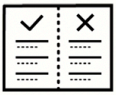
CREATING AND MANAGING SECURITY POLICY RULES



GET TRAFFIC FLOWING

- Security policy fundamental concepts
- Security policy administration

EDU-210 Version A
PAN-OS® 10.2

paloalto NETWORKS

Learning Objectives

After you complete this module,
you should be able to:

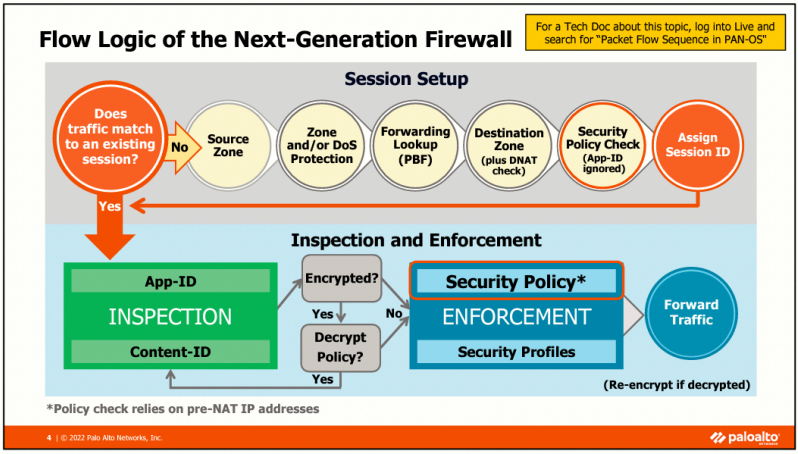
- Describe Security policy concepts and operation
- Configure a Security policy rule
- Manage a Security policy
- Create and use tags and custom services in a Security policy

This module covers the topics listed here. Read through the list before proceeding.

After you complete this module, you should be able to:

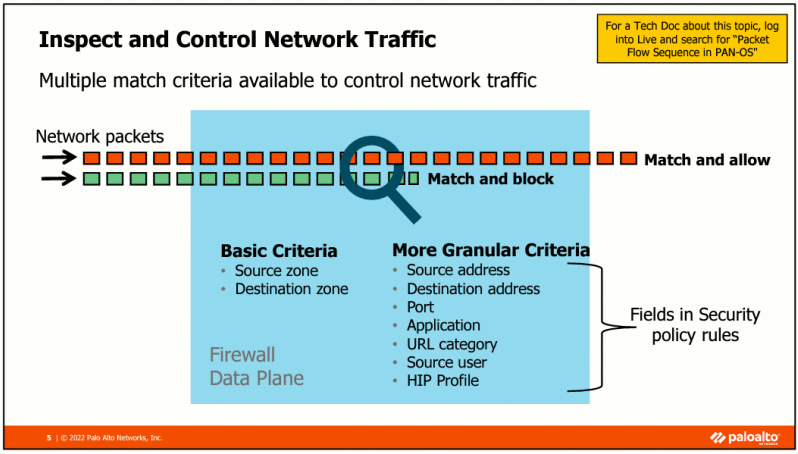
- Describe Security policy concepts and operation
- Configure a Security policy rule
- Manage a Security policy
- Create and use tags and custom services in a Security policy

This section introduces some fundamental concepts and terminology necessary to understand the operation of a Security policy.



This diagram is a simplified version of the flow logic of a packet traveling through a Palo Alto Networks firewall. The course will reference this diagram to address where specific concepts fit into the packet processing sequence.

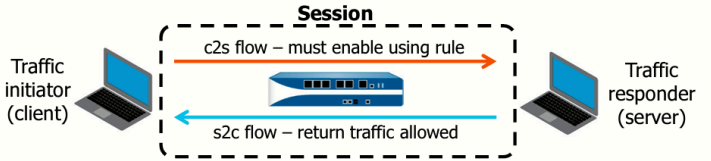
For more information about the packet handling sequence inside a PAN-OS® device, log into Live and search for "Packet Flow Sequence" or see the Packet Flow Sequence in the PAN-OS document available on the Palo Alto Networks Support website at https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClVHCA0.



Security policies protect network assets from threats and disruptions. Individual Security policy rules determine whether to block or allow a session based on traffic attributes, such as the source and destination security zone, the source and destination IP address, the application, the user, and the service. All traffic traversing the data plane of the Palo Alto Networks firewall is matched against a Security policy. This traffic matching does not include traffic originating from the management interface of the firewall because, by default, this traffic does not pass through the data plane of the firewall.

Sessions and Flows

For a Tech Doc about this topic, log into Live and search for "Palo Alto Networks Firewall Session Overview"



- A packet is matched to a session; each session is matched to a Security policy rule.
- A session can consist of one or two flows:
  - Single flow example: multicast traffic
  - Two flow example: TCP traffic
- Server definition for a firewall is different from server definition for hosts:
  - Traffic responder versus providing a service

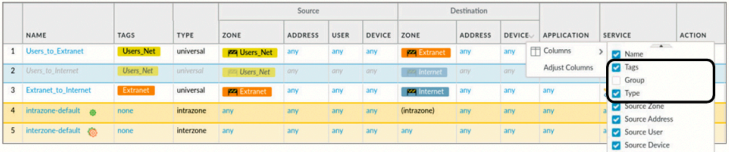
All traffic passing through the firewall is matched against a session, and each session is matched against a Security policy rule. Each session is assigned a unique session ID number. When a session match occurs, the firewall applies the matching Security policy rule to bidirectional traffic in that session, client to server (C2S) and server to client (S2C). The endpoint where traffic is initiated always is the client, and the destination endpoint is the server. When you define Security policy rules, consider only the c2s flow direction. Define policy rules that allow or deny traffic from the source zone to the destination zone in the c2s direction. The return s2c flow does not require a separate rule because the return traffic is automatically allowed.

The default rules apply for traffic that does not match any custom-defined rules. The default rules, displayed at the bottom of the security rule base, are predefined to allow all intrazone traffic (within a zone) and deny all interzone traffic (between zones). Although these rules are part of the predefined configuration and are read-only by default, you can override them and change a limited number of settings, including the tags, action (allow or block), log settings, and security profiles.

Display Security Policy Rules

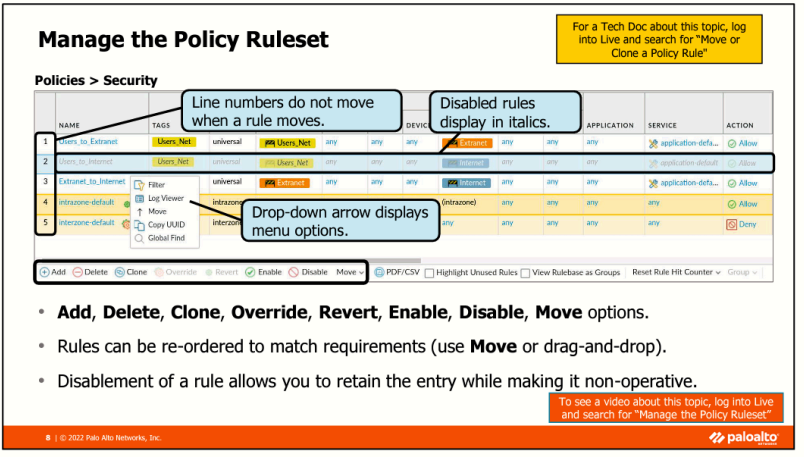
For a Tech Doc about this topic, log into Live and search for "Components of a Security Policy Rule"

Policies > Security



- Display and manage Security policy rules using the web interface.
- Click any column header to change the number of displayed columns:
  - Customized per user
- The list order matches the column order displayed in the web interface.

To display your Security policy rules in the web interface, browse **Policies > Security**. Each logged-in administrative user can customize their web interface display. Modify the number of columns displayed by clicking any column header and selecting from the web interface list. The order in the list matches the columns' order shown in the web interface. For example, notice that the **Group** column is deselected in the list and that the corresponding column is missing in the web interface display. The **Group** column would have been displayed between the **Tags** and **Type** columns.



