BLOCKING THREATS USING SECURITY AND NAT POLICIES

GET TRAFFIC FLOWING

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

paloalto NETWORKS

Learning Objectives

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

- Describe Security policy concepts and operation
- Configure a Security policy rule
- Manage a Security policy
- Create and use tags and custom services in a Security policy
- Configure a NAT policy to implement source NAT
- Configure a NAT policy to implement destination NAT

Security policy fundamental concepts

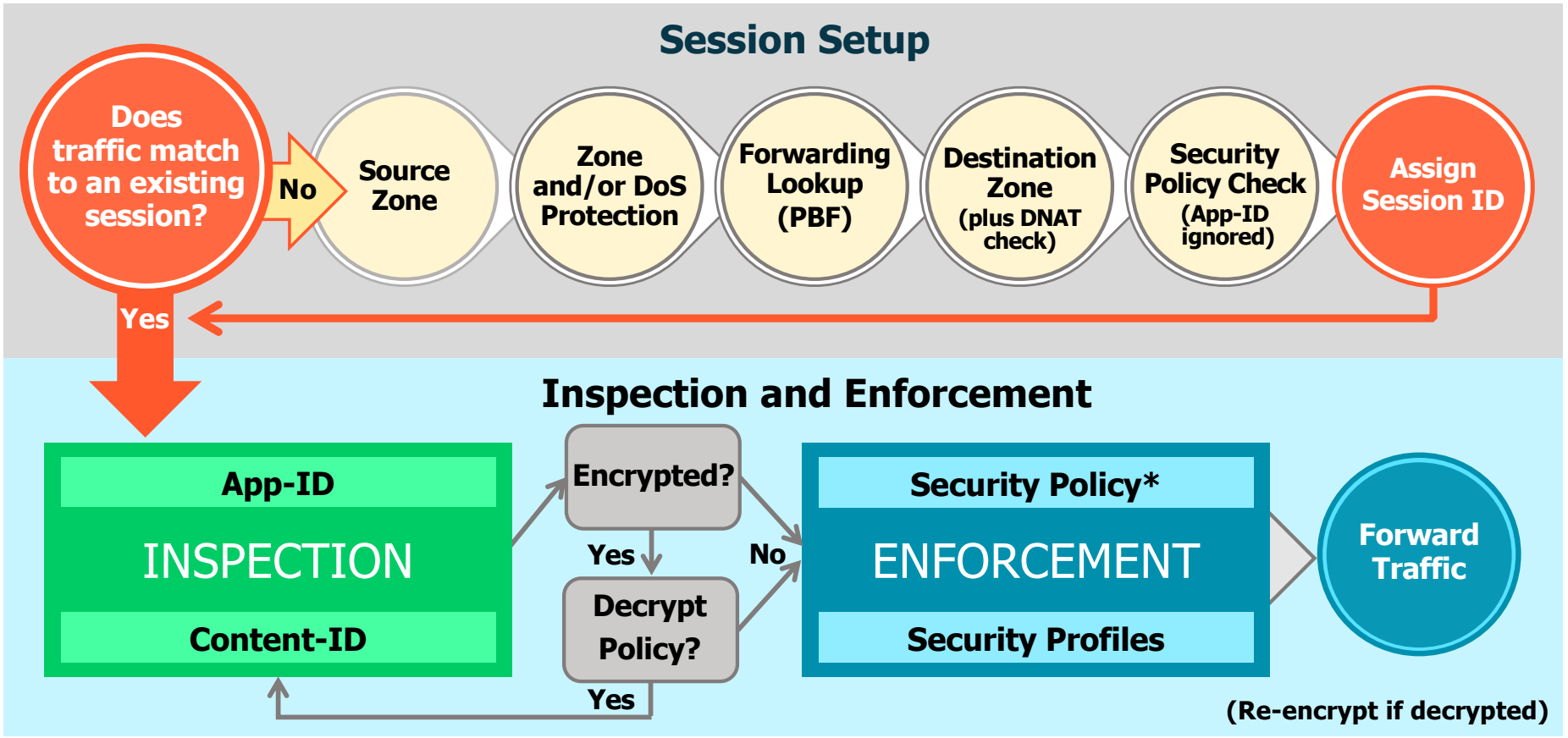
Security policy administration

Network address translation

Source NAT configuration

Destination NAT configuration

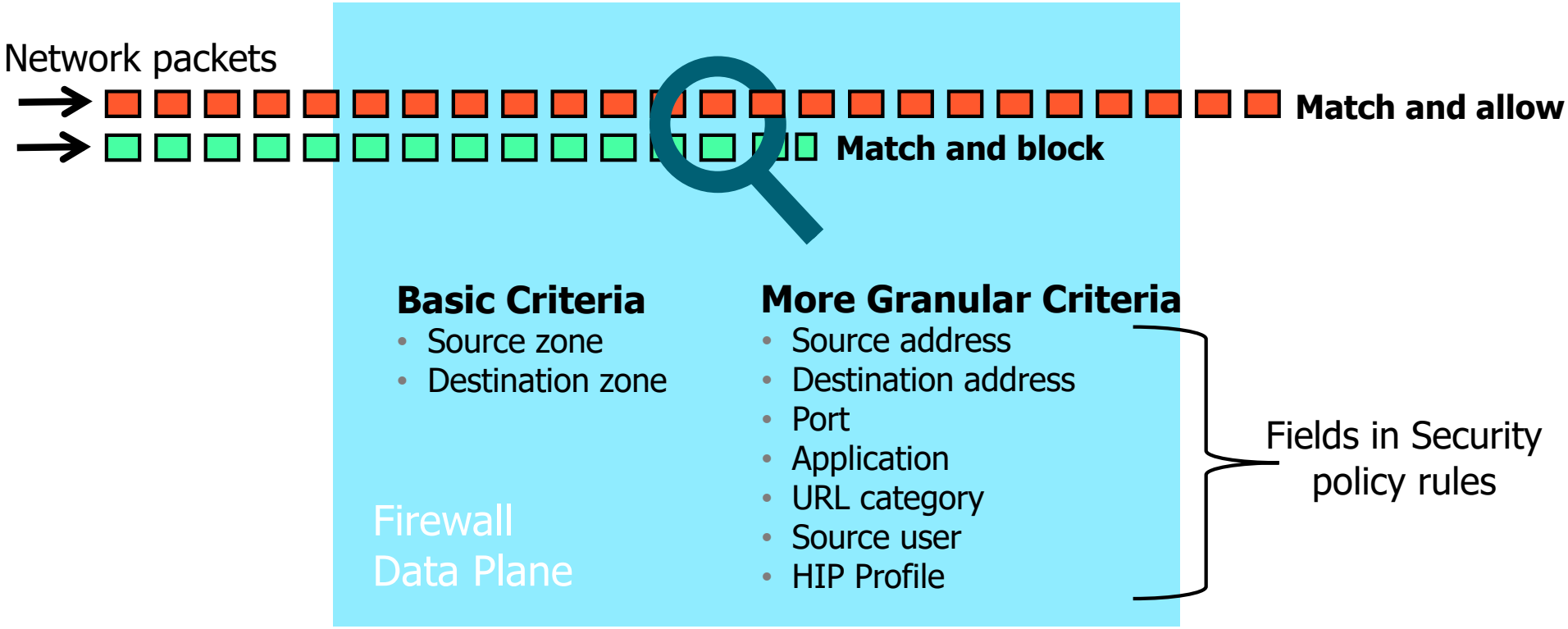
Flow Logic of the Next-Generation Firewall



