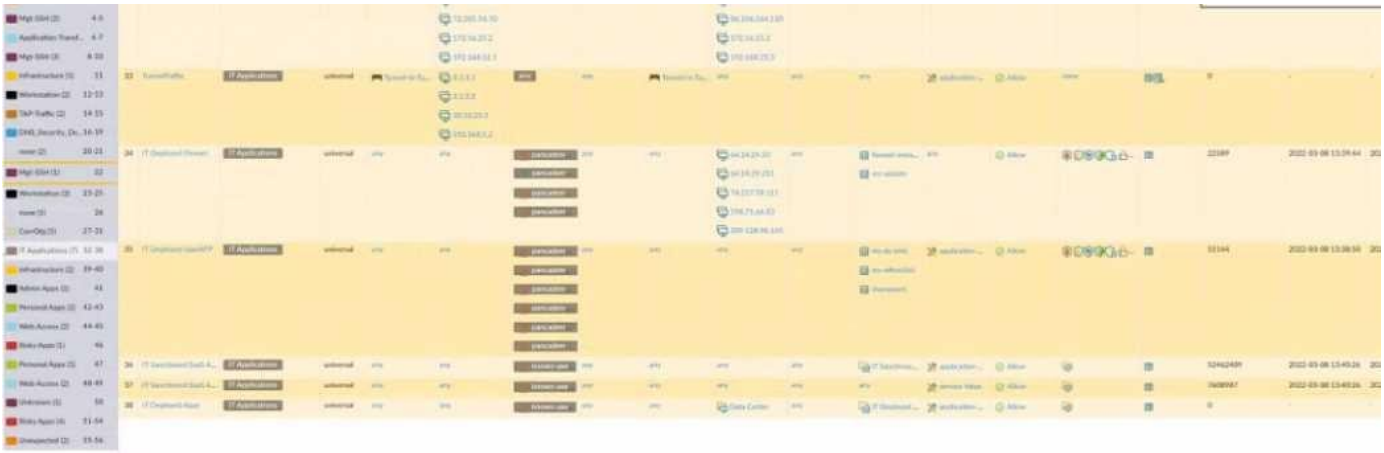
References:

1. Palo Alto Networks, PAN-OS Administrator's Guide 10.2, "Revert Changes to the Running Configuration" section.
"If you make changes to the candidate configuration and then decide you don't want to commit them, you can revert the candidate configuration to the current running configuration. This action discards all the changes you made since the last commit." This directly supports the use of

"Revert to running configuration" for the scenario described.
2. Palo Alto Networks, PAN-OS Administrator's Guide 10.2, "Save and Revert Firewall Configuration Changes" section.
This section distinguishes between the different revert options. It clarifies that "Revert to Running Configuration" discards the candidate configuration, while "Revert to Last Saved Configuration" loads the last explicitly saved running-config.xml, highlighting the critical difference between the running and last-saved states.
3. Palo Alto Networks, PCNSA Study Guide, "Chapter 2: Initial Configuration" section on Configuration Management.
The study guide explains the operational states of firewall configurations, including the candidate and running configurations. It details the functions available in Device Setup Operations, confirming that "Revert to running configuration" is the specific tool for discarding uncommitted changes and reloading the active configuration.

Question: 5

An administrator is reviewing the Security policy rules shown in the screenshot below. Which statement is correct about the information displayed?



A. Eleven rules use the "Infrastructure* tag.

B. The view Rulebase as Groups is checked.

C. There are seven Security policy rules on this firewall.

D. Highlight Unused Rules is checked.

Answer:

B

Explanation:

The screenshot shows the Security policy rulebase organized into collapsible sections labeled "Infrastructure," "Outbound," and "Inbound." This hierarchical presentation is a direct result of enabling the "View Rulebase as Groups" feature. This feature groups rules based on their assigned tags, allowing for better organization and management of large rulebases. The number in parentheses next to each group name, such as "(11)" for Infrastructure, indicates the total number of rules within that specific group.

Why Incorrect Options are Wrong:

A. Eleven rules use the "Infrastructure tag.
"Infrastructure" is the name of the rule group, not a tag. The view groups rules by tags, but the text shown is the group name.
C. There are seven Security policy rules on this firewall.
The total number of rules is 17, which is the sum of the rules in each group (11 + 3 + 3), not seven.
D. Highlight Unused Rules is checked.

There is no visual evidence in the screenshot to confirm that the "Highlight Unused Rules" feature is enabled.

References:

1. Palo Alto Networks, PAN-OS Administrator's Guide 10.2, "Group Security Policy Rules" section.
This section explicitly describes the "View Rulebase as Groups" feature. It states, "To help you better organize your rulebase, you can group security policy rules based on their tags. When you group rules, the firewall displays the rulebase as a set of collapsible sections, where each section corresponds to a tag." This directly supports the correct answer (B).
2. Palo Alto Networks, PAN-OS Administrator's Guide 10.2, "Monitor Policy Rule Usage" section.
This section details how to identify unused rules, including the "Highlight Unused Rules" option. The documentation shows that when enabled, unused rules are highlighted in a distinct color. The provided screenshot does not contain the specific visual cues to confirm this feature is active, making option (D) incorrect.
3. Palo Alto Networks, PAN-OS Administrator's Guide 10.2, "Security Policy" section.
The general documentation on the Security Policy page shows the standard layout. The screenshot clearly deviates from the default flat list and matches the description of the grouped view, further reinforcing that "View Rulebase as Groups" is the correct interpretation of the display. The rule count mechanism (parentheses) is also an inherent part of this GUI feature.

Question: 6

What are the two default behaviors for the intrazone-default policy? (Choose two.)

A. Allow

B. Logging disabled

C. Log at Session End

D. Deny

Answer:

A, B

Explanation:

The Palo Alto Networks firewall includes two predefined, default security policy rules. The intrazone-default rule governs traffic where the source and destination are within the same security zone. By default, this rule is configured with an "allow" action, permitting all traffic to flow freely between interfaces assigned to the same zone. To prevent the generation of excessive and often unnecessary logs for this trusted internal traffic, the default logging behavior for this rule is disabled. These settings can be overridden if required, but the question asks for the default behaviors.

Why Incorrect Options are Wrong:

C. Log at Session End: This is a specific logging action, but the default for the intrazone-default rule is to have logging completely disabled.
D. Deny: This is the default action for the interzone-default rule, which applies to traffic flowing between different security zones, not within the same one.

References:

1. Palo Alto Networks. (2021). PAN-OS Administrator's Guide 10.2. "Default Security Policy Rules". In the section "Security Policy," the documentation states, "The intrazone-default rule allows all traffic between interfaces in the same zone. By default, this rule does not log traffic."
2. Palo Alto Networks. (2023). Palo Alto Networks Certified Network Security Administrator (PCNSA) Study Guide. "Module 3: Securing Traffic with Security Policies". This guide explains that the intrazone-default rule has a default action of "allow" and that logging is not enabled by default.

Question: 7

What are two valid selections within an Antivirus profile? (Choose two.)

A. deny

B. drop

C. default

D. block-ip

Answer:

B, C

Explanation:

Within a Palo Alto Networks Antivirus profile, you configure actions for various protocol decoders to take when a virus is detected. The drop action will silently discard the packet/session containing the virus. The default action instructs the decoder to use the action that is configured for the specific Antivirus signature rule that was matched. Both drop and default are valid, configurable actions for each protocol decoder within the Antivirus profile settings.

Why Incorrect Options are Wrong:

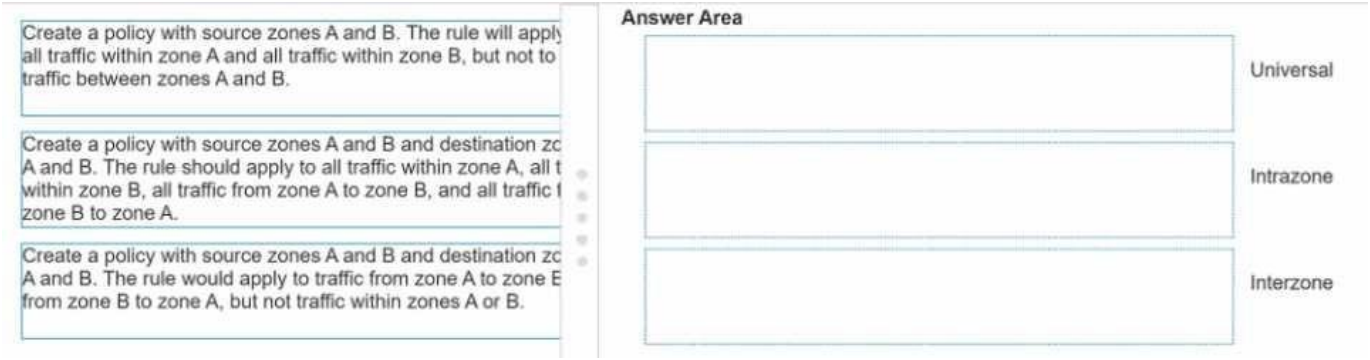
A. deny: The deny action is used in Security Policy rules to explicitly block traffic, but it is not an available action within an Antivirus profile.
D. block-ip: The block-ip action, which blocks traffic from a source or to a destination IP address for a specified time, is available in Anti-Spyware and Vulnerability Protection profiles, not in Antivirus profiles.

