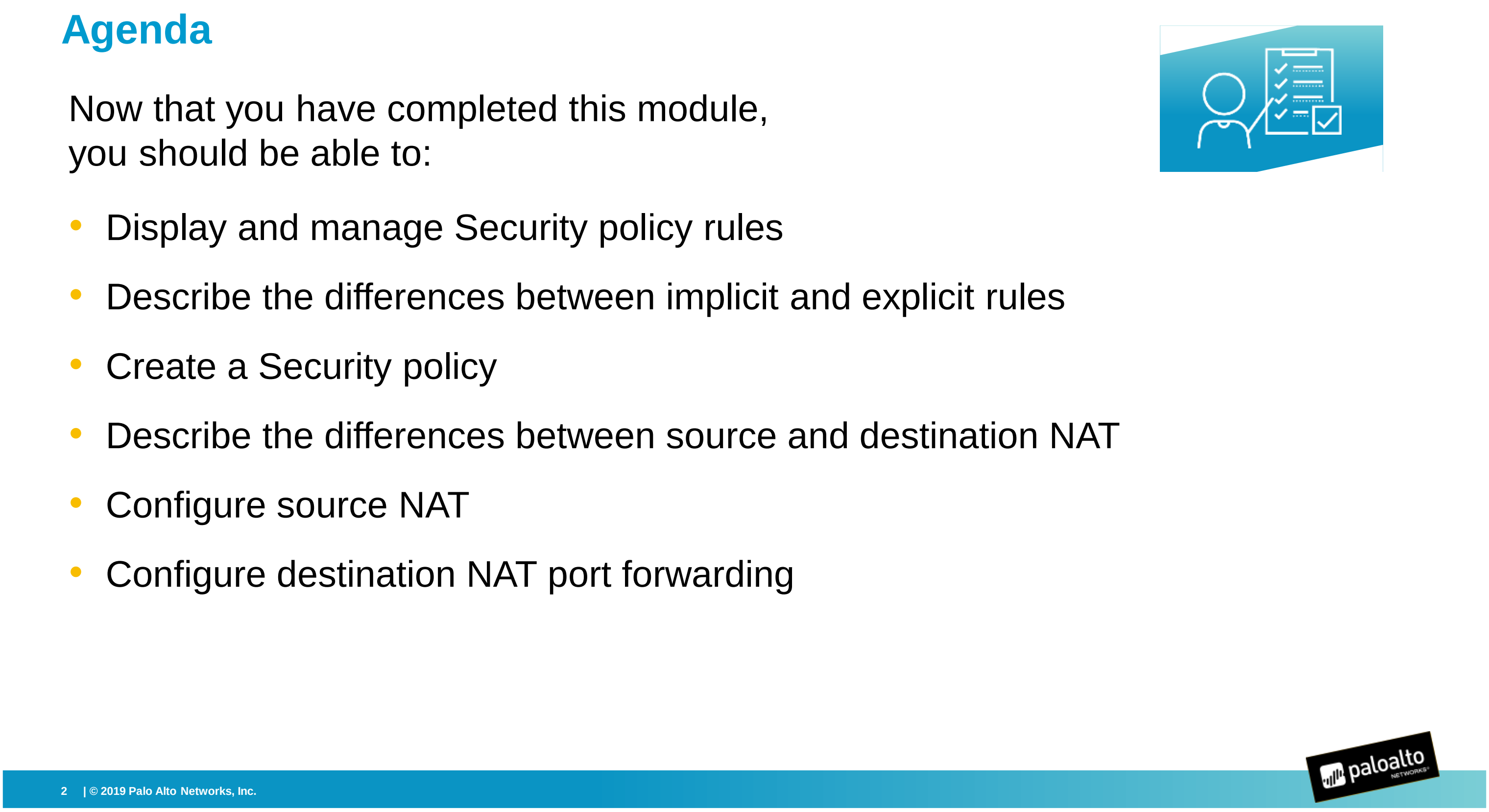
SECURITY AND NAT POLICIES

EDU-210 Version A
PAN-OS® 9.0

GET TRAFFIC FLOWING

- Security policy fundamental concepts
- Security policy administration
- Network address translation
- Source NAT configuration
- Destination NAT configuration



Agenda

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

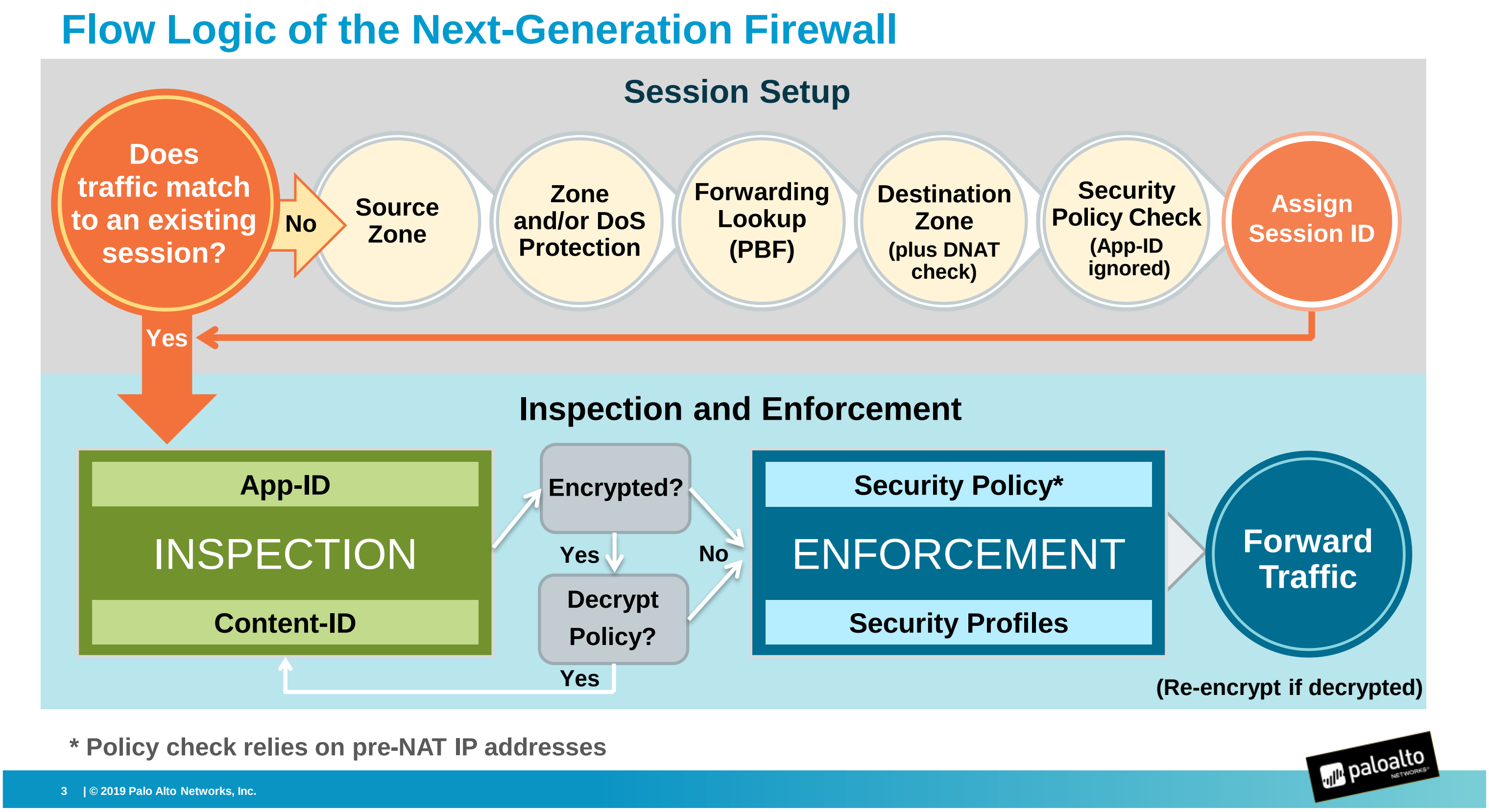
- Display and manage Security policy rules
- Describe the differences between implicit and explicit rules
- Create a Security policy
- Describe the differences between source and destination NAT
- Configure source NAT
- Configure destination NAT port forwarding

2 | © 2019 Palo Alto Networks, Inc.

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

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

- Display and manage Security policy rules
- Describe the differences between implicit and explicit rules
- Create a Security policy
- Describe the differences between source and destination NAT
- Configure source NAT
- Configure destination NAT port forwarding



Flow Logic of the Next-Generation Firewall

Session Setup
Does traffic match to an existing session?
No
Source Zone
Zone and/or DoS Protection
Forwarding Lookup (PBF)
Destination Zone (plus DNAT check)
Security Policy Check (App-ID ignored)
Assign Session ID
Yes
Inspection and Enforcement
App-ID
INSPECTION
Content-ID
Encrypted?
Yes
No
Decrypt Policy?
Yes
Security Policy*
ENFORCEMENT
Security Profiles
Forward Traffic
(Re-encrypt if decrypted)

* Policy check relies on pre-NAT IP addresses

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 of a PAN-OS® device, see the *Packet Flow Sequence in PAN-OS* document available on the Palo Alto Networks Support website at https://live.paloaltonetworks.com/docs/DOC-1628.

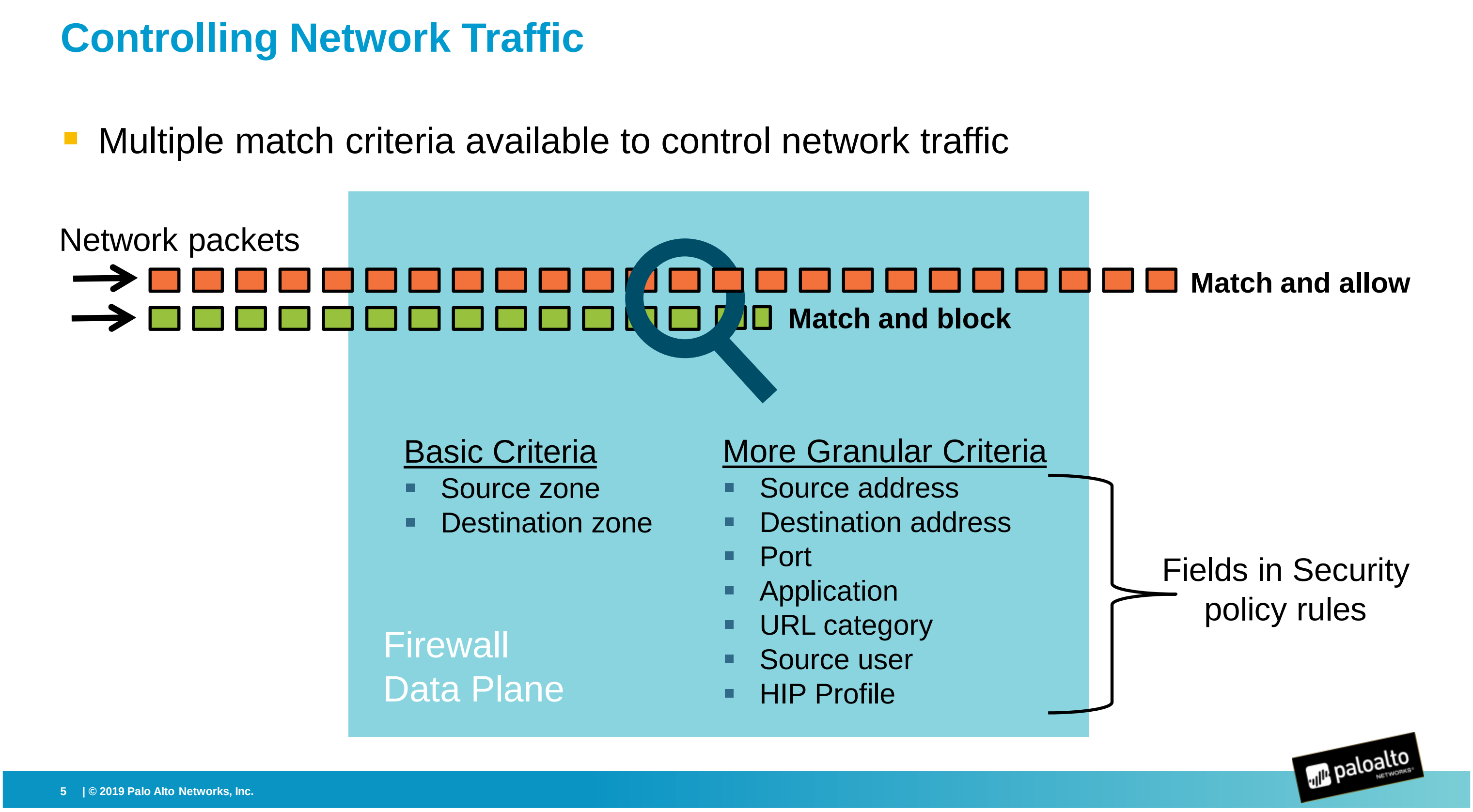
Security policy fundamental concepts

Security policy administration

Network address translation

Source NAT configuration

Destination NAT configuration



Controlling Network Traffic

- Multiple match criteria available to control network traffic

Network packets

Match and allow

Match and block

Basic Criteria

- Source zone
- Destination zone

More Granular Criteria

- Source address
- Destination address
- Port
- Application
- URL category
- Source user
- HIP Profile

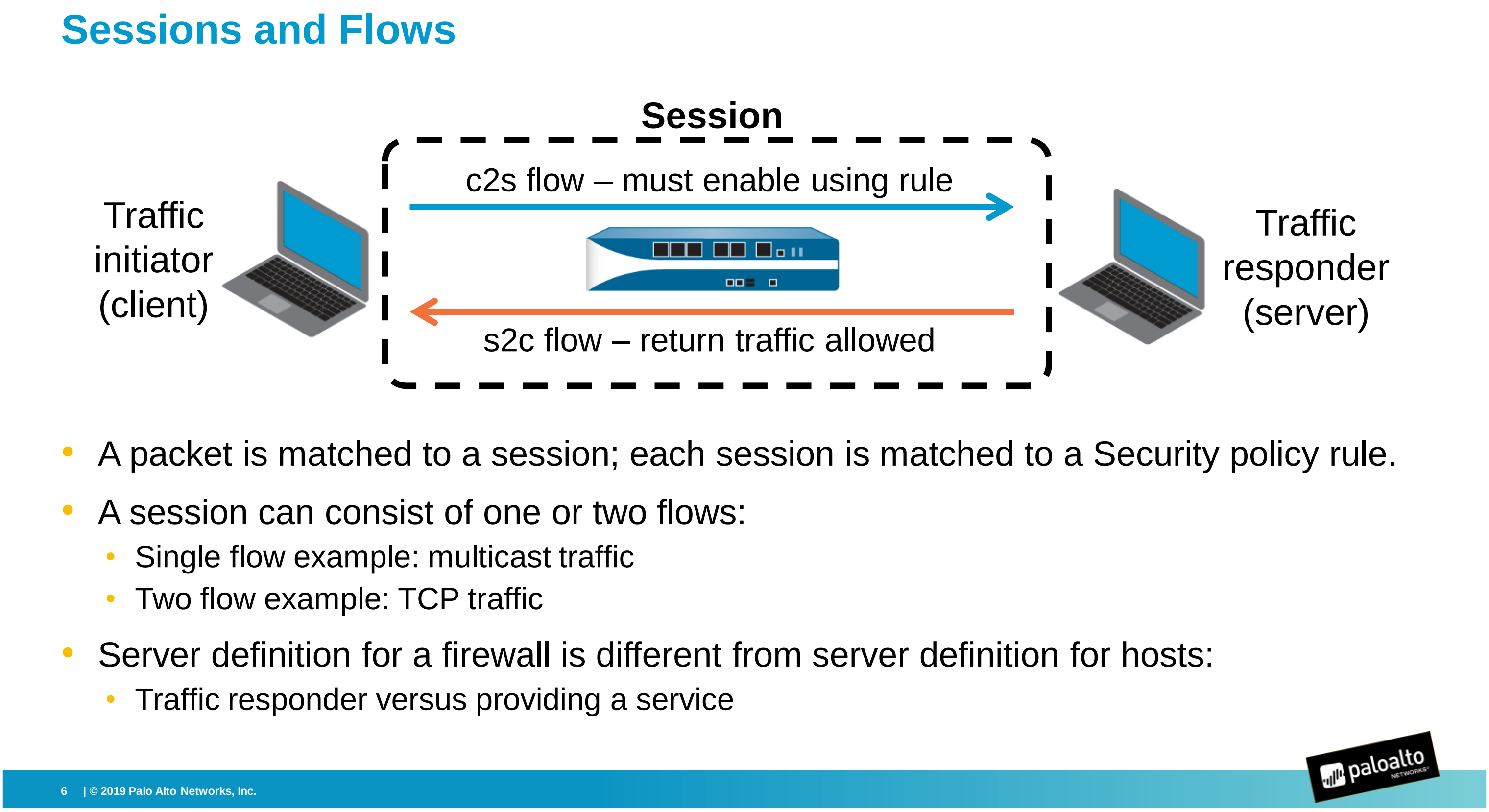
Fields in Security policy rules

Firewall
Data Plane

5 | © 2019 Palo Alto Networks, Inc.

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. You define Security policy rules on the firewall using various criteria such as zones, applications, IP addresses, ports, users, and host information profile (HIP) Profiles.

You can define Security policy rules to allow or deny traffic starting with the source and destination zones as the broad criteria, then fine-tune the rules with more granular options such as source and destination IP addresses, ports, applications, URL categories, source users, and HIP Profiles.



Sessions and Flows

Session
c2s flow – must enable using rule
Traffic initiator (client)
Traffic responder (server)
s2c flow – return traffic allowed

- 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

6 | © 2019 Palo Alto Networks, Inc.

The Palo Alto Networks firewall is a stateful firewall, which means that all traffic passing through the firewall is matched against a session and each session is then matched against a Security policy rule. Each session is identified by a six tuple consisting of:

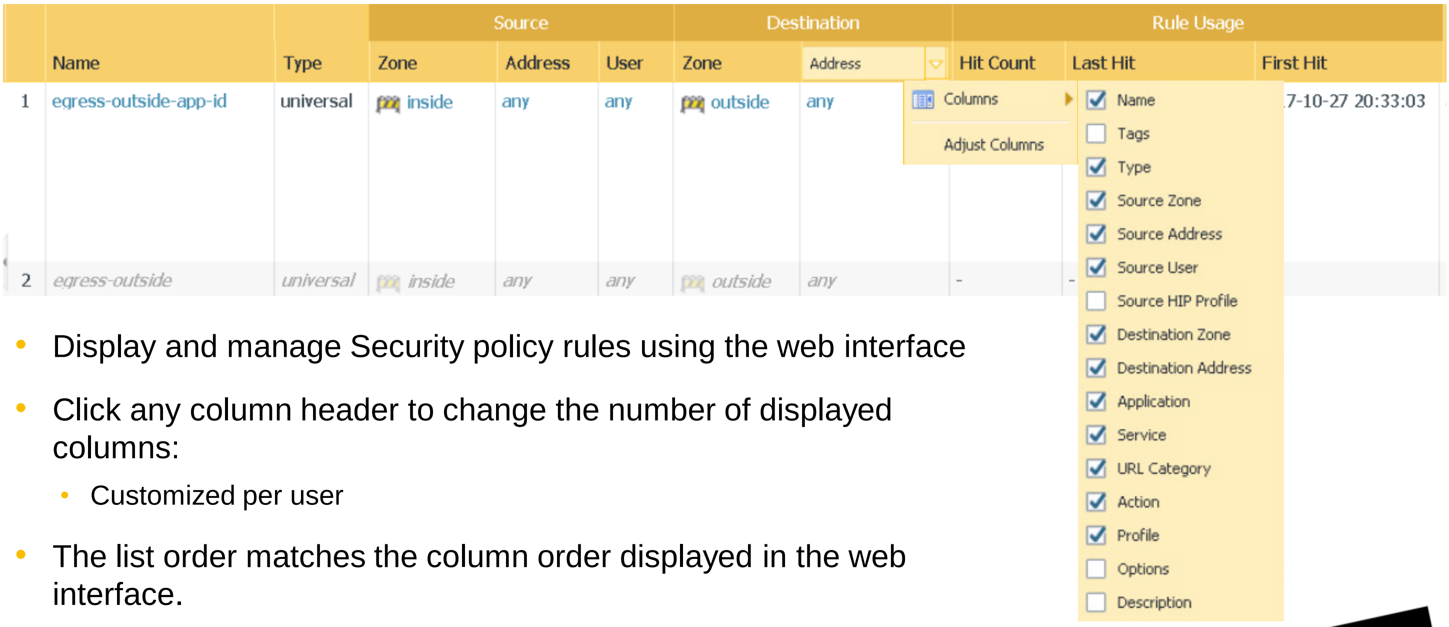
- Source and destination IP address
- Source and destination port number: For non-UDP/TCP traffic, different protocol fields are used.
- Protocol
- Source security zone

Each session is assigned a unique session ID number.

A session can consist of one or two flows: the client-to-server flow (c2s flow) and the server-to-client flow (s2c flow). The endpoint where traffic initiates always is the client, and the endpoint where traffic is destined 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, that is, in the c2s direction. The return s2c flow does not require a separate rule because the return traffic automatically is allowed.

Displaying and Managing Security Policy Rules

Policies > Security

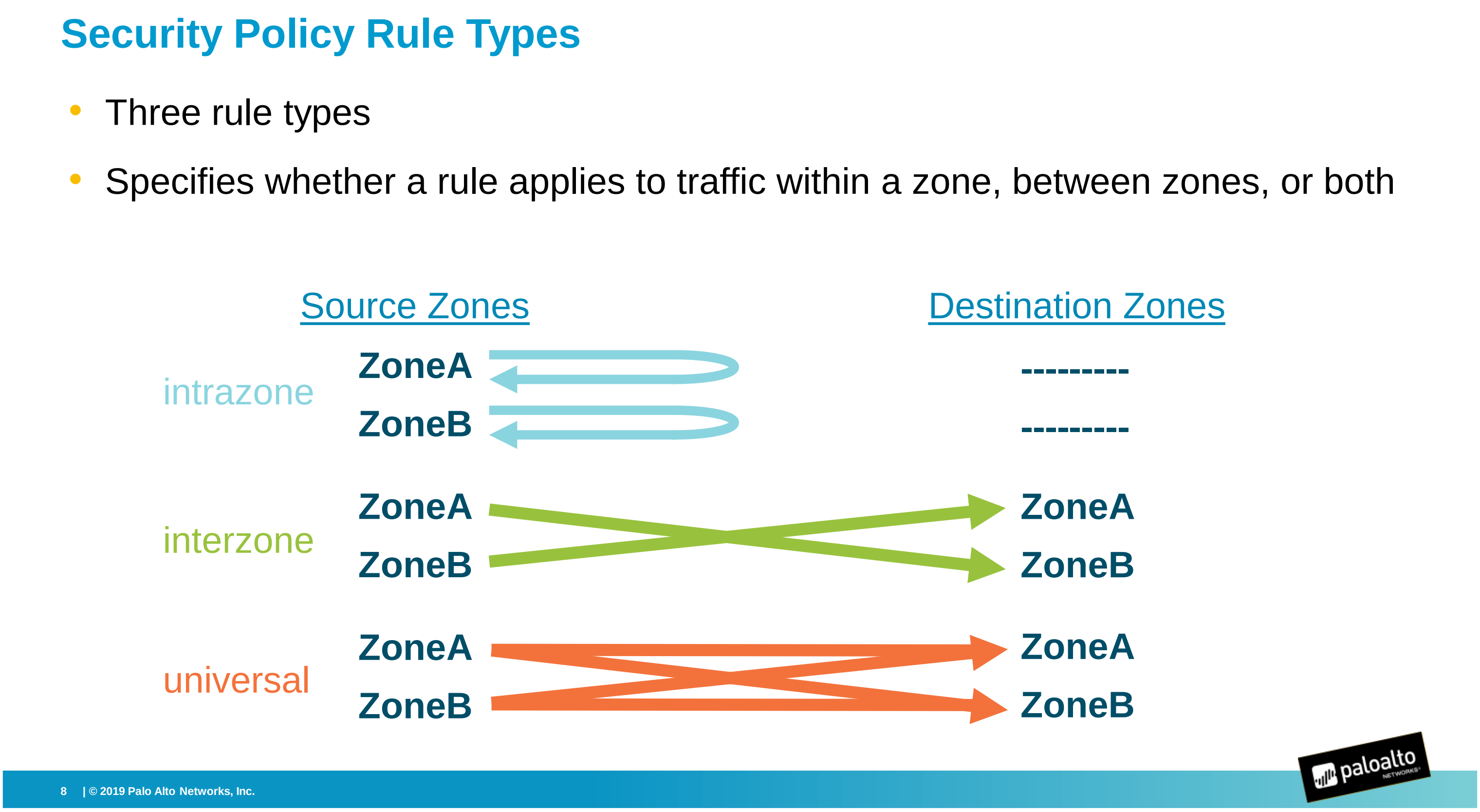


			Source			Destination		Rule Usage		
	Name	Type	Zone	Address	User	Zone	Address	Hit Count	Last Hit	First Hit
1	egress-outside-app-id	universal	inside	any	any	outside	any			7-10-27 20:33:03
2	*egress-outside*	*universal*	*inside*	*any*	*any*	*outside*	*any*	-	-	

☑ Name
□ Tags
☑ Type
☑ Source Zone
☑ Source Address
☑ Source User
□ Source HIP Profile
☑ Destination Zone
☑ Destination Address
☑ Application
☑ Service
☑ URL Category
☑ Action
☑ Profile
□ Options
□ Description

- 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 to **Policies** > **Security**. Each logged-in user can customize their web interface display. Modify the number of columns displayed by clicking any column header and selecting from the list that the web interface displays. The order in the list matches the order in which the columns are displayed in the web interface. For example, note that the **Tags** column is deselected in the list and that the corresponding column is missing in the web interface display. The **Tags** column would have been displayed between the **Name** and **Type** columns.