*Policy check relies on pre-NAT IP addresses

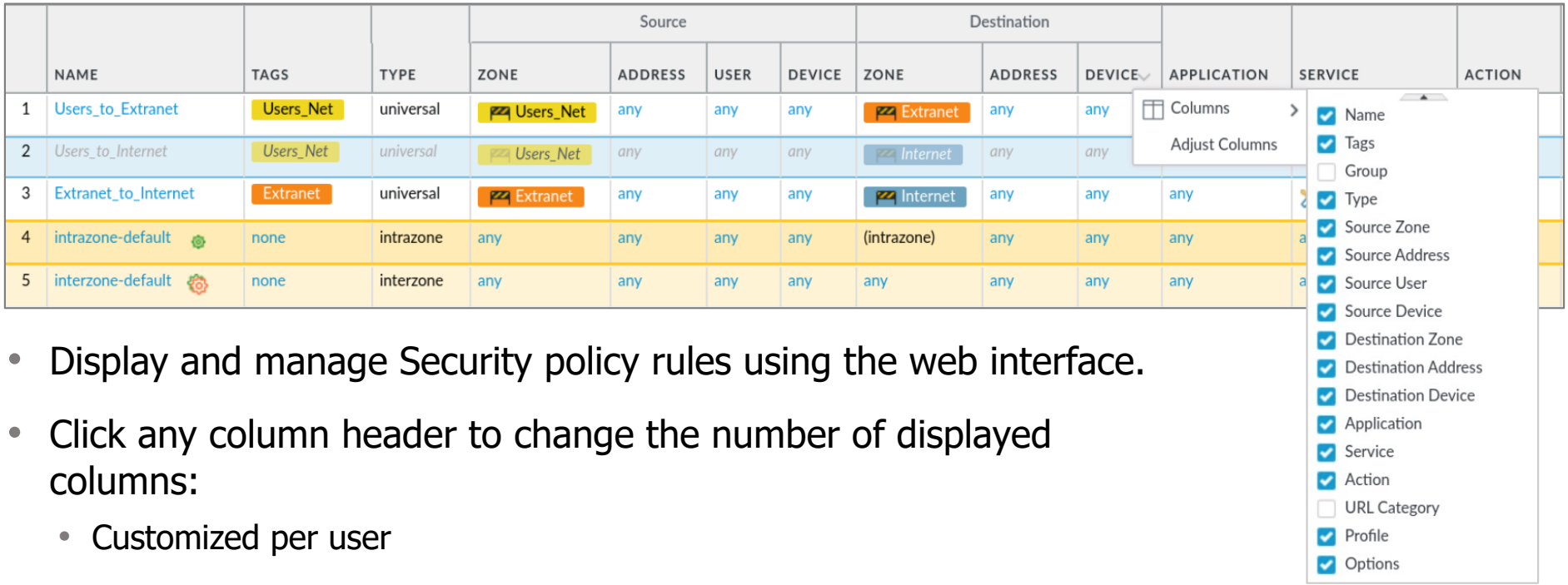
Inspect and Control Network Traffic

Multiple match criteria available to control network traffic



Display Security Policy Rules

Policies > Security

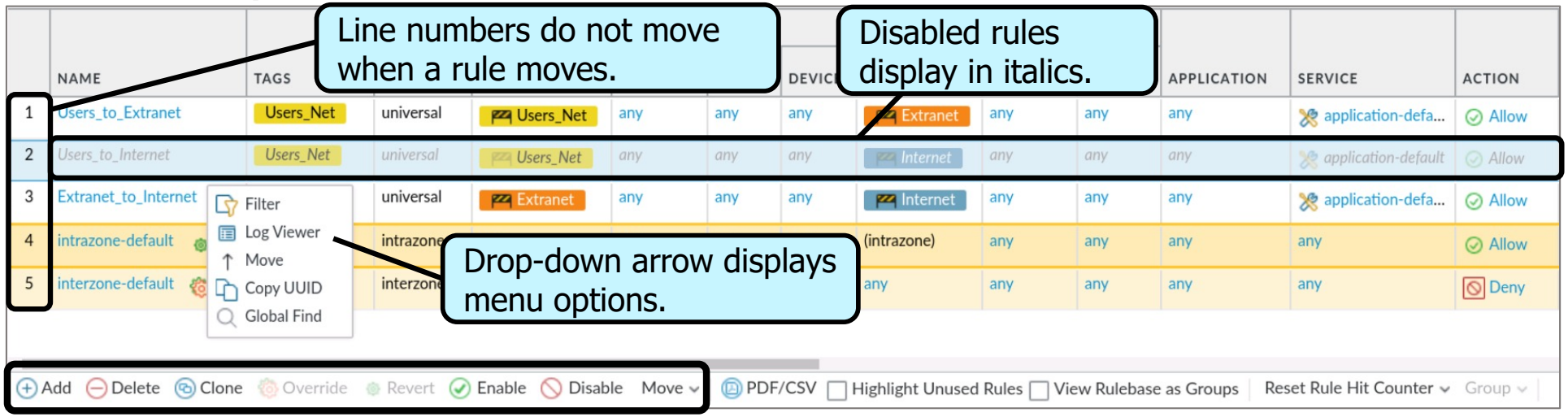


	NAME	TAGS	TYPE	Source ZONE	Source ADDRESS	Source USER	Source DEVICE	Destination ZONE	Destination ADDRESS	Destination DEVICE	APPLICATION	SERVICE	ACTION
1	Users_to_Extranet	Users_Net	universal	Users_Net	any	any	any	Extranet	any	any			