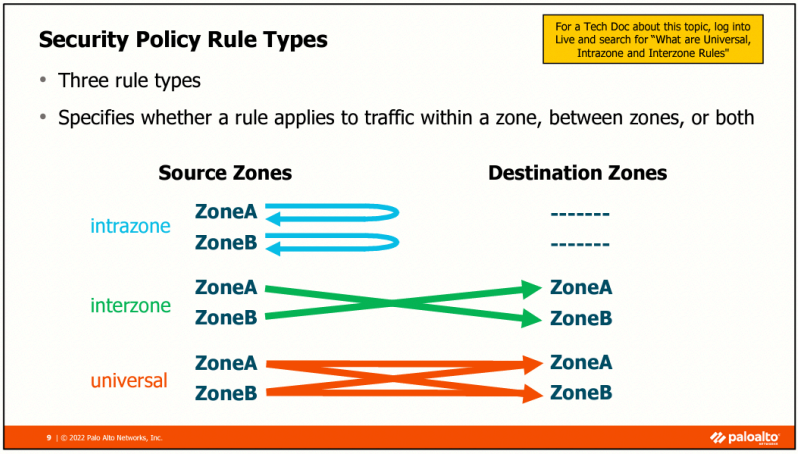
After rules are created, they are listed and numbered. The numbers in the first column are not part of the rules and never move when a rule is moved. The toolbar below the rules helps you manage the rules and enables you to perform actions on your rules.

To add a rule, click **Add**. To delete a rule, select it and click **Delete**. To use an existing rule as a template to create a new rule, select it and click **Clone**.

To modify an implicit intrazone-default or interzone-default rule, select it and click **Override**. To revert it to its original state, click **Revert**.

To disable a rule without removing it, select it and click **Disable**. You can disable a rule to stage it or temporarily make it inactive to troubleshoot a problem. A disabled rule appears in gray italic font.

Remember that the firewall matches traffic to rules from the top down, so arrange the rules properly to yield the desired behavior. The web interface provides multiple methods to reorder rules. First, select the rule that you want to re-order and then click Move to use the Move option. You can then see the options to move the rule up, down, to the top or the bottom. You also can use the mouse pointer to drag and drop a rule to the desired location within your ruleset.



You can define three types of rules in a Security policy. Each rule type specifies whether a rule applies to traffic within a zone, between zones, or both.

An intrazone rule applies to all matching traffic within the specified source zone. You cannot select a destination zone for an intrazone rule. For example, if you set the source zones to ZoneA and ZoneB, the rule would apply to all traffic within ZoneA and all traffic within ZoneB but not to traffic between ZoneA and ZoneB.

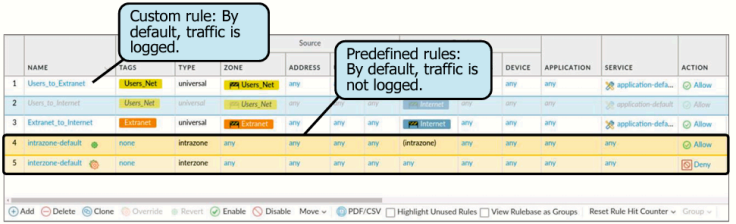
An interzone rule applies to all matching traffic between the specified source and destination zones. For example, if you set the source zones to ZoneA and ZoneB and the destination zones to ZoneA and ZoneB, the rule would apply to traffic from ZoneA to ZoneB and from ZoneB to ZoneA but not to traffic within ZoneA or ZoneB.

A universal rule applies to all matching interzone and intrazone traffic in the specified source and destination zones. For example, if you create a universal role with source zones ZoneA and ZoneB and destination zones ZoneA and ZoneB, the rule would apply to all traffic within ZoneA, all traffic within ZoneB, all traffic from ZoneA to ZoneB, and all traffic from ZoneB to ZoneA.

Custom and Predefined Rules

For a Tech Doc about this topic, log into Live and search for "Create a Security Policy Rule"

- By default, the firewall implicitly allows intrazone traffic and denies interzone traffic.
- Create explicit rules to control all other traffic.

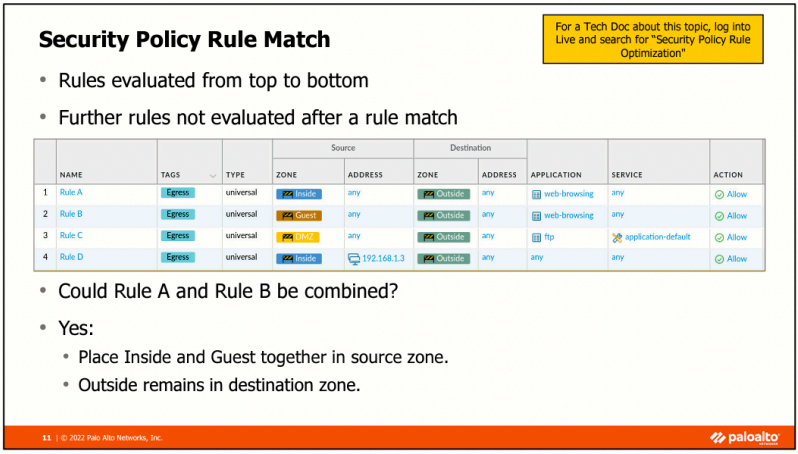


To see a video about this topic, log into Live and search for "Custom and Predefined Rules"

By default, the firewall implicitly allows intrazone traffic (within a zone) and implicitly denies interzone traffic (between zones). These implicit actions are predefined by the mostly read-only intrazone-default and interzone-default rules. By default, the two implicit rules are processed after all the explicit administrator-defined rules on the firewall and match traffic that has not matched any other Security policy rule. The interzone-default rule eliminates the need to create a rule that blocks all traffic not explicitly allowed by a Security policy.

The default firewall behavior is to log all traffic that is matched to an administrator-defined Security policy rule to the Traffic log. By default, traffic allowed or denied by the implicit Security policy rules is not logged on the firewall. However, Palo Alto Networks recommends logging all traffic and changing the default behavior.

Caution: Placement of an explicit "deny all" rule at the end of your administrator-defined policy rules, but before the predefined intrazone-default rule, will result in all intrazone traffic being denied. This explicit "deny all" rule can disrupt normal application traffic flowing within your networks.



Security policy rules are evaluated for a match from top to bottom. After a rule match is found, no other rules are evaluated.

Policy rules are unidirectional, which means that they allow only traffic that is initiated in the direction that the policy rule specifies: source zone(s) to destination zone(s). The replies to the client always are allowed as part of the policy. If traffic is intended to be initiated in both directions, two policy rules are required: one for each direction.

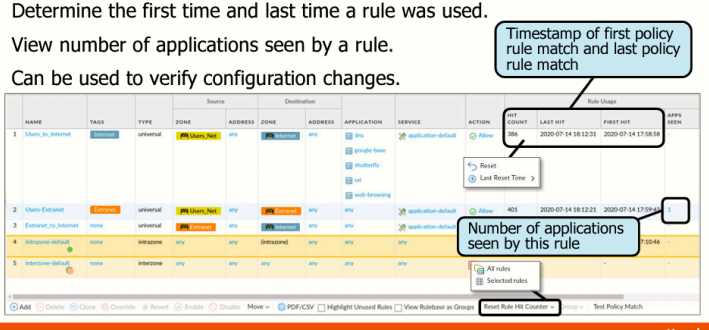
In the configuration shown, when the application web-browsing on TCP port 80 from the Inside zone to the Outside zone passes through the firewall, Rule A matches the traffic because the traffic matches *web-browsing* in the **Application** column and TCP port 80 matches *any* in the **Service** column.

The optimal way of configuring Security policy rules is to minimize the use of *any* in the columns and use specific values when possible. Reduction of the use of the word *any* reduces the number of unnecessary Security policy lookups by the firewall.

Policy Rule Hit Count

For a Tech Doc about this topic, log into Live and search for "View Policy Rule Usage"

- Identify rules that are frequently or seldom used.
- Determine the first time and last time a rule was used.
- View number of applications seen by a rule.
- Can be used to verify configuration changes.



As an administrator, how do you know which Security policy is being used and how often? The policy rule hit count feature enables you to identify rules that are used frequently and to determine which rules are unused and should be removed. The policy rule hit count feature also allows you to validate rule additions or changes and monitor the time frame of when a specific rule was used. The policy rule hit count data will include the number of traffic matches for each rule, the timestamp of the first match, the timestamp of the last match, the number of applications seen, and the number of days with no new applications seen by this rule.