Security Policy Rule Types

- Three rule types
- Specifies whether a rule applies to traffic within a zone, between zones, or both

Source Zones

Destination Zones

intrazone

ZoneA ---------

ZoneB ---------

interzone

ZoneA ZoneA

ZoneB ZoneB

universal

ZoneA ZoneA

ZoneB ZoneB

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.

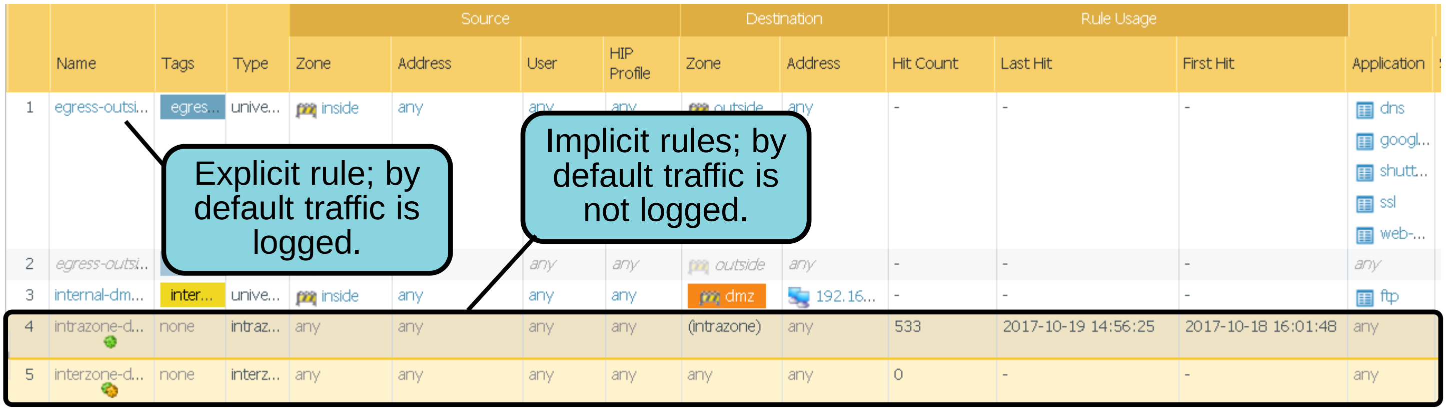
An intrazone rule applies to all matching traffic within the specified source zones. You cannot specify a destination zone for an intrazone rule. For example, if you set the source zones to ZoneA and ZoneB, the rule would apply to all traffic within ZoneA and all traffic within ZoneB, but not to traffic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

Implicit and Explicit Rules

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



				Source				Destination		Rule Usage			
	Name	Tags	Type	Zone	Address	User	HIP Profile	Zone	Address	Hit Count	Last Hit	First Hit	Application
1	egress-outsi...	egres...	unive...	inside	any	any	any	outside	any	-	-	-	dns googl... shutt... ssl web-...
2	egress-outsi...					any	any	outside	any	-	-	-	any
3	internal-dm...	inter...	unive...	inside	any	any	any	dmz	192.16...	-	-	-	ftp
4	intrazone-d...	none	intraz...	any	any	any	any	(intrazone)	any	533	2017-10-19 14:56:25	2017-10-18 16:01:48	any
5	interzone-d...	none	interz...	any	any	any	any	any	any	0	-	-	any

Explicit rule; by default traffic is logged.

Implicit rules; by default traffic is not logged.

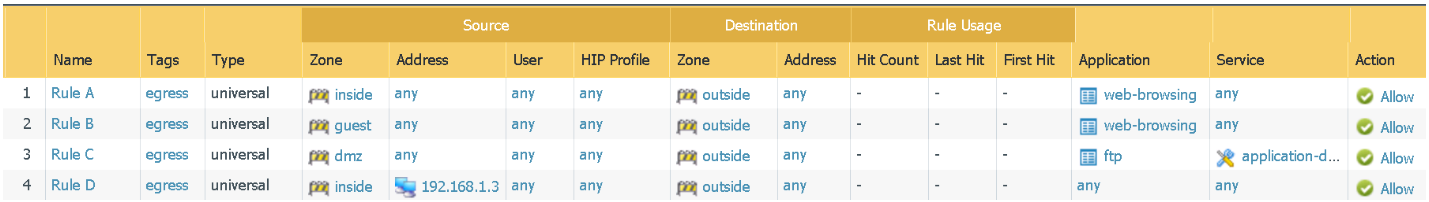
By default the firewall implicitly allows intrazone traffic and implicitly denies interzone traffic. These implicit actions are predefined by the mostly read-only intrazone-default and interzone-default rules. By default the two implicit rules are processed after all the explicit administrator-defined 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 to the Traffic log all traffic that is matched to an administrator-defined Security policy rule. By default traffic allowed or denied by the implicit Security policy rules is not logged on the firewall. However, Palo Alto Networks recommends that you log all traffic and change the default behavior. Logging and logging configuration are described later in this module.

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 deny all intrazone traffic. This explicit “deny-all” rule can disrupt normal application traffic flowing within your networks.

Security Policy Rule Match

- Rules evaluated from top to bottom
- Further rules not evaluated after a rule match



				Source				Destination		Rule Usage					
	Name	Tags	Type	Zone	Address	User	HIP Profile	Zone	Address	Hit Count	Last Hit	First Hit	Application	Service	Action
1	Rule A	egress	universal	inside	any	any	any	outside	any	-	-	-	web-browsing	any	Allow
2	Rule B	egress	universal	guest	any	any	any	outside	any	-	-	-	web-browsing	any	Allow
3	Rule C	egress	universal	dmz	any	any	any	outside	any	-	-	-	ftp	application-d...	Allow
4	Rule D	egress	universal	inside	192.168.1.3	any	any	outside	any	-	-	-	any	any	Allow

- Could Rule A and Rule B be combined? Yes.
  - Place Inside and Guest together in source zone
  - Outside remains in destination zone

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

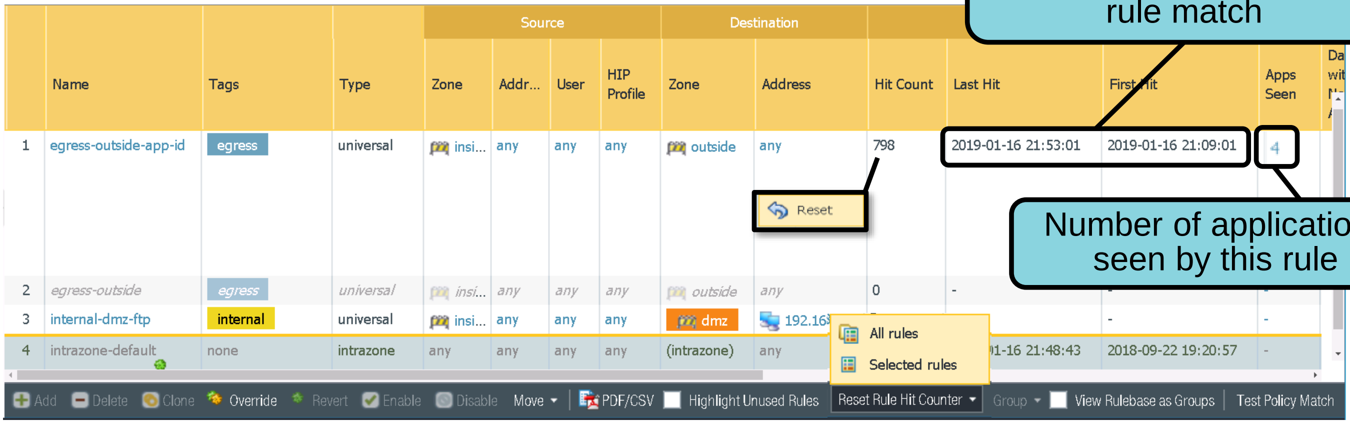
Policy rules are unidirectional, which means that they allow only traffic that is initiated in the direction that the policy rule specifies: source zone(s) to destination zone(s). The replies to the client always are allowed as part of the policy. If traffic is intended to be initiated in both directions,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

- 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 config changes



Timestamp of first policy rule match and last policy rule match

				Source				Destination						
	Name	Tags	Type	Zone	Addr...	User	HIP Profile	Zone	Address	Hit Count	Last Hit	First Hit	Apps Seen	Da wi
1	egress-outside-app-id	egress	universal	insi...	any	any	any	outside	any	798	2019-01-16 21:53:01	2019-01-16 21:09:01	4	
2	egress-outside	egress	universal	insi...	any	any	any	outside	any	0	-			
3	internal-dmz-ftp	internal	universal	insi...	any	any	any	dmz	192.16			-	-	
4	intrazone-default	none	intrazone	any	any	any	any	(intrazone)	any		1-16 21:48:43	2018-09-22 19:20:57	-	

Number of applications seen by this rule

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 provides you the ability to validate rule additions or changes, and to 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 to gauge rule use within a given period of time. Policy rule Hit Count data is not stored on the firewall. After you have cleared the data using the reset option, the cleared data no longer will be available.

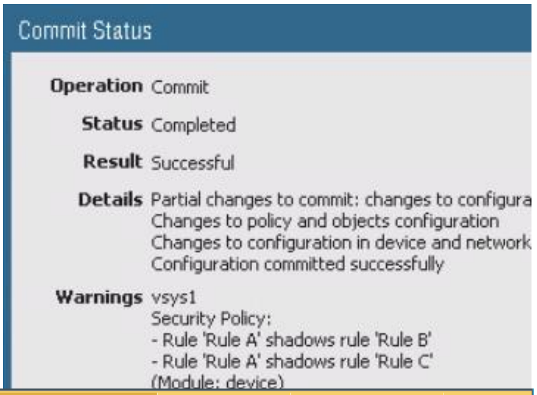
The policy rule Hit Count data also is available through the CLI and API.

Supplemental Notes

An example for using the policy rule Hit Count is when you migrate port-based rules to app-based rules. You start by creating an app-based rule and place it in order above the port-based rule. To verify the configuration of your app-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 app-based rule until you can validate that all traffic is being serviced by the app-based rule. You now can safely remove the port-based rule, thereby reducing the firewall attack surface.

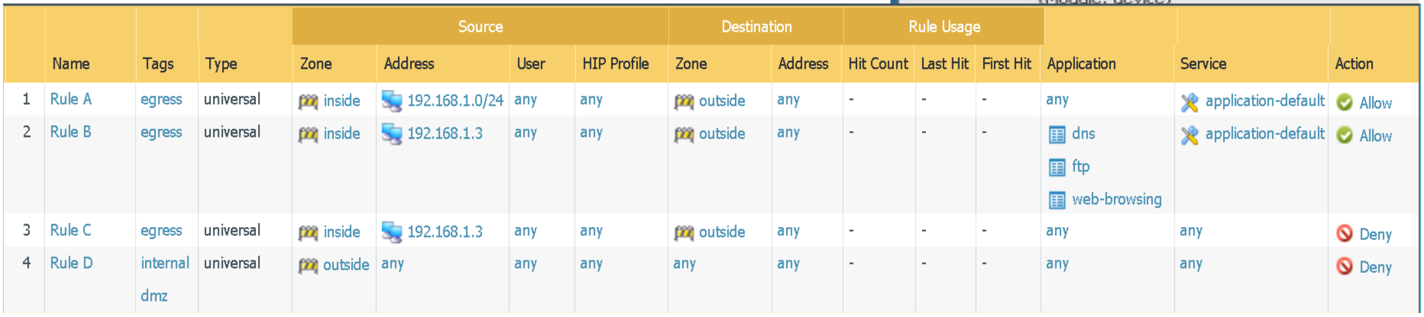
Rule Shadowing

- Traffic can match multiple rules.
- Earlier rule hides (casts a shadow over) later rule.
- Reorder or refine rules to remove shadowing.



Commit Status

Operation Commit
Status Completed
Result Successful
Details Partial changes to commit: changes to configura
Changes to policy and objects configuration
Changes to configuration in device and network
Configuration committed successfully
Warnings vsys1
Security Policy:
- Rule 'Rule A' shadows rule 'Rule B'
- Rule 'Rule A' shadows rule 'Rule C'
(Module: device)



				Source				Destination		Rule Usage					
	Name	Tags	Type	Zone	Address	User	HIP Profile	Zone	Address	Hit Count	Last Hit	First Hit	Application	Service	Action
1	Rule A	egress	universal	inside	192.168.1.0/24	any	any	outside	any	-	-	-	any	application-default	Allow
2	Rule B	egress	universal	inside	192.168.1.3	any	any	outside	any	-	-	-	dns ftp web-browsing	application-default	Allow
3	Rule C	egress	universal	inside	192.168.1.3	any	any	outside	any	-	-	-	any	any	Deny
4	Rule D	internal dmz	universal	outside	any	any	any	any	any	-	-	-	any	any	Deny

In the example, the IP address 192.168.1.3 belongs to the Inside zone and the subnet 192.168.1.0/24. Because the firewall does a Security policy lookup from top to bottom, all traffic from IP address 192.168.1.3 matches “Rule A.” Although the traffic from 192.168.1.3 also matches “Rule B” and “Rule C,” these rules will not be used because “Rule A” matches first. This behavior between Security policy rules is called shadowing because “Rule A” casts a shadow over, or hides, rules “Rule B” and “Rule C.”

At a minimum, “Rule B” and “Rule C” should precede “Rule A” to avoid shadowing in this example. “Rule A” also could be removed and replaced by another, better-defined rule.

The **Commit Status** window warns when one rule shadows one or more other rules. Use the information provided in the **Commit Status** window to reorder or modify the rules to remove shadowing.

Security policy fundamental concepts

Security policy administration

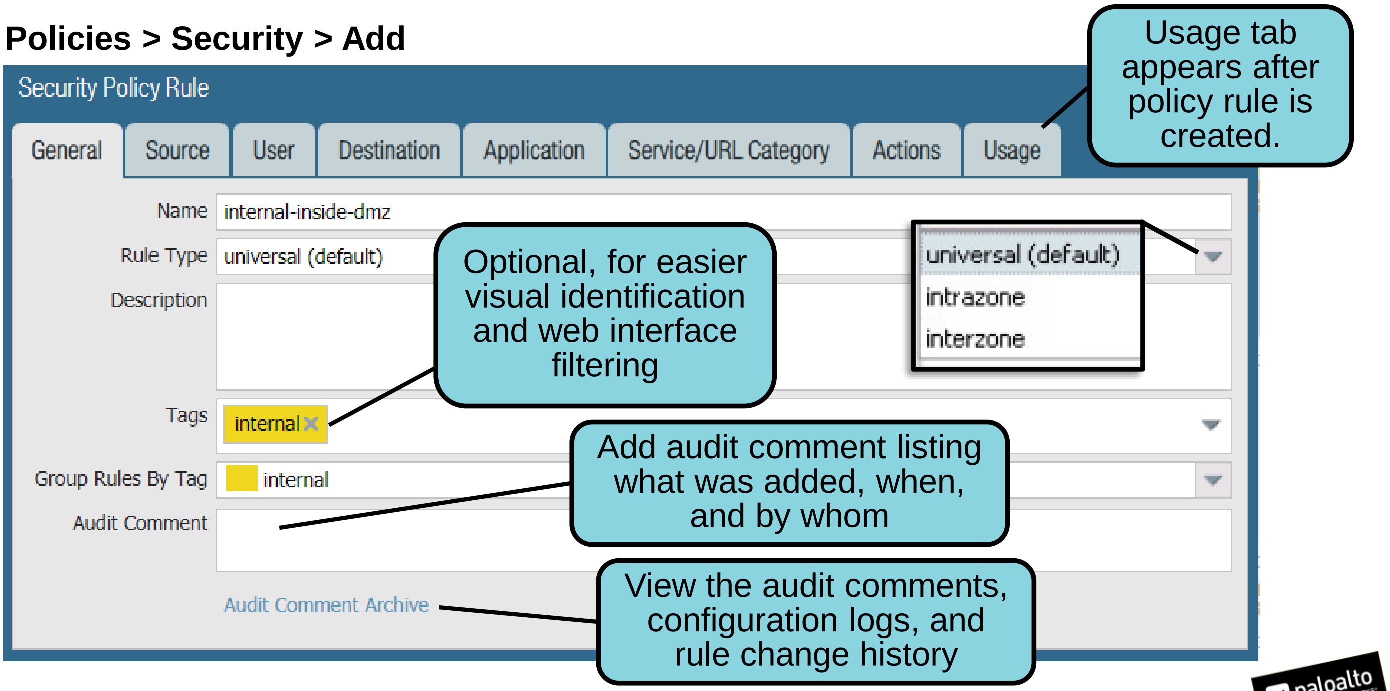
Network address translation

Source NAT configuration

Destination NAT configuration

Creating Security Policy Rules: General Tab

Policies > Security > Add



Name: internal-inside-dmz

Rule Type: universal (default)

Tags: internal

Group Rules By Tag: internal

Usage tab appears after policy rule is created.

Optional, for easier visual identification and web interface filtering

Add audit comment listing what was added, when, and by whom

View the audit comments, configuration logs, and rule change history

14 | © 2019 Palo Alto Networks, Inc.

To create a new Security policy rule, browse to **Policies** > **Security** and click **Add**. The **Security Policy Rule** window has eight tabs that enable you to configure or modify a Security policy rule. 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, numbers, 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.

Optionally, enter a **Description** that describes the purpose or operation of the rule.

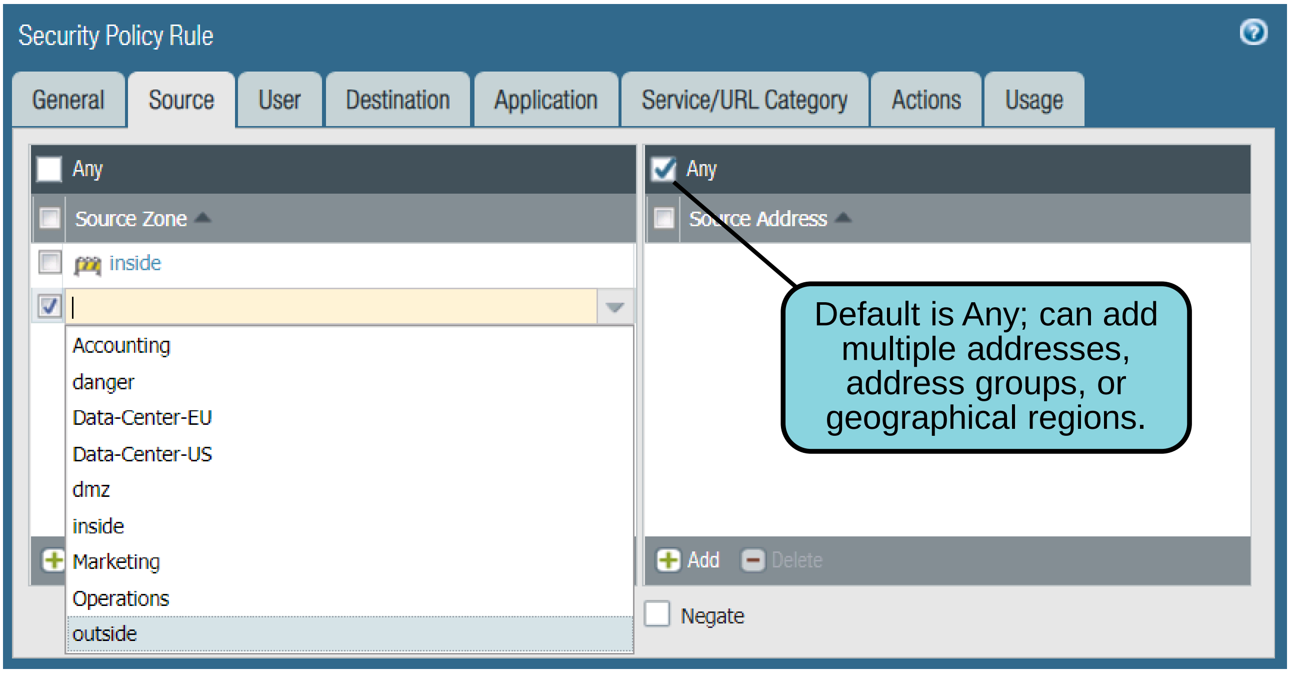
Optionally, create or select a tag. A policy tag is a keyword or phrase that enables you to visually or programmatically sort or filter policy rules. The ability to filter rules is useful when you have defined many rules and want to view only those that are tagged with a particular keyword. For example, 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 specific types of addresses, zones, or services. Tag creation is described later in this module.

Audit Comments can be added to a Security Policy Rule to provide a complete audit history of a Security Policy rule. Comments can include why a rule was created or what was added to a policy rule, when the changes were made, and by whom. An Audit Comment can help provide the information required to maintain regulatory compliance.

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

Creating Security Policy Rules: Source Tab



Default is Any; can add multiple addresses, address groups, or geographical regions.

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

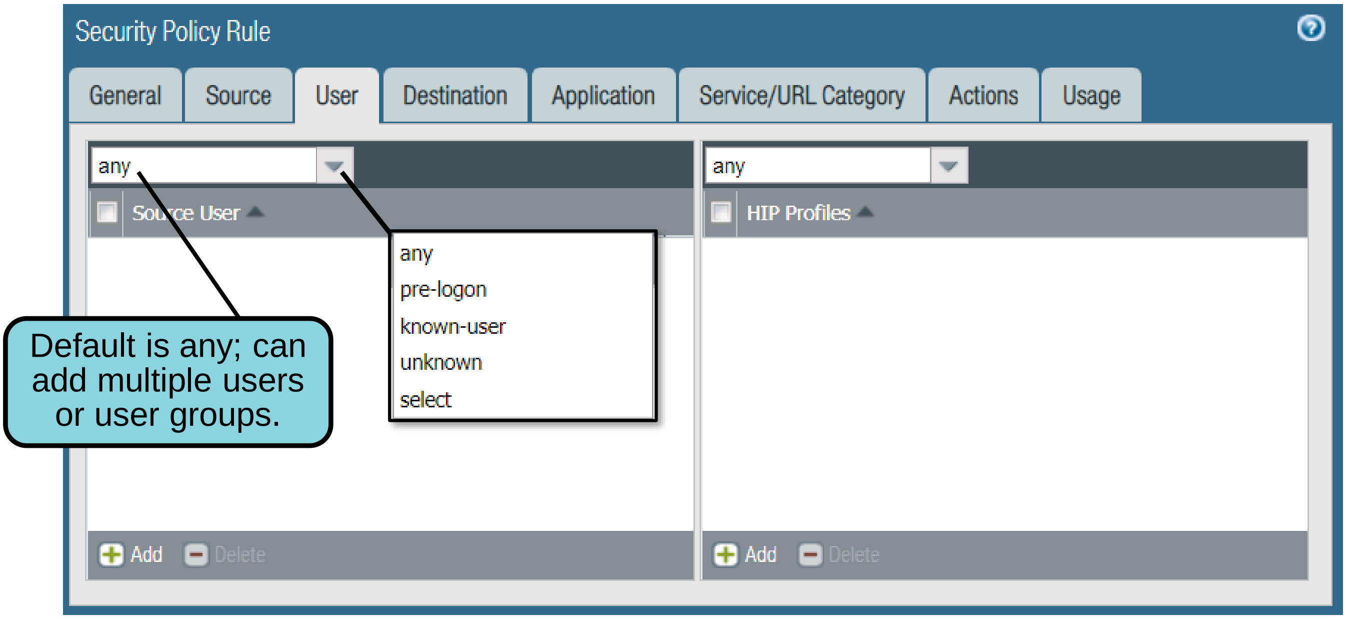
The default source zone is Any. You can select one or more source zones for a rule. Multiple zones are used to simplify policy management. For example, if you have three different internal source zones that all should have access to the same destination zone, you can create a single rule to cover all 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 creation of Address objects that encompass multiple addresses is described later in this module.