2	Users_to_Internet	Users_Net	universal	Users_Net	any	any	any	Internet	any	any			
3	Extranet_to_Internet	Extranet	universal	Extranet	any	any	any	Internet	any	any	any		
4	intrazone-default	none	intrazone	any	any	any	any	(intrazone)	any	any	any		
5	interzone-default	none	interzone	any	any	any	any	any	any	any	any		

- 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.

Manage the Policy Ruleset

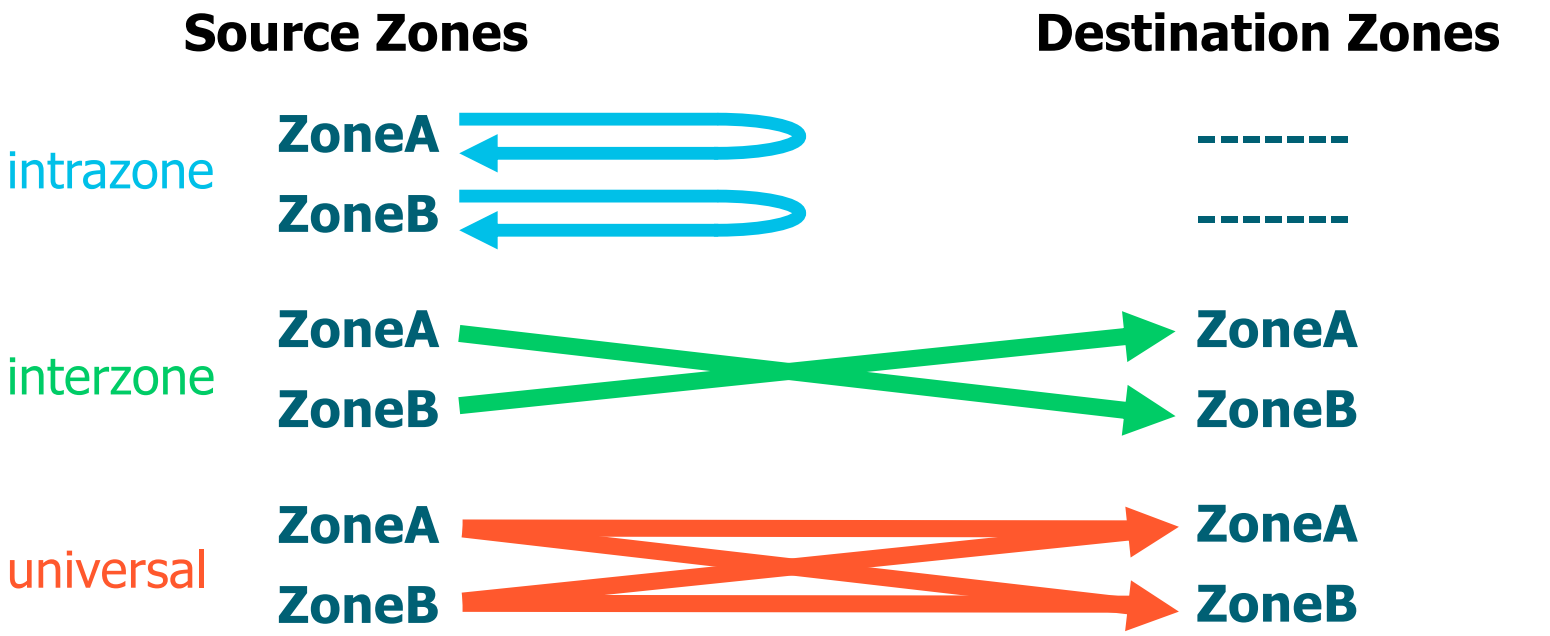
Policies > Security



- **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.