You can reset the rule hit count data to validate an existing rule or gauge rule use within a given timeframe. Policy rule hit count data is not stored on the firewall. After you have cleared the data using the Reset option, the removed data will no longer be available.

The policy rule hit count data also is available through the CLI and the API.

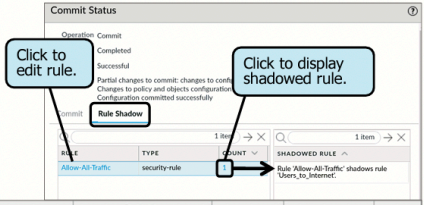
Supplemental Notes

An example of using the policy rule hit count is when you migrate port-based rules to application-based rules. You start by creating an application-based rule and place it in the order above the port-based rule. To verify the configuration of your application-based rule, you reset the policy rule hit count data and monitor the rule hit count to see if any traffic matched the port-based rule. Continue to edit the application-based rule until you can validate that the rule is servicing all traffic. You can safely remove the port-based rule and reduce the firewall attack surface.

Rule Shadowing

For a Tech Doc about this topic, log into Live and search for "What is a Shadow Rule"

- Traffic can match multiple rules.
- Earlier rule hides (casts a shadow) over later rule.
- **Rule Shadow** tab in **Commit Status** window reports shadowed rules.
- Reorder or refine rules to remove shadowing.



	NAME	TAGS	TYPE	Source ZONE	Source ADDRESS	Source USER	Source DEVICE	Destination ZONE	Destination ADDRESS	Destination DEVICE	APPLICATION	SERVICE	ACTION
1	Allow-All-Traffic	Internet	universal	Users_Net	any	any	any	Internet	any	any	any	application-default	Allow
2	Users_to_Internet	Internet	universal	Users_Net	any	any	any	Internet	any	any	dns google-base shutterfly ssl web-browsing	application-default	Allow

13 | © 2022 Palo Alto Networks, Inc.

Because the firewall does a Security policy lookup from top to bottom, Google web traffic would match the "Allow-All-Traffic" rule in the example here before it matched the "Users_to_Internet" rule. The "Allow-All-Traffic" rule is said to "shadow" the Users_Net-Internet rule. Rule shadowing is detected during a commit operation and reported in the **Commit Status** window on the **Rule Shadow** tab.

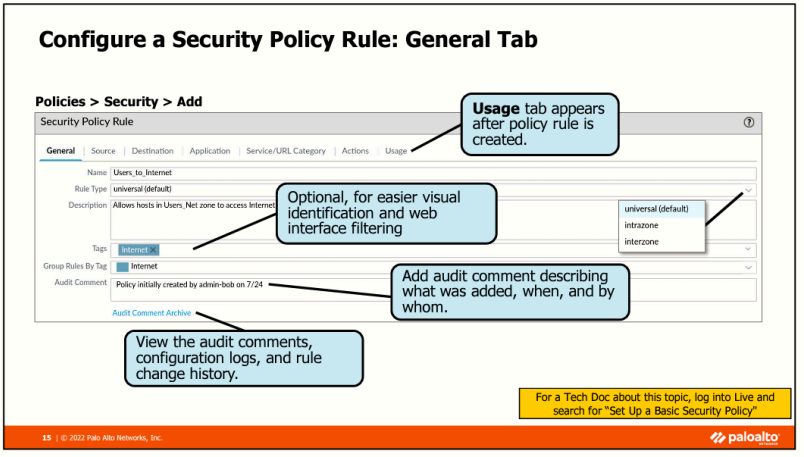
To determine which rule is shadowed by the "Allow-All-Traffic" rule, click the number in the **Count** column to display the shadowed rule in the **Shadowed Rule** pane.

The options for resolving shadowed rules are editing, removing, or re-ordering the rules. In the example, the application list in the "Allow-All-Traffic" rule could be modified to not shadow the application list in the "Users_to_Internet" rule. To edit the "Allow-All-Traffic" rule, you can click **Allow-All-Traffic** on the **Rule Shadow** tab.

You also could remove the "Allow-All-Traffic" rule. A rule that allows any application is dangerous, so either modifying or removing such a rule is a best practice.

You also could re-order the rules. However, re-ordering the rules would not remove rule shadowing in this example. It only would change which rule was shadowed because some applications still would match both rules.

This section describes how to create and manage Security policy rules.



To create a new Security policy rule, browse **Policies > Security** and click **Add**. Initially, the Security Policy Rule window has six tabs that enable you to configure or modify a Security policy rule. A seventh tab (the **Usage** tab) will be displayed after a policy rule is created. Decide which tabs to use and which fields to complete, primarily by the level of granularity that you require in your match conditions.

Click the **General** tab to specify a name to identify a rule. Names are case-sensitive and can be up to 31 characters (letters, numerals, spaces, hyphens, and underscores) in length. The name itself must be unique on the firewall.

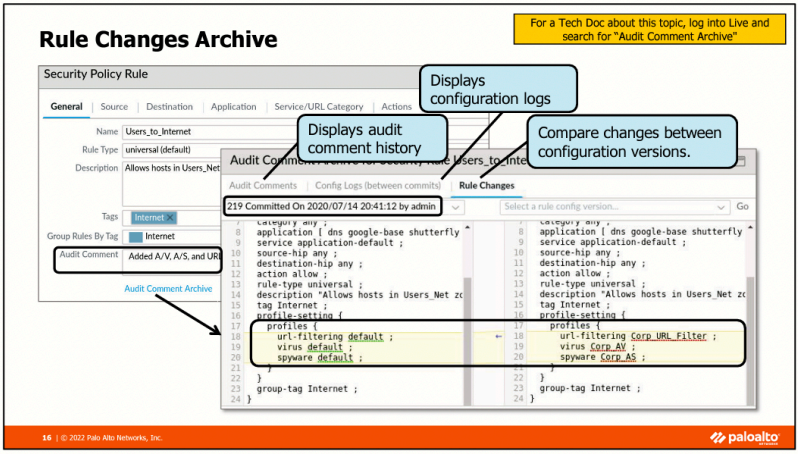
Select the **Rule Type** from the drop-down list. A **universal rule** is the default and most common type. The other choices are **intrazone** and **interzone**.

Enter a **Description** that describes the purpose or operation of the rule (optional).

Create or select a tag (optional). A tag is a keyword or phrase that enables you to visually or programmatically sort or filter policy rules. The ability to filter rules is useful when you have defined many rules and want to view only those tagged with a particular keyword. For example, you might want to tag certain rules with specific words such as Decrypt and No-decrypt. Tags are not unique to policy rules. For example, you can create and apply tags to highlight particular types of addresses, zones, dynamic user groups, or services. Tag creation is described later in this module.

Information in the **Audit Comment** field is added to a Security policy rule to provide a complete audit history. Comments can include why a rule was created or what configuration setting was added to or removed from a policy rule, when the changes were made, and by whom.

The **Audit Comment Archive** link enables the administrator to display the audit comments, configuration logs, and rule change history of the Security policy rule.

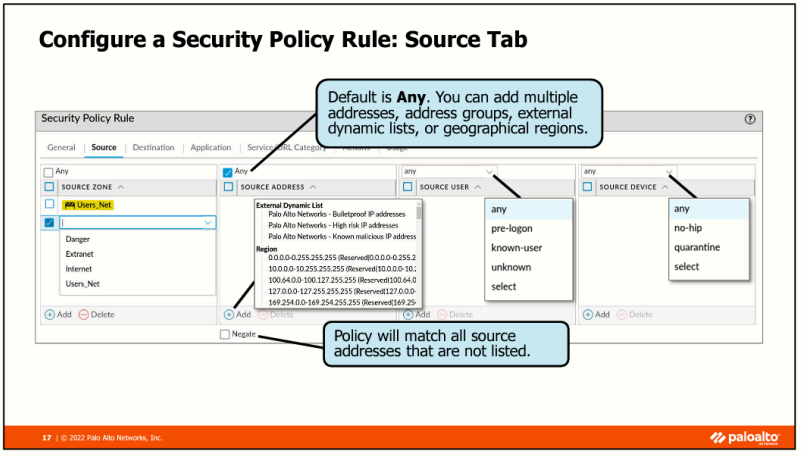


To meet your regulatory compliance requirements, you might need to track all changes that have been made to your Security policy rules. As your rulebase changes, audit information can get lost. Since the release of PAN-OS 9.0, the rule changes archive can track all changes made to your Security policy rules. After clicking the **Audit Comment Archive** link in the properties of a Security policy rule, you can view the audit comment history and configuration log history between commits. You can compare configuration versions to see what has changed in your Security policy.