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 that are not in the network 201.10.10.0/24.

Creating Security Policy Rules: User Tab

- The User-ID feature is mandatory to use source user as a match criterion.



Default is any; can add multiple users or user groups.

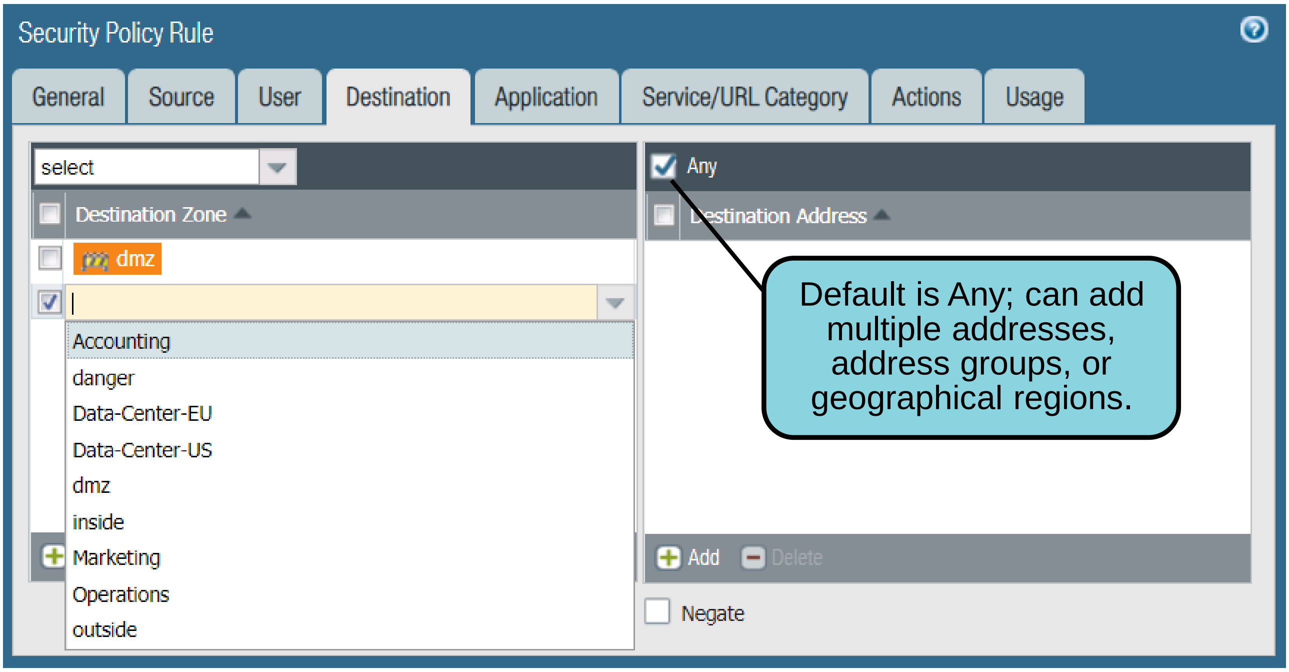
Click the **User** tab to add, display, or modify the source user and HIP Profile match criteria for a rule. Before you can use source users or groups, you must enable the User-ID feature that maps IP addresses to usernames. The firewall can use locally defined user and group information or it can acquire user and group information from a distributed service such as LDAP or RADIUS.

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 that are connected to the network using GlobalProtect, but are 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, 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 that are not mapped to a user by User-ID. For example, you could use “unknown” to match a host where no user has logged in and yet the host needs network access to perform a Microsoft update.
- select: Selected users or groups that have been added using the **Add** link. For example, you might want to add one or more specific users or user groups.

The default for HIP Profiles is any. A HIP Profile defines a collection of machine attributes. The addition of a HIP Profile to a Security policy rule enables you to define the characteristics that a machine must possess before it is allowed to connect to network resources. For example, a HIP Profile enables you to collect information about the security status of your end hosts, such as whether they have the latest security patches, whether they have encrypted disks, or whether they have a particular vendor’s latest antivirus definitions installed.

Creating Security Policy Rules: Destination Tab



Default is Any; can add multiple addresses, address groups, or geographical regions.

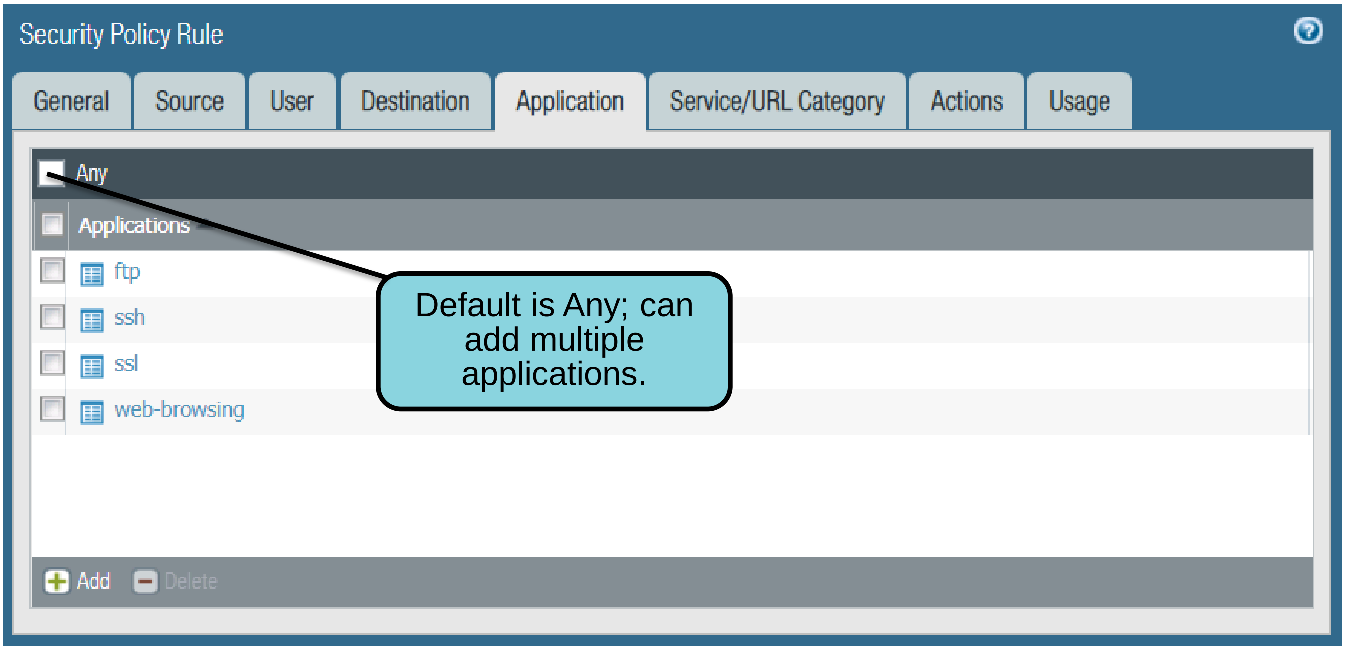
Click the **Destination** tab to add, display, or modify the destination zone and destination address match criteria for a rule.

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 that should have access to 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. All these choices are available when you click **Add**. We describe creation of Address objects that include multiple IP addresses later in this module.

The **Negate** option enables you to specify addresses, address ranges, and 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 that are not in the network 212.45.1.0/24.

Creating Security Policy Rules: Application Tab

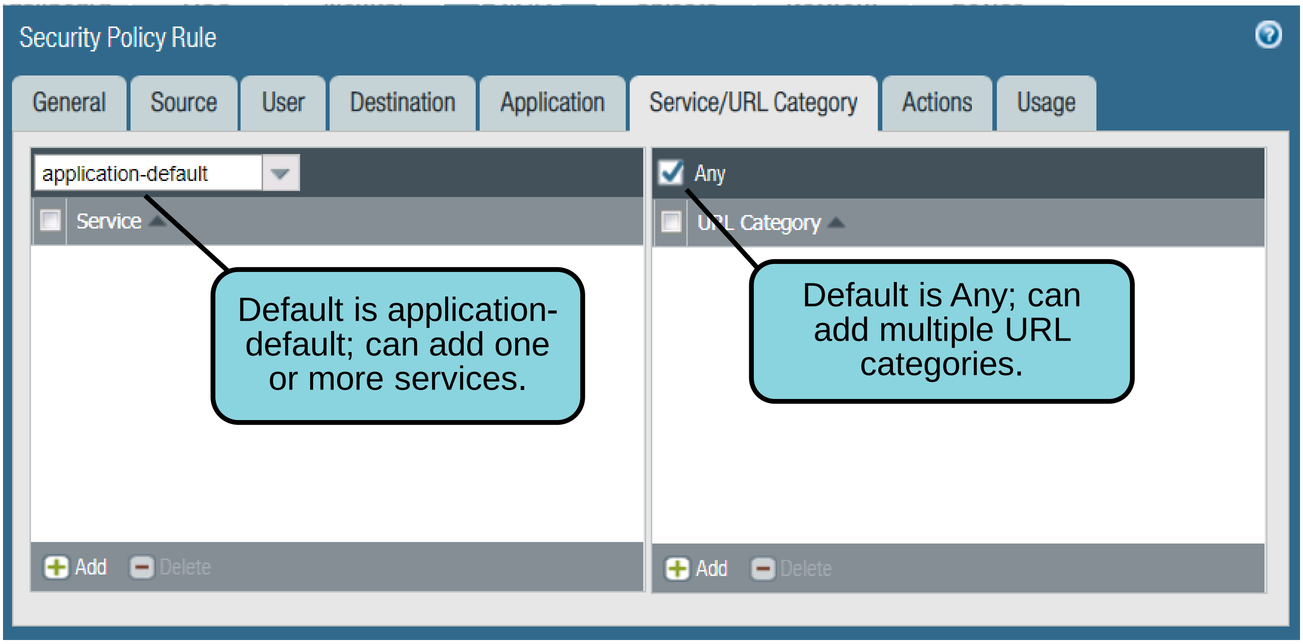


Default is Any; can add multiple applications.

Click the **Application** tab to add, display, or modify the applications to use as match criteria for the rule. Click **Add** to add specific applications.

If an application has multiple functions, you can select the overall parent application or individual child functions. If you select 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 other facebook functions. Alternatively, you can explicitly select only specific functions, which would disallow the application’s non-selected functions.

Creating Security Policy Rules: Service/URL Category Tab



Default is application-default; can add one or more services.

Default is Any; can add multiple URL categories.

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

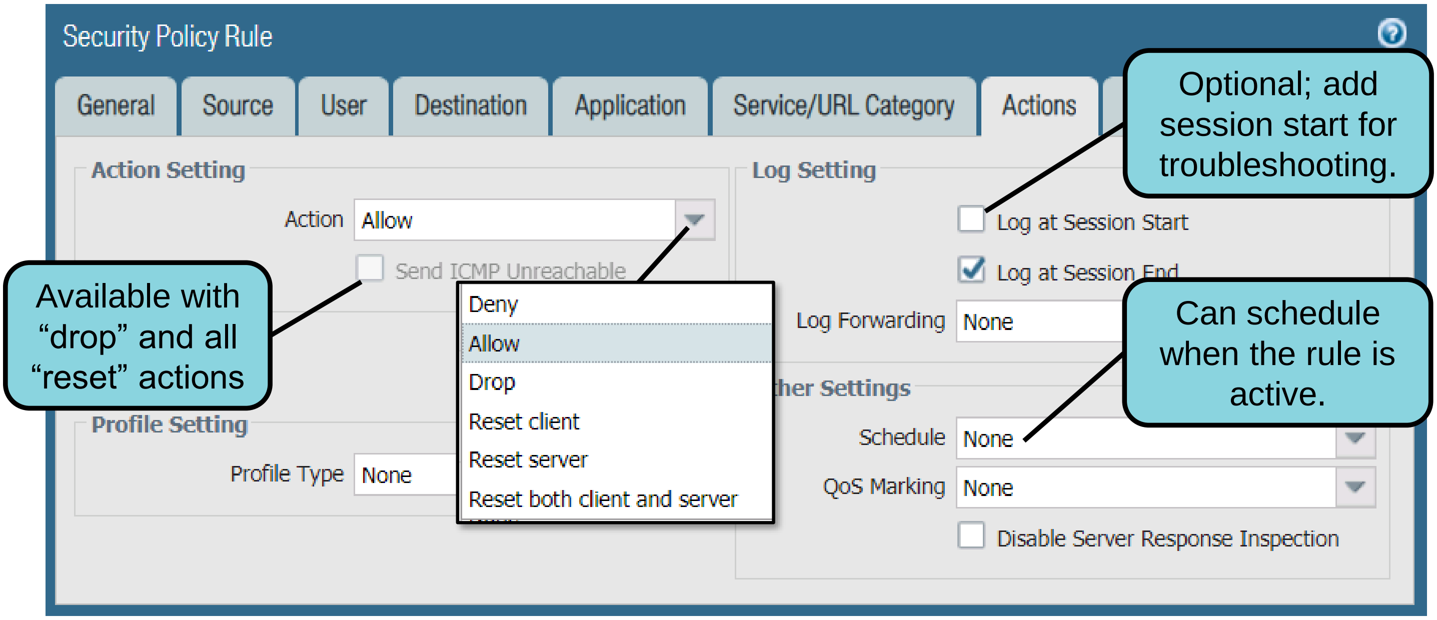
The Service drop-down list has these three choices:

- 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 on only their default protocol ports as predefined in the Palo Alto Networks application-ID database. To display application information, browse to **Objects** > **Applications**. The application-default option is recommended when a policy rule allows a connection because it prevents applications from running on unusual ports and protocols. Unusual ports and protocols can be a sign of malicious application behavior and use. Note that, 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 dozens of topic categories such as alcohol-and-tobacco, auctions, and business-and-economy. A firewall that has a valid URL Filtering license can access this database and use URL categories as part of a Security policy rule.

URL filtering is described in more detail in another module.

Creating Security Policy Rules: Actions Settings



Security Policy Rule

General | Source | User | Destination | Application | Service/URL Category | Actions

Action Setting

Action: Allow

□ Send ICMP Unreachable

Deny
Allow
Drop
Reset client
Reset server
Reset both client and server

Profile Setting

Profile Type: None

Log Setting

□ Log at Session Start

☑ Log at Session End

Log Forwarding: None

Other Settings

Schedule: None

QoS Marking: None

□ Disable Server Response Inspection

Optional; add session start for troubleshooting.

Available with “drop” and all “reset” actions

Can schedule when the rule is active.

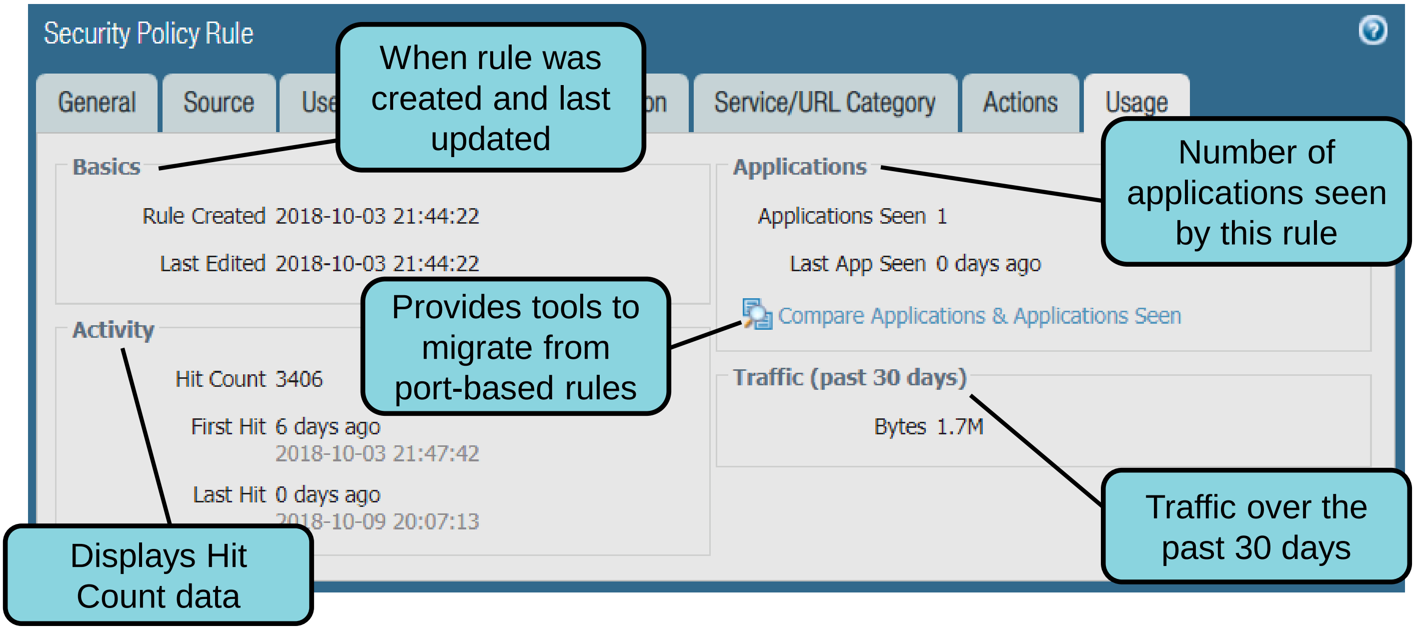
Click the **Action** tab to display or modify the actions taken on matched traffic:

- 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. To send an ICMP unreachable response to the client, select the **Send ICMP Unreachable** check box.
- Reset client: Sends TCP reset to the client (traffic initiator) device. To send an ICMP unreachable response to the client, select the **Send ICMP Unreachable** check box.
- Reset server: Sends TCP reset to the server (traffic responder) device. To send an ICMP unreachable response to the client, select the **Send ICMP Unreachable** check box.
- Reset both client and server: Sends TCP reset to both the client and server devices. To send an ICMP unreachable response to the client, select the **Send ICMP Unreachable** check box.

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 behave improperly. 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, which normally is done only in the short term for troubleshooting purposes. Addition of logging at session start captures 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 additional storage space required for the log entries.

Creating Security Policy Rules: Usage Settings



Basics

Rule Created 2018-10-03 21:44:22

Last Edited 2018-10-03 21:44:22

Activity

Hit Count 3406

First Hit 6 days ago 2018-10-03 21:47:42

Last Hit 0 days ago 2018-10-09 20:07:13

Applications

Applications Seen 1

Last App Seen 0 days ago

Compare Applications & Applications Seen

Traffic (past 30 days)

Bytes 1.7M

When rule was created and last updated

Number of applications seen by this rule

Provides tools to migrate from port-based rules

Traffic over the past 30 days

Displays Hit Count data

Click the **Usage** tab to display the rule’s usage.

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.

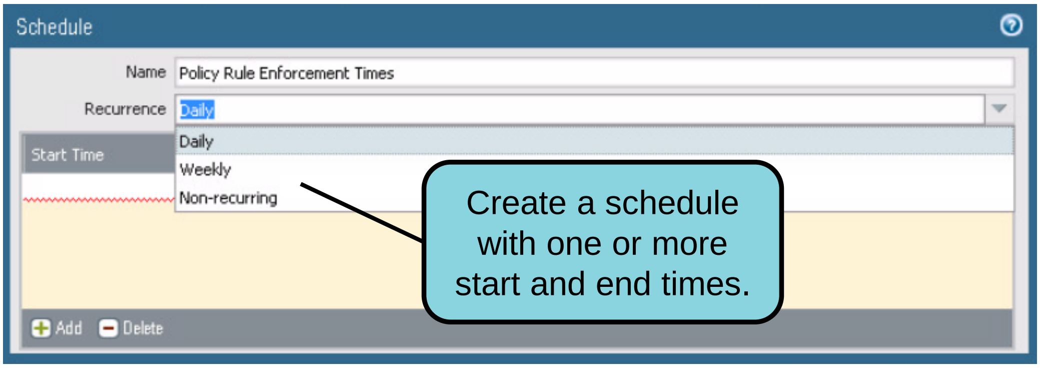
The **Applications** section displays the number of applications that were seen by this rule. Click the **Compare Applications & Applications Seen** link to access tools that can help you migrate from port-based Security policy rules to application-based Security policy rules.

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

Scheduling 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



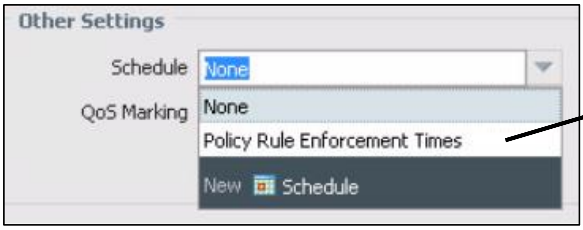
Schedule

Name: Policy Rule Enforcement Times

Recurrence: Daily

Create a schedule with one or more start and end times.

Policies > Security > <select_rule> > Actions



Other Settings

Schedule: None

Apply schedule to a rule.

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**.

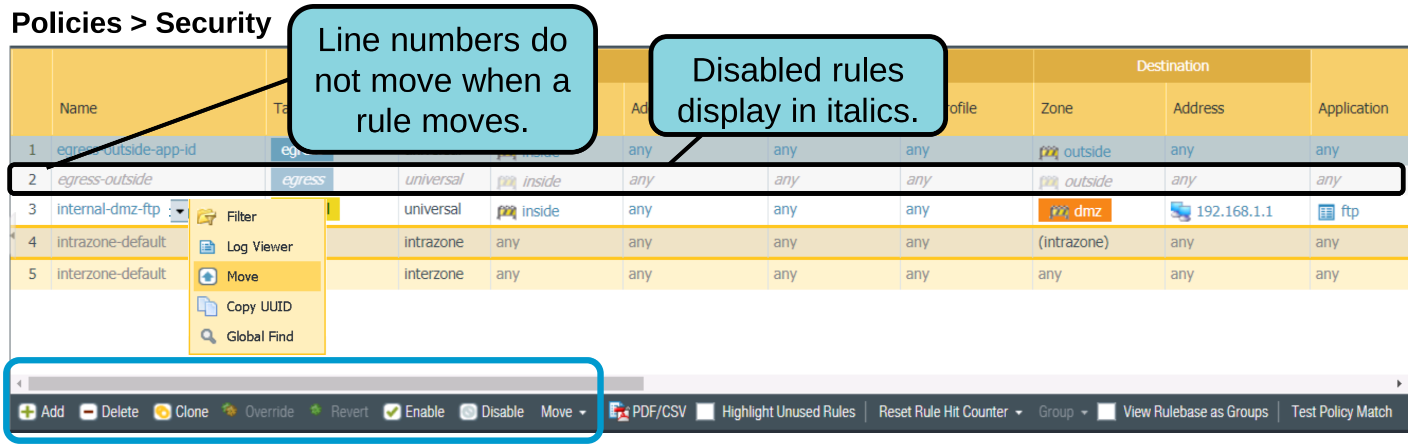
The firewall scheduler supports a daily schedule with multiple start and end times. It also supports a day-of-the-week schedule for those situations where a scheduled change should not occur every day of the week. You still can specify multiple start and end times to any scheduled day of the week. The 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 you have defined 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.

Managing the Policy Ruleset

Policies > Security



			Destination		
	Name	Ta	Zone	Address	Application
1	egress-outside-app-id	eg	outside	any	any
2	*egress-outside*	*egress*	*outside*	*any*	*any*
3	internal-dmz-ftp		dmz	192.168.1.1	ftp
4	intrazone-default		(intrazone)	any	any
5	interzone-default		any	any	any

Name			Ad		ofile
egress-outside-app-id			any	any	any
egress-outside	*universal*	*inside*	*any*	*any*	*any*
internal-dmz-ftp	universal	inside	any	any	any
intrazone-default	intrazone	any	any	any	any
interzone-default	interzone	any	any	any	any

- **Add**, **Delete**, **Clone**, **Override**, **Revert**, **Enable**, **Disable**, **Move** options
- Rules can be re-ordered to match requirements (use **Move** or drag-and-drop).
- Disablement of a rule allows you to retain the entry while making it non-operative.

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 tool bar below the rules helps you to manage the rules and enables you to perform actions on your rules.

To add a new 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**.