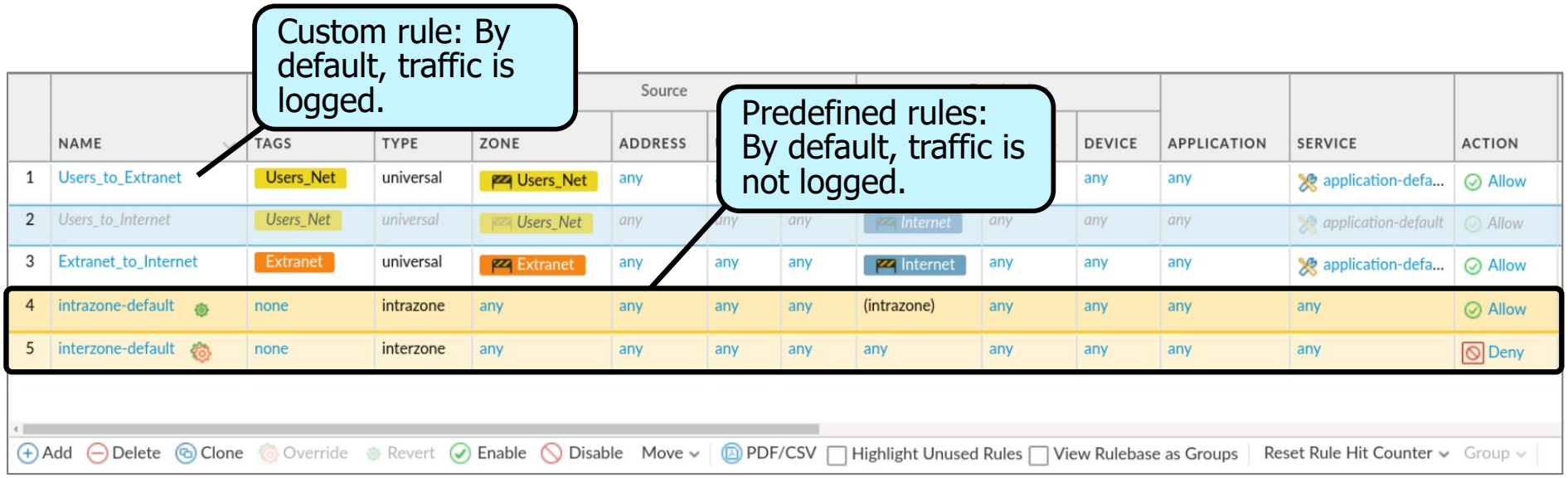
Security Policy Rule Types

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



Custom and Predefined Rules

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



Security Policy Rule Match

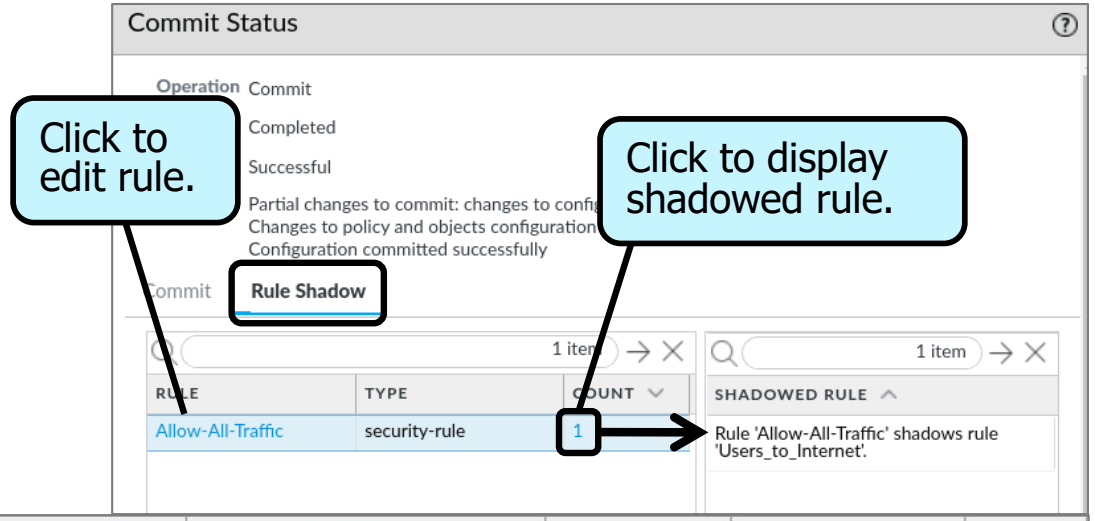
- Rules evaluated from top to bottom
- Further rules not evaluated after a rule match

	NAME	TAGS	TYPE	Source		Destination		APPLICATION	SERVICE	ACTION
				ZONE	ADDRESS	ZONE	ADDRESS			
1	Rule A	Egress	universal	Inside	any	Outside	any	web-browsing	any	Allow
2	Rule B	Egress	universal	Guest	any	Outside	any	web-browsing	any	Allow
3	Rule C	Egress	universal	DMZ	any	Outside	any	ftp	application-default	Allow
4	Rule D	Egress	universal	Inside	192.168.1.3	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.