References:

1. Palo Alto Networks PAN-OS Administrator's Guide 10.2: In the section "Objects Security Profiles Antivirus Configure Antivirus Profiles," the table under "Antivirus Profile Decoder Actions" lists the available actions. It includes default and drop, but not deny or block-ip.
2. Palo Alto Networks PCNSA Study Guide (EDU-210): Module 5, "Securing Traffic with Security Profiles," page 10, describes the actions available for Antivirus profiles. It states, "The available actions for each decoder are default, allow, alert, drop, reset-client, reset-server, and reset-both." This confirms drop and default as valid options.
3. Palo Alto Networks PAN-OS Administrator's Guide 10.2: The section "Objects Security Profiles Anti-Spyware" details the block-ip action, confirming it is a feature of the Anti-Spyware profile, not the Antivirus profile. The description states: "Block IP: Blocks traffic from the source or to the destination IP address for a specified time."

Question: 8

DRAG DROP Match each rule type with its example



Answer:

Universal: Create a policy with source zones A and B and destination zones A and B. The rule should apply to all traffic within zone A, all traffic within zone B, all traffic from zone A to zone B, and all traffic from zone B to zone A.

Intrazone: Create a policy with source zones A and B. The rule will apply to all traffic within zone A and all traffic within zone B, but not to traffic between zones A and B.

Interzone: Create a policy with source zones A and B and destination zones A and B. The rule would apply to traffic from zone A to zone B and from zone B to zone A, but not traffic within zones A or B.

Explanation:

Security policy rules control network traffic based on its source and destination security zones. The three rule types are defined as follows:

• Universal: This rule type is the most comprehensive, applying to all traffic combinations for the zones specified. It matches both traffic between different zones (interzone) and traffic that stays within a single zone (intrazone).

• Intrazone: This rule type specifically applies to traffic where the source and destination are within the same zone. It does not apply to traffic crossing zone boundaries.

• Interzone: This rule type applies only to traffic that moves between different zones, meaning the source zone is different from the destination zone. It does not control traffic that originates and terminates in the same zone.

References:

Palo Alto Networks. (2023). PAN-OS Administrator's Guide, Version 11.0. In the "Security Policy" chapter, the section "Security Policy Rule Types" defines the universal, intrazone, and interzone rule types. It states, "A universal rule... applies to all matching interzone and intrazone traffic in the specified source and destination zones." It defines an intrazone rule as applying to traffic "where the source and destination zones are the same" and an interzone rule as applying to traffic "where the source and destination zones are different."

St. Petersburg College. CNT 2402: Network Security and Countermeasures (Firewall). Course materials on firewall policy configuration explain that policies are differentiated based on whether they control traffic within a security segment (intrazone) or between different security segments (interzone), which aligns with the logic presented in the question.

Question: 9

An administrator wants to create a NAT policy to allow multiple source IP addresses to be translated to the same public IP address. What is the most appropriate NAT policy to achieve this?

A. Dynamic IP and Port

B. Dynamic IP

C. Static IP

D. Destination

Answer:

A

Explanation:

Dynamic IP and Port (DIPP) NAT is the correct policy for a many-to-one translation scenario. This method translates the original source IP address to a single, specified public IP address. To differentiate between the multiple, concurrent sessions from various internal hosts, the firewall also translates the original source port to a unique, available port on the translated public IP address. This process, also known as Port Address Translation (PAT) or NAT Overload, allows thousands of internal devices to share a single public IP address for outbound communication.

Why Incorrect Options are Wrong:

B. Dynamic IP: This policy creates a one-to-one mapping from a private IP to the next available IP in a pool of public addresses, which is not a many-to-one translation to a single IP.
C. Static IP: This creates a permanent, one-to-one mapping between a specific private IP and a specific public IP, typically used for servers. It does not support multiple sources.
D. Destination: This is Destination NAT (DNAT), which modifies the destination address of incoming packets to redirect traffic to an internal host, not the source address of outgoing packets.

References:

1. Palo Alto Networks PAN-OS Administrator's Guide 10.2, "NAT Policy Rules," Section: "NAT Policy Rule Types."
Page/Section: In the description of Dynamic IP and Port (DIPP), it states: "Uses a single public IP address to translate multiple internal addresses. The firewall tracks the source port of the internal host and assigns a unique source port for each session on the public IP address. This type of NAT is also known as Port Address Translation (PAT) or NAT Overload." This directly supports the correct answer.

2. Palo Alto Networks PAN-OS Administrator's Guide 10.2, "NAT Policy Rules," Section: "NAT Policy Rule Types."
Page/Section: The description for Dynamic IP states: "Translates a private source IP address to a public IP address from a pool of available IP addresses. The translation is one-to-one..." This confirms why option B is incorrect for this scenario.
3. Palo Alto Networks PCNSA Study Guide 10.1, "Module 6: NAT."
Page/Section: The section on "Source NAT Types" explains that DIPP is used when you want to "conserve public IP addresses by allowing many hosts to share a single public IP address." This aligns with the question's requirement.

Question: 10

Which action can be set in a URL Filtering Security profile to provide users temporary access to all websites in a given category using a provided password?

A. exclude

B. continue

C. hold

D. override

Answer:

D

Explanation:

The 'override' action in a URL Filtering Security profile is designed to grant temporary, password-protected access to a blocked URL category. When a user attempts to access a site in a category configured with this action, the firewall presents a response page requiring a password. If the correct password is entered, the user is granted access to all sites within that category for a duration configured by the administrator (e.g., 15 minutes, 1 hour). This provides a mechanism for controlled, temporary exceptions to the policy.

Why Incorrect Options are Wrong:

A. exclude: 'Exclude' is not a configurable action for a URL category within a Security profile. It refers to the concept of excluding specific URLs from filtering, typically via an allow list.
B. continue: The 'continue' action presents a warning page that the user can bypass by clicking a button, but it does not require a password for access.
C. hold: 'Hold' is not a valid action within a Palo Alto Networks URL Filtering Security profile.

References:

1. Palo Alto Networks PAN-OS Administrator's Guide 10.2, "URL Filtering Profile Actions":
Section: Objects Security Profiles URL Filtering
Content: This section explicitly describes the 'override' action: "Displays a response page that prompts the user for a password to access the site. You must define an override password when you configure this action. After the user enters the password, the firewall allows the user to access all sites in the category for a configurable amount of time..." It also describes the 'continue' action, confirming it does not use a password.
2. Palo Alto Networks PAN-OS Administrator's Guide 11.0, "Configure URL Filtering":
Section: Objects Security Profiles URL Filtering Configure URL Filtering
Content: This document details the configuration steps and available actions. It confirms that 'override' is the action that "allows users to access blocked sites by entering a password." It does

not list 'exclude' or 'hold' as valid category actions.

Question: 11

What is a function of application tags?

A. creation of new zones

B. application prioritization

C. automated referenced applications in a policy

D. IP address allocations in DHCP

Answer:

C

Explanation:

Application tags are metadata labels assigned by Palo Alto Networks to App-ID signatures based on their characteristics (e.g., category, technology, risk). Administrators use these tags to create dynamic Application Filters. When a security policy references an Application Filter, it automatically incorporates all applications that match the specified tags. As Palo Alto Networks releases new content updates with new applications, any application with a matching tag is automatically included in the filter and, consequently, the policy. This automates the process of keeping security policies current without manual intervention.

Why Incorrect Options are Wrong:

A. creation of new zones: Zones are logical groupings of network interfaces configured by an administrator and are entirely independent of application identification or tags.
B. application prioritization: Application prioritization is a function of Quality of Service (QoS) policies, which control bandwidth allocation, not a direct function of application tags.
D. IP address allocations in DHCP: DHCP is a network service for dynamically assigning IP addresses to clients; it is unrelated to the firewall's application identification and tagging features.

References:

1. Palo Alto Networks. (2021). PAN-OS Administrator's Guide, Release 10.1. "Objects Applications". In the section on Application Filter, it states: "When you use tags to create an application filter, the filter is dynamic. As Palo Alto Networks adds new applications with new content updates, any application that has a tag that you have used in a filter is automatically added to the filter." This directly supports the automated referencing of applications in a policy.
2. Palo Alto Networks. (2023). Palo Alto Networks Certified Network Security Administrator (PCNSA) Study Guide. "Module 3: Securing Traffic with Policies". The guide explains that Application Filters use tags to dynamically group applications. It states, "As new App-IDs are created and existing ones are modified, the firewall can dynamically update the application filters

to include or exclude applications based on their attributes." This confirms the automated nature of policies using these filters.

Question: 12

What are three Palo Alto Networks best practices when implementing the DNS Security Service? (Choose three.)

A. Implement a threat intel program.

B. Configure a URL Filtering profile.

C. Train your staff to be security aware.

D. Rely on a DNS resolver.

E. Plan for mobile-employee risk

Answer:

A, B, E

Explanation:

Palo Alto Networks lists five recommendations for deploying the DNS Security Service. The three that directly address technical implementation on the NGFW are:
• Implement a threat-intelligence program so the firewall can correlate local findings with cloud-delivered DNS threat data.
• Complement DNS inspection with URL Filtering by attaching a URL Filtering profile to the same security-policy rules; this blocks follow-on HTTP/HTTPS calls if a malicious domain resolves.
• Plan for mobile-employee risk by ensuring roaming and VPN users' DNS traffic is routed through the NGFW or Prisma Access so it can be examined by the service.

Why Incorrect Options are Wrong:

C. Train your staff to be security aware - sound advice but classified by Palo Alto Networks as a general security practice, not a core firewall-side best practice for DNS Security deployment.
D. Rely on a DNS resolver - best practice is the opposite: "Don't rely on DNS resolvers alone"; resolvers can be bypassed and provide no inline enforcement at the firewall.

References:

1. Palo Alto Networks, "Top 5 Best Practices for DNS Security You Should Be Following," Tech Blog, 4 June 2020 - sections 1, 2, 4.
2. Palo Alto Networks TechDocs, PAN-OS 10.2, "DNS Security Service Best Practices" - paragraphs under "Build a Threat Intelligence Program," "Plan for Mobile User Risk," and "Complement DNS With URL Filtering."
3. Palo Alto Networks White Paper, "Best Practices for Securing DNS With Palo Alto Networks Next-Generation Firewalls," pp. 3-5 (Threat Intel, Mobile Users, URL Filtering integration).

Question: 13

An administrator is investigating a log entry for a session that is allowed and has the end reason of aged-out. Which two fields could help in determining if this is normal? (Choose two.)

A. Packets sent/received

B. IP Protocol

C. Action

D. Decrypted

Answer:

A, B

Explanation:

To determine if an aged-out session is normal, an administrator must verify if the connection was successfully established and if the timeout behavior is expected for the protocol in use.
1. Packets sent/received: This field is crucial. If a TCP session shows packets sent but zero packets received, it indicates the initial connection attempt (e.g., SYN packet) received no reply (e.g., SYN-ACK). The session was created but never established, eventually aging out. This is an abnormal condition pointing to a network or server issue. A healthy exchange of packets before aging out is normal.

2. IP Protocol: This field provides context for the session's expected behavior and timeout value. For example, UDP is connectionless and has a short default idle timeout (30 seconds). A UDP session aging out is very common and normal. A TCP session has a much longer default timeout (3600 seconds), and its aging out may require more scrutiny depending on the application.

Why Incorrect Options are Wrong:

C. Action: The question already states the session was allowed. This field provides no additional information to determine if the session termination was normal.
D. Decrypted: Whether a session was decrypted or not is unrelated to the session timeout mechanism. Both encrypted and unencrypted sessions can age out for normal or abnormal reasons.

References:

1. Palo Alto Networks PAN-OS Administrator's Guide 10.2, "Traffic Log Fields": This section details the available columns in the traffic log. The descriptions for Packets Sent and Packets Received confirm their role in tracking the bidirectional flow of traffic, which is fundamental to diagnosing incomplete sessions that result in an aged-out state. The Protocol field is defined as the IP protocol for the session. (Reference: PAN-OS Administrator's Guide 10.2, Chapter: Monitor, Section: Logs, Subsection: Traffic Log Fields)

2. Palo Alto Networks PAN-OS Administrator's Guide 10.2, "Session Timeouts": This documentation specifies the default idle-timeout values for different protocols (e.g., TCP: 3600s, UDP: 30s). This confirms that the IP Protocol is essential context for evaluating if an aged-out event is normal, as the expected idle time varies significantly by protocol. (Reference: PAN-OS Administrator's Guide 10.2, Chapter: Objects, Section: Session Settings)
3. Palo Alto Networks Knowledge Base, Article 2613, "Session End Reason: Aged-out": This article explains that aged-out is a normal reason for a session to close. It further clarifies that troubleshooting abnormal aged-out scenarios often involves checking for asymmetrical routing or unresponsive servers, conditions that are directly diagnosed by examining the Packets sent/received counts in the traffic log.

Question: 14

What does an application filter help you to do?

A. It dynamically provides application statistics based on network, threat, and blocked activity,

B. It dynamically filters applications based on critical, high, medium, low. or informational severity.

C. It dynamically groups applications based on application attributes such as category and subcategory.

D. It dynamically shapes defined application traffic based on active sessions and bandwidth usage.

Answer:

C

Explanation:

An Application Filter is a configuration object in PAN-OS that allows for the dynamic grouping of applications based on their defined attributes. These attributes include Category, Subcategory, Technology, Risk, and Characteristics. When an Application Filter is used in a Security policy rule, the firewall automatically includes any new or updated applications from the App-ID database that match the specified filter criteria. This simplifies administration by ensuring policies remain current without manual intervention as new applications emerge.

Why Incorrect Options are Wrong:

A. This describes the function of the Application Command Center (ACC) or other monitoring/reporting tools, not an Application Filter object used for policy creation.
B. While severity (risk) is one of the attributes that can be used in an Application Filter, this option is too specific and incomplete. The filter's primary purpose is to group applications based on a wide range of attributes, not just severity.
D. This describes the function of Quality of Service (QoS) policies, which are used to manage bandwidth and prioritize traffic, not to group applications for security policy matching.

References:

1. Palo Alto Networks. (2023). PAN-OS Administrator's Guide, Version 11.0. "Objects Application Filters". The documentation states, "You can create an application filter to group applications dynamically based on application attributes... When you use an application filter in a policy rule, the firewall automatically includes in the rule any new applications that match the filter criteria."
2. Palo Alto Networks. (2021). Palo Alto Networks Certified Network Security Administrator (PCNSA) Study Guide. "Chapter 4: Securing Traffic with Policies". The guide explains that Application Filters are used to "dynamically group applications based on their attributes" and lists Category, Subcategory, and Technology as examples of these attributes. This object is then used

within Security policy rules.

Question: 15

Prior to a maintenance-window activity, the administrator would like to make a backup of only the running configuration to an external location. What command in Device Setup Operations would provide the most operationally efficient way to achieve this outcome?

A. save named configuration snapshot

B. export device state

C. export named configuration snapshot

D. save candidate config

Answer:

C

Explanation:

The most operationally efficient method to back up only the running configuration to an external location is to use the export named configuration snapshot command. This operation, found under Device Setup Operations, directly prompts the user to save the current running-config.xml file to their local client system. This single action fulfills both requirements of the task: backing up the running configuration and saving it to an external location. Other options either save the configuration locally, requiring an extra step for export, or include unnecessary system state data.

Why Incorrect Options are Wrong:

A. save named configuration snapshot: This action saves a snapshot of the running configuration locally on the firewall's disk, not to an external location. An additional export step would be required.
B. export device state: This exports a comprehensive bundle including logs, certificates, and licenses in addition to the configuration. The question specifically asks for only the running configuration.
D. save candidate config: This action saves the candidate configuration (uncommitted changes), not the active running configuration as required by the question.

References:

1. Palo Alto Networks PAN-OS Administrator's Guide 10.2. (2021). Save and Export Configuration Backups. Page 1011.
For Correct Answer (C): "To export a configuration version to your client system, select Device Setup Operations and click Export named configuration snapshot." This confirms the function directly exports the configuration to an external client.
For Incorrect Answer (A): "To save a snapshot of the current candidate or running configuration

on the firewall, select Device Setup Operations and click Save named configuration snapshot." This confirms the save operation is local to the firewall.
For Incorrect Answer (B): "The device state is a collection of files that contain the running configuration of the firewall and the logs, licenses, and certificates that are on the firewall... To export the device state, select Device Setup Operations and click Export device state." This shows it includes more than just the configuration.
For Incorrect Answer (D): "To save the candidate configuration, select Device Setup Operations and click Save candidate config." This confirms it saves the candidate, not the running, configuration.

Question: 16

Your company is highly concerned with their Intellectual property being accessed by unauthorized resources. There is a mature process to store and include metadata tags for all confidential documents. Which Security profile can further ensure that these documents do not exit the corporate network?

A. File Blocking

B. Data Filtering

C. Anti-Spyware

D. URL Filtering

Answer:

B

Explanation:

Data Filtering profiles are the specific Security profile feature designed for Data Loss Prevention (DLP). They work by scanning traffic for predefined or custom data patterns. In this scenario, a custom data pattern can be created to match the specific metadata tags or content within the company's confidential documents. When a file containing this pattern is detected in outbound traffic (e.g., an email attachment or a web upload), the Data Filtering profile, applied to a Security policy rule, can block the session, thus preventing the intellectual property from leaving the corporate network.

Why Incorrect Options are Wrong:

A. File Blocking: This profile blocks files based on their type (e.g., PDF, EXE) or name, not their specific content or metadata.
C. Anti-Spyware: This profile detects and blocks command-and-control (C2) traffic from malware, but it does not inspect legitimate files for sensitive data patterns.
D. URL Filtering: This profile controls access to websites based on their category but does not inspect the content of files being uploaded to permitted sites.

References:

1. Palo Alto Networks, PAN-OS Administrator's Guide 10.2 (2022).
Section: Objects Security Profiles Data Filtering.
Content: "Data filtering profiles scan for sensitive information, such as credit card and social security numbers, or for custom data patterns that you define. When traffic matches a data filtering profile, the firewall can block the traffic to prevent data exfiltration." This directly supports the use of Data Filtering for preventing the loss of documents with specific patterns.