Click the **Audit Comments** tab to display the audit comment history of the selected rule. The audit comment history includes the time the audit comment was committed, the comment itself, the administrator who added the audit comment, and the configuration version.

Click the **Config Logs (between commits)** tab to display the device configuration logs with traffic matches for the policy rule. Config logs can be filtered to show all changes over a given time frame or by a specific administrator.

Click the **Rule Changes** tab and select the configuration versions to compare the rule configuration changes. The differences will be highlighted.



Click the **Source** tab to add, display, or modify the source zone and source address match criteria for a rule.

The default source zone is **Any**. You can select one or more source zones for a rule. Multiple zones are used to simplify policy management. For example, if you have three different internal source zones that all should have access to the same destination zone, you can create a single rule to cover all these cases.

You can specify one or more source addresses. The default is any address. The source address can be a single address, an address range, an address group, or a geographical region. All these choices are available when you click **Add**.

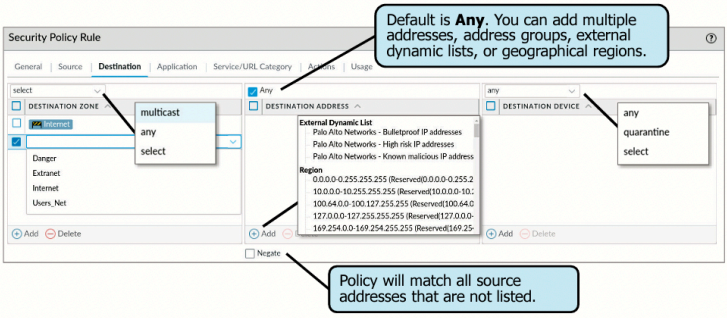
The **Negate** option enables you to specify addresses, address ranges, address groups, or geographical regions that will not match the traffic. For example, consider the scenario where the network address 201.10.10.0/24 has been added to the **Source Address** field. In this scenario, the rule would match all source addresses not in the network 201.10.10.0/24.

The default for the **Source User** value is **any**. However, you can specify one or more source users or user groups as match criteria. These source user types are supported:

- **any**: Any user of any type
- **Pre-logon**: Remote users connected to the network using GlobalProtect but not logged in to their system. When the **pre-logon** option is configured on the GlobalProtect Portal for GlobalProtect clients, any users who are not currently logged in to their system will be identified with the username pre-logon. You can create policy rules for pre-logon users, and although the users are not logged in, their systems are authenticated as if they were fully logged in.
- **known-user**: All authenticated users, which means any IP address with a username mapped to it by User-ID
- **unknown**: All unauthenticated users, which means any IP addresses not mapped to a user by User-ID. For example, you could use **unknown** to match a host where no user has logged in yet, but the host needs network access to perform a Microsoft update.
- **select**: Selected users or groups added using the **Add** link. For example, you might want to add one or more specific users or user groups.

The default for the **Source Device** value is **any**. However, you can specify one or more defined IoT devices as match criteria.

Configure a Security Policy Rule: Destination Tab



Click the **Destination** tab to add, display, or modify the destination zone and destination address match criteria for a rule.

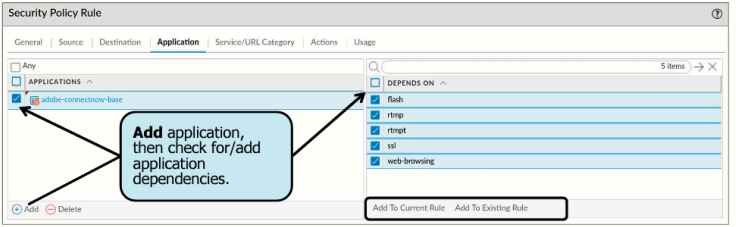
The default for **Destination Zone** is **Any**. You can select one or more destination zones for the rule. Multiple zones are used to simplify policy management. For example, if you have a source zone with three different destination zones, you can create a single rule to cover all these cases.

You can specify a destination address. The default for **Destination Address** is **Any**. The destination address can be a single address, an address range, an address group, or a geographical region. The default for **Destination Device** is **any**. The destination device can be one or more defined IoT devices. All these choices are available when you click **Add**.

The **Negate** option enables you to specify addresses, address ranges, address groups, or geographical regions that will not match the traffic. For example, consider the scenario where the network address 212.45.1.0/24 has been added to the **Destination Address** field. In this scenario, the rule would match all destination addresses not in the network 212.45.1.0/24.

Configure a Security Policy Rule: Application Tab

Default is **Any**. You should add specific applications as match criteria.

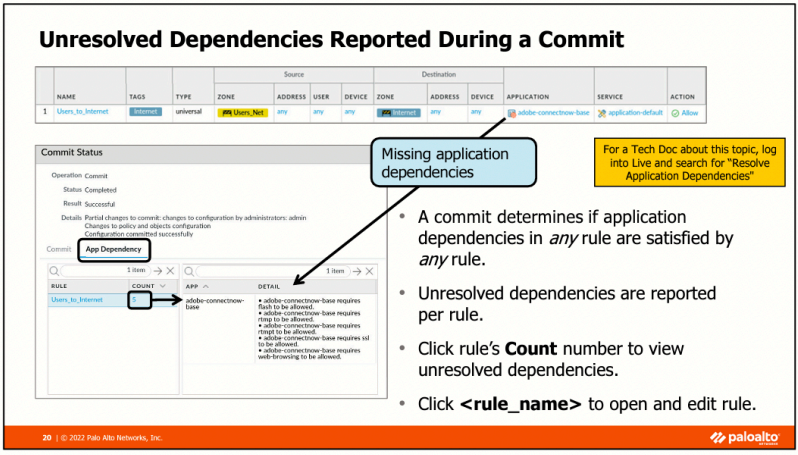


Click the **Application** tab to add, display, or modify the applications as match criteria for the rule. Click **Add** to add specific applications from a drop-down list.

If the selected application has application dependencies, they are displayed in the **Depends On** pane. You must permit the chosen application and other supporting applications for some applications to function correctly. Unless the supporting applications are allowed in your policy, the selected application will not work correctly in your environment.

In the **Depends On** pane, select the application dependencies to add to the Security policy and then choose the rule to add the applications. You can click **Add to Current Rule** to add the application dependencies to the rule being edited or click **Add to Existing Rule** to add the application dependencies to another rule you choose in the policy.

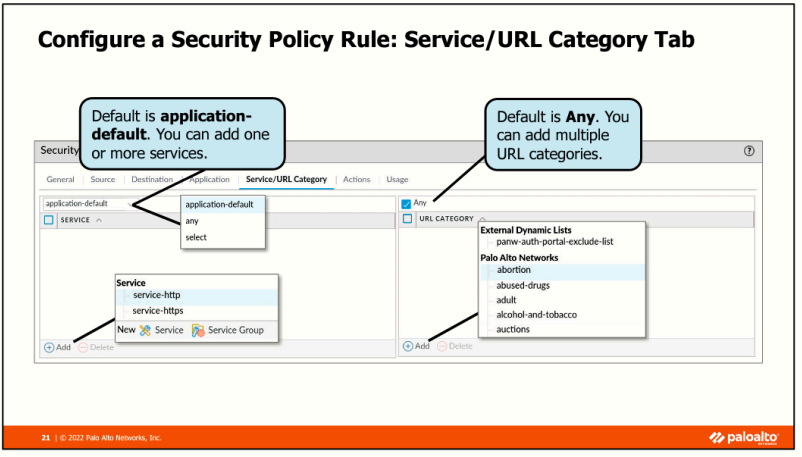
If an application has multiple functions, you can select the general parent application or individual child functions. If you choose the parent application, all child functions are included. If Palo Alto Networks adds child functions to the parent, the new child functions automatically are added if the parent application is allowed. For example, the parent facebook application includes facebook-chat, facebook-mail, facebook-apps, and many other functions. Selection of the parent facebook application automatically includes all the facebook functions. Alternatively, you can explicitly select only specific functions, which would disallow the application's non-selected functions.