Rule Shadowing

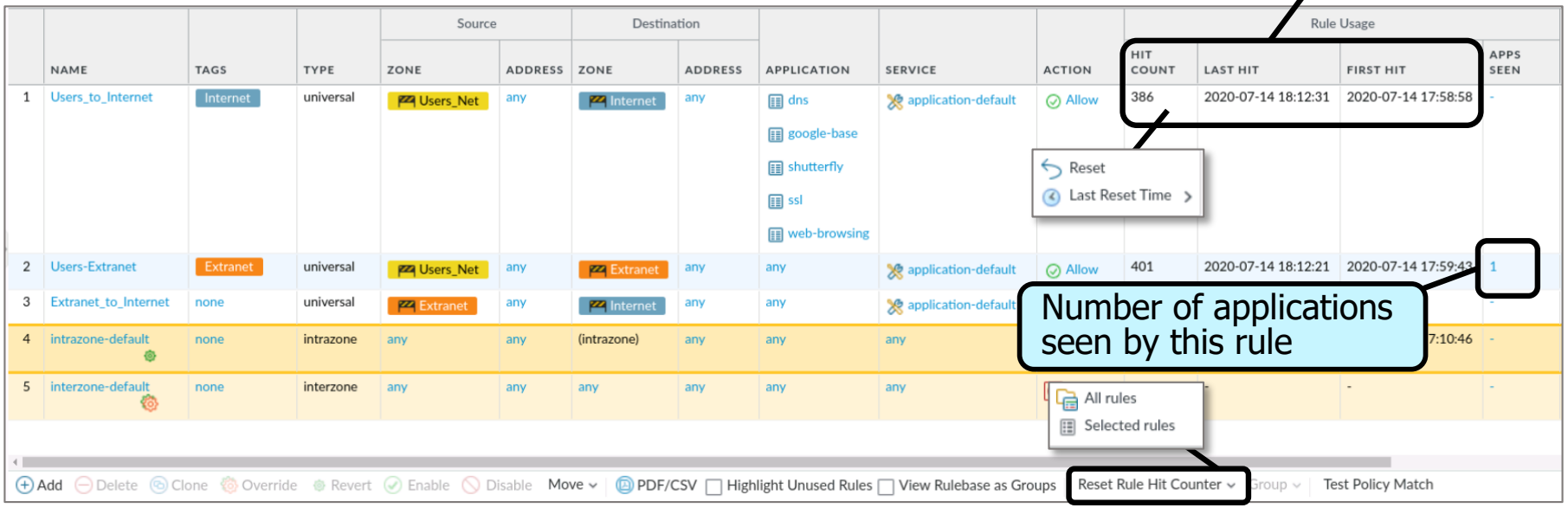
- Traffic can match multiple rules.
- Earlier rule hides (casts a shadow) over later rule.
- **Rule Shadow** tab in **Commit Status** window reports shadowed rules.
- Reorder or refine rules to remove shadowing.



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

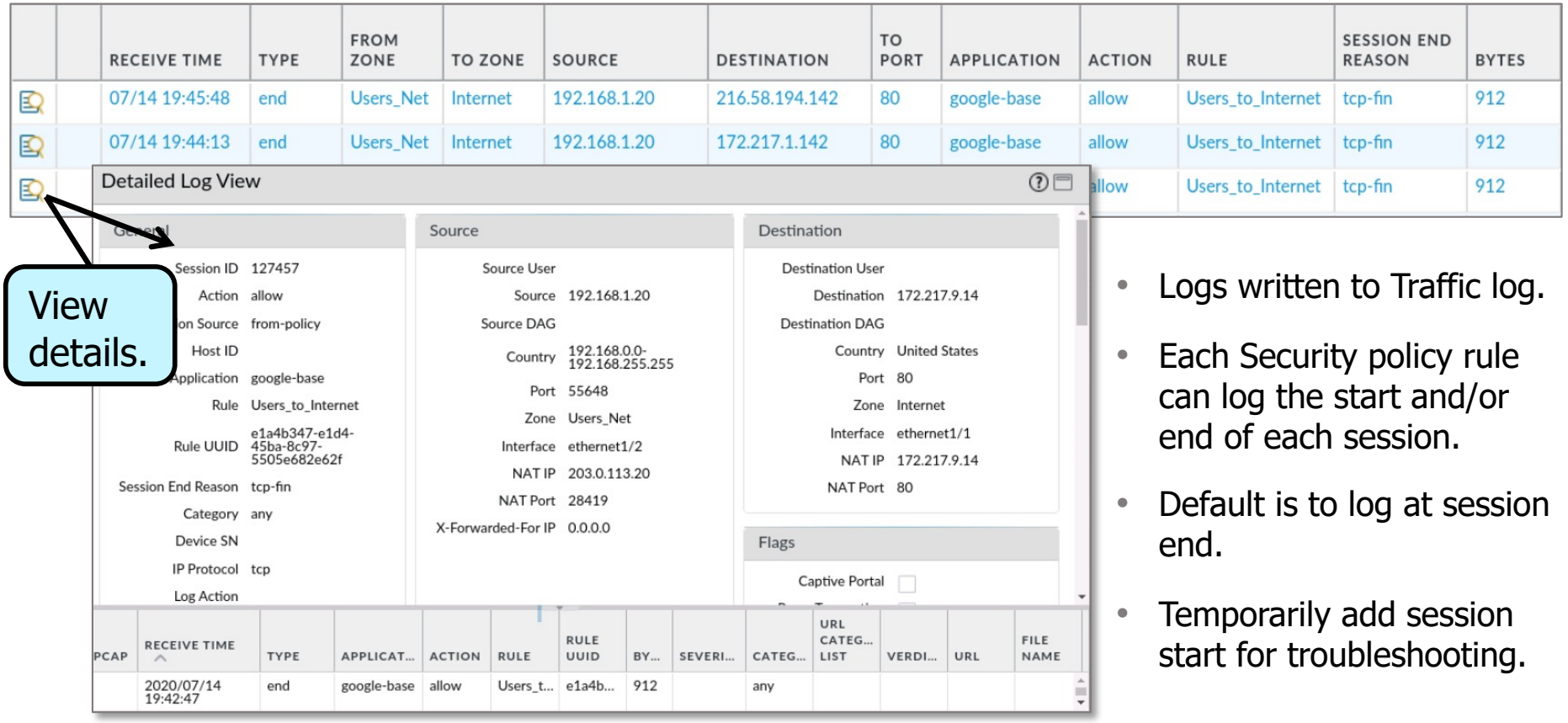
Policy Rule Hit Count

- 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 configuration changes.