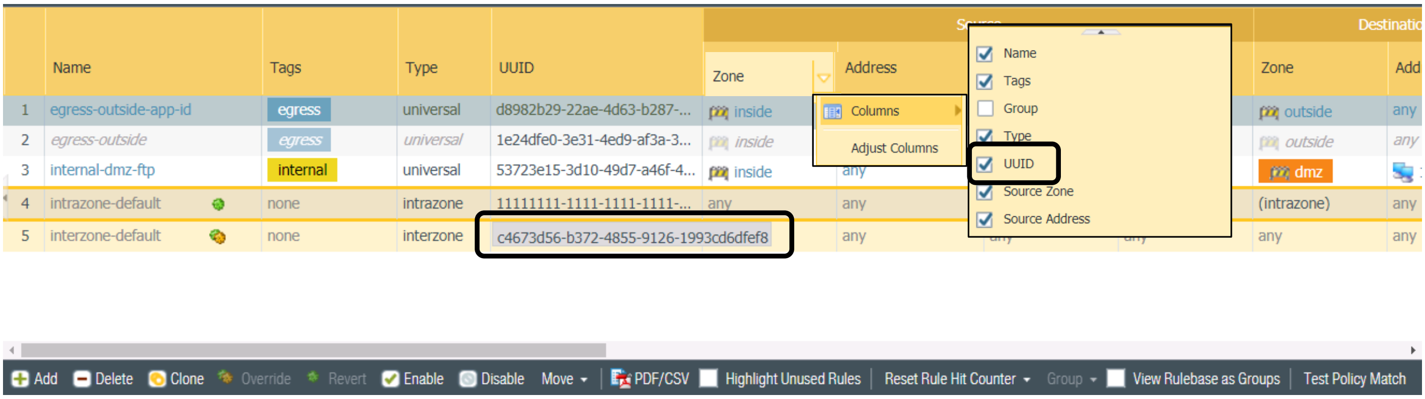
To modify an implicit intrazone-default or interzone-default rule, select it and click **Override**. To revert it to its original state, click **Revert**.

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

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

Universally Unique Identifiers (UUIDs)

Policies > Security



					Source		Destination	
	Name	Tags	Type	UUID	Zone	Address	Zone	Add
1	egress-outside-app-id	egress	universal	d8982b29-22ae-4d63-b287-...	inside		outside	any
2	*egress-outside*	*egress*	*universal*	1e24dfe0-3e31-4ed9-af3a-3...	*inside*		*outside*	*any*
3	internal-dmz-ftp	internal	universal	53723e15-3d10-49d7-a46f-4...	inside	any	dmz	
4	intrazone-default	none	intrazone	11111111-1111-1111-1111-...	any	any	(intrazone)	any
5	interzone-default	none	interzone	c4673d56-b372-4855-9126-1993cd6dfef8		any	any	any

☑ Name
☑ Tags
□ Group
☑ Type
☑ UUID
☑ Source Zone
☑ Source Address

- Creates a unique identifier for every Security policy rule
- Provides a complete history of a Security policy rule, even if the rule name is changed
- Must add column to display UUIDs

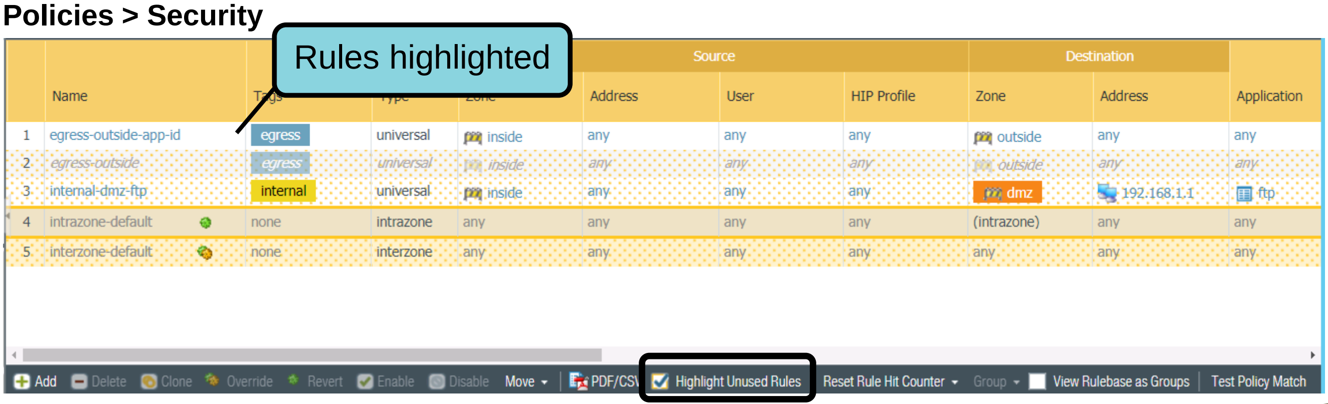
Universally Unique Identifiers, or UUIDs, are created and assigned to a Security policy rule when the rule is created. The UUID helps to provide a complete audit trail that captures the entire operational history of a rule. Historical data can include when a rule was created and who made the most recent change to the rule. Before PAN-OS 9.0, if a rule was renamed, the record of changes for that rule was not retained. Now the firewall can refer to the rule’s UUID to preserve the complete history for the rule, regardless of any operational changes to the rule.

A Security policy rule UUID standardizes the tracking of policy modifications, which makes compliance with regulatory requirements easier to demonstrate. For example, you can include the UUIDs when you export the rulebase to PDF or CSV to present for internal review or audits. Inclusion of the UUID in your reports makes tracking of a rule easier, even if the name of the rule has changed.

Finding Unused Security Policy Rules

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

Policies > Security



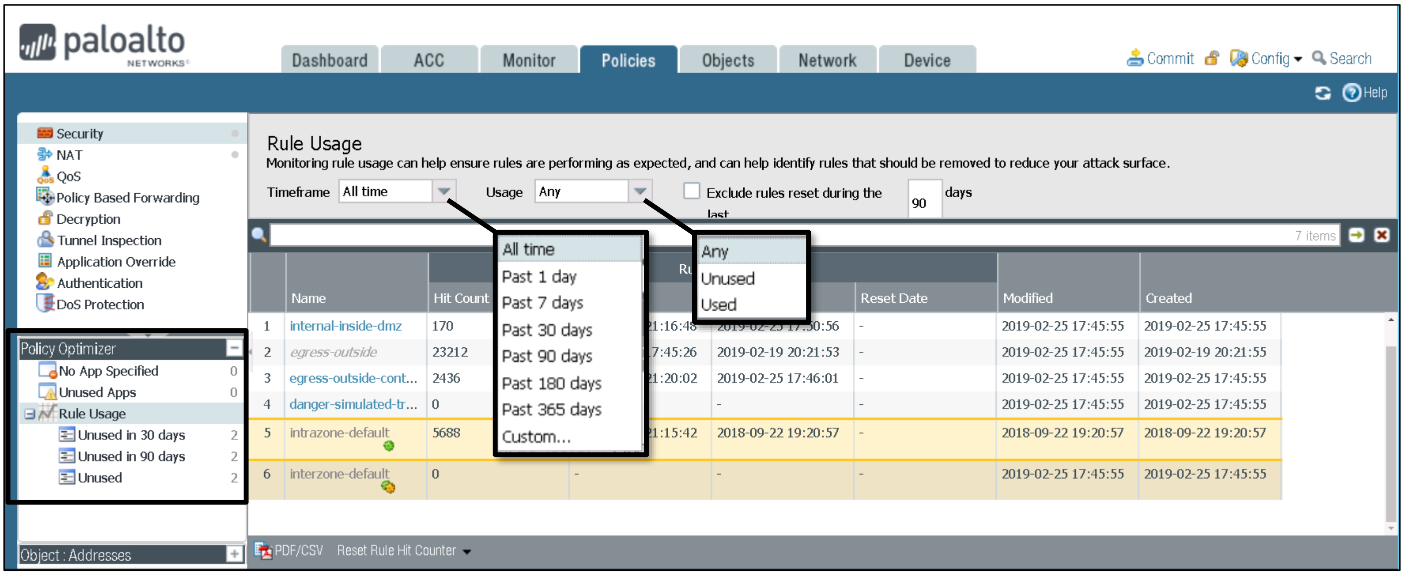
Rules highlighted

	Name	Tags	Type	Source				Destination		Application
				Zone	Address	User	HIP Profile	Zone	Address	
1	egress-outside-app-id	egress	universal	inside	any	any	any	outside	any	any
2	*egress-outside*	*egress*	*universal*	*inside*	*any*	*any*	*any*	*outside*	*any*	*any*
3	internal-dmz-ftp	internal	universal	inside	any	any	any	dmz	192.168.1.1	ftp
4	intrazone-default	none	intrazone	any	any	any	any	(intrazone)	any	any
5	interzone-default	none	interzone	any	any	any	any	any	any	any

Administrators should cull their Security policy rulebase from time to time. You can perform cleanup quickly and easily by using the **Highlight Unused Rules** option, which enables you to see which rules have not matched any traffic since the last restart of the data plane. This option can be used to 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 > Policy Optimizer > Rule Usage



Rule Usage

Monitoring rule usage can help ensure rules are performing as expected, and can help identify rules that should be removed to reduce your attack surface.

Timeframe: All time | Usage: Any | □ Exclude rules reset during the last 90 days

7 items

Timeframe: All time, Past 1 day, Past 7 days, Past 30 days, Past 90 days, Past 180 days, Past 365 days, Custom...

Usage: Any, Unused, Used

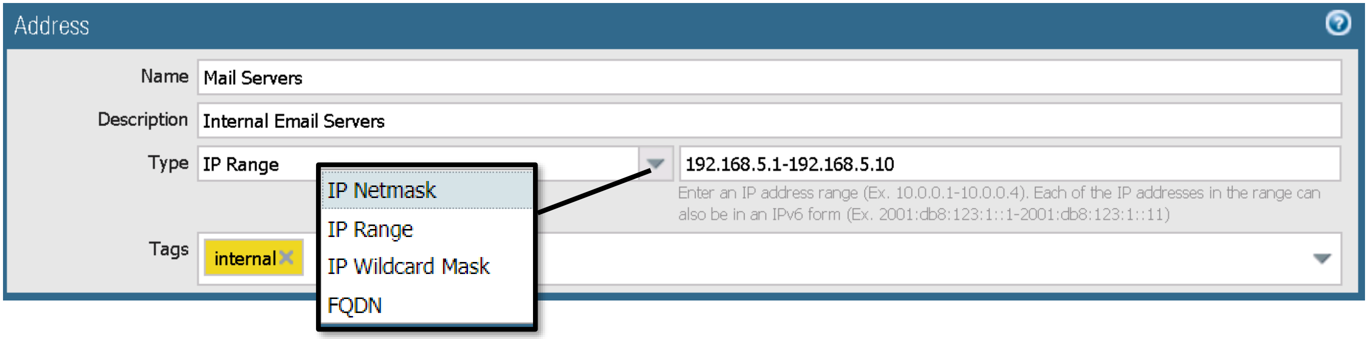
	Name	Hit Count		Ru		Reset Date	Modified	Created
1	internal-inside-dmz	170		1:16:48	2019-02-25 17:50:56	-	2019-02-25 17:45:55	2019-02-25 17:45:55
2	*egress-outside*	23212		7:45:26	2019-02-19 20:21:53	-	2019-02-25 17:45:55	2019-02-19 20:21:55
3	egress-outside-cont...	2436		1:20:02	2019-02-25 17:46:01	-	2019-02-25 17:45:55	2019-02-25 17:45:55
4	danger-simulated-tr...	0			-	-	2019-02-25 17:45:55	2019-02-25 17:45:55
5	intrazone-default	5688		1:15:42	2018-09-22 19:20:57	-	2018-09-22 19:20:57	2018-09-22 19:20:57
6	interzone-default	0		-	-	-	2019-02-25 17:45:55	2019-02-25 17:45:55

If you have overprovisioned access on the firewall, you can be exploited by attacks. Firewall administrators need to periodically check for rules that are out-of-date or unused. In PAN-OS 9.0, the Rule Usage Filter enables 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 management of rule lifecycles if you can find unused rules and then disable or delete the rules to maintain an up-to-date rulebase.

Address Objects

- Represents one or more IP addresses
- Used in policy rule source and destination address fields

Objects > Addresses > Add



Address

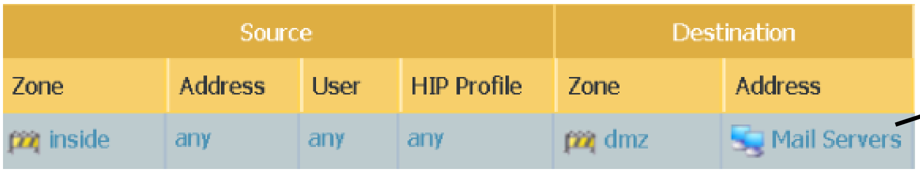
Name: Mail Servers

Description: Internal Email Servers

Type: IP Range — 192.168.5.1-192.168.5.10

Enter an IP address range (Ex. 10.0.0.1-10.0.0.4). Each of the IP addresses in the range can also be in an IPv6 form (Ex. 2001:db8:123:1::1-2001:db8:123:1::11)

Tags: internal



Source				Destination	
Zone	Address	User	HIP Profile	Zone	Address
inside	any	any	any	dmz	Mail Servers

Use new Address object.

An Address object is a name-value pair that can represent a single IP address, a range of IP addresses, an IP subnet, or the fully qualified domain name, or FQDN. You can use an Address object in the source or destination IP address fields in a Security policy. An Address object also can be used in any of the other policy types on a firewall.

Address objects are used to simplify firewall administration by enabling you to create the 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.

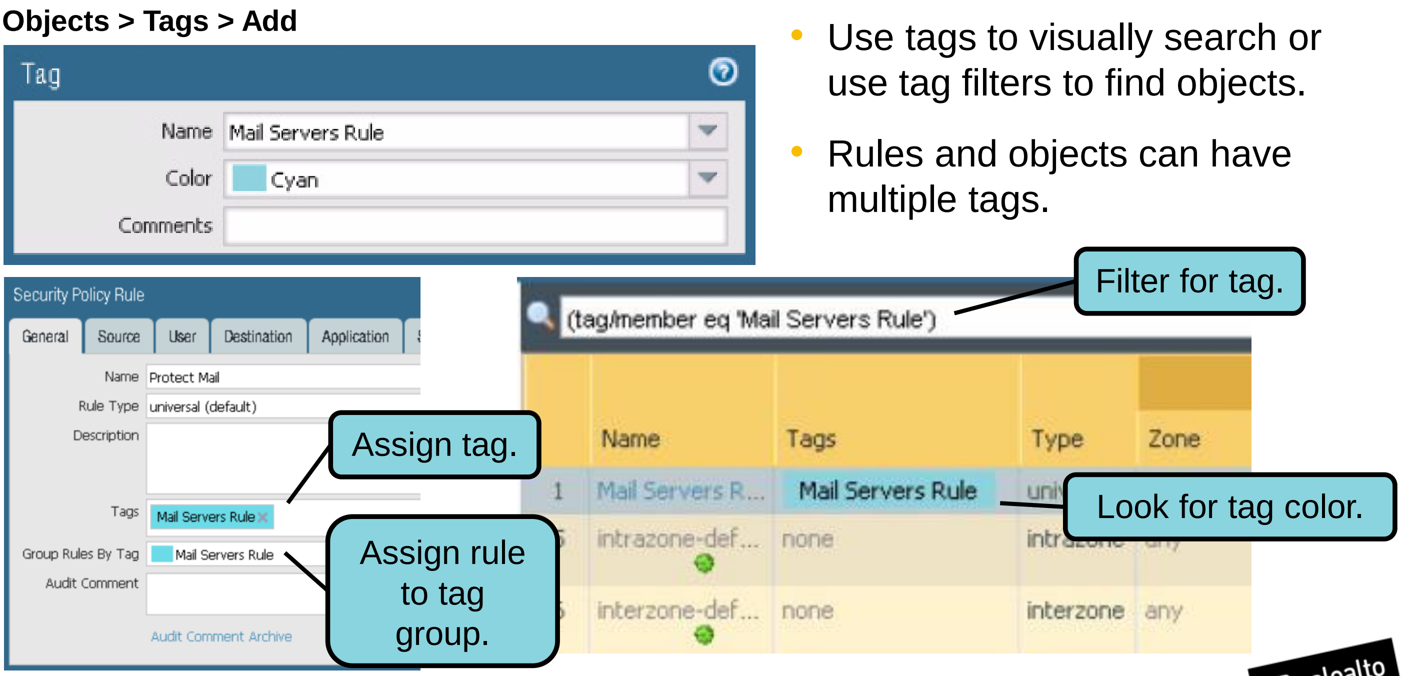
Consider using an Address object in the destination address field to enable access to specific internal servers or groups of servers only, particularly for services such as DNS and SMTP that commonly are exploited. When you restrict users to specific destination server addresses, you can prevent data exfiltration and command-and-control traffic from establishing communication through techniques such as DNS tunneling.

To create an Address object, browse to **Objects** > **Addresses** and click **Add**. The four types of Address objects are:

- IP Netmask: Specifies a single IP address (192.168.1.1) or an IP subnet (192.168.1.0/24)
- IP Range: Specifies a range of IP addresses (192.168.1.1 to 192.168.1.10)
- IP Wildcard Mask: Specifies an IP address and wildcard mask (192.168.1.1/0.0.2.255)
- FQDN: Specifies a fully qualified domain name (hostA.west.paloaltonetworks.com)

For Address objects containing only FQDNs, the list of FQDNs can be changed without the need to recommit the firewall configuration. The FQDNs are resolved by the firewall and are refreshed after their DNS time-to-live value has expired.

Tags



Objects > Tags > Add

Tag

Name: Mail Servers Rule

Color: Cyan

Comments:

Security Policy Rule

Name: Protect Mail

Rule Type: universal (default)

Description:

Tags: Mail Servers Rule

Group Rules By Tag: Mail Servers Rule

Audit Comment:

(tag/member eq 'Mail Servers Rule')

	Name	Tags	Type	Zone
1	Mail Servers R...	Mail Servers Rule	uni	
	intrazone-def...	none	intr	
	interzone-def...	none	interzone	any

- Use tags to visually search or use tag filters to find objects.
- Rules and objects can have multiple tags.

Tags enable you to group objects using keywords or phrases. Tags can be assigned a color, which makes 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.

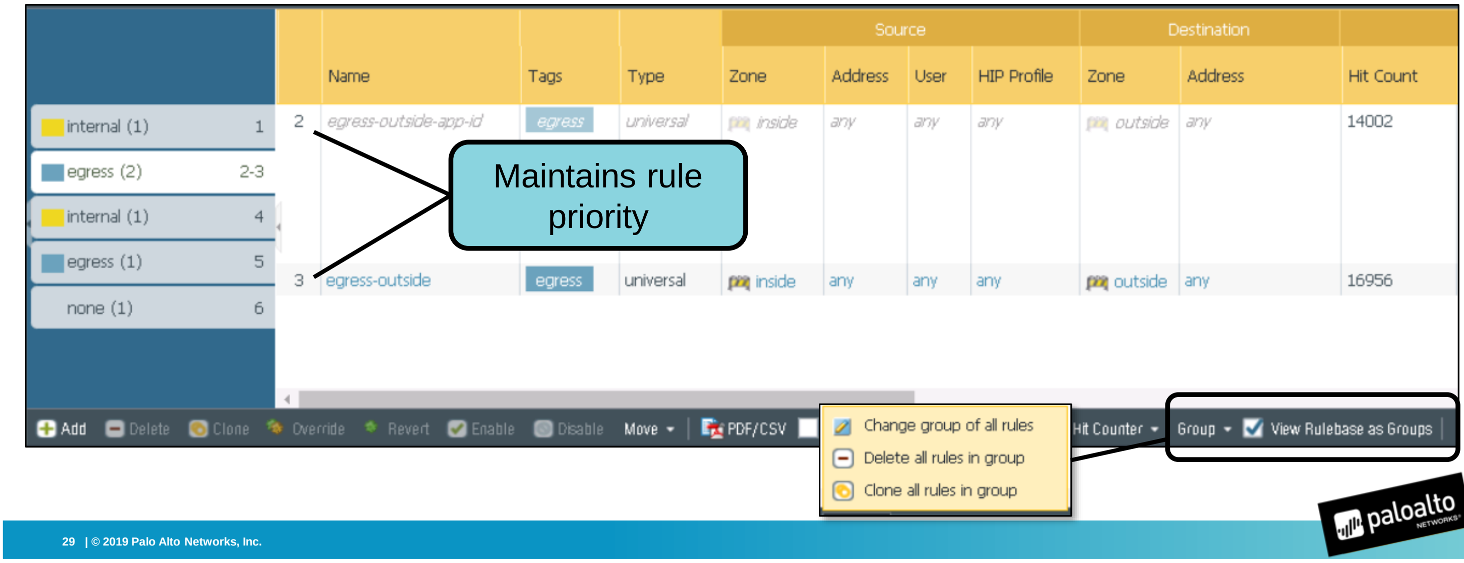
To create a tag, browse to **Objects** > **Tags** and click **Add**. Provide a descriptive **Name** for the tag based on it purpose. Tags enable you to choose a **Color** and add **Comments** that describe the tag.

With the release of PAN-OS 9.0, you can require that all of your Security policies have a tag assigned to them. To require that tags be assigned to your Security policies, browse to **Device** > **Setup** > **Management** and select the **Require Tag on 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 groups rules based on tagging structure
- Can perform operational procedures within the selected tag group

Policies > Security



🟨 internal (1)	1
🟦 egress (2)	2-3
🟨 internal (1)	4
🟦 egress (1)	5
none (1)	6

				Source				Destination		
	Name	Tags	Type	Zone	Address	User	HIP Profile	Zone	Address	Hit Count
2	egress-outside-app-id	egress	universal	inside	any	any	any	outside	any	14002
3	egress-outside	egress	universal	inside	any	any	any	outside	any	16956

Maintains rule priority

PAN-OS 9.0 replaces the tag browser with the ability 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.

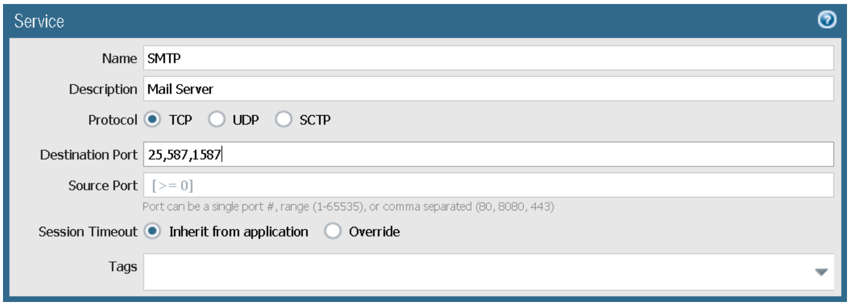
Rule tag groups are displayed in the same order as the rules in the rulebase. As a result, a single tag group may appear multiple times throughout the rulebase to visually preserve the rule hierarchy. However, all rule operations are applied to all rules in the same tag group, regardless of their positioning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

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

Creating a New Service Definition

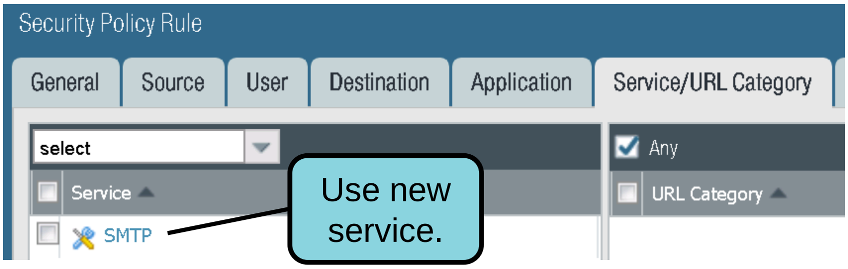
- Service definitions are assigned ports.
- Services limit ports that applications can use.
- service-http and service-https are the only predefined services.

Objects > Services > Add



Service

Name: SMTP
Description: Mail Server
Protocol: ● TCP ○ UDP ○ SCTP
Destination Port: 25,587,1587
Source Port: [>= 0]
Port can be a single port #, range (1-65535), or comma separated (80, 8080, 443)
Session Timeout: ● Inherit from application ○ Override
Tags:



☑ Any

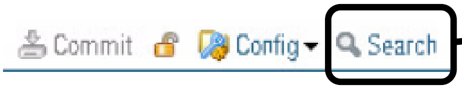
□ SMTP

Use new service.