What happens if you have not resolved application dependencies while creating or editing your policy rules? Starting with PAN-OS 9.1, unresolved application dependencies during commit operations are reported on the **App Dependency** tab in the **Commit Status** window.

During a commit operation, the firewall checks whether the applications listed in the policy have dependent applications and then determines whether *any* rule in the policy includes these dependent applications. You can add the missing application dependencies to any rule in the policy and commit again. Click the rule's name to add the missing application dependencies to the rule reported in the Status Window. The **Security Policy Rule** window will open to that rule and enable you to edit the application list for the rule.

To see the list of missing application dependencies in the **Commit Status** window, click the **Count** number next to the rule's name. The missing application dependencies for the rule are displayed in the window. These are the applications that must be added to some rule in the policy. After adding the missing applications, perform another commit and verify no more reported application dependency warnings.



Click the **Service/URL Category** tab to add, display, or modify the services and URL categories to match the criteria for a rule. Click **Add** to add specific services or URL categories.

The **Service** drop-down list has these three options:

- **any**: Any application is allowed or denied on any protocol or port. This rule choice is the least restrictive.
- **application-default**: Applications are allowed or denied only their default protocol ports as predefined in the Palo Alto Networks App-ID database. To display application information, browse to **Objects > Applications**. The **application-default** option is recommended when a policy rule allows a connection to prevent applications from running on unusual ports and protocols. Unusual ports and protocols can signify malicious application behavior and use. Even with the application-default setting, the firewall still checks for all applications on all ports, but the rule would match only applications connecting with their default ports and protocols.
- **select**: Click **Add** and select an existing service. A service is an object that defines a protocol and one or more ports. Only service-http (TCP 80, 8080) and service-https (TCP 443) are predefined, but you can create your own custom services.

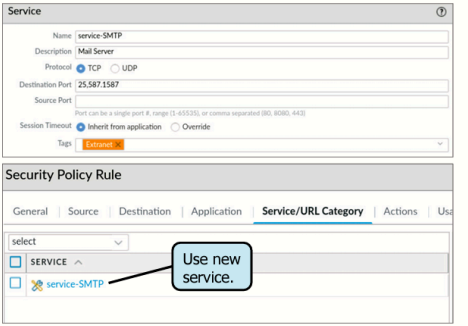
Palo Alto Networks maintains the PAN-DB URL category database that divides millions of URLs into various topic categories such as *alcohol-and-tobacco*, *auctions*, and *business-and-economy*. A firewall with a valid URL Filtering license can access this database and use URL categories as part of a Security policy rule.

Advanced URL filtering is described in more detail in another module.

Configure a New Service Definition

- Service definitions are assigned ports.
- Services limit ports that applications can use.
- service-http and service-https are the only predefined services.

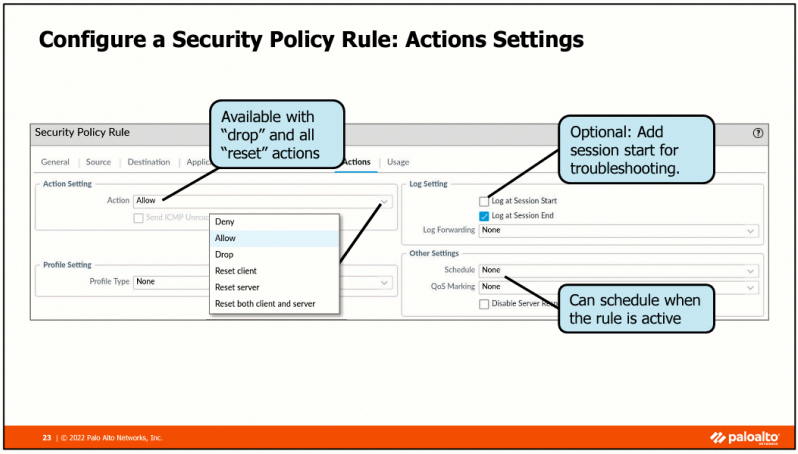
Objects > Services > Add



For a Tech Doc about this topic, log into Live and search for "Objects > Services"

When you define Security policy rules for specific applications, you can select one or more services to limit the port numbers that the applications can use. The default port for services in Security policy rules is **any**, enabling an application to use any TCP or UDP port. The only predefined service definitions are service-http and service-https, but you can create additional service definitions.

To create a service definition, browse to **Objects > Services** and click **Add**. Provide a descriptive **Name** for the new service and, optionally, provide a **Description** of the service. Select either the TCP or the UDP protocol because both cannot be simultaneously selected. Then specify the allowed destination ports from 0 to 65535. You can list a single port number, a hyphenated range of port numbers, or a comma-separated list of port numbers, or you can specify ports by mixing and matching all these formats. Specification of source port numbers is optional. You also can select a tag.



Click the **Action** tab to display or modify the actions taken on matched traffic:

- **Allow**: Default action.
- **Deny**: Blocks traffic and enforces the default "deny" action defined for the application that is being denied. To view the default "deny" action defined for an application, display the application details in **Objects > Applications**.
- **Drop**: Silently drops the traffic. For an application, it overrides the default "deny" action. A TCP reset is not sent to the host or application. Select the Send ICMP Unreachable check box to send an ICMP unreachable response to the client.
- **Reset client**: Sends TCP reset to the client (traffic initiator) device. Select the Send ICMP Unreachable check box to send an ICMP unreachable response to the client.
- **Reset server**: Sends TCP reset to the server (traffic responder) device. Select the Send ICMP Unreachable check box to send an ICMP unreachable response to the client.
- **Reset both client and server**: Sends TCP reset to both the client and server devices. Select the Send ICMP Unreachable check box to send an ICMP unreachable response to the client.

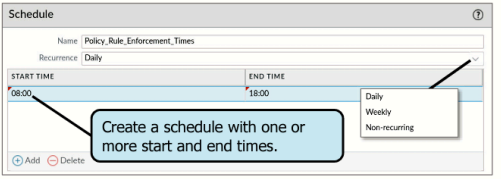
Palo Alto Networks firewall protection is based on application intelligence, so in the case of TCP, a TCP session must be established before the application can be discovered. However, after a TCP session has been established, silent dropping of packets without sending a TCP reset can be dangerous. The "drop" action could break the application and cause it to misbehave. An application might hang, continue to send packets, or unnecessarily hold system resources open. Therefore, the default "deny" action defined for more than half of the applications recognized by the firewall is to send a TCP reset.

The default logging action is to log only at the session end. However, you also may enable logging at session start, typically done only in the short term for troubleshooting purposes. The logging at the session starts to capture the initial connection setup and any initial application identification. The primary drawback with logging session start and session end is the additional load on the management plane CPUs and the extra storage space required for the log entries.

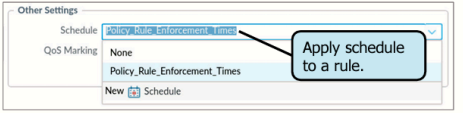
Schedule Security Policy Rules

- Policy rules may be enforced on only specific days and time periods.
- Use 24-hour time format.
- Can specify:
  - Daily
  - Days of week
  - Calendar days

Objects > Schedules > Add



Policies > Security > <select_rule> > Actions



For a Tech Doc about this topic, log into Live and search for "Objects > Schedules"

By default, a Security policy rule always is in effect. However, you can define and apply a schedule to a rule that limits when the rule is in effect. To define a schedule, browse to **Objects > Schedules** and click **Add**.

The firewall scheduler supports a daily schedule with multiple start and end times. It also supports a day-of-the-week schedule for those situations where a scheduled change should not occur every day of the week. You can still specify multiple start and end times to any scheduled day of the week. The scheduler also supports a non-recurring schedule where you specify a start date and time followed by an end date and time. A non-recurring schedule also supports multiple start and end times.