View the Traffic Log

Monitor > Logs > Traffic



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

Security policy fundamental concepts

Security policy administration

Network address translation

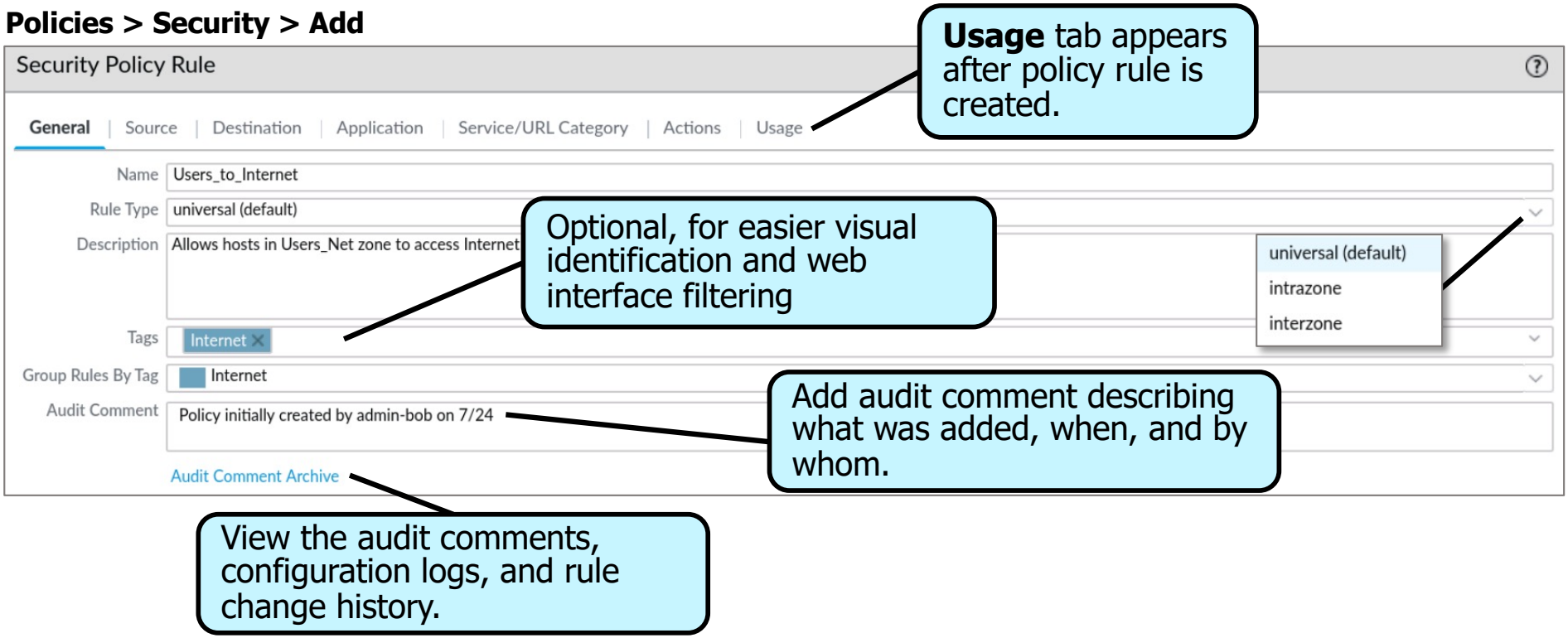