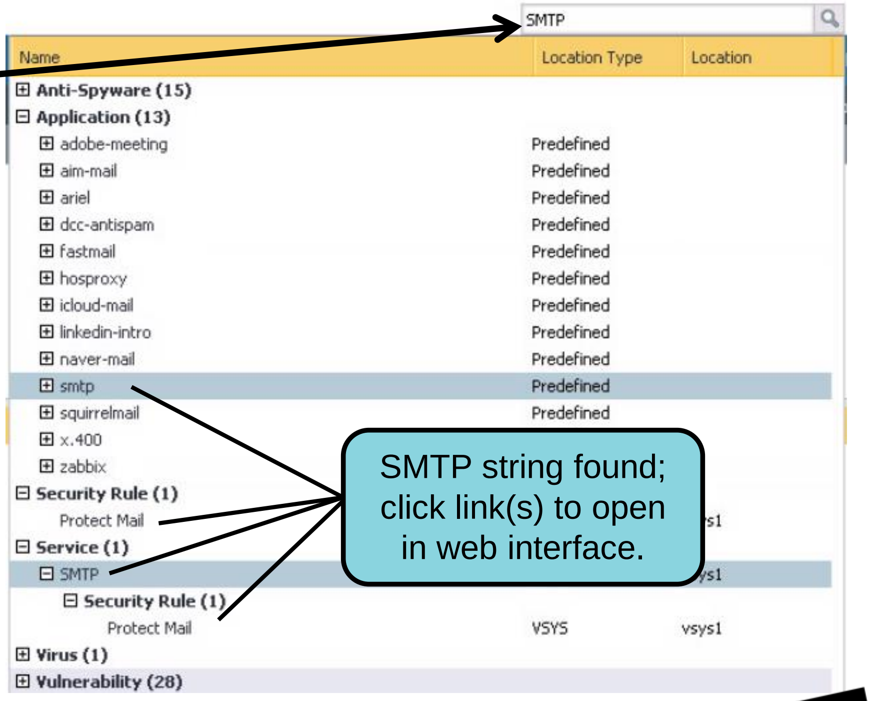
When you define Security policy rules for specific applications, you can select one or more services to limit the port numbers that the applications can use. The default port for services in Security policy rules is any, which enables an application to use any TCP or UDP port. The only predefined service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

To create a new 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 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 specify a tag.

Using Global Find



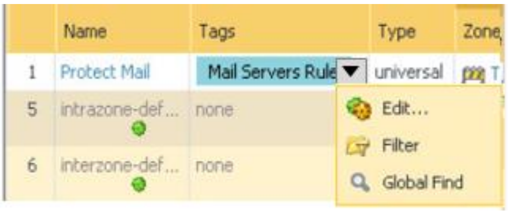
- Search candidate configuration and content databases for occurrences of a string
- Launch from Search or Context menu



SMTP

Name	Location Type	Location
⊞ **Anti-Spyware (15)**		
⊟ **Application (13)**		
⊞ adobe-meeting	Predefined	
⊞ aim-mail	Predefined	
⊞ ariel	Predefined	
⊞ dcc-antispam	Predefined	
⊞ fastmail	Predefined	
⊞ hosproxy	Predefined	
⊞ icloud-mail	Predefined	
⊞ linkedin-intro	Predefined	
⊞ naver-mail	Predefined	
⊞ smtp	Predefined	
⊞ squirrelmail	Predefined	
⊞ x.400		
⊞ zabbix		
⊟ **Security Rule (1)**		
Protect Mail		s1
⊟ **Service (1)**		
⊟ SMTP		ys1
⊟ **Security Rule (1)**		
Protect Mail	VSYS	vsys1
⊞ **Virus (1)**		
⊞ **Vulnerability (28)**		

SMTP string found; click link(s) to open in web interface.



	Name	Tags	Type	Zone
1	Protect Mail	Mail Servers Rule	universal	T
5	intrazone-def...	none		
6	interzone-def...	none		

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 from 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 to identify other objects that depend on or make reference to the search string. For example, if you are deprecating an application, enter the application name in Global Find to locate all instances of the application and then click each instance to navigate to the configuration location and make the necessary changes.

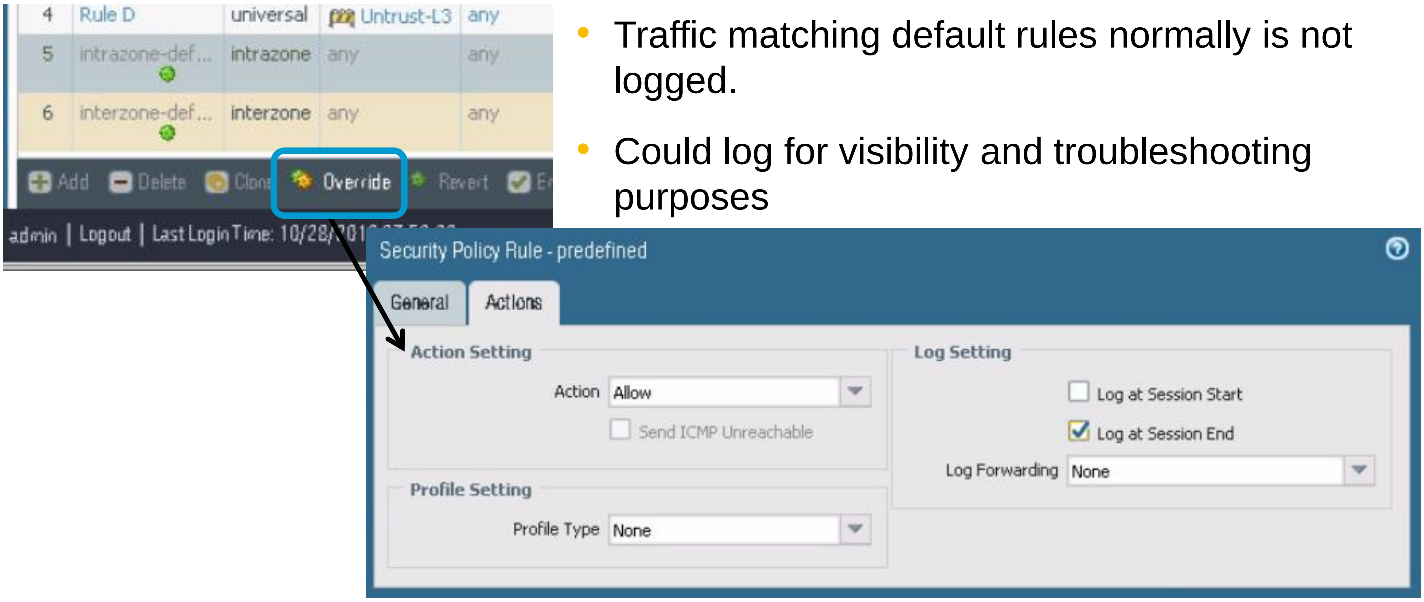
Global Find will not search dynamic content such as logs, address ranges, or allocated DHCP addresses. Global Find also does not search for individual username or group names identified by User-ID unless the user or group is defined in a policy. In general, you can search only content that the firewall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

Example use cases for the Global Find feature are:

- Find all objects with a given tag
- See 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 user group
- See 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 a report query
- Find a ticket number that was added to a comment in a policy or on another object

Enabling Intrazone and Interzone Logging

Policies > Security > <select_default_rule>



4	Rule D	universal	Untrust-L3	any
5	intrazone-def...	intrazone	any	any
6	interzone-def...	interzone	any	any

Security Policy Rule - predefined

Action Setting

Action: Allow

□ Send ICMP Unreachable

Profile Setting

Profile Type: None

Log Setting

□ Log at Session Start

☑ Log at Session End

Log Forwarding: None

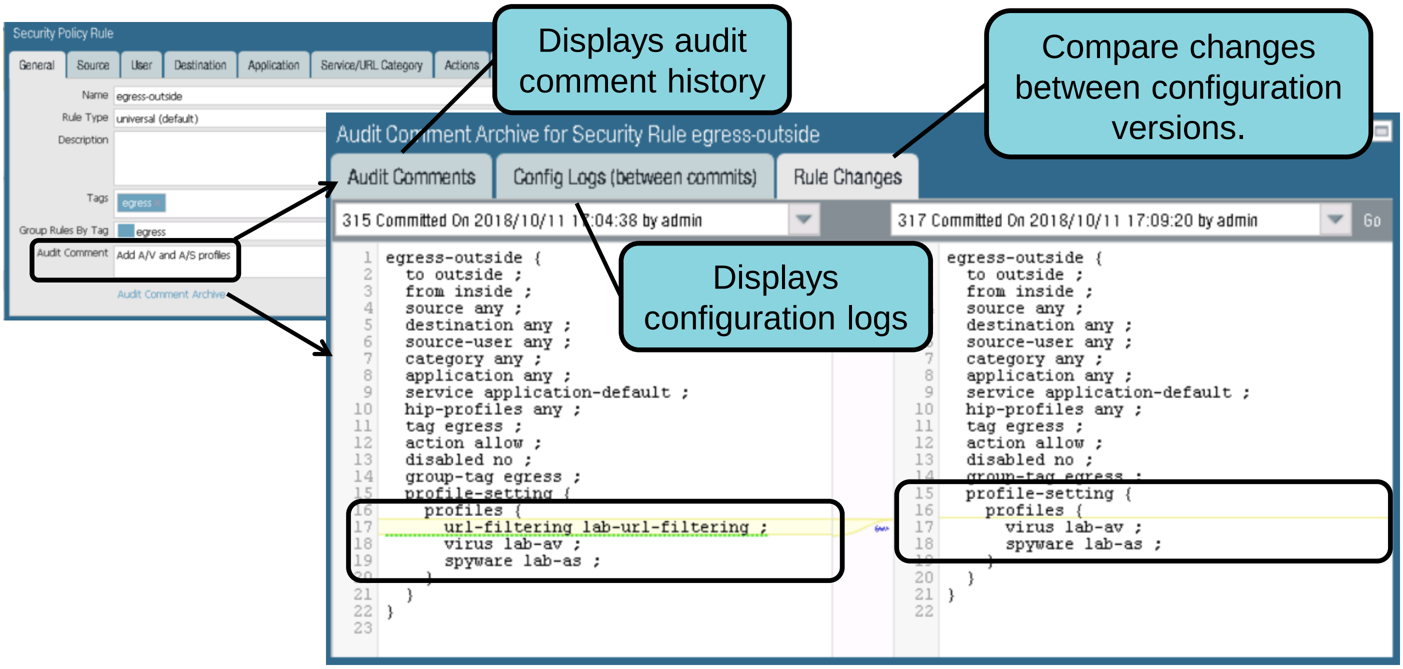
- Traffic matching default rules normally is not logged.
- Could log for visibility and troubleshooting purposes

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.

To configure logging on the implicit rules, select a rule and click **Override**. 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.

Rule Changes Archive



Displays audit comment history

Compare changes between configuration versions.

Displays configuration logs

Name: egress-outside
Rule Type: universal (default)
Description:
Tags: egress
Group Rules By Tag: egress
Audit Comment: Add A/V and A/S profiles

Audit Comment Archive
Audit Comment Archive for Security Rule egress-outside
Audit Comments
Config Logs (between commits)
Rule Changes
Go

315 Committed On 2018/10/11 17:04:38 by admin

```
egress-outside {
  to outside ;
  from inside ;
  source any ;
  destination any ;
  source-user any ;
  category any ;
  application any ;
  service application-default ;
  hip-profiles any ;
  tag egress ;
  action allow ;
  disabled no ;
  group-tag egress ;
  profile-setting {
    profiles {
      url-filtering lab-url-filtering ;
      virus lab-av ;
      spyware lab-as ;
    }
  }
}
```

317 Committed On 2018/10/11 17:09:20 by admin

```
egress-outside {
  to outside ;
  from inside ;
  source any ;
  destination any ;
  source-user any ;
  category any ;
  application any ;
  service application-default ;
  hip-profiles any ;
  tag egress ;
  action allow ;
  disabled no ;
  group-tag egress ;
  profile-setting {
    profiles {
      virus lab-av ;
      spyware lab-as ;
    }
  }
}
```

To meet your regulatory compliance requirements, you may need to track all changes that have been made to your Security policy rules. As your rulebase changes, audit information can get lost. With the release of PAN-OS 9.0, the Rule Changes Archive can track all changes made to your Security policy rules. After you select 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, and you can compare configuration versions to see what has changed in your Security policy.

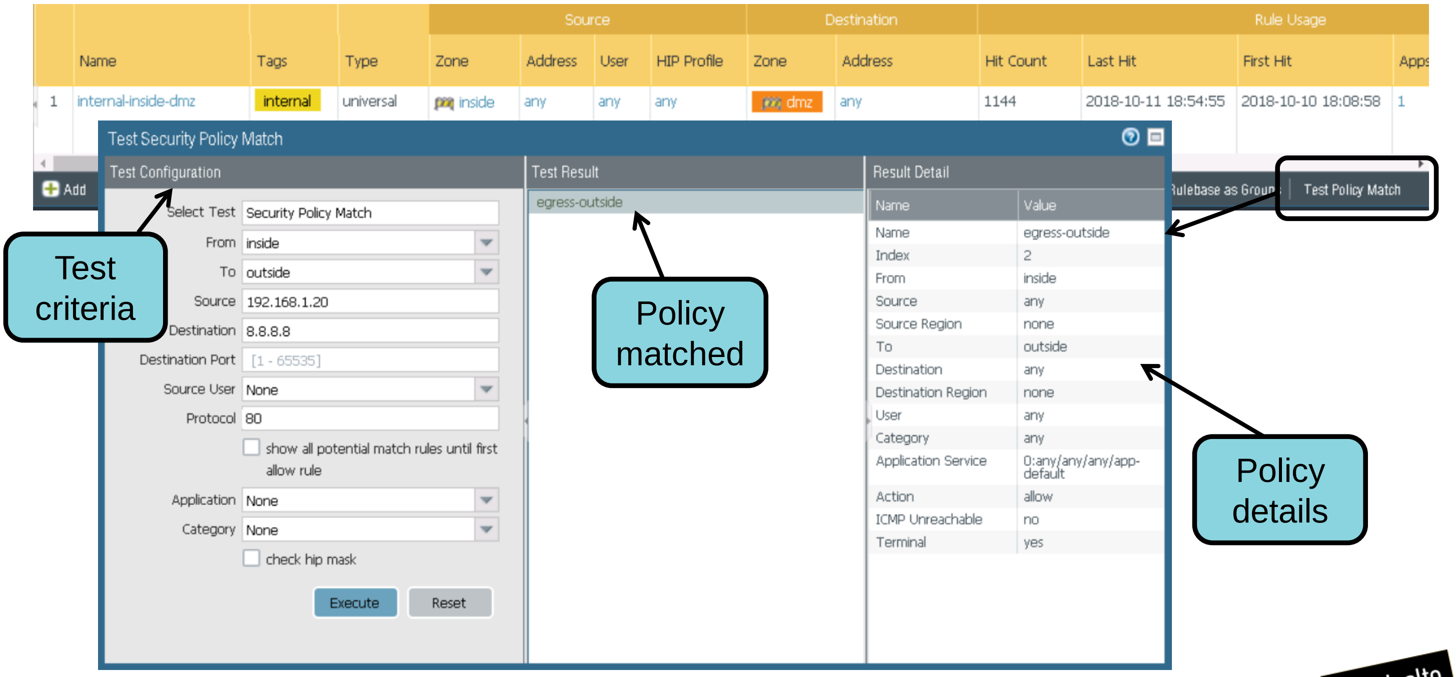
Select the **Audit Comments** tab to display the audit comment history of the selected rule. The audit comment history includes the time the audit comment was committed, the audit comment itself, the administrator who added the audit comment, and the configuration version of the audit comment.

Select the **Config Logs (between commits)** tab to display the configuration logs generated by devices with traffic matches for the policy rule. Config logs can be filtered to display all changes that took place 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.

Test Policy Functionality

Policies > Security



				Source				Destination		Rule Usage			
	Name	Tags	Type	Zone	Address	User	HIP Profile	Zone	Address	Hit Count	Last Hit	First Hit	Apps
1	internal-inside-dmz	internal	universal	inside	any	any	any	dmz	any	1144	2018-10-11 18:54:55	2018-10-10 18:08:58	1

Test Security Policy Match

Test Configuration

Select Test: Security Policy Match
From: inside
To: outside
Source: 192.168.1.20
Destination: 8.8.8.8
Destination Port: [1 - 65535]
Source User: None
Protocol: 80
□ show all potential match rules until first allow rule
Application: None
Category: None
□ check hip mask

Test Result

egress-outside

Result Detail

Name	Value
Name	egress-outside
Index	2
From	inside
Source	any
Source Region	none
To	outside
Destination	any
Destination Region	none
User	any
Category	any
Application Service	0:any/any/any/app-default
Action	allow
ICMP Unreachable	no
Terminal	yes

Test criteria

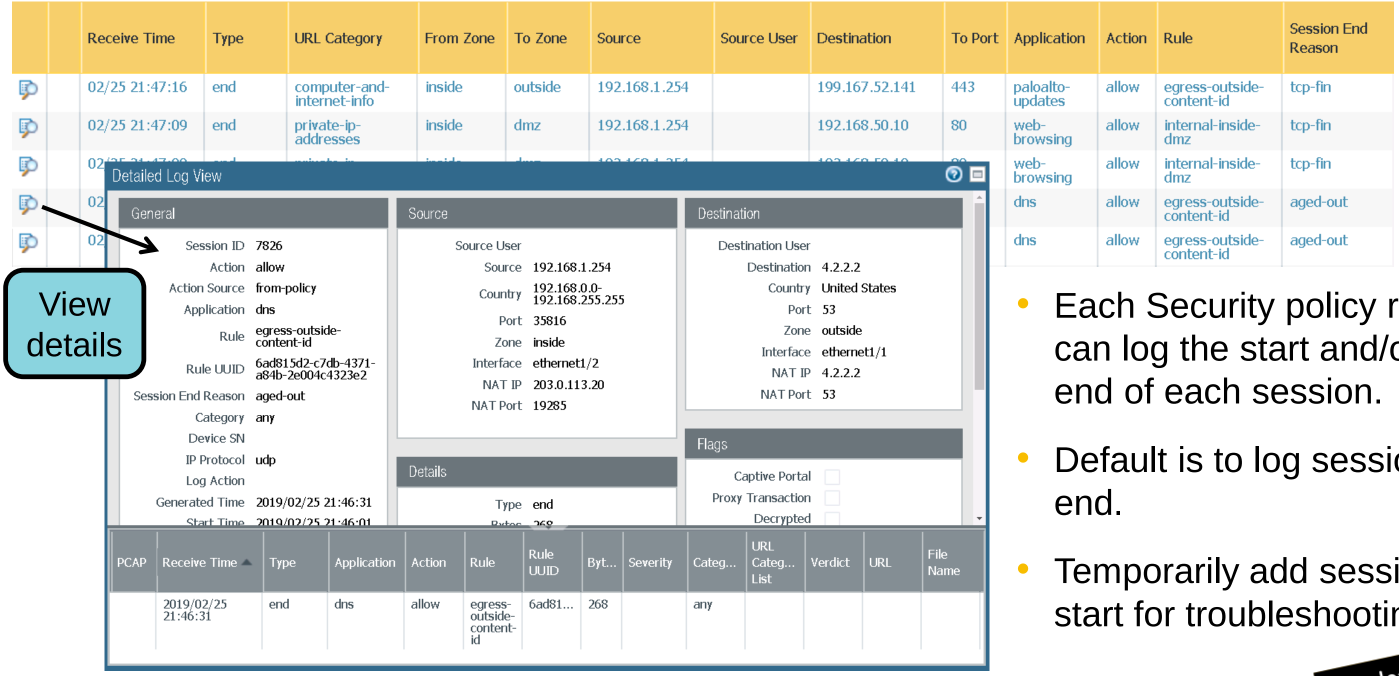
Policy matched

Policy details

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

Viewing the Traffic Log

Monitor > Logs > Traffic



	Receive Time	Type	URL Category	From Zone	To Zone	Source	Source User	Destination	To Port	Application	Action	Rule	Session End Reason
🔍	02/25 21:47:16	end	computer-and-internet-info	inside	outside	192.168.1.254		199.167.52.141	443	paloalto-updates	allow	egress-outside-content-id	tcp-fin
🔍	02/25 21:47:09	end	private-ip-addresses	inside	dmz	192.168.1.254		192.168.50.10	80	web-browsing	allow	internal-inside-dmz	tcp-fin
🔍	02/25 21:47:00	end	private-ip-	inside	dmz	192.168.1.254		192.168.50.10	80	web-browsing	allow	internal-inside-dmz	tcp-fin
🔍	02									dns	allow	egress-outside-content-id	aged-out
🔍	02									dns	allow	egress-outside-content-id	aged-out

View details

Detailed Log View

General

Session ID	7826
Action	allow
Action Source	from-policy
Application	dns
Rule	egress-outside-content-id
Rule UUID	6ad815d2-c7db-4371-a84b-2e004c4323e2
Session End Reason	aged-out
Category	any
Device SN	
IP Protocol	udp
Log Action	
Generated Time	2019/02/25 21:46:31
Start Time	2019/02/25 21:46:01

Source

Source User	
Source	192.168.1.254
Country	192.168.0.0-192.168.255.255
Port	35816
Zone	inside
Interface	ethernet1/2
NAT IP	203.0.113.20
NAT Port	19285

Details

Type	end
Bytes	268

Destination

Destination User	
Destination	4.2.2.2
Country	United States
Port	53
Zone	outside
Interface	ethernet1/1
NAT IP	4.2.2.2
NAT Port	53

Flags

Captive Portal	□
Proxy Transaction	□
Decrypted	□

PCAP	Receive Time ▲	Type	Application	Action	Rule	Rule UUID	Byt...	Severity	Categ...	URL Categ... List	Verdict	URL	File Name
	2019/02/25 21:46:31	end	dns	allow	egress-outside-content-id	6ad81...	268		any				

- Each Security policy rule can log the start and/or end of each session.
- Default is to log session end.
- Temporarily add session start for troubleshooting

Each Security policy rule can be configured to log session information to the Traffic log. The default is to log at session end. However, you can choose to not log at all, log at session start, log at session end, or log 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 session end is sufficient for viewing firewall operation. If you need to troubleshoot firewall operation, then 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 that blocked the traffic was configured to match *any* application. If the firewall drops the traffic before the application has been identified, the **Application** column displays *not-applicable*. The type “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.

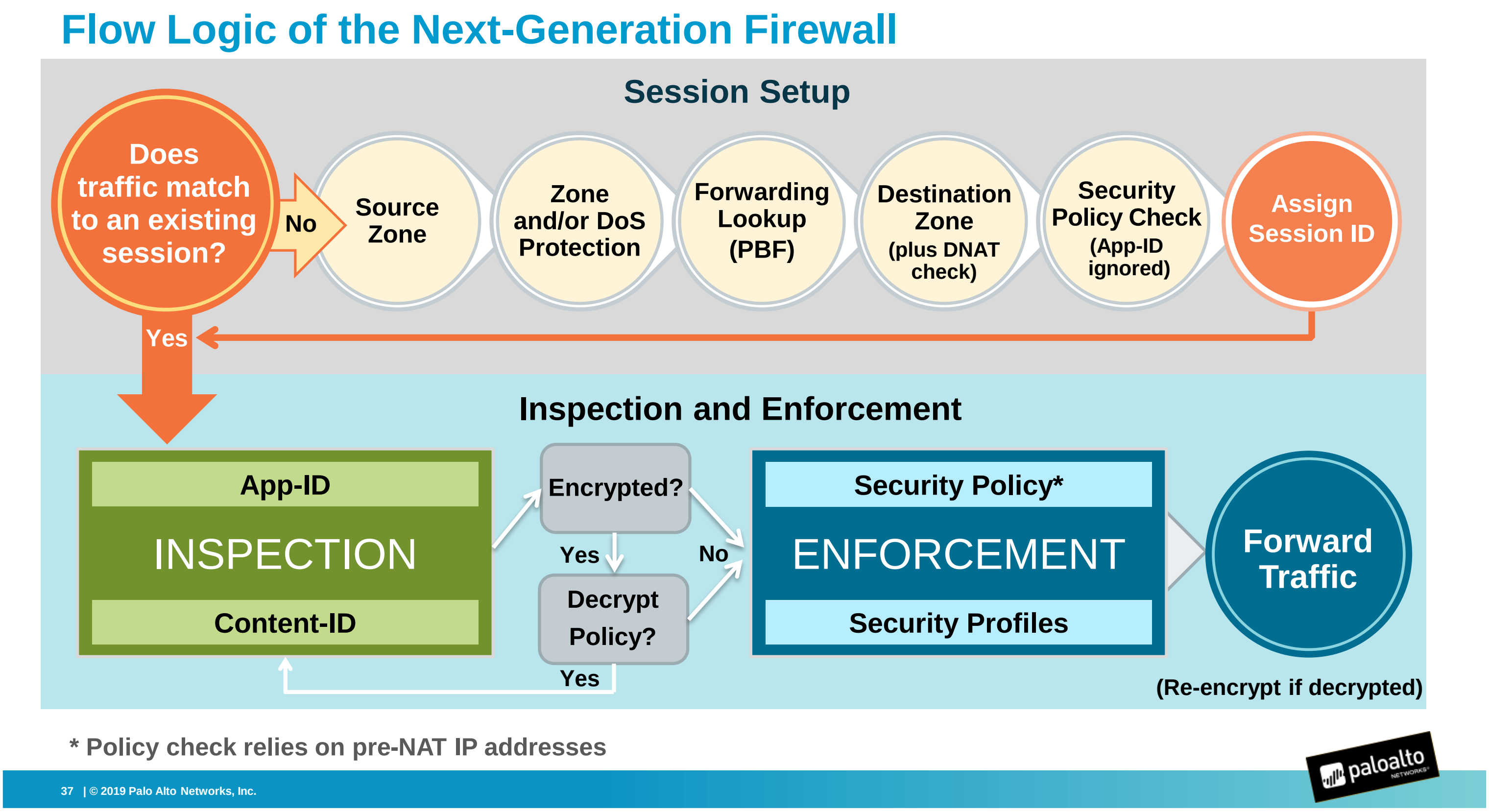
Security policy fundamental concepts

Security policy administration

Network address translation

Source NAT configuration

Destination NAT configuration



Flow Logic of the Next-Generation Firewall

Session Setup

Does traffic match to an existing session?