After defining a schedule, browse to **Policies > Security**, select a rule, and click its **Actions** tab. Select your schedule from the **Schedule** drop-down list.

Established sessions are not affected by a rule made active by the scheduler. For example, an existing FTP session would not be blocked if a scheduled rule that blocks FTP becomes active. Only new FTP requests would be blocked after the scheduled rule became active.

Configure a Security Policy Rule: Usage Settings

For a Tech Doc about this topic, log into Live and search for "Monitor Policy Rule Usage"

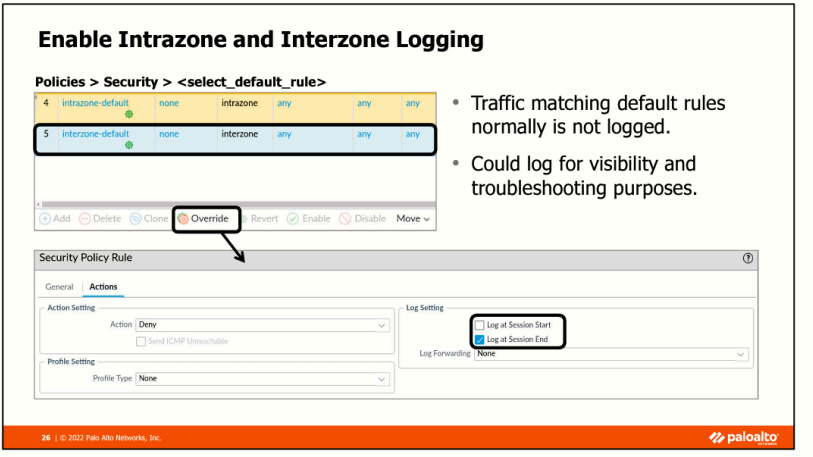
Click the **Usage** tab to display the rule's usage. The **Usage** tab is not displayed during initial rule creation.

The **Basics** section displays the date and time when the rule was created and when the rule was last edited.

The **Activity** section displays the rules hit count data, including the date and time when traffic first matched this rule and the last traffic match.

The **Applications** section displays the number of applications seen by this rule. Click the **Compare Applications & Applications Seen** link to access tools that can help you migrate from port-based Security policy rules to application-based Security policy rules.

The **Traffic** section displays the amount of traffic, in bytes, over the past 30 days.



By default, the implicit intrazone-default and interzone-default rules do not generate Traffic log entries. However, you can enable logging on each of these rules so that you can see all traffic encountered by your firewall.

Select a rule and click Override to configure logging on the implicit rules. Then choose to log at session end or, for short-term troubleshooting purposes, log at both session start and session end.

In addition to having logging capabilities, you can apply Security Profiles to the default intrazone and interzone policy rules. We describe Security Profiles in another module.

Find Unused Security Policy Rules

For a Tech Doc about this topic, log into Live and search for "Creating and Managing Policies"

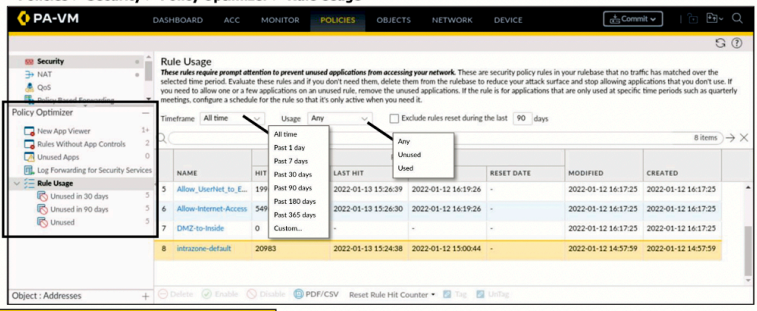
- Remove unused rules to:
  - Increase firewall operational efficiency
  - Simplify rule management
- Firewall tracks rules unused since last time the data plane restarted.

Policies > Security

Administrators periodically should cull their Security policy rulebase from time to time. You can perform clean-up quickly and easily by using the **Highlight Unused Rules** option, which lets you see which rules have not matched any traffic since the last restart of the data plane. This option can be used to help troubleshoot a misconfigured Security policy. This option also can be helpful if you migrated your rules from a previous, non-Palo Alto Networks firewall solution.

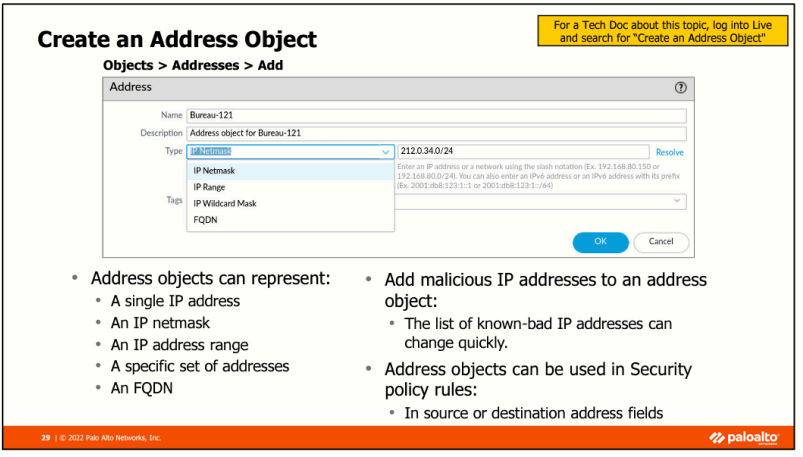
Rule Usage Filter

Policies > Security > Policy Optimizer > Rule Usage



For a Tech Doc about this topic, log into Live and search for "Sorting and Filtering Security Policy Rules"

If you have overprovisioned access to the firewall, you are at greater risk of being exploited by attacks. Firewall administrators need to periodically check for rules that are out of date or unused. Starting with PAN-OS 9.0, the **Rule Usage** filters enable you to quickly filter the selected rulebase based on the rule usage data. Rule usage data can include the rule creation and last modified dates, hit count data, and the first and last hit dates within a customizable timeframe. For example, you can simplify the management of rule lifecycles if you find unused rules and then disable or delete the rules to maintain an up-to-date rulebase.



An Address object is a name-value pair representing a single IP address, a range of IP addresses, an IP subnet, or the fully qualified domain name (or FQDN). Address objects are used to simplify firewall administration by enabling you to create or update an object once and then reuse it multiple times across different policy types. When the IP address or range defined for the Address object changes, you can edit the Address object. The change in value automatically is inherited by all instances where the Address object is used.

You can use an Address object in the source or destination IP address fields in a Security policy. An Address object can also be used in any other policy type on a firewall.

To create an address object in the web interface, browse to **Objects > Addresses** and click **Add**. Enter a name for your address object and, optionally, enter a description. Then select the type of address object that you are creating. The menu choices are **IP Netmask**, **IP Range**, **IP Wildcard Match**, and **FQDN**.

If you select **IP Netmask**, then you can enter a single IP address or an IP network number with the netmask.

If you select **IP Range**, then you can enter a network range. For example, you could type **`204.10.20.1-204.10.20.254`**.

If you select **IP Wildcard Mask**, then you can enter a network mask that defines a set of specific IP addresses.

You also can select **FQDN** and then enter a domain name. After entering a domain name, click **Resolve** to ensure that the firewall can map the domain name to an IP address. To resolve the domain name to an IP address, the firewall performs a DNS lookup on the domain name. The FQDN resolves up to 30 IP addresses and relies highly on a properly functioning DNS configuration.

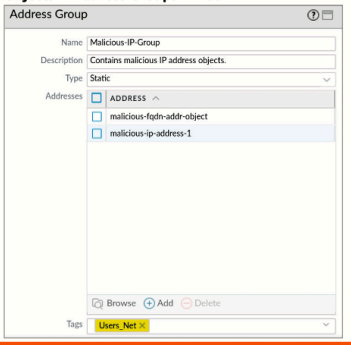
Supplemental Notes

The firewall uses the DNS server to resolve the FQDN to an address as soon as you commit the firewall configuration. After initial address resolution, the firewall refreshes the IP address at the interval specified by the TTL time of the DNS entry unless that time is less than the firewall **Minimum FQDN Refresh Time** (sec) found at **Device > Setup > Services**. If the DNS TTL time is less than the firewall minimum refresh

time, it uses its minimum refresh time instead.