Source NAT configuration

Destination NAT configuration

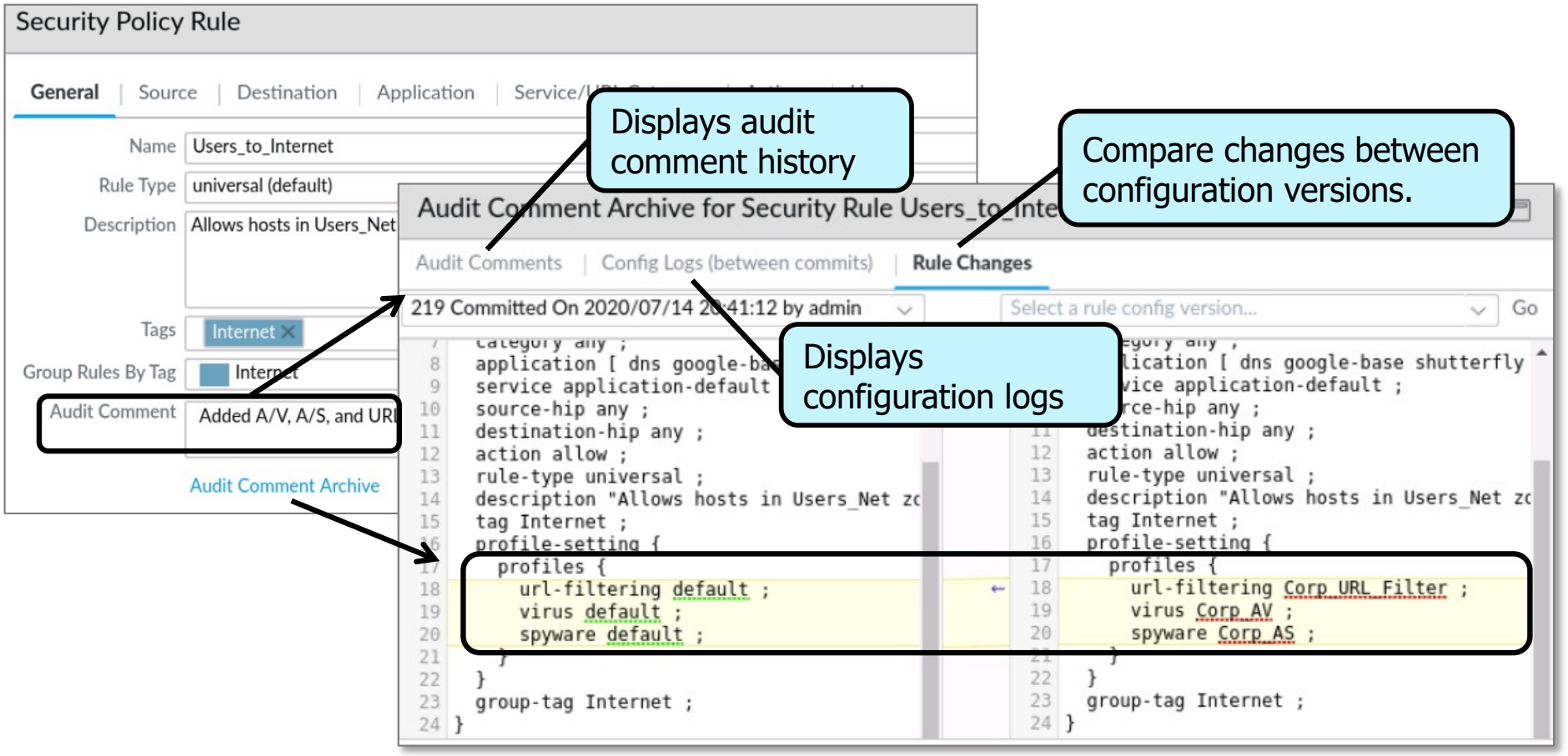
paloalto NETWORKS

Configure a Security Policy Rule: General Tab

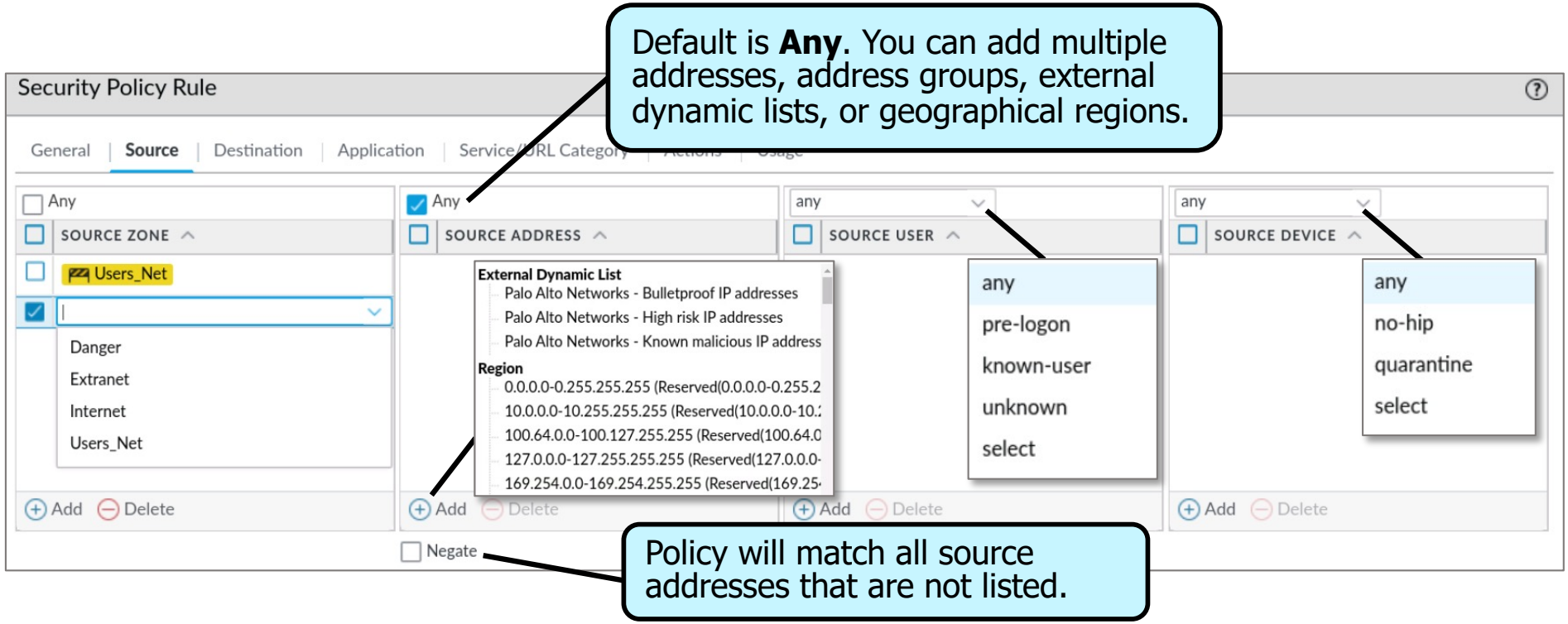
Policies > Security > Add



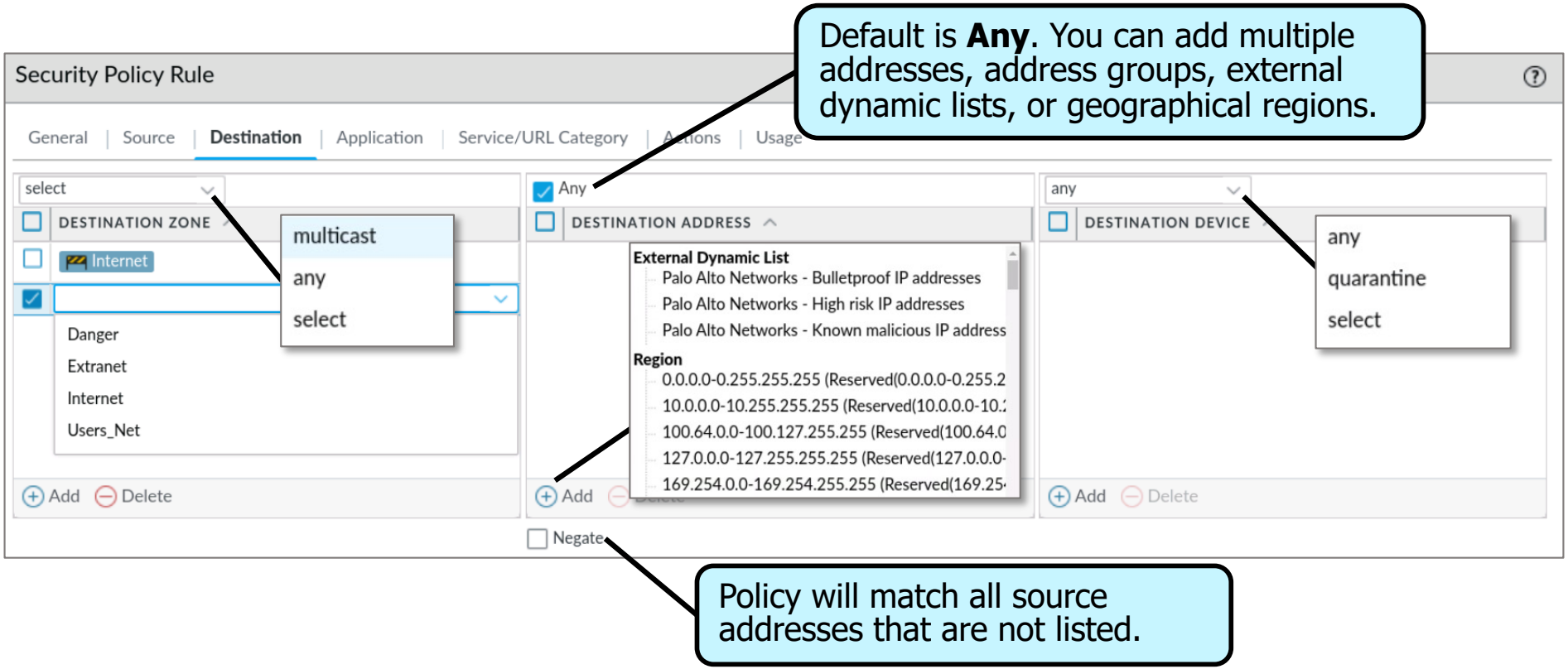
Rule Changes Archive



Configure a Security Policy Rule: Source Tab

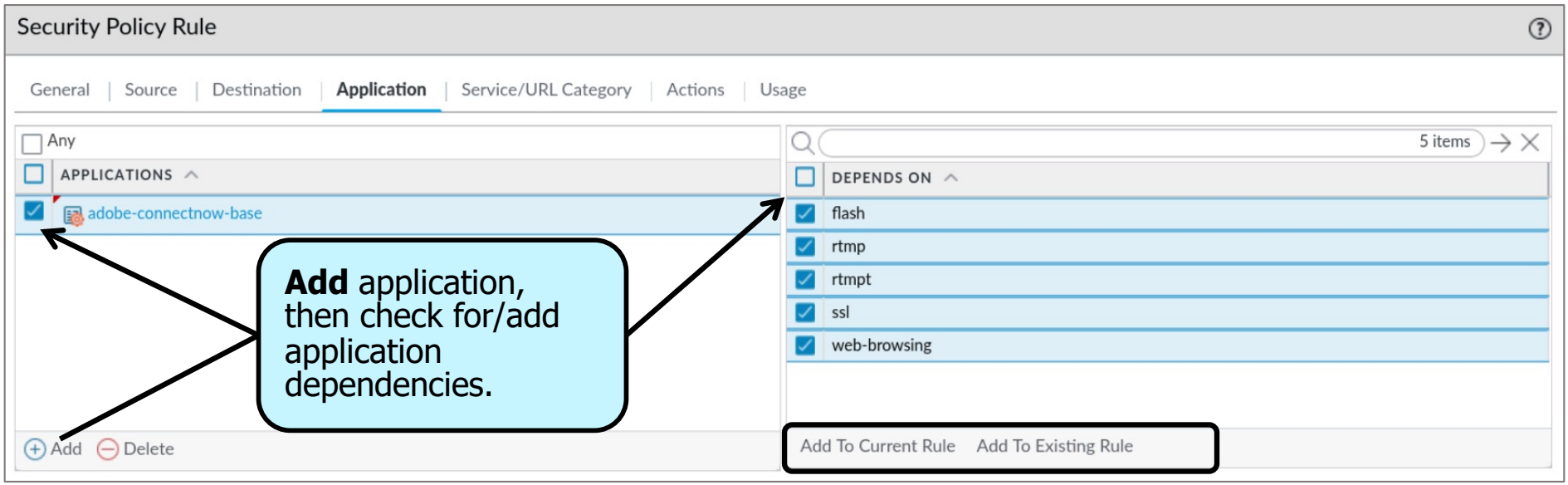


Configure a Security Policy Rule: Destination Tab