No

Source Zone

Zone and/or DoS Protection

Forwarding Lookup (PBF)

Destination Zone (plus DNAT check)

Security Policy Check (App-ID ignored)

Assign Session ID

Yes

Inspection and Enforcement

App-ID

INSPECTION

Content-ID

Encrypted?

Yes

No

Decrypt Policy?

Yes

Security Policy*

ENFORCEMENT

Security Profiles

Forward Traffic

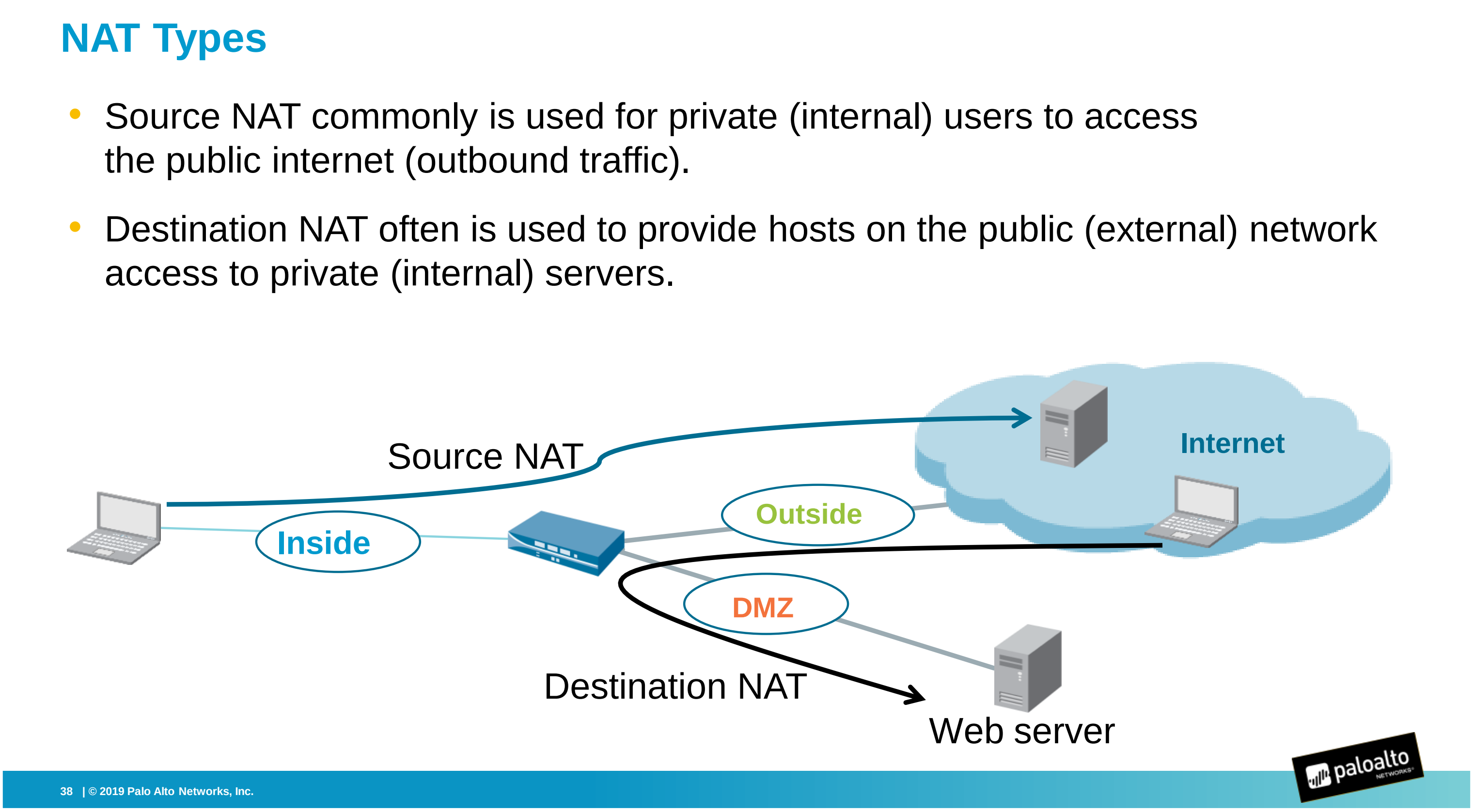
(Re-encrypt if decrypted)

* Policy check relies on pre-NAT IP addresses

37 | © 2019 Palo Alto Networks, Inc.

Administrators are better equipped to create Security policy rules and NAT policy rules if they understand how the firewall processes packets and uses NAT to translate IP addresses. Security policy rules must allow traffic that will be manipulated by NAT policy rules.

The Layer 3 information is processed when the packet is received by the firewall, before the deep inspection of the packet and its payload begins. At this stage in the logic flow, the NAT policy is evaluated to determine if packets would be subjected to a NAT policy rule and, if so, the kind of translation that is applicable. However, no translation takes place yet. The packet retains all original header information. This retention has implications for the Security policy rules that will be matched to the NAT traffic.



NAT Types

- Source NAT commonly is used for private (internal) users to access the public internet (outbound traffic).
- Destination NAT often is used to provide hosts on the public (external) network access to private (internal) servers.

38 | © 2019 Palo Alto Networks, Inc.

NAT configuration can take two forms: source NAT and destination NAT. The forms are directional and are described from the perspective of the NAT device, the firewall.

You often will use source NAT to translate the address of outbound traffic, that is, traffic originating on a private network and being forwarded out toward the internet.

You often will use destination NAT to translate the address of inbound traffic, that is, traffic coming from the internet into the local private network.

For both source and destination NAT, the firewall maintains the mapping of pre-NAT to post-NAT IP addresses. In the example shown, both the Inside zone and DMZ zone are within the private network. The Outside link is the firewall’s connection to the internet.

Note: This example shows the common practice of creating a DMZ zone for the purpose of securely segmenting externally accessible web servers.

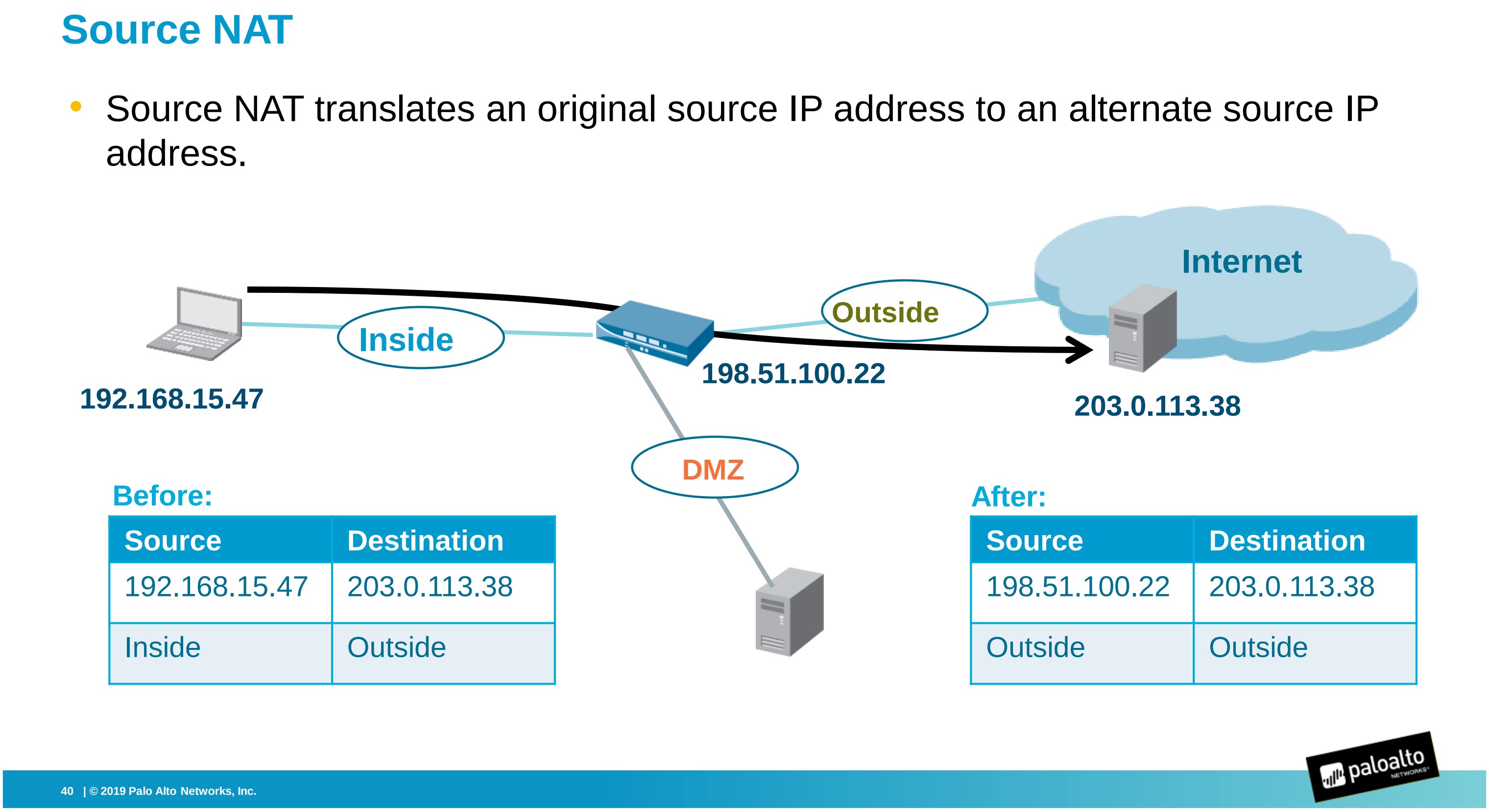
Security policy fundamental concepts

Security policy administration

Network address translation

Source NAT configuration

Destination NAT configuration



Source NAT

- Source NAT translates an original source IP address to an alternate source IP address.

Before:

Source	Destination
192.168.15.47	203.0.113.38
Inside	Outside

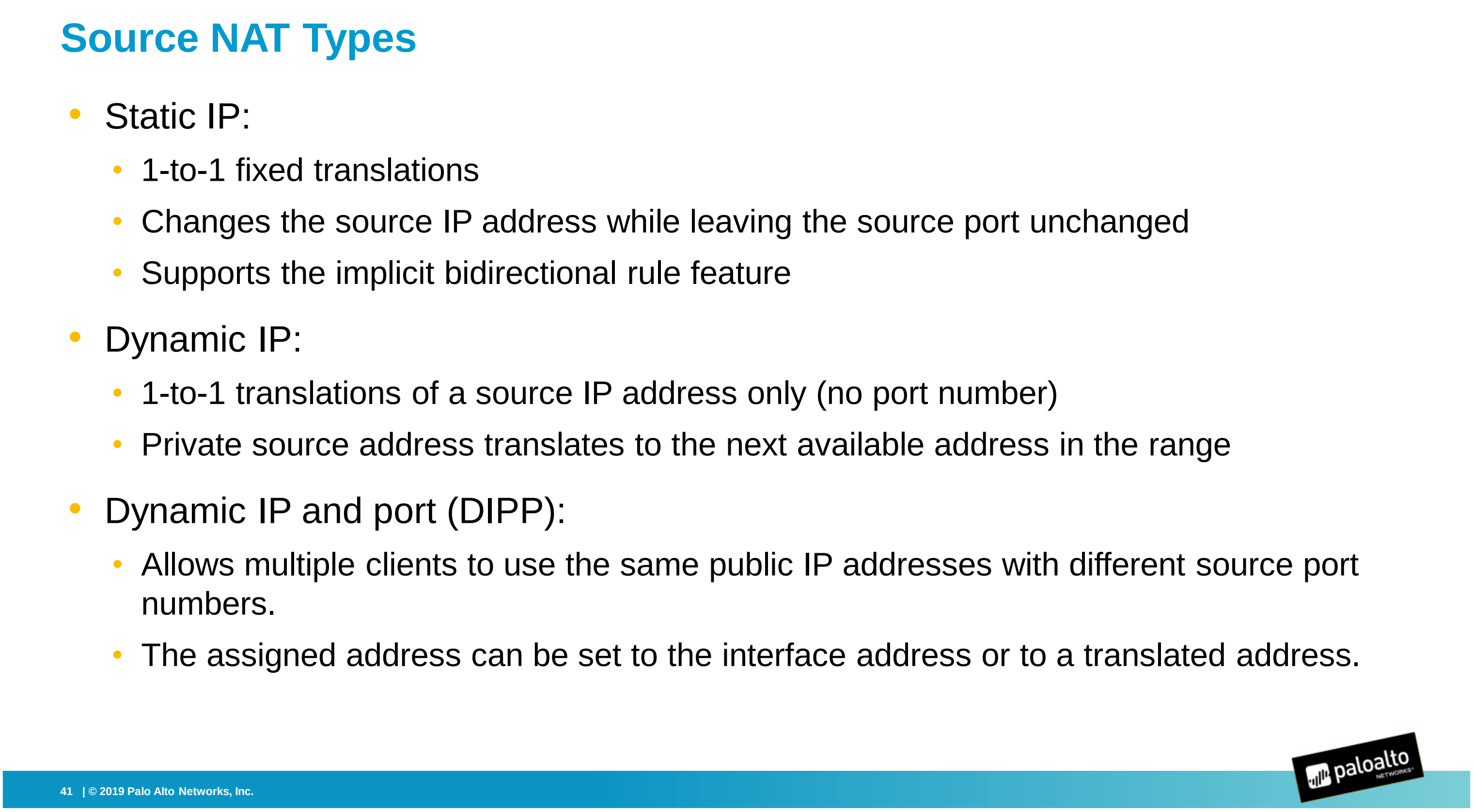
After:

Source	Destination
198.51.100.22	203.0.113.38
Outside	Outside

Source NAT by definition changes the source address of packets that match the NAT policy as the packets transit the firewall. Depending on the firewall configuration, source NAT also might change the source port number. Source NAT commonly is used to allow host devices configured with a private IP address to send and receive traffic on the internet.

This graphic shows the firewall performing a source NAT function. A host residing at 192.168.15.47 on the private network needs to access a service residing at 203.0.113.38 on the public internet. The firewall receives the host traffic on the Inside interface and forwards it on the Outside interface, replacing the original source IP of the packet with the configured Outside interface IP of the firewall.

Without this translation, traffic from the host would be discarded by the ISP carrier because it would be sourced from a private address, 192.168.15.47. Source NAT translates the private address and makes the traffic routable across the internet.



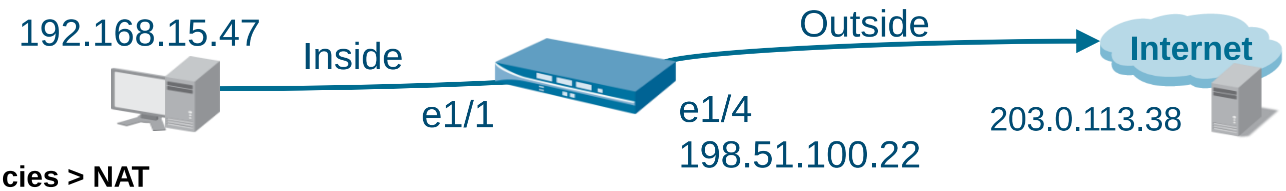
Source NAT Types

- Static IP:
  - 1-to-1 fixed translations
  - Changes the source IP address while leaving the source port unchanged
  - Supports the implicit bidirectional rule feature
- Dynamic IP:
  - 1-to-1 translations of a source IP address only (no port number)
  - Private source address translates to the next available address in the range
- Dynamic IP and port (DIPP):
  - Allows multiple clients to use the same public IP addresses with different source port numbers.
  - The assigned address can be set to the interface address or to a translated address.

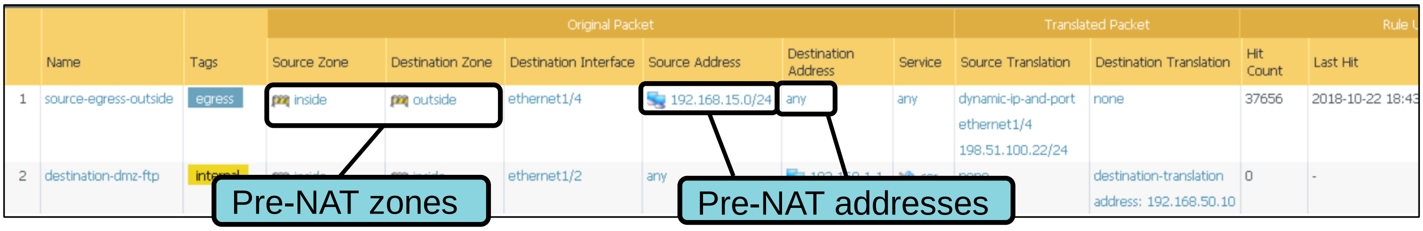
Source NAT types provide the administrator different options for setting the size and nature of the translated source address pool. The firewall supports three ways of provisioning a translated source address pool:

- Static IP: Static IP is used to change the source IP address while leaving the source port unchanged. **Note:** Use of the bidirectional option in static source NAT rules implicitly creates a destination NAT rule for traffic to the same resources in the reverse direction.
- Dynamic IP: With this form of NAT, private source addresses are translated to the next available address in the specified address range. Dynamic IP NAT policies allow you to specify a single IP address, a range of IP addresses, a subnet, or a combination as the translation address pool. By default, if the source address pool is larger than the translated address pool, new IP addresses seeking translation are blocked while the translated address pool is fully used. You can choose to use a DIPP configuration if the pool is exhausted.
- DIPP: Multiple clients can use the same public IP address with different source port numbers. Dynamic IP and port NAT rules allow translation to a single IP address, a range of IP addresses, a subnet, or a combination. In cases where an egress interface has a dynamically assigned IP address, specify the interface itself as the translated address. By specifying the interface in the DIPP rule, you ensure that NAT policy updates automatically to use any address acquired by the interface for subsequent translations. You also can configure a new address to serve as the assigned address by choosing a translated address.

Source NAT and Security Policies

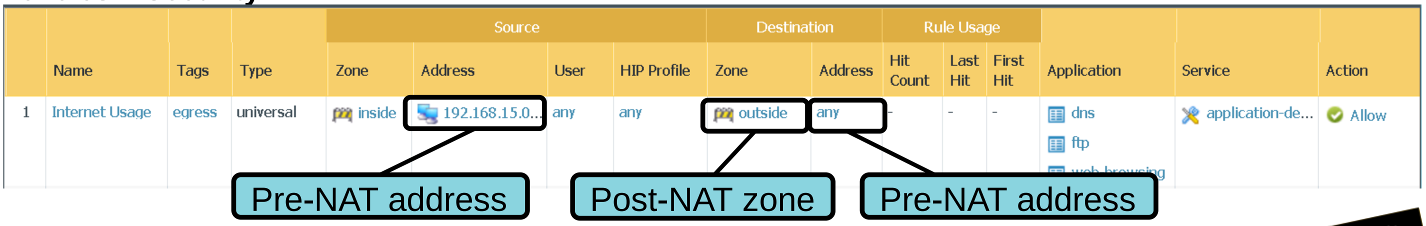


Policies > NAT



			Original Packet						Translated Packet		Rule U	
	Name	Tags	Source Zone	Destination Zone	Destination Interface	Source Address	Destination Address	Service	Source Translation	Destination Translation	Hit Count	Last Hit
1	source-egress-outside	egress	inside	outside	ethernet1/4	192.168.15.0/24	any	any	dynamic-ip-and-port ethernet1/4 198.51.100.22/24	none	37656	2018-10-22 18:43
2	destination-dmz-ftp	internal	inside	inside	ethernet1/2	any	[illegible]	[illegible]	none	destination-translation address: 192.168.50.10	0	-

Policies > Security



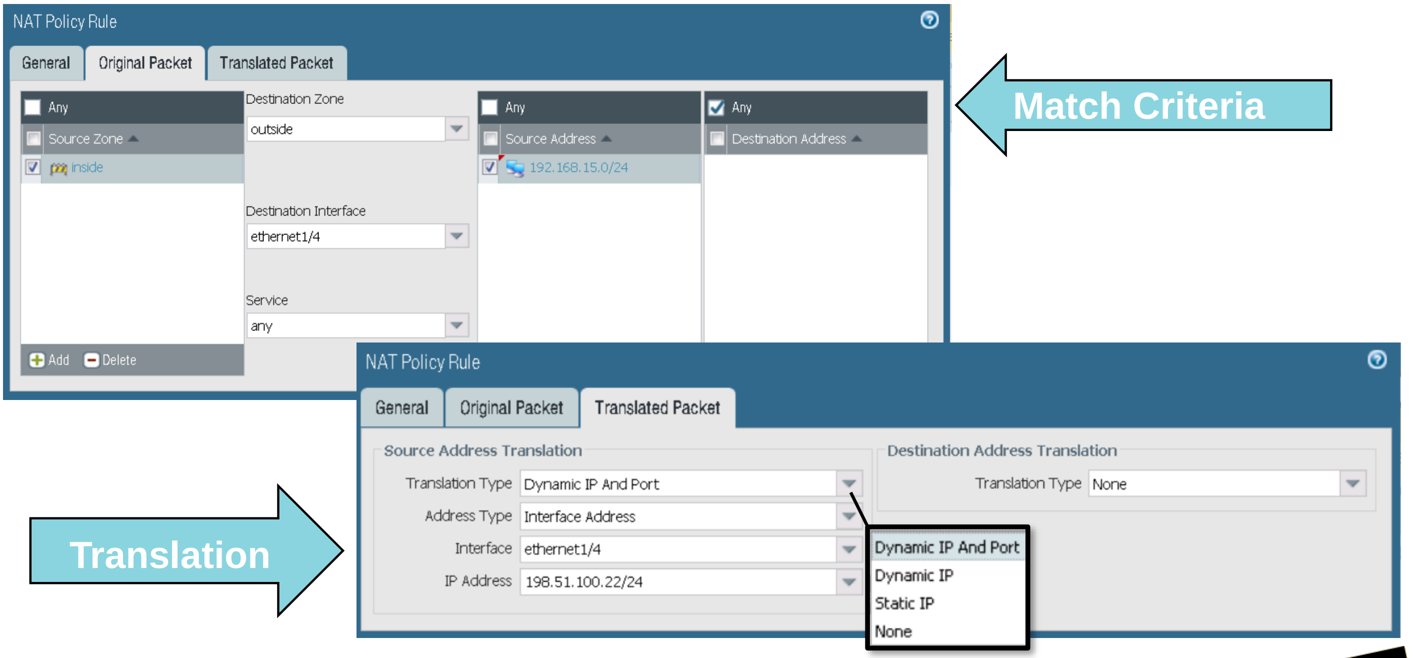
				Source				Destination		Rule Usage					
	Name	Tags	Type	Zone	Address	User	HIP Profile	Zone	Address	Hit Count	Last Hit	First Hit	Application	Service	Action
1	Internet Usage	egress	universal	inside	192.168.15.0...	any	any	outside	any	-	-	-	dns ftp web-browsing	application-de...	Allow

To configure source NAT, first create a NAT policy rule. When you create a source NAT policy rule, identify the **Original Packet** characteristics. Use the fields in the **Original Packet** tab to define the match criteria that will be used to select traffic for the NAT translation. A NAT policy rule matches the packet based on the original pre-NAT source and destination addresses and the pre-NAT destination zone.