Create a Static Address Group

Objects > Address Groups > Add



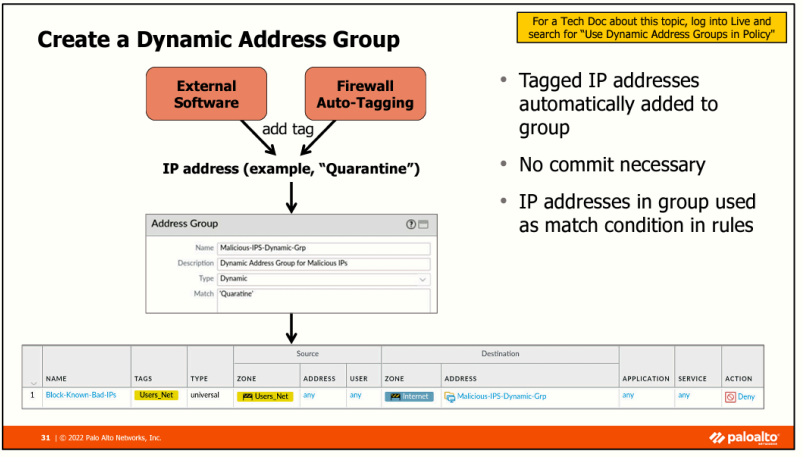
- Use to shorten and simplify a policy rule
- Membership must be manually updated
- Updates require a commit operation
- Can contain:
  - Address objects
  - Other address groups

For a Tech Doc about this topic, log into Live and search for "Objects > Address Groups"

You also can add IP addresses to a static address group and then use the group in Security policy rules.

Use address groups to shorten and simplify a policy rule. Group all addresses that require the same security settings in an address group and then add the address group to a policy rule. Address membership in a static address group will not change unless you change it. After changing the membership of a static address group, you must perform a commit operation for the changes to take effect.

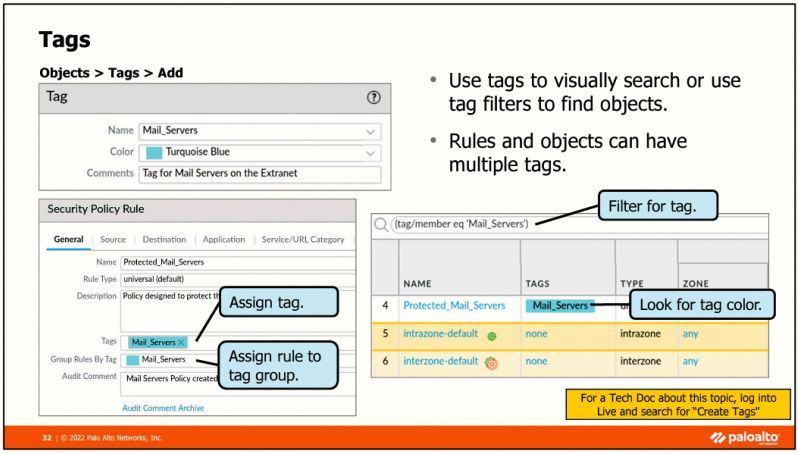
To create a static address group, browse to **Objects > Address Groups** and click **Add**. When the **Address Group** window opens, enter the **Name** of the address group and verify that **Static** is selected in the **Type** field. Then click **Add** to add address objects or other address groups to the new static address group.



IP address membership in a dynamic address group can fluctuate, but membership changes do not require you to perform a commit operation. Membership in a dynamic address group is determined using tag names or tag-based filters. Either external software or the firewall can automatically add a tag to an IP address, and then you can associate that tag with a dynamic address group. For example, VMware NSX software can assign a tag to the IP address of a newly created virtual machine, or the auto-tagging capability included in the log forwarding feature of the firewall can add a tag to an IP address. The screenshot shows that any IP address assigned the **Quarantine** tag would become a member of the Malicious-IPS-Dynamic-Grp's dynamic address group.

To create a dynamic address group, browse to **Objects > Address Groups** and click **Add**. Enter the **Name** of the address group and select **Dynamic** as the **Type**. Then add either a tag name or a tag filter. After creating the dynamic address group, add the group to either the **Source Address** or **Destination Address** field in a policy rule. The rule uses any IP addresses assigned to the tag as match conditions.

For more information about the firewall auto-tagging feature, search for the following video in YouTube - Tutorial: Auto-tagging & DNS Sinkhole. Or use the URL https://www.youtube.com/watch?v=SaknKHwdnCI. For information about managing auto-tagging from the command line, log into Live and search for "CLI Commands for Dynamic IP Addresses and Tags" or see the documentation at https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/policy/cli-commands-for-dynamic-ip-addresses-and-tags.



Tags enable you to group objects using keywords or phrases. Tags can be assigned a color, making a visual search for a tag easier in the web interface. You can use a filter in the web interface to display only those objects that have been assigned a particular tag. You can assign your Security policy to a tag group. In the example, a filter for the tag name Mail Servers Rule was applied to the Security policy ruleset, which caused only the explicit rules with that tag to be displayed. Implicit rules always are displayed.

Tags can be assigned to address objects, address groups, zones, services, service groups, and policy rules. You can assign multiple tags to a rule or object. If a rule or object is assigned multiple tags, only the color of the first assigned tag is displayed.

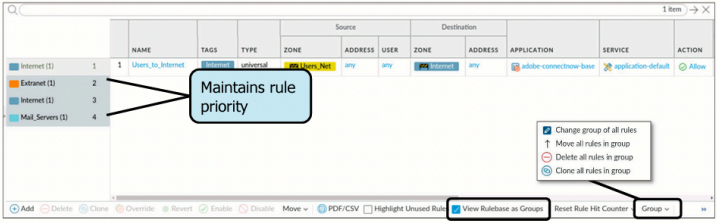
To create a tag, browse to **Objects > Tags** and click **Add**. Provide a descriptive **Name** for the tag based on its purpose. Tags enable you to choose a **Color** and add **Comments** that describe the tag.

Since the release of PAN-OS 9.0, you require that all of your Security policy rules have a tag assigned to them. To require that tags be assigned to your rules, browse Device > Setup > Management and select the Require Tag on the **policies** check box. To ensure that tags are added to a policy rule, select the **Fail commit if policies have no tags or description** check box, which forces the commit to fail if tags are not assigned.

Tag-Based Rule Groups

- Visually group rules based on tagging structure
- Can perform operational procedures within the selected tag group

Policies > Security

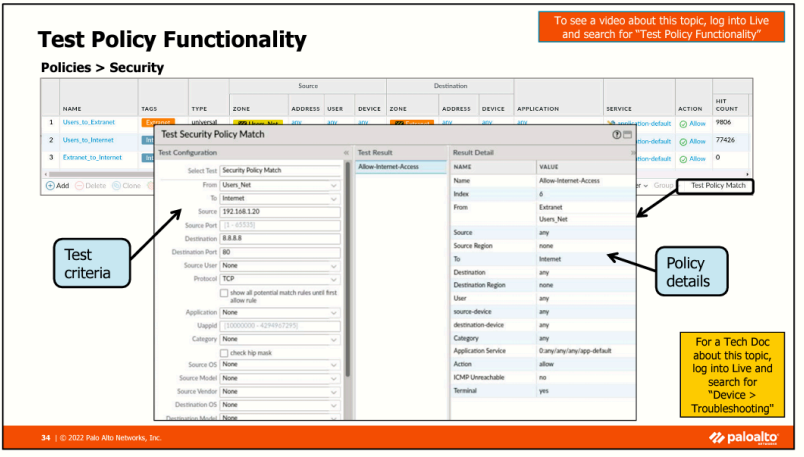


For a Tech Doc about this topic, log into Live and search for "View Rulebase as Groups"

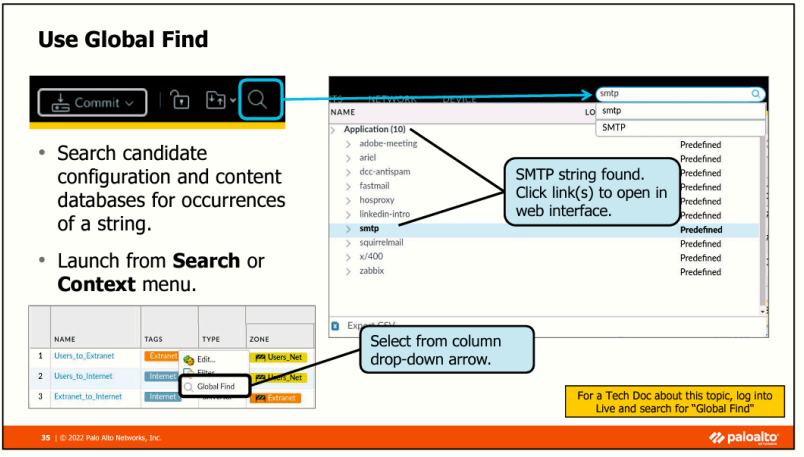
PAN-OS 9.0 replaced the tag browser to assign rules to tag groups. After your rules are assigned to a tag group, you can view the rulebase as a tag group to visually group rules based on the tagging structure you created. When you view the rulebase as groups, you can perform operational procedures such as adding, deleting, or moving the rules within the selected tag group for simplified management of your rulebase.