2. Palo Alto Networks, PCNSA Study Guide, PAN-OS 10.0 (2020).
Section: Chapter 6: Securing Traffic with Security Profiles, "Data Filtering Profiles" subsection.
Content: The guide explains that Data Filtering profiles "prevent the loss of sensitive data, such as confidential information, from leaving the network." It explicitly mentions the ability to create custom data patterns to match proprietary or sensitive information, which aligns with the scenario's requirement to identify documents by metadata tags.
3. Palo Alto Networks, TechDocs - Data Filtering (PAN-OS 11.0).
Section: Data Filtering Overview.
Content: "Data filtering enables you to prevent sensitive data, such as credit card or social security numbers and other sensitive information, from leaving the network... You can also define custom data patterns to protect other sensitive information that is important to your organization." This confirms that custom patterns, which could be used for metadata tags, are a core function of the Data Filtering profile.

Question: 17

An administrator wants to create a No-NAT rule to exempt a flow from the default NAT rule. What is the best way to do this?

A. Create a Security policy rule to allow the traffic.

B. Create a new NAT rule with the correct parameters and leave the translation type as None

C. Create a static NAT rule with an application override.

D. Create a static NAT rule translating to the destination interface.

Answer:

B

Explanation:

To exempt a specific traffic flow from Network Address Translation (NAT), the correct method is to create a dedicated NAT policy rule. This rule must be configured to match the specific source and destination parameters of the traffic flow you wish to exempt. Within this rule, the "Translation Type" must be set to "None." This explicitly instructs the firewall not to perform any address translation on the matching packets. For this exemption to be effective, the No-NAT rule must be placed higher in the rule order than any broader NAT rule that would otherwise match and translate the traffic.

Why Incorrect Options are Wrong:

A. Security policy rules are processed separately from NAT rules and are used to allow or deny traffic, not to control address translation.
C. A static NAT rule is typically used for inbound one-to-one address mapping, and an application override is for bypassing App-ID, neither of which creates a NAT exemption.
D. A static NAT rule inherently performs translation, which is the opposite of the "No-NAT" requirement to exempt a flow from translation.

References:

1. Palo Alto Networks. (2021). PAN-OS Administrator's Guide 10.2. Chapter: "NAT", Section: "NAT Policy Rules", Subsection: "Translated Packet Tab". The documentation states: "None-Select if you do not want to apply NAT to traffic that matches the Original Packet criteria. This is useful when you want to exempt a specific address or range of addresses from NAT."
2. Palo Alto Networks. (2023). Palo Alto Networks Certified Network Security Administrator (PCNSA) Study Guide. Chapter 7: "NAT", Section: "NAT Policy Rules". This official study guide explains that to exclude traffic from NAT, a NAT policy rule must be created with the translation type set to "None" and placed before other matching NAT rules.

Question: 18

When creating a Panorama administrator type of Device Group and Template Admin, which two things must you create first? (Choose two.)

A. password profile

B. access domain

C. admin rote

D. server profile

Answer:

B, C

Explanation:

When creating a custom, role-based administrator in Panorama, two components are mandatory prerequisites. First, an Admin Role profile must be created to define the administrator's permissions, specifying what actions they can perform within the web interface and CLI. Second, an Access Domain must be configured to define the administrator's scope, limiting their management capabilities to specific device groups, templates, and virtual systems. The question's use of "type of Device Group and Template Admin" implies the creation of a custom role with this function, which necessitates both an Admin Role and an Access Domain.

Why Incorrect Options are Wrong:

A. password profile: This is an optional configuration used to enforce password complexity and expiration policies for local administrator accounts. It is not a mandatory prerequisite.
D. server profile: This is only required when configuring an administrator account that authenticates to an external service like RADIUS, TACACS+, or LDAP. It is not required for local administrators.

References:

1. Palo Alto Networks. (2021). Panorama Administrator's Guide 10.1. pp. 65-68, "Administrative Accounts and Roles". The guide details that for a "Role Based" administrator, you must select a pre-configured "Role Profile" (Admin Role) and an "Access Domain".
2. Palo Alto Networks. (2021). Panorama Administrator's Guide 10.1. p. 70, "Configure an Admin Role Profile". This section states, "To define a custom set of privileges for a role-based administrator, you create an admin role profile."
3. Palo Alto Networks. (2021). Panorama Administrator's Guide 10.1. p. 74, "Configure an Access Domain". This section explains, "An access domain enables you to create a logical container of device groups and templates to which you can grant access for a role-based administrator."

Question: 19

An administrator is troubleshooting traffic that should match the interzone-default rule. However, the administrator doesn't see this traffic in the traffic logs on the firewall. The interzone-default was never changed from its default configuration. Why doesn't the administrator see the traffic?

A. Traffic is being denied on the interzone-default policy.

B. The Log Forwarding profile is not configured on the policy.

C. The interzone-default policy is disabled by default

D. Logging on the interzone-default policy is disabled

Answer:

D

Explanation:

By default, the interzone-default security policy rule on a Palo Alto Networks firewall is configured with an action of "deny" but has logging disabled. This is to prevent the firewall's log database from being overwhelmed by implicitly denied traffic. For an administrator to view traffic that matches this rule in the Monitor Logs Traffic section, they must first override the default rule and explicitly enable the "Log at Session End" option within the rule's "Actions" tab.

Why Incorrect Options are Wrong:

A. While the traffic is indeed denied by default, this fact does not explain the absence of log entries. Denied traffic is logged if the rule is configured to do so.
B. A Log Forwarding profile is used to send logs to external collectors (e.g., Panorama, Syslog). Its absence does not prevent logs from being generated locally on the firewall.
C. The interzone-default policy is enabled by default. It serves as the final, implicit rule for all traffic between different security zones that is not explicitly allowed.

References:

1. Palo Alto Networks, PAN-OS Administrator's Guide 10.2, "Security Policy," section "Default Security Rules." The documentation states, "By default, the intrazone-default and interzone-default rules are configured with the Log at Session End option disabled." (p. 598)
2. Palo Alto Networks, Firewall Essentials: Configuration and Management (EDU-210) Student Guide, Module 4: "Security Policy." The courseware explains that the two default rules, intrazone-default and interzone-default, do not log traffic by default and must be overridden to enable logging for troubleshooting purposes.
3. Palo Alto Networks, PCNSA Study Guide, "Domain 2: Core Concepts," section "Security Policies." The guide clarifies the behavior of default security rules, noting, "The two predefined rules do not log any traffic by default." (p. 56)

Question: 20

An administrator is configuring a NAT rule At a minimum, which three forms of information are required? (Choose three.)

A. name

B. source zone

C. destination interface

D. destination address

E. destination zone

Answer:

B, D, E

Explanation:

When configuring a NAT policy rule on a Palo Alto Networks firewall, the primary goal is to define the specific traffic that requires translation. This is accomplished in the "Original Packet" tab of the rule configuration. The three most fundamental and mandatory pieces of information to match the traffic are the Source Zone (where the packet enters the firewall), the Destination Zone (the zone the packet is destined for), and the original Destination Address. Together, these parameters define the traffic flow that the NAT rule will act upon.

Why Incorrect Options are Wrong:

A. name: While a rule name is a mandatory field for creating any policy, it serves as an administrative identifier and is not a criterion for matching traffic flow.
C. destination interface: Specifying a destination interface is an optional parameter. The firewall typically determines the egress interface using its routing table based on the destination zone.

References:

1. Palo Alto Networks, PAN-OS Administrator's Guide 10.2, "NAT Policy Rules," Page 789. The guide details the configuration of NAT policy rules. In the section describing the "Original Packet" tab, it explicitly lists "Source Zone," "Destination Zone," and "Destination Address" as required fields for matching the original packet characteristics.
2. Palo Alto Networks, PCNSA Study Guide, "Chapter 6: Network Address Translation," Page 136. The study guide states, "The Original Packet section of a NAT policy rule specifies the source and destination zones, and the source and destination addresses of the packets that are subject to the NAT policy rule." This confirms that zones and addresses are the core matching criteria.
3. Palo Alto Networks, PAN-OS Administrator's Guide 10.2, "NAT Policy Rule Original Packet

Tab," Page 791. This section provides a table of the settings. It shows that "Destination Interface" is an optional setting, stating, "Select the destination interface for incoming traffic. If you do not specify an interface, the setting defaults to any." In contrast, Source Zone, Destination Zone, and Destination Address are presented as fundamental matching criteria that must be defined.

Question: 21

Which type of address object is www.paloaltonetworks.com?

A. IP range

B. IP netmask

C. named address

D. FQDN

Answer:

D

Explanation:

The string "www.paloaltonetworks.com" is a Fully Qualified Domain Name (FQDN). In Palo Alto Networks firewalls, an FQDN address object is used to represent a host for which the IP address may change over time. The firewall periodically resolves the FQDN to its corresponding IP address(es) using DNS. This allows administrators to create security policies based on a consistent domain name rather than constantly updating IP addresses, which is particularly useful for cloud services and other dynamic environments.

Why Incorrect Options are Wrong:

A. IP range: An IP range defines a contiguous block of IP addresses, specified by a starting and ending address (e.g., 192.168.1.10-192.168.1.20), not a hostname.
B. IP netmask: An IP netmask defines a network or a single host with a subnet mask (e.g., 10.1.1.0/24 or 10.1.1.1/32), not a hostname.
C. named address: This is not a valid address object type. While all address objects are given a name for identification, "named address" does not describe the format of the address itself.

References:

1. Palo Alto Networks. (2023). PAN-OS Administrator's Guide 10.2. "Objects Addresses". In this section, the guide lists the available address object types. It explicitly defines the FQDN type as "A hostname that the firewall can resolve to an IP address using a DNS server." This directly matches the question's example.
2. Palo Alto Networks. (2021). Palo Alto Networks Certified Network Security Administrator (PCNSA) Study Guide. "Chapter 4: Securing Traffic with Policies". Under the section "Building Blocks of a Security Policy," the guide discusses Address Objects and lists FQDN as a type used for domain names that resolve to IP addresses.
3. Palo Alto Networks. (2021). EDU-210 Firewall 10.1 Essentials: Configuration and Management Student Guide. "Module 4: Managing Firewall Objects". This courseware details the creation of Address Objects and specifies FQDN as a type for objects like "www.paloaltonetworks.com".

Question: 22

What are three characteristics of the Palo Alto Networks DNS Security service? (Choose three.)

A. It uses techniques such as DGA.DNS tunneling detection and machine learning.

B. It requires a valid Threat Prevention license.

C. It enables users to access real-time protections using advanced predictive analytics.

D. It requires a valid URL Filtering license.

E. It requires an active subscription to a third-party DNS Security service.

Answer:

A, B, C

Explanation:

The Palo Alto Networks DNS Security service is a cloud-based solution designed to protect against advanced threats that use DNS. It leverages machine learning (ML) and predictive analytics to provide real-time protection against new and emerging threats. Key techniques include detecting command-and-control (C2) activity by identifying domains generated by Domain Generation Algorithms (DGAs) and preventing data exfiltration through DNS tunneling. For on-premises firewalls, the DNS Security service is activated through the Threat Prevention subscription, which provides the necessary license to enable these advanced DNS-layer protections.

Why Incorrect Options are Wrong:

D. It requires a valid URL Filtering license.
This is incorrect. DNS Security and URL Filtering are distinct, separately licensed services, although they can be used together for layered security.
E. It requires an active subscription to a third-party DNS Security service.
This is incorrect. The DNS Security service is a first-party solution developed and maintained by Palo Alto Networks, leveraging its own threat intelligence infrastructure.

References:

1. Palo Alto Networks. (2021). DNS Security Datasheet.
Page 1, "Highlights" section: "Applies predictive analytics, machine learning, and automation to block attacks that use DNS." (Supports options A and C).
Page 1, "Prevent C2 and Data Theft" section: "Protections for DNS tunneling, DGA, and more..." (Supports option A).
Page 2, "Licensing Information" section: "The DNS Security subscription is available as a

standalone subscription, as part of the Threat Prevention subscription..." While available standalone, its inclusion with Threat Prevention is a primary characteristic and common deployment model, making option B a valid characteristic of its licensing structure.
2. Palo Alto Networks. (2021). PAN-OS Administrator's Guide, Version 10.1.
Section: "DNS Security" "DNS Security Concepts": "To use DNS Security, you must purchase and install a DNS Security license. The DNS Security license is included with the Threat Prevention (TP) license." (Directly supports option B).
Section: "DNS Security" "DNS Security Analytics": "The DNS Security service uses machine learning and predictive analytics to provide real-time DNS request analysis..." (Supports option C).
3. Palo Alto Networks. (2023). PCNSA Study Guide.
Domain 2: "Deploy and Configure Security Components" Objective 2.2: This section details the security subscriptions, clarifying that DNS Security is bundled with the Threat Prevention license and is distinct from the URL Filtering license. It also describes the service's use of ML, predictive analytics, and detection of DGA and DNS tunneling. (Supports A, B, C and refutes D).

Question: 23

What are the requirements for using Palo Alto Networks EDL Hosting Sen/ice?

A. any supported Palo Alto Networks firewall or Prisma Access firewall

B. an additional subscription free of charge

C. a firewall device running with a minimum version of PAN-OS 10.1

D. an additional paid subscription

Answer:

A

Explanation:

The Palo Alto Networks External Dynamic List (EDL) Hosting Service is a cloud-based solution that allows customers to maintain and host their own custom EDLs. According to official documentation, this service is available for use on all supported Palo Alto Networks next-generation firewalls and Prisma Access instances. While a minimum PAN-OS version is required and the service is free with a support contract, option A provides the most accurate and comprehensive description of the platforms on which the service can be deployed, which is a primary requirement.

Why Incorrect Options are Wrong:

B. an additional subscription free of charge: The service is not an "additional subscription." It is a feature available to all customers who have a valid, standard support account.
C. a firewall device running with a minimum version of PAN-OS 10.1: This statement is factually correct but incomplete. It omits Prisma Access, which is also a supported platform for the EDL Hosting Service.
D. an additional paid subscription: This is incorrect. The EDL Hosting Service is provided free of charge to customers with a valid support account.

References:

1. Palo Alto Networks. (2023). PAN-OS Administrator's Guide Version 11.0. "Objects External Dynamic Lists External Dynamic List Hosting Service". The guide states, "The EDL Hosting Service is available for all supported Palo Alto Networks firewalls and Prisma Access." It also clarifies, "The EDL Hosting Service is available free of charge to all Palo Alto Networks customers with a valid support account."
2. Palo Alto Networks. (2021). PAN-OS New Features Guide Version 10.1. "Policy External Dynamic List Hosting Service". This document confirms the feature's introduction: "The External Dynamic List (EDL) Hosting service is a new cloud-based solution...This feature is introduced in PAN-OS 10.1." This supports the fact that option C is a valid but incomplete requirement.

Question: 24

An administrator would like to block access to a web server, while also preserving resources and minimizing half-open sockets. What are two security policy actions the administrator can select? (Choose two.)

A. Reset server

B. Reset both

C. Drop

D. Deny

Answer:

A, C

Explanation:

The administrator's goals are to block traffic to a web server while preserving resources and minimizing half-open sockets, particularly on the server being protected.
1. Drop (C): This action silently discards incoming packets without sending any notification. When the firewall drops the initial SYN packet from a client, the server never receives it. Consequently, the server does not allocate any resources or create a half-open socket. This effectively blocks access and preserves server resources, making it a highly efficient method from both the firewall's and the server's perspective.

2. Reset server (A): This action actively sends a TCP RST (reset) packet to the server. This explicitly instructs the server to terminate the connection and tear down any associated state, including a half-open socket. This directly achieves the goal of minimizing half-open sockets and preserving resources on the server.
Both actions effectively protect the server's resources from being consumed by unwanted connection attempts.

Why Incorrect Options are Wrong:

B. Reset both: While this action also preserves server resources, it sends a reset to the client as well. This notifies the source that a firewall is present, which is often undesirable from a security standpoint as it aids in network reconnaissance.
D. Deny: In the context of a configurable Security policy rule action, Deny and Drop are functionally identical; both silently discard the packet. However, Drop is the specific action name listed in the policy configuration, making it the more precise term.

References:

1. Palo Alto Networks PAN-OS Administrator's Guide 10.2, "Security Policy Actions".
Page/Section: In the chapter on Security Policies, the section "Security Policy Actions" describes the different termination actions.
Quote/Content for 'Drop': "Silently drops the traffic; does not send a response to the host or server. Use a drop action to thwart network scanning attempts because it provides no indication of a live port." This supports Drop as a method to preserve resources by preventing engagement.
Quote/Content for 'Reset server': "Sends a TCP reset to the server-side of the connection. This option is useful for applications that do not gracefully handle a client-side reset." This confirms it is a distinct action focused on clearing the server's state.
2. Palo Alto Networks PAN-OS Administrator's Guide 9.1, "Take Action on a Security Policy Rule".
Page/Section: In the chapter "Create and Manage Security Policy Rules", the section on actions details the behavior of each option.
Content: The guide explains that a drop action prevents the session from being established, thereby conserving server resources. It also describes the reset-server action as a method to terminate the session specifically on the server side, which directly addresses the goal of clearing server-side sockets.

Question: 25

An administrator would like to apply a more restrictive Security profile to traffic for file sharing applications. The administrator does not want to update the Security policy or object when new applications are released. Which object should the administrator use as a match condition in the Security policy?

A. the Content Delivery Networks URL category

B. the Online Storage and Backup URL category

C. an application group containing all of the file-sharing App-IDs reported in the traffic logs

D. an application filter for applications whose subcategory is file-sharing

Answer:

D

Explanation:

An application filter is a dynamic object that groups applications based on their defined attributes, such as category, subcategory, technology, or risk factor. By creating a filter for the 'file-sharing' subcategory, the Security policy will automatically include any new applications that Palo Alto Networks classifies under this subcategory in future content updates. This approach ensures the policy remains current without requiring the administrator to manually update the policy or a static object group each time a new file-sharing application is identified, directly fulfilling the core requirement of the question.

Why Incorrect Options are Wrong:

A. A URL category matches traffic based on the website's URL, not the specific application (App-ID) being used for file sharing.
B. This is also a URL category. It is not a dynamic application-based object and would not automatically incorporate new file-sharing App-IDs.
C. An application group is a static list of specific applications. It would require manual updates to add new file-sharing App-IDs.

References:

1. Palo Alto Networks. (2021). PAN-OS Administrator's Guide 10.2. "Objects Application Objects Create an Application Filter". The guide states, "An application filter dynamically groups applications based on application attributes... When a content update includes a new application that matches the attributes you defined for the filter, the new application is automatically added to the filter."
2. Palo Alto Networks. (2023). PCNSA Study Guide. "Chapter 4: Securing Traffic with Security Policies". This guide contrasts static application groups with dynamic application filters, explaining

that filters are the appropriate tool when the goal is to create a policy that automatically adapts to new applications matching specific criteria, such as a subcategory.
3. Palo Alto Networks TechDocs. "Application Filter". This document explicitly details the dynamic nature of application filters: "Because an application filter is a dynamic object, you don't have to update it when a content release includes new applications that match the filter criteria."

Question: 26

A network administrator is required to use a dynamic routing protocol for network connectivity. Which three dynamic routing protocols are supported by the NGFW Virtual Router for this purpose? (Choose three.)

A. RIP

B. OSPF

C. IS-IS

D. EIGRP

E. BGP

Answer:

A, B, E

Explanation:

The Palo Alto Networks Next-Generation Firewall (NGFW) virtual router supports three primary dynamic routing protocols to facilitate automated route discovery and network topology updates. These protocols are the Routing Information Protocol (RIP), specifically RIPv1 and RIPv2; Open Shortest Path First (OSPF), including OSPFv2 and OSPFv3; and the Border Gateway Protocol (BGP), specifically BGPv4. These protocols enable the firewall to integrate seamlessly into diverse and complex network environments by dynamically learning and advertising routes, ensuring efficient and resilient traffic forwarding.

Why Incorrect Options are Wrong:

C. IS-IS: Intermediate System to Intermediate System (IS-IS) is a standardized routing protocol, but it is not supported by the PAN-OS virtual router.
D. EIGRP: Enhanced Interior Gateway Routing Protocol (EIGRP) is a Cisco-proprietary protocol and is therefore not supported on Palo Alto Networks firewalls.

References:

1. Palo Alto Networks. (2021). PAN-OS Administrator's Guide 10.2. In the "Networking Virtual Routers Dynamic Routing Protocols" section, the document explicitly states, "The firewall supports the following dynamic routing protocols: BGP, OSPFv2, OSPFv3, RIPv1, and RIPv2."
2. Palo Alto Networks. (2021). Palo Alto Networks Certified Network Security Administrator (PCNSA) Study Guide 10.1. In "Module 3: Simplifying the Network with Routing Virtual Routers," the guide lists the supported dynamic routing protocols as BGP, OSPF, and RIP.

Question: 27

Given the detailed log information above, what was the result of the firewall traffic inspection?

A. It was blocked by the Vulnerability Protection profile action.

B. It was blocked by the Anti-Virus Security profile action.

C. It was blocked by the Anti-Spyware Profile action.

D. It was blocked by the Security policy action.

Answer:

C

Explanation:

The provided image is a Threat log entry from a Palo Alto Networks firewall. The "Type" column explicitly identifies the threat as spyware. The "Threat/Content Name" (Generic.TCP.C2) and "Category" (command-and-control) are consistent with signatures used by the Anti-Spyware profile to detect malicious C2 traffic. The "Action" column shows block-ip, which is the enforcement action taken by the profile. Therefore, the traffic was inspected and subsequently

blocked by the Anti-Spyware Security profile.

Why Incorrect Options are Wrong:

A. It was blocked by the Vulnerability Protection profile action.
This is incorrect because the log "Type" is spyware. A block by a Vulnerability Protection profile would result in a log entry with the "Type" of vulnerability.
B. It was blocked by the Anti-Virus Security profile action.
This is incorrect because the log "Type" is spyware. A block by an Anti-Virus profile would result in a log entry with the "Type" of virus.
D. It was blocked by the Security policy action.
This is incorrect. The Security policy rule "Outbound-Traffic" permitted the session, which then triggered inspection by the attached Security Profiles. The block action was a result of the profile's threat detection, not the policy rule's primary action.

References:

1. Palo Alto Networks. (2021). PAN-OS Administrator's Guide 10.2.
Section: Monitor Logs Threat Log Fields.
Content: This section defines the fields in the Threat log. The "Type" field is described as the "Subtype of the threat log," with possible values including spyware, vulnerability, and virus, directly corresponding to the Security Profile that generated the log. This confirms that a spyware type log is generated by the Anti-Spyware profile.
2. Palo Alto Networks. (2023). Palo Alto Networks Certified Network Security Administrator (PCNSA) Study Guide.
Section: Chapter 5, "Decryption and Threat Prevention," sub-section "Anti-Spyware."
Content: The guide explains that the Anti-Spyware profile protects against malicious spyware and command-and-control (C2) traffic. It states that when the firewall detects a threat matching a signature in the profile, it takes the configured action (e.g., block) and generates a Threat log entry of the spyware type.
3. Palo Alto Networks. (2021). Firewall 10.2 Essentials: Configuration and Management (EDU-210) Student Guide.
Section: Module 8, "Denying Threats Using Security Profiles."
Content: This courseware details how Security Profiles are attached to Security policy rules to inspect allowed traffic. It clarifies that a Threat log is generated when a signature is matched within a profile (such as Anti-Spyware), and the action in the log reflects the profile's configuration, not the parent Security policy rule's action.

Question: 28

Which three interface deployment methods can be used to block traffic flowing through the Palo Alto Networks firewall? (Choose three.)

A. Layer 2

B. Virtual Wire

C. Tap

D. Layer 3

E. HA

Answer:

A, B, D

Explanation:

Palo Alto Networks firewalls can be deployed in-line to actively inspect and control traffic. The three interface deployment methods that facilitate this are Layer 2, Layer 3, and Virtual Wire. In each of these modes, the firewall is positioned directly in the path of network traffic. This in-line placement is a prerequisite for enforcing Security policies, which include rules to block malicious or unwanted traffic. Layer 3 interfaces route traffic, Layer 2 interfaces switch traffic, and Virtual Wire interfaces transparently pass traffic between a pair of ports, but all three can apply security policies to the traffic they handle.

Why Incorrect Options are Wrong:

C. Tap: A Tap interface operates in a passive, listen-only mode. It receives a copy of traffic from a switch's SPAN port and cannot be used to block or modify the live traffic stream.
E. HA: High Availability (HA) is a feature for firewall redundancy, not an interface deployment method for inspecting transit traffic. Dedicated HA interfaces are used for synchronization and state-sharing between firewalls.

References:

1. Palo Alto Networks PAN-OS Administrator's Guide 10.2
Virtual Wire: "A virtual wire deployment simplifies installation because you can insert the firewall into an existing topology... You can apply Security, DoS Protection, and QoS policies on the virtual wire to control traffic and protect your network." (Reference: Chapter: Plan Your Network Deployment Firewall Interface Deployment Methods Virtual Wire Deployment)
Layer 2: "In a Layer 2 deployment, the firewall is installed transparently on a network segment... You can enable traffic inspection by configuring Security, DoS Protection, and QoS policies..." (Reference: Chapter: Plan Your Network Deployment Firewall Interface Deployment Methods

Layer 2 Deployment)
Layer 3: "In a Layer 3 deployment, the firewall routes traffic between multiple ports... The firewall protects the network by inspecting all traffic that it routes and applying Security, DoS Protection, and QoS policies." (Reference: Chapter: Plan Your Network Deployment Firewall Interface Deployment Methods Layer 3 Deployment)
Tap: "In tap mode, the firewall monitors traffic flowing across a network... Because the firewall is not in-line with traffic, a tap deployment is for monitoring only; you cannot use it to control traffic." (Reference: Chapter: Plan Your Network Deployment Firewall Interface Deployment Methods Tap Deployment)

Question: 29

An administrator configured a Security policy rule where the matching condition includes a single application and the action is set to deny. What deny action will the firewall perform?

A. Drop the traffic silently

B. Perform the default deny action as defined in the App-ID database for the application

C. Send a TCP reset packet to the client- and server-side devices

D. Discard the session's packets and send a TCP reset packet to let the client know the session has
been terminated

Answer:

D

Explanation:

In a Palo Alto Networks firewall, the "deny" action in a Security policy rule is an alias for the "reset-client" action. When a session matches a rule with this action, the firewall discards the packet and sends a response to the initiating host (the client) to gracefully terminate the connection. For TCP traffic, this response is a TCP reset (RST) packet. For UDP traffic, it is an ICMP "port unreachable" message. This behavior informs the client application that the session has been terminated, preventing it from waiting for a response that will never arrive.

Why Incorrect Options are Wrong:

A. This describes the "drop" action, which silently discards packets without sending any notification to the client or server.
B. The App-ID database is used for application identification, not for defining default deny actions within a specific Security policy rule.
C. This describes the "reset-both" action, which sends a TCP reset packet to both the client and the server, not just the client.

References:

1. Palo Alto Networks. (2021). PAN-OS Administrator's Guide 10.1. "Objects Security Policy Actions". In this section, the guide specifies the behavior for the "Deny" action: "For TCP, the firewall sends a TCP reset to the client-side of the connection... The Deny action is a 'graceful' close to the session because a notification is sent to the client."
2. Palo Alto Networks. (2020). Palo Alto Networks Certified Network Security Administrator (PCNSA) Study Guide. Module 4: "Securing Traffic with Security Policies". The guide states, "Deny: For TCP traffic, this action sends a TCP reset to the client. For UDP traffic, it sends an ICMP Port Unreachable message to the client." This confirms that "deny" is a client-side

notification action.

Question: 30

Which object would an administrator create to enable access to all applications in the office-programs subcategory?

A. HIP profile

B. Application group

C. URL category

D. Application filter

Answer:

D

Explanation:

An Application Filter is a dynamic object used to group applications based on their attributes, such as Category, Subcategory, Technology, Risk, and Characteristic. To enable access to all applications in the "office-programs" subcategory, an administrator would create an Application Filter that specifies this subcategory. The firewall will automatically include all current and future applications that Palo Alto Networks classifies under this subcategory, ensuring the policy remains up-to-date without manual intervention.

Why Incorrect Options are Wrong:

A. HIP profile: A Host Information Profile (HIP) is used to assess the security posture of an endpoint, not to group or control applications based on their function or category.
B. Application group: An Application Group is a static list of manually selected applications. While it could be used, it is not dynamic and would require manual updates if new office-program applications are added.
C. URL category: A URL Category is used for web filtering to control access to websites based on their URLs. It does not group applications identified by App-ID.

References:

1. Palo Alto Networks, PAN-OS Administrator's Guide 10.2, "Objects Application Filters": "Create an Application Filter to dynamically group applications based on application attributes that you define: Category, Subcategory, Technology, Risk, and Characteristic. The firewall dynamically populates an application filter with applications that match the attributes you define. When Palo Alto Networks adds new applications with attributes that match your filter, the firewall automatically adds the new applications to your filter and to any policy that uses the filter." (This directly supports the use of Application Filters for subcategories).
2. Palo Alto Networks, PAN-OS Administrator's Guide 10.2, "Objects Application Groups": "An

application group is a static list of applications that you can use in policies." (This confirms Application Groups are static, making them less suitable than dynamic filters).
3. Palo Alto Networks, PAN-OS Administrator's Guide 10.2, "Objects Security Profiles URL Filtering": "URL Filtering enables you to safely enable web access and control the sites users can access." (This clarifies that URL categories are for web access, not application control).
4. Palo Alto Networks, PAN-OS Administrator's Guide 10.2, "GlobalProtect Host Information": "A Host Information Profile (HIP) is a report of the security status of an end-user's computer... You can use this information in a HIP object and then attach the object to a security policy to enforce access privileges based on the security of the endpoint." (This confirms HIP profiles are for endpoint posture assessment).

Question: 31

What do you configure if you want to set up a group of objects based on their ports alone?

A. Application groups

B. Service groups

C. Address groups

D. Custom objects

Answer:

B

Explanation:

In Palo Alto Networks' PAN-OS, a "Service" object is used to define a protocol (TCP or UDP) and its associated port number or range. To group multiple such port-based definitions together for simplified management and application in security policies, you configure a "Service Group." This allows you to reference a single group object in a policy rule instead of listing each individual service, streamlining the rulebase.

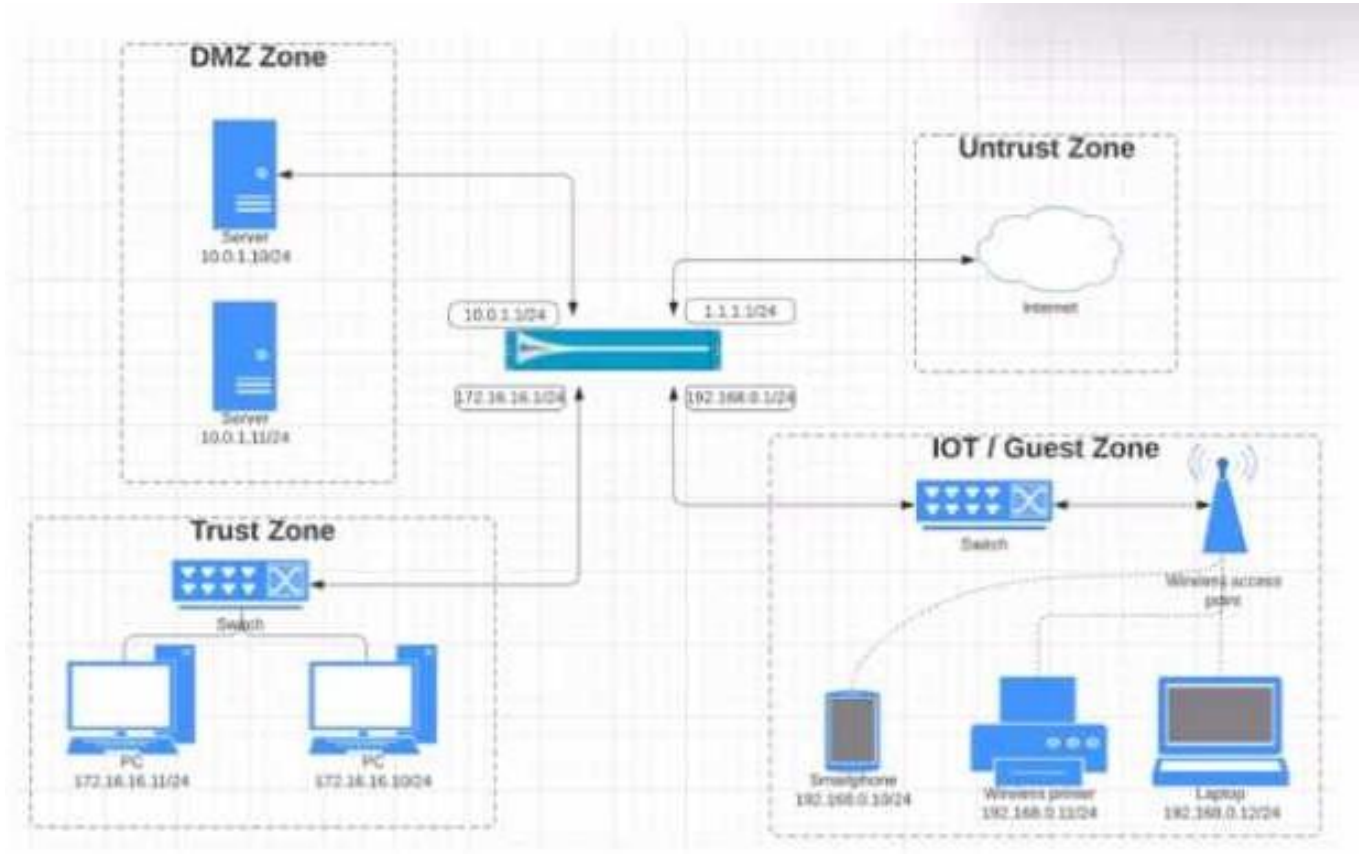
Why Incorrect Options are Wrong:

A. Application groups: These are collections of applications identified by App-ID, not just port numbers. They provide a more granular, Layer 7 classification.
C. Address groups: These are used to group IP addresses, subnets, or FQDNs, which relate to the source or destination of traffic, not the port.
D. Custom objects: This is too general. While you create custom service objects, the specific container for grouping them is a "Service Group."

References:

1. Palo Alto Networks. (2021). PAN-OS Administrator's Guide, Release 10.1.
Section: Objects Services
Content: "A service is a combination of a protocol and port that you can use in policies and other firewall functions... A service group is a collection of services that you can use to simplify rule creation and management." This directly states that services (port-based objects) are collected in service groups.
2. Palo Alto Networks. (2021). PCNSA Study Guide.
Section: Module 3: Security and NAT Policies
Content: The guide explains the components of a security policy rule, explicitly defining the "Service" column as representing TCP/UDP ports. It further details that "Service Groups" are used to combine multiple service objects into a single entity for use in these rules.

Question: 32



View the diagram. What is the most restrictive, yet fully functional rule, to allow general Internet and SSH traffic into both the DMZ and Untrust/Internet zones from each of the IOT/Guest and Trust Zones? A)

			Source				Destination				
NAME	TAGS	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE
02-A	none	universal	IOT-Guest Trust	172.16.18.0/24 192.168.0.0/24	any	any	DMZ Untrust	any	any	ssh ssl web-browsing	application-default

B)

			Source				Destination				
NAME	TAGS	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE
03-A	none	universal	IOT-Guest Trust	172.16.16.0/24 192.168.0.0/24	any	any	DMZ Untrust	1.1.1.0/24 10.0.1.0/24	any	ssh ssl web-browsing	application-default

C)

			Source				Destination				
NAME	TAGS	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE
01-A	none	universal	IOT-Guest Trust	10.0.1.0/24 172.16.16.0/12	any	any	DMZ Untrust	1.1.1.0/24 192.168.0.0/24	any	ssh ssl web-browsing	application-default

D)

A. Option A

B. Option B

C. Option C

D. Option D

Answer:

C

Explanation:

The objective is to create the most restrictive, yet fully functional, Security policy rule. The rule must allow traffic from the Trust and IOT/Guest zones to the Untrust and DMZ zones. The permitted traffic types are "general Internet" and "SSH".
Option C correctly configures:
Source Zones: Trust, IOT/Guest
Destination Zones: Untrust, DMZ

Applications: web-browsing and ssh
The web-browsing application-default group includes common web protocols (HTTP, HTTPS/SSL), satisfying the "general Internet" requirement. Including ssh covers the second requirement. This configuration is specific and avoids overly permissive settings, adhering to the principle of least privilege.

Why Incorrect Options are Wrong:

A: This option is not restrictive because using any for the application allows all traffic, not just the specified web and SSH traffic.
B: This option is redundant. The web-browsing application-default group already includes the ssl application, so adding it separately is unnecessary.
D: This option is insecurely permissive. Using any for both source and destination zones allows traffic between all zones, violating the specific requirements.

References:

1. Palo Alto Networks, "PAN-OS Administrator's Guide 10.2": In the "Security Policy" chapter, the section "Security Policy Rule Components" details the need to specify source zones, destination zones, and applications to control traffic. This supports the structure of the correct rule in Option C.

2. Palo Alto Networks, "PCNSA Study Guide": Chapter 4, "Securing Traffic with Security Policies," emphasizes the best practice of creating specific rules. It states, "A best practice is to be as specific as possible when you define the applications that you want to allow or deny in a policy rule." This principle invalidates options A and D, which use any.
3. Palo Alto Networks, "PAN-OS Administrator's Guide 10.2": In the "Objects" chapter, the section "Applications and Application Groups" explains that predefined application groups like web-browsing simplify rule creation. The web-browsing group inherently includes the ssl application, which makes its explicit inclusion in Option B redundant.

Question: 33

A website is unexpectedly allowed due to miscategorization. What are two ways to resolve this issue for a proper response? (Choose two.)

A. Identify the URL category being assigned to the website.
Edit the active URL Filtering profile and update that category's site access settings to block.

B. Create a URL category and assign the affected URL.
Update the active URL Filtering profile site access setting for the custom URL category to block.

C. Review the categorization of the website on https://urlfiltering.paloaltonetworks.com.
Submit for "request change*, identifying the appropriate categorization, and wait for confirmation before testing again.

D. Create a URL category and assign the affected URL.
Add a Security policy with a URL category qualifier of the custom URL category below the original policy. Set the policy action to Deny.

Answer:

B, C

Explanation:

There are two primary methods to address a miscategorized URL that is being incorrectly allowed. The first is an immediate, local fix, and the second is a long-term, global fix.
Option B provides the immediate local fix. By creating a custom URL category containing the specific website and setting the action for this category to "block" in the active URL Filtering profile, you override the incorrect PAN-DB categorization. This ensures the specific URL is blocked immediately without affecting other sites in the same miscategorized PAN-DB category.
Option C describes the long-term, correct solution. Submitting a request to Palo Alto Networks to change the URL's category corrects the master PAN-DB database. Once updated, all firewalls using the service will apply the correct policy, resolving the root cause of the issue.

Why Incorrect Options are Wrong:

A. Blocking the entire category assigned to the website would result in blocking all other, correctly categorized websites within that same category, leading to excessive and unintended traffic denial.
D. Security policies are evaluated top-down. Placing a new "Deny" policy below the original "Allow" policy that is permitting the traffic would be ineffective, as the traffic would match the first "Allow" rule and policy evaluation would stop.

References:

1. Palo Alto Networks PAN-OS Administrator's Guide 10.2: "URL Filtering" section, under "Configure URL Filtering". This section details how to create a URL Filtering profile and set actions for different categories, including custom categories. This supports the method described in option B.
2. Palo Alto Networks PAN-OS Administrator's Guide 10.2: "Create a Custom URL Category" section. This guide explains: "For more granular control, you can create custom URL categories... and use them in a URL Filtering profile... to define policy for a specific set of URLs." This directly supports the first step in option B.
3. Palo Alto Networks Live Community, "How to Request a URL Category Change": This official resource outlines the process: "Go to https://urlfiltering.paloaltonetworks.com/. Enter the URL... If you do not agree with the categorization, click on 'Request Change'." This directly validates the procedure in option C.
4. Palo Alto Networks PAN-OS Administrator's Guide 10.2: "Security Policy Rule Evaluation" section. The documentation states, "The firewall evaluates policy rules in order (from top to bottom) and the first rule that matches the traffic is applied." This principle confirms that the rule placement described in option D is incorrect.

Question: 34

Why should a company have a File Blocking profile that is attached to a Security policy?

A. To block uploading and downloading of specific types of files

B. To detonate files in a sandbox environment

C. To analyze file types

D. To block uploading and downloading of any type of files

Answer:

A

Explanation:

A File Blocking profile is a security feature that allows administrators to identify and control the flow of specific file types through the firewall. When attached to a Security policy rule, it can be configured to block, alert on, or allow the uploading and/or downloading of files based on their type (e.g., executables, PDFs, multimedia files). This is a critical function for preventing malware from entering the network (e.g., blocking .exe files from web-browsing) and stopping sensitive data from leaving the network.

Why Incorrect Options are Wrong:

B. To detonate files in a sandbox environment: This describes the function of the WildFire analysis profile, which forwards unknown files for sandboxing, not the primary role of a File Blocking profile.
C. To analyze file types: While the firewall does analyze files to determine their type, this is the mechanism, not the ultimate purpose. The purpose is to enforce a policy (block/allow) based on that analysis.
D. To block uploading and downloading of any type of files: This is too broad. The key value of a File Blocking profile is its granularity in controlling specific file types, not blocking all files indiscriminately.

References:

1. Palo Alto Networks. (2023). PAN-OS Administrator's Guide 10.2. "File Blocking Profiles". In the overview, the document states, "You can block files from being uploaded or downloaded based on the application, file type, and direction (upload or download). For example, you can prevent users from downloading executable files from a high-risk application, and prevent users from uploading specific file types to a file-sharing application."
2. Palo Alto Networks. (2021). Palo Alto Networks Certified Network Security Administrator (PCNSA) Study Guide. Chapter 6, "Securing Traffic with Security Profiles," Section: "File-Blocking Profiles". The guide explains, "File-Blocking profiles block or allow files from being transferred

based on their file type, the application that is transferring them, and the direction of the transfer (upload or download)."

3. Palo Alto Networks. (2020). Firewall 10.0 Essentials: Configuration and Management (EDU-210). Module 6, "Securing Traffic with Security Profiles". The courseware details that File Blocking profiles are used to "control file transfers by type and application" and that the primary actions are "alert, block, and continue."

Question: 35

An administrator is troubleshooting traffic that should match the interzone-default rule. However, the administrator doesn't see this traffic in the traffic logs on the firewall. The interzone-default was never changed from its default configuration. Why doesn't the administrator see the traffic?

A. Logging on the interzone-default policy is disabled.

B. Traffic is being denied on the interzone-default policy.

C. The Log Forwarding profile is not configured on the policy.

D. The interzone-default policy is disabled by default.

Answer:

A

Explanation:

By default, PAN-OS includes two predefined security policy rules: intrazone-default and interzone-default. The interzone-default rule applies to all traffic between different security zones and has a default action of deny. Crucially, logging for this default rule is disabled by default to prevent the firewall's log database from being overwhelmed by entries for implicitly denied traffic. For an administrator to see traffic that is being denied by this rule, they must first override the default rule and explicitly enable the "Log at Session End" option. Since the rule was never changed from its default configuration, logging remains disabled, which is why no log entries are visible.

Why Incorrect Options are Wrong:

B. Traffic is being denied on the interzone-default policy.
While the default action is deny, this does not explain the absence of logs. If logging were enabled, denied traffic would still generate a log entry.
C. The Log Forwarding profile is not configured on the policy.
A Log Forwarding profile sends logs to external systems (e.g., Panorama, Syslog). Its absence does not prevent logs from being written to the firewall's local Traffic log.
D. The interzone-default policy is disabled by default.
This rule is enabled by default. It is the final rule in the policy evaluation and enforces the default-deny security posture for traffic between zones.

References:

1. Palo Alto Networks PAN-OS Administrator's Guide 10.2: In the section "Security Policy," under the subsection "Default Security Rules," the documentation states: "By default, logging is not enabled for the default rules. To enable logging for traffic that matches a default rule, you must override it and select the Log at Session End check box." This directly supports the correct

answer.

2. Palo Alto Networks PAN-OS Administrator's Guide 10.2: The same section, "Default Security Rules," also clarifies the rule's action and state: "interzone-default - Controls traffic between zones of different types (for example, from the trust zone to the untrust zone). The default action is deny." This confirms the rule is active and its action is deny, making options B and D incorrect.