Then, create a Security policy rule to support the NAT traffic flow. The Security policy rule will include **Source**, **Destination**, and **Application** characteristics, along with an **Action**. Because of the flow logic discussed, you know that the Security policy rule is enforced after the NAT policy rule is evaluated but before the NAT translation is applied. Therefore, as is shown, a Security policy rule matches the packet based on the original pre-NAT source and destination addresses, but matches the post-NAT destination zone. **Note:** The rule action must be configured as “Allow” to permit traffic matching the defined characteristics to cross the specified zone.

In this example, a host with the IP address 192.168.15.47 wants to connect to a server on the internet residing at IP address 203.0.113.38. To support this connectivity, the firewall administrator has configured a NAT policy rule so that all traffic from the private network appears to come from the publicly routable address on the ethernet1/4 interface. For this configuration example, the administrator has chosen to use the DIPP type source NAT. When you configure DIPP, use **Address Type** to define addresses for the pool. There are two options. The **Translated Address** option uses a new address that is not on an external interface. It is used for interfaces that receive an IP address dynamically from a pool. The **Interface Address** option uses an existing address that is on an external interface. In the example shown, the **Interface Address** option was used and the interface specified is ethernet1/4 with IP address 198.51.100.22.

Configuring Source NAT



NAT Policy Rule

General | Original Packet | Translated Packet

☐ Any

☐ Source Zone ▲

☑ inside

Destination Zone: outside

Destination Interface: ethernet1/4

Service: any

☐ Any

☐ Source Address ▲

☑ 192.168.15.0/24

☑ Any

☐ Destination Address ▲

Match Criteria

NAT Policy Rule

General | Original Packet | Translated Packet

Source Address Translation

Translation Type: Dynamic IP And Port

Address Type: Interface Address

Interface: ethernet1/4

IP Address: 198.51.100.22/24

Destination Address Translation

Translation Type: None

Translation

NAT rules are based on source and destination zones, source and destination IP addresses, and application services. As with Security policy rules, NAT policy rules are compared against incoming traffic in sequence. The first rule that matches the traffic is applied. Every NAT policy rule is configured in the web interface under **Policies** > **NAT**.

To configure source NAT, use the **Original Packet** tab to define the source and destination zones of the packets that the firewall will translate and, optionally, specify the destination interface and type of service. You can configure multiple source and destination zones of the same type, and you can apply the rule to specific networks or specific IP addresses. Select the **Translated Packet** tab to configure the type of translation to perform on the source and the address and/or port to which the source will be translated.

Although the **General** tab is not shown here, it is used to name the NAT policy and to specify which type of traffic the NAT rule will translate. Options are:

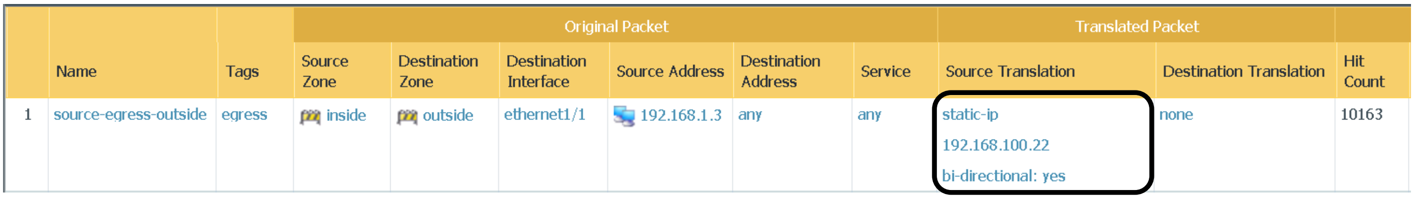
- **ipv4** for translation between IPv4 addresses
- **nat64** (pronounced “NAT 6-to-4”) for translation between IPv6 and IPv4 addresses. This option most commonly is used for connecting IPv6 corporate intranets to the internet.
- **natv6** for translation between IPv6 addresses

Examples in this module will use translation type IPv4 because it is the most common type implemented.

Source NAT Examples

Static 1:1 Translation

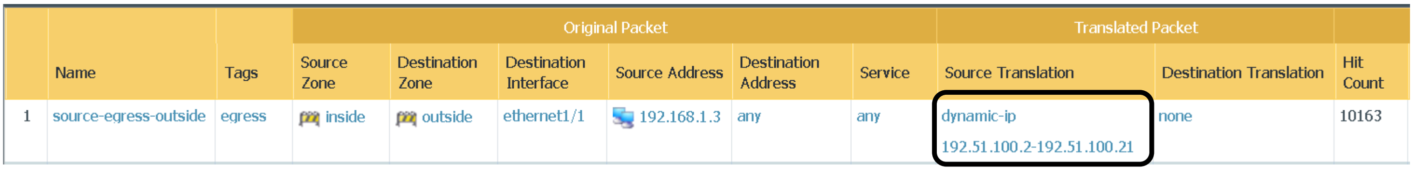
Policies > NAT



			Original Packet						Translated Packet		
	Name	Tags	Source Zone	Destination Zone	Destination Interface	Source Address	Destination Address	Service	Source Translation	Destination Translation	Hit Count
1	source-egress-outside	egress	inside	outside	ethernet1/1	192.168.1.3	any	any	static-ip 192.168.100.22 bi-directional: yes	none	10163

Dynamic IP Translation

Policies > NAT



			Original Packet						Translated Packet		
	Name	Tags	Source Zone	Destination Zone	Destination Interface	Source Address	Destination Address	Service	Source Translation	Destination Translation	Hit Count
1	source-egress-outside	egress	inside	outside	ethernet1/1	192.168.1.3	any	any	dynamic-ip 192.51.100.2-192.51.100.21	none	10163

44 | © 2019 Palo Alto Networks, Inc.

Translated Packet characteristics determine which translation will be done with packets that match the criteria defined under the **Original Packet** tab. **Translated Packet** characteristics include translation types. Two translation types correspond to the two types of source NAT:

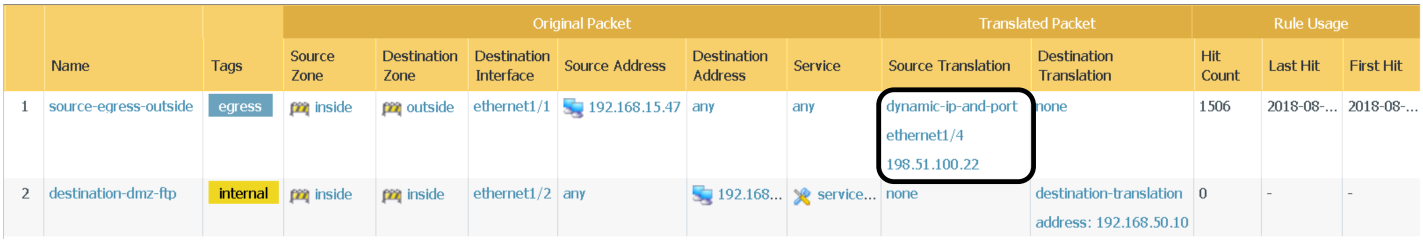
- Static IP: For this type, a single **Original Packet** IP address is mapped to a single **Translated Packet** IP address. The same address always is used, and the port is unchanged. For example, if the configured source range is 192.168.0.1 to 192.168.0.10 and the configured translation range is 10.0.0.1 to 10.0.0.10, address 192.168.0.2 is always translated to 10.0.0.2. However, the number of source IPs using this policy must exactly match the translated address range.
- Dynamic IP: With this type of NAT, the next available address in the specified range is used, but the port number is unchanged. Each concurrent session uses an address from the configured pool, making it unavailable to other source IPs. This option most commonly is used when there are two or more public IPs from the ISP, but not enough public IPs to allocate one to each internal host on the network, and you want to assign them to outbound hosts only as needed.

Be careful when using dynamic IP. The translated pool of addresses can be exhausted if the number of internal hosts concurrently creating outbound sessions exceeds the number of IP addresses in the dynamic pool. As a way to protect against IP address exhaustion, you can set the **Advanced (Dynamic IP/Port Failback)** button (in the **Translated Packet** tab when you choose dynamic IP), which results in the use of DIPP if the dynamic IP pool runs out of unused IP addresses.

Source NAT Examples (Cont.)

Dynamic IP and Port Translation

Policies > NAT



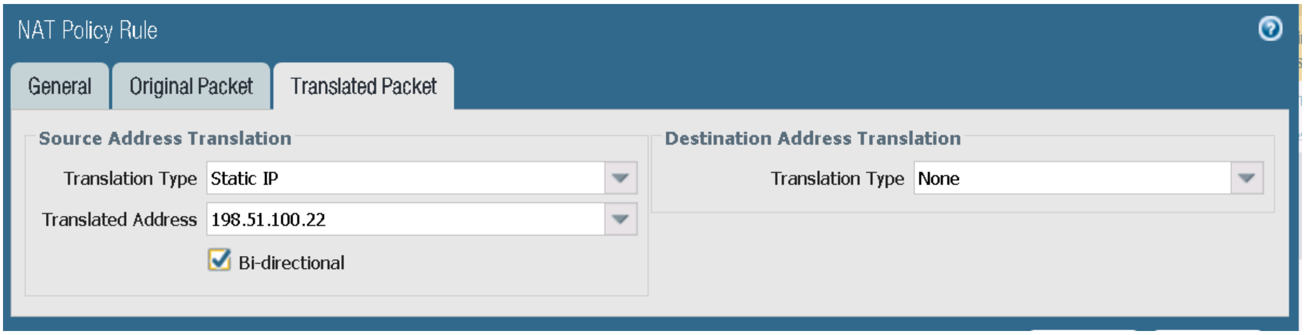
			Original Packet						Translated Packet		Rule Usage		
	Name	Tags	Source Zone	Destination Zone	Destination Interface	Source Address	Destination Address	Service	Source Translation	Destination Translation	Hit Count	Last Hit	First Hit
1	source-egress-outside	egress	inside	outside	ethernet1/1	192.168.15.47	any	any	dynamic-ip-and-port ethernet1/4 198.51.100.22	none	1506	2018-08-...	2018-08-...
2	destination-dmz-ftp	internal	inside	inside	ethernet1/2	any	192.168...	service...	none	destination-translation address: 192.168.50.10	0	-	-

Dynamic IP and port: With this type of NAT, an available address in the specified range can be used multiple times because each time the address is paired with a different port number. This option most commonly is used when there are two or more public IPs from the ISP, but not enough public IPs to allocate one to each internal host on the network. Because each address is used multiple times by pairing it with a unique port number, DIPP mitigates the problem of having more internal hosts than there are external, routable IP addresses.

Configuring Bidirectional Source NAT

- Enables internal servers to send and receive traffic through the firewall
- Available only for static NAT

Policies > NAT



NAT Policy Rule

General | Original Packet | Translated Packet

Source Address Translation

Translation Type: Static IP

Translated Address: 198.51.100.22

☑ Bi-directional

Destination Address Translation

Translation Type: None

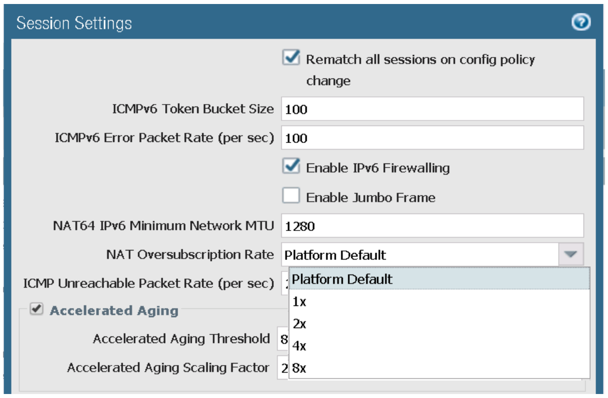
Your public-facing servers must be able to both send and receive packets. You need a reciprocal policy that translates the public address (the destination IP address in incoming packets from internet users) into the private address so that the firewall can route the packet to an IP address on your internal network. You create a bidirectional static NAT rule. Bidirectional translation is an option for static NAT only.

To create a bidirectional source NAT rule, click the **Bi-directional** check box as shown in the example. This action creates an invisible rule in your NAT policy that enables the server to both send and receive network traffic through the firewall.

DIPP NAT Oversubscription

- The same translated IP address and port pair can be used multiple times in concurrent sessions:
  - Assumes that hosts are connecting to different destinations

Device > Setup > Session > Session Settings



Session Settings

☑ Rematch all sessions on config policy change

ICMPv6 Token Bucket Size 100

ICMPv6 Error Packet Rate (per sec) 100

☑ Enable IPv6 Firewalling

□ Enable Jumbo Frame

NAT64 IPv6 Minimum Network MTU 1280

NAT Oversubscription Rate Platform Default

Platform Default
1x
2x
4x
8x

ICMP Unreachable Packet Rate (per sec)

☑ Accelerated Aging

Accelerated Aging Threshold 8

Accelerated Aging Scaling Factor 2

Internal Source Port	Firewall Source Port	Destination Address
26435	25661	51.6.33.12
35435	25661	161.8.55.4
21569	25661	201.55.45.1
51043	25661	17.39.25.6

Concurrent sessions = oversubscription rate (8/4/2) x address pool size

For a given IP address, the TCP protocol recognizes a maximum of about 64,000 port numbers (16 header bits for source port yields 65,536 total – 1,024 well known = 64,512 available ports). Based on this limitation, DIPP source NAT will support a maximum of about 64,000 concurrent sessions on each IP address configured within the NAT pool.

On some platforms, the PAN-OS DIPP NAT implementation supports oversubscription. Oversubscription allows the reuse of port numbers by using destination IP address as an additional NAT session identifier. In the example, the same post-NAT translated source IP and source port are being used for traffic streams flowing to four different IP addresses, which constitutes 4x oversubscription.

The NAT oversubscription rate is configurable up to the maximum rate supported by the platform. To display the oversubscription information for each firewall model, see https://www.paloaltonetworks.com/products/product-selection.

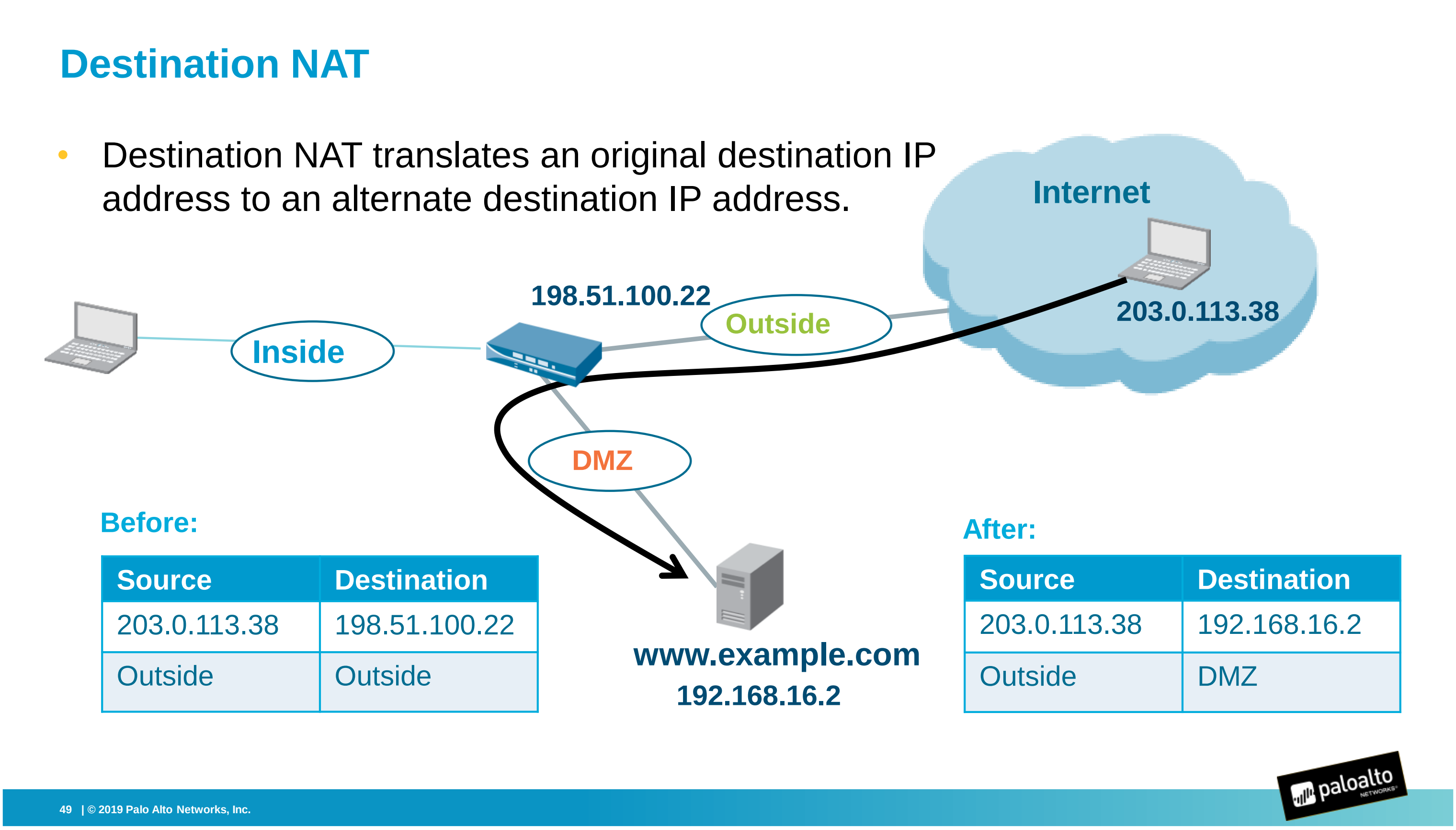
Security policy fundamental concepts

Security policy administration

Network address translation

Source NAT configuration

Destination NAT configuration



Destination NAT

- Destination NAT translates an original destination IP address to an alternate destination IP address.

Internet

198.51.100.22

Outside

203.0.113.38

Inside

DMZ

www.example.com

192.168.16.2

Before:

Source	Destination
203.0.113.38	198.51.100.22
Outside	Outside

After:

Source	Destination
203.0.113.38	192.168.16.2
Outside	DMZ

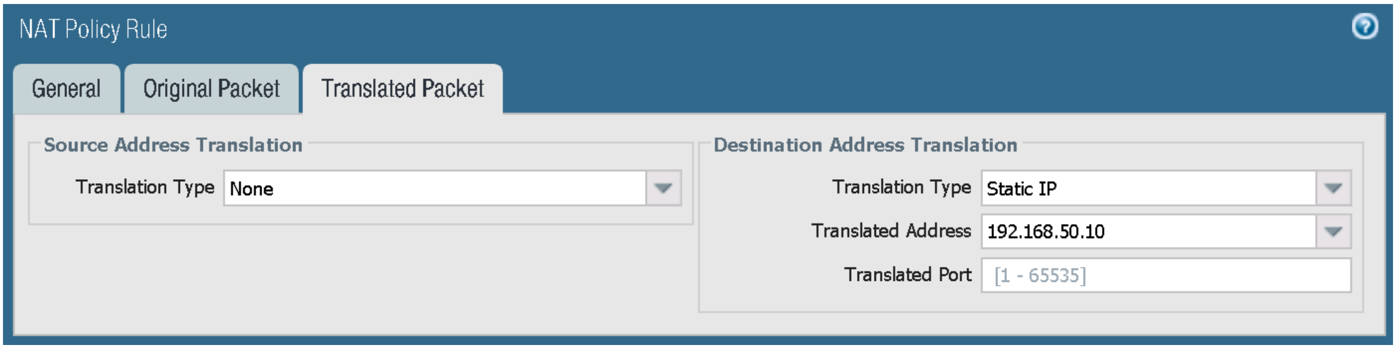
Destination NAT by definition will change the destination address in the IP header of packets that match the NAT policy as they transit the firewall. Destination NAT commonly is used to make a server within a private network reachable from the public internet.

In the example shown, a user at an external system with the IP address 203.0.113.38 queries the DNS server for the IP address of the web server www.example.com. The DNS server returns an address of 198.51.100.22, which is the external address of the firewall interface in the Outside zone. For the packet to reach the web server, the destination IP address must be translated to the private IP address 192.168.16.2.

Destination NAT Attributes

- Static IP:
  - 1-to-1 fixed translations
  - Changes the destination IP address while leaving the destination port unchanged
  - Also enabled by Static Source NAT with the **Bi-directional** option set

Policies > NAT > Add



NAT Policy Rule

Source Address Translation

Translation Type: None

Destination Address Translation

Translation Type: Static IP

Translated Address: 192.168.50.10

Translated Port: [1 - 65535]

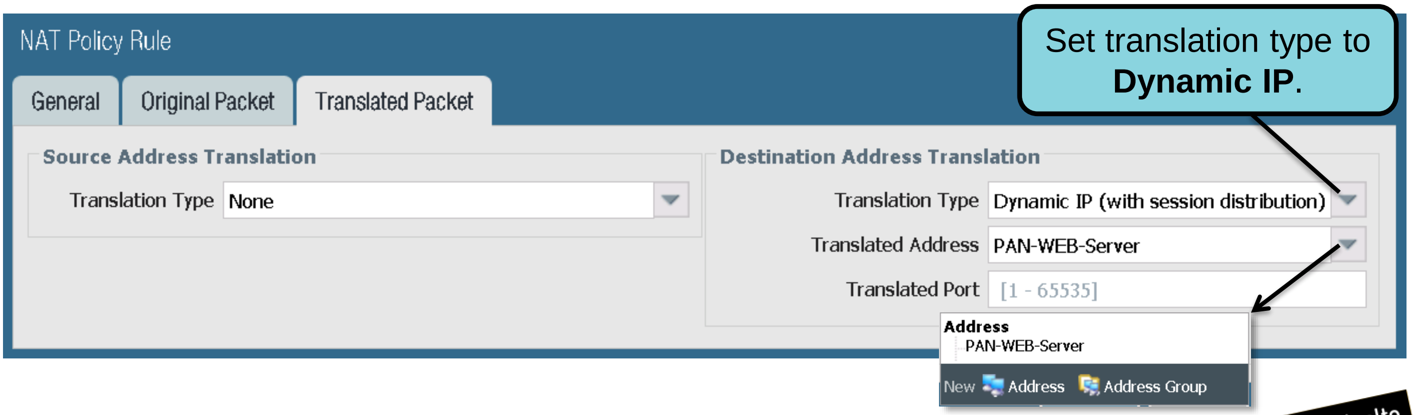
Destination NAT provides the administrator options for provisioning public access to servers and services within their network. Destination NAT uses static IP mapping with optional port forwarding.

Static IP is used for 1-to-1 translation of inbound traffic. Static IP allows you to change the destination IP address and, optionally, the port. When destination address translation is used to map a single public IP address to multiple private servers and services, destination ports can stay the same or be directed to different destination ports. Use static IP to change the destination IP address while leaving the destination port unchanged.

Dynamic IP Address Support for Destination NAT

- Translates original IP address to destination host with a DHCP-assigned IP address
- Translated address can be an FQDN, address object, or address group.