Rule tag groups are displayed in the same order as the rules in the rule-base. As a result, a single tag group may appear multiple times throughout the rulebase to visually preserve the rule hierarchy. However, all rule operations apply to all rules in the same tag group, regardless of their position in the rulebase hierarchy.

Before assigning a group tag to a rule, you must first create the tag and assign it to the Security policy rule.



Since the release of PAN-OS 9.0, you can test policy rules and manage device configurations to ensure that candidate configurations appropriately secure your network and maintain connectivity to essential network resources. The **Test Security Policy Match** window enables you to enter a set of criteria directly from the web interface rather than from the CLI. After a test is executed, the criteria are evaluated against the current Security policy rules to determine if the simulated traffic matches an existing policy. After running the policy match and connectivity tests in the web interface, you can quickly and easily test connectivity to ensure that policy rules allow or deny the correct traffic, and those devices can connect to network resources such as WildFire® or Log Collectors.



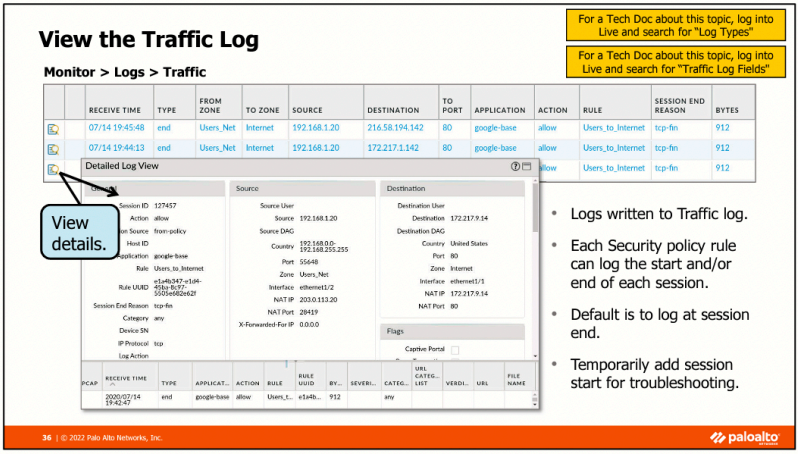
Global Find enables you to search the candidate configuration and content databases on a firewall for a particular string, such as an IP address, an object name, a policy rule name, a threat ID, or an application name. Global Find is launched from the **Search** link or a **Context** menu.

The search results are grouped by category. Links are provided to the object's location in the web interface so that you can easily display all the places where the string is referenced. The search results also help you identify other objects that depend on or reference the search string. For example, if you are deprecating an application, enter the application name in Global Find to locate all application instances and then click each instance to navigate to the configuration location and make the necessary changes.

Global Find will not search dynamic content such as logs, address ranges, or allocated DHCP addresses. Global Find also does not search for individual usernames or group names identified by User-ID unless the user or group is defined in a policy. You can generally search only content that the firewall writes to the candidate configuration.

Example use cases for the Global Find feature are:

- Find all objects with a given tag.
- View where a given IP address is used in the configuration, including address objects, dynamic objects, literals in policies, and network configuration.
- Find a policy that includes a username or a user group.
- View any place a given username appears in the config, including user activity reports and policies.
- Find out if an application is used in a policy, application group, application filter, or report query.
- Find a ticket number added to a comment in a policy or on another object.



Each Security policy rule can be configured to log session information to the Traffic log. The default is to log at the session end. However, you can choose not to log at all, at session start, at session end, or at both session start and session end. Traffic logs show entries for each URL category transition only if **Log at Session Start** also is configured. Under normal circumstances, logging at the session end is sufficient for viewing firewall operation. If you need to troubleshoot firewall operation, you might need to temporarily configure one or more Security policy rules to log at session start and session end, which will place additional load on the management plane CPUs and consume more disk space to hold the additional log entry information.

The **Type** column indicates whether the entry is for the *start* or *end* of the session or whether the session was denied or dropped. The type "drop" indicates that the security rule blocking traffic was configured to match *any* application. Suppose the firewall drops the traffic before the application has been identified. In that case, the **Application** column displays *not-applicable*. "deny" indicates that the security rule was configured to match and block a specific, named application.

Click the **magnifying glass** icon next to an entry to display additional details about the session. For example, a count value greater than one indicates that an ICMP entry aggregates multiple sessions between the same source and destination.

Module Summary

Now that you have completed this module, you should be able to:

- Describe Security policy concepts and operation
- Configure a Security policy rule
- Manage a Security policy

Now that you have completed the module, you should be able to perform the tasks listed.

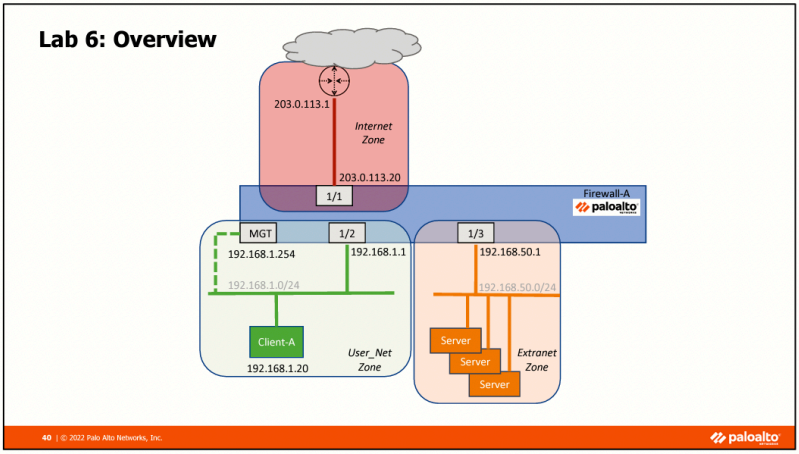
Additional Resources

For a digital review of this module, log into Beacon and search for:

"Next-Generation Firewall Setup and Management Connection"

Review Questions

1. Which two items are required to match criteria in a Palo Alto Networks Security policy rule? (Choose two.)
   a. source zone
   b. destination zone
   c. destination address
   d. destination port
2. Which type of Security policy rule is the default rule type?
   a. intrazone
   b. interzone
   c. universal
   d. default
3. Which action in a Security policy rule results in traffic being silently rejected?
   a. deny
   b. drop
   c. reset server
   d. reset client
4. True or false? Logging on intrazone-default and interzone-default Security policy rules is enabled by default.
   a. true
   b. false



Your instructor can provide an overview of the lab environment and the details needed for this lab. See the following page for a list of tasks that you will carry out in this lab.

Lab 6: Creating and Managing Security Policy Rules

- Configure a Security policy rule to allow access from Users_Net to Extranet
- Test access from client to Extranet servers
- View the Traffic log
- Examine policy Rule Hit Count
- Reset rule hit counts
- Customize policy tables
- Enable intrazone and interzone logging
- Create Security Policy Rules to Internet Zone
- Create Block Rules for Known-Bad IP Addresses

Answers to Review Questions

1. a, b
2. c
3. b
4. c
5. b (false)