Policies > NAT > Add



NAT Policy Rule

Source Address Translation

Translation Type: None

Destination Address Translation

Translation Type: Dynamic IP (with session distribution)

Translated Address: PAN-WEB-Server

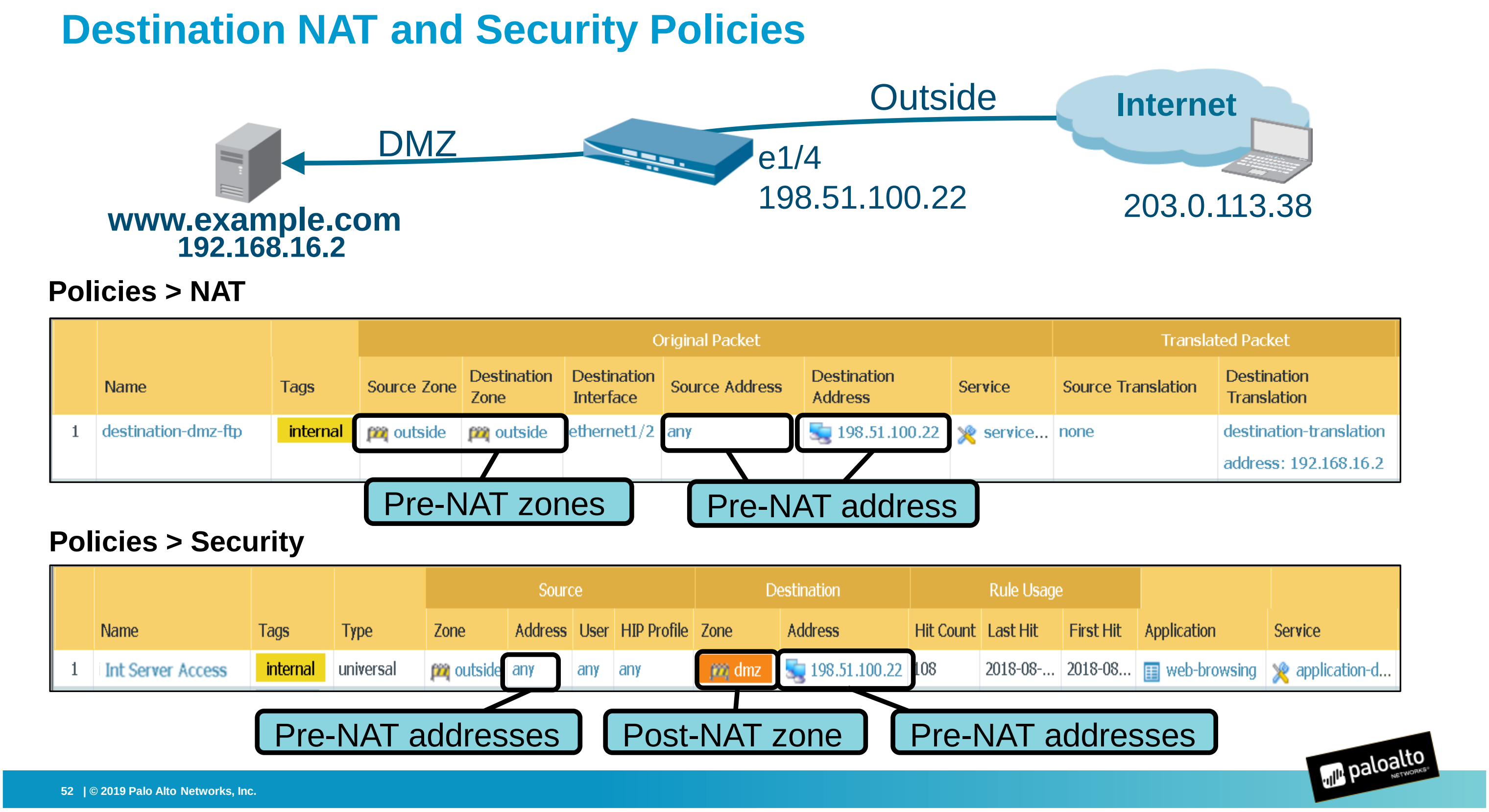
Translated Port: [1 - 65535]

Address
PAN-WEB-Server

Set translation type to **Dynamic IP**.

In PAN-OS 8.1, destination NAT has been enhanced to translate the original destination address to a destination host that has a DHCP-assigned IP address. The translated address can be an FQDN, an address object, or an address group that uses an FQDN. After the DHCP server assigns a new address to the host, you will not have to manually update the FQDN, the DNS server, or the NAT policy rule. You also will not need to use a separate external component to update the DNS server with the latest FQDN-to-IP address mapping. This new translation type is in addition to the static, one-to-one translation that previously was the only type of destination NAT available.

If an FQDN in the translated destination address resolves to more than one address, the firewall automatically will distribute translated sessions among those addresses, based on a round-robin algorithm, to provide more equitable session loading. Each FQDN can support up to 32 IPv4 addresses and 32 IPv6 addresses. If a DNS server returns more than 32 addresses for an FQDN, the firewall uses the first 32 addresses in the packet.



Destination NAT and Security Policies

Policies > NAT

			Original Packet						Translated Packet	
	Name	Tags	Source Zone	Destination Zone	Destination Interface	Source Address	Destination Address	Service	Source Translation	Destination Translation
1	destination-dmz-ftp	internal	outside	outside	ethernet1/2	any	198.51.100.22	service...	none	destination-translation address: 192.168.16.2

Policies > Security

				Source				Destination		Rule Usage				
	Name	Tags	Type	Zone	Address	User	HIP Profile	Zone	Address	Hit Count	Last Hit	First Hit	Application	Service
1	Int Server Access	internal	universal	outside	any	any	any	dmz	198.51.100.22	108	2018-08-...	2018-08...	web-browsing	application-d...

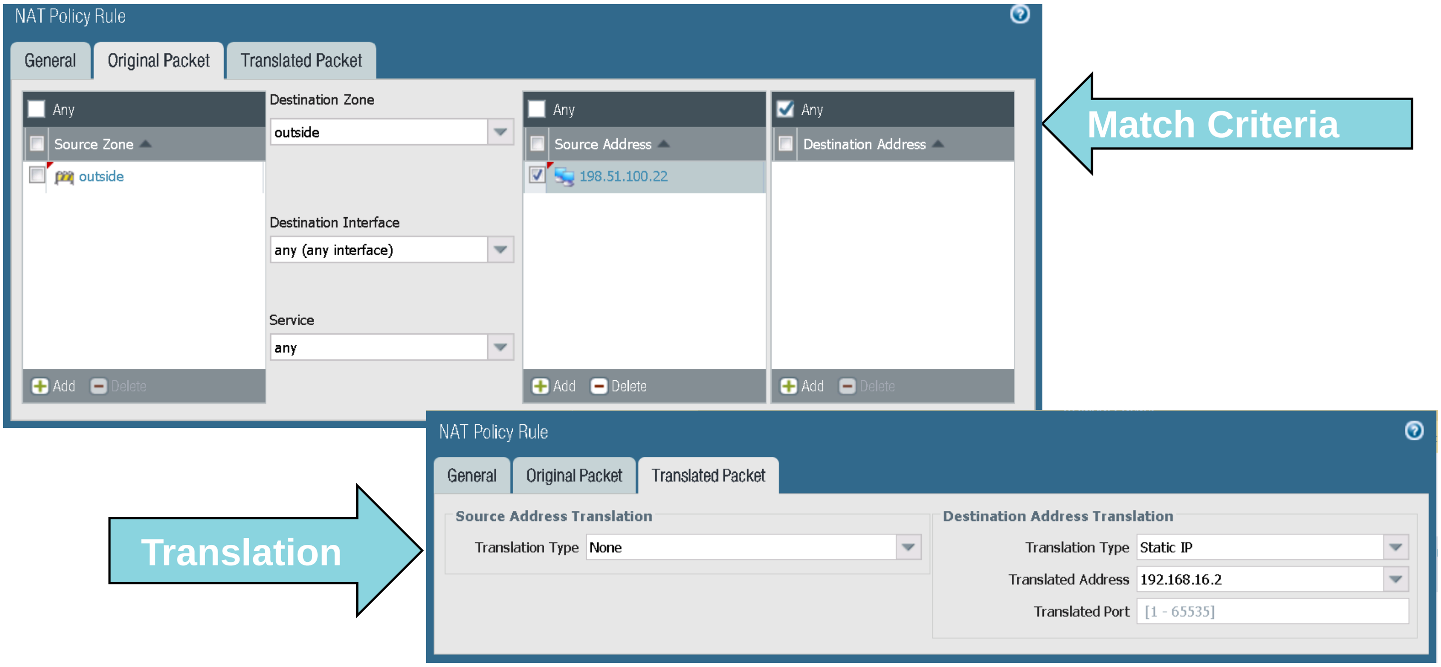
52 | © 2019 Palo Alto Networks, Inc.

To configure destination NAT, first create a NAT policy rule. When you create a destination NAT policy rule, identify the **Original Packet** characteristics. Use the fields in the **Original Packet** tab to define the match criteria that will be used to select traffic for the NAT translation. A NAT policy rule matches the packet based on the original pre-NAT source and destination addresses and the pre-NAT destination zone. Use the **Translated Packet** tab to specify the desired translation of packets that meet the **Original Packet** criteria.

Then, create a Security policy rule to support the NAT traffic flow. The Security policy rule will include **Source**, **Destination**, and **Application** characteristics, along with an **Action**. Because of the flow logic discussed, you know that the Security policy is enforced after the NAT policy is evaluated, but before the NAT translation is applied. Therefore, as is shown, the Security policy rule matches on the post-NAT destination zones and the pre-NAT destination IP addresses.

In this example, a user with IP address 192.0.2.5 wants to browse webpages hosted at www.example.com. Though DNS resolution is not shown in the diagram, you should assume that www.example.com is associated with 198.51.100.22, the IP address on the e1/4 interface of the firewall. To support this connectivity, the firewall administrator has configured a destination NAT policy rule so that traffic arriving at e1/4 destined for 198.51.100.22 has its destination address changed to 192.168.16.2. After the firewall determines the translated address, the firewall performs a route lookup to determine the egress interface. In this example, the egress interface is e1/2. To support this traffic flow, the administrator has configured a Security policy rule. The Security policy rule permits web browsing traffic from the pre-NAT zone, Outside, with a pre-NAT destination IP address of 198.51.100.22 to cross into the DMZ zone.

Configuring Destination NAT



Match Criteria

Translation

NAT Policy Rule

General | Original Packet | Translated Packet

☐ Any

☐ Source Zone

☐ outside

Destination Zone: outside

Destination Interface: any (any interface)

Service: any

☐ Any

☐ Source Address

☑ 198.51.100.22

☑ Any

☐ Destination Address

NAT Policy Rule

General | Original Packet | Translated Packet

Source Address Translation

Translation Type: None

Destination Address Translation

Translation Type: Static IP

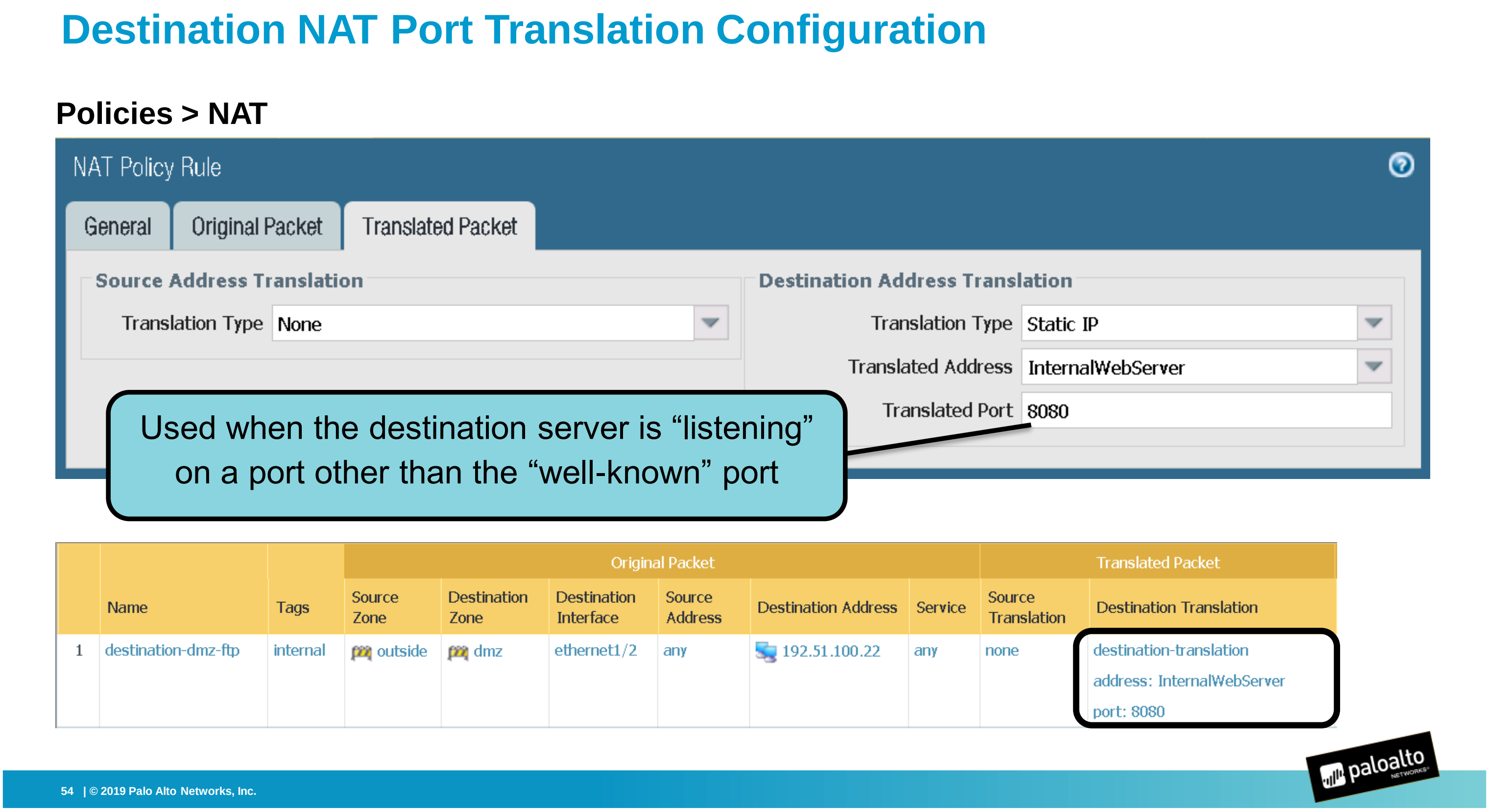
Translated Address: 192.168.16.2

Translated Port: [1 - 65535]

Configuration of destination NAT is similar to configuration of source NAT. As with source NAT, destination NAT uses the **Original Packet** tab to define the source and destination zones of the packets that the firewall will translate and, optionally, specify the destination interface and type of service.

You can configure multiple source and destination zones of the same type and you can apply the rule to specific networks or a specific IP address. Select the **Translated Packet** tab and check the **Destination Address Translation check** box to flag this rule as a destination-NAT rule. Leave the **Source Address Translation Translation Type** set to **None** if this rule is a destination-NAT-only rule.

Note: NAT rules must be configured to use the zones associated with pre-NAT IP addresses configured in the policy. In the example, the source and destination zones are the same. A Security policy differs from the NAT policy because post-NAT zones must be used to control traffic. NAT may influence the source or destination IP addresses and can modify the outgoing interface and zone. After you create Security policy rules with specific IP addresses, the pre-NAT IP addresses are used in the Security policy rule match. Traffic subjected to NAT must be permitted explicitly by the Security policy when that traffic traverses multiple zones.



Destination NAT Port Translation Configuration

Policies > NAT

NAT Policy Rule

Source Address Translation

Translation Type: None

Destination Address Translation

Translation Type: Static IP

Translated Address: InternalWebServer

Translated Port: 8080

Used when the destination server is “listening” on a port other than the “well-known” port

			Original Packet						Translated Packet	
	Name	Tags	Source Zone	Destination Zone	Destination Interface	Source Address	Destination Address	Service	Source Translation	Destination Translation
1	destination-dmz-ftp	internal	outside	dmz	ethernet1/2	any	192.51.100.22	any	none	destination-translation address: InternalWebServer port: 8080

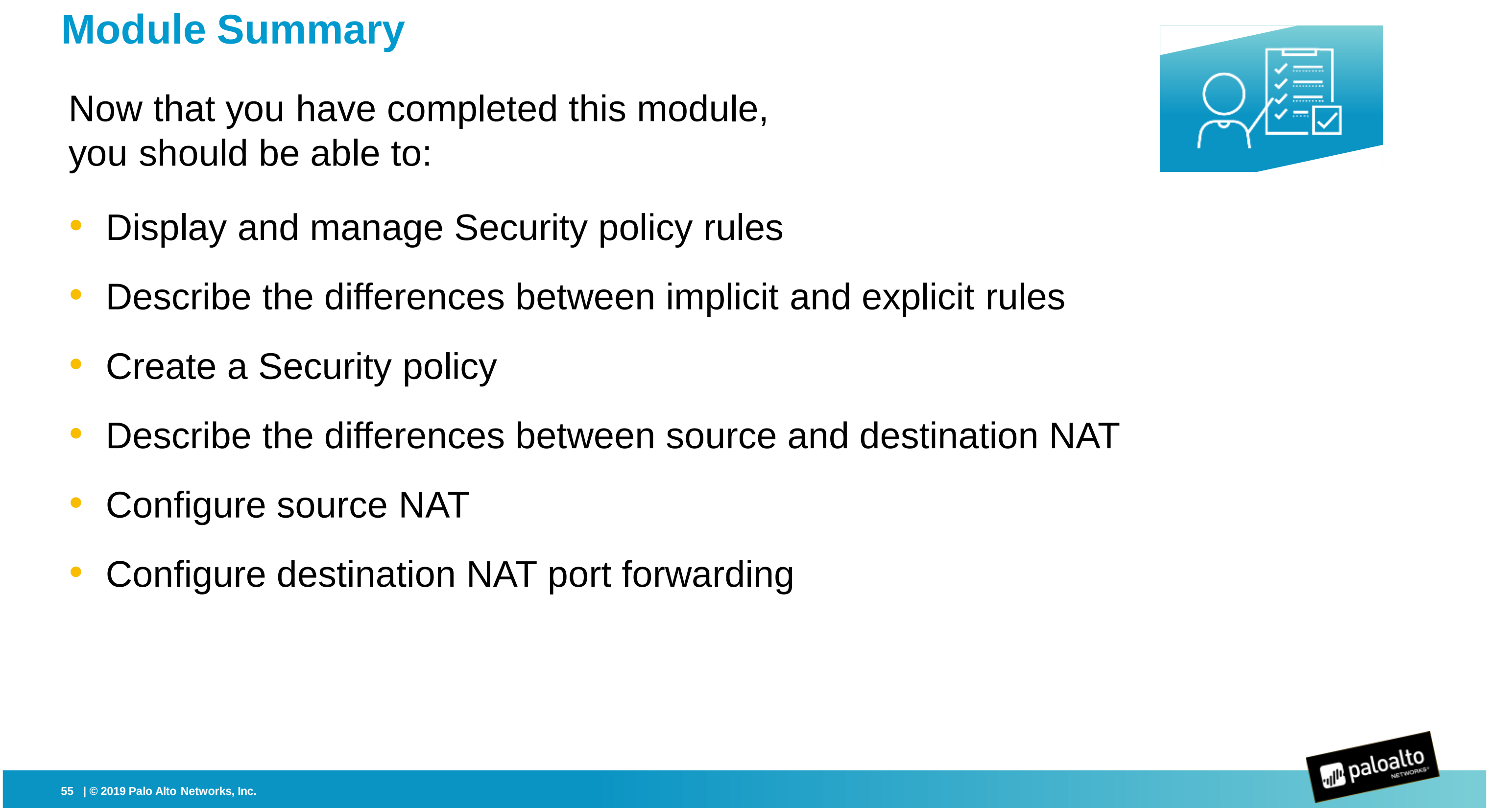
54 | © 2019 Palo Alto Networks, Inc.

PAN-OS software supports two destination NAT types:

- Static IP, which is used for 1-to-1 translation of inbound traffic. Configuration of static IP destination NAT changes the destination IP address while leaving the destination port unchanged.
- Port forwarding, which is a technique used to manage traffic through NAT policies based on destination port numbers. For example, assume that a company has three separate servers: one for email, one for web hosting, and an application server that exists in a zone named Server-Trust. All systems in Server-Trust are configured with a NAT policy to appear as if they have the same IP address. When traffic is received at the shared address, the port forwarding feature of the inbound NAT policy can send the traffic to the appropriate server based on the destination port associated with the session.

To configure destination NAT, enter an IP address or range of IP addresses and a translated port number (1 to 65535) that the destination address and port number are translated to. If the **Translated Port** field is blank, the destination port is not changed. Destination translation typically is used to allow an internal server, such as an email server, to be accessed from the public network.

You can complete the **Translated Address** field with either an IP address or an Address object. Address objects are named objects configured on the firewall to help administrators more easily complete configurations with a predefined address. To configure Address objects, go to **Objects** > **Addresses**.



Module Summary

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

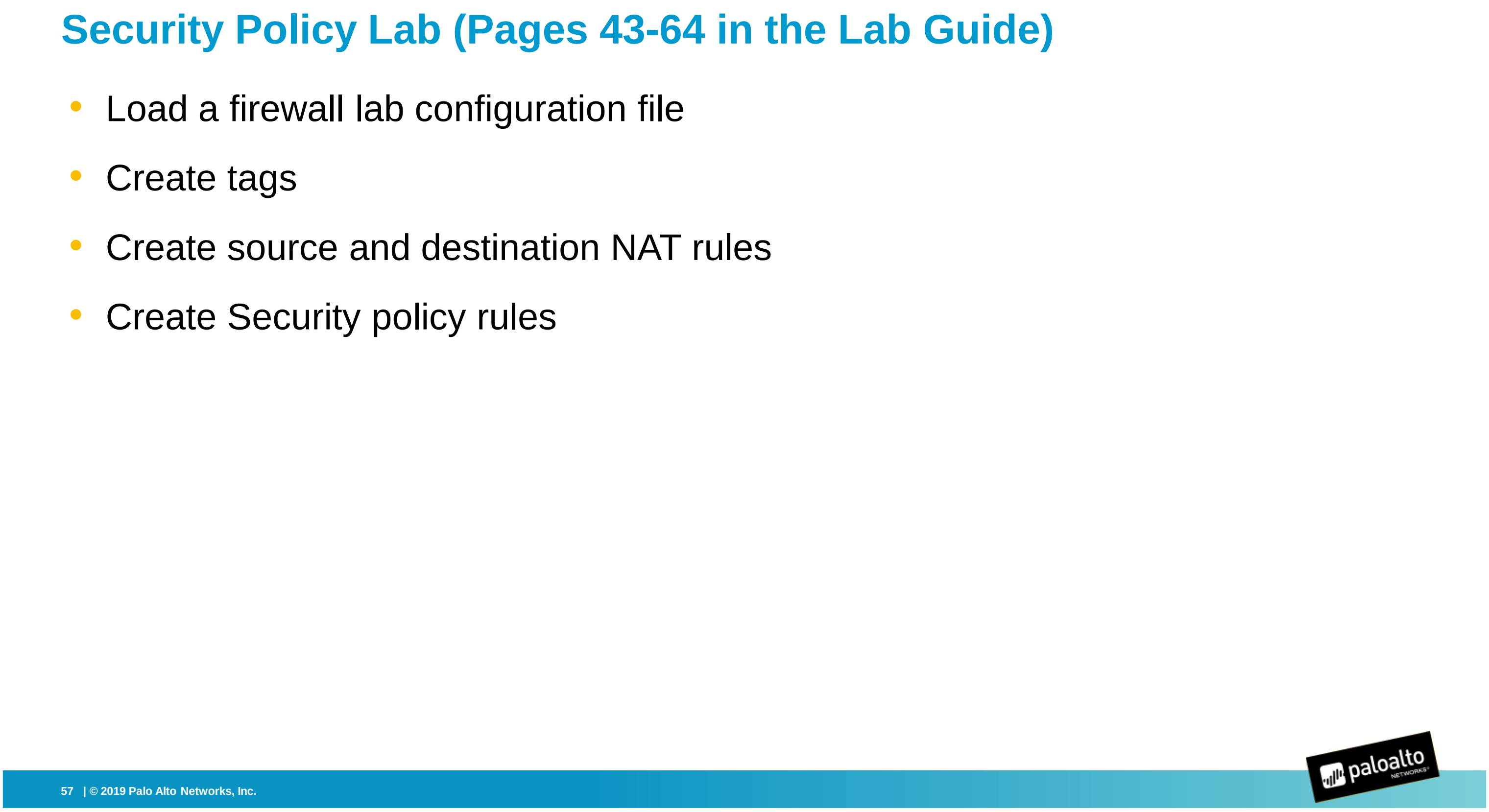
- Display and manage Security policy rules
- Describe the differences between implicit and explicit rules
- Create a Security policy
- Describe the differences between source and destination NAT
- Configure source NAT
- Configure destination NAT port forwarding

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

Questions?

Review Questions

1. Which four items are possible network traffic match criteria in a Security policy on a Palo Alto Networks firewall? (Choose four.)
    a. Source Zone
    b. Username
    c. DNS Domain
    d. URL
    e. Application
2. Which of the three types of Security policy rules that can be created is the default rule type?
    a. intrazone
    b. interzone
    c. universal
3. True or false? The intrazone-default and interzone-default rules cannot be modified.
    a. true
    b. false
4. Which three items are names of valid source NAT translation types? (Choose three.)
    a. dynamic IP
    b. dynamic IP/Port
    c. port forwarding
    d. static
5. True or false? Logging on intrazone-default and interzone-default Security policy rules is enabled by default.
    a. true
    b. false



Security Policy Lab (Pages 43-64 in the Lab Guide)

- Load a firewall lab configuration file
- Create tags
- Create source and destination NAT rules
- Create Security policy rules

PROTECTION. DELIVERED.

Answers to Review Questions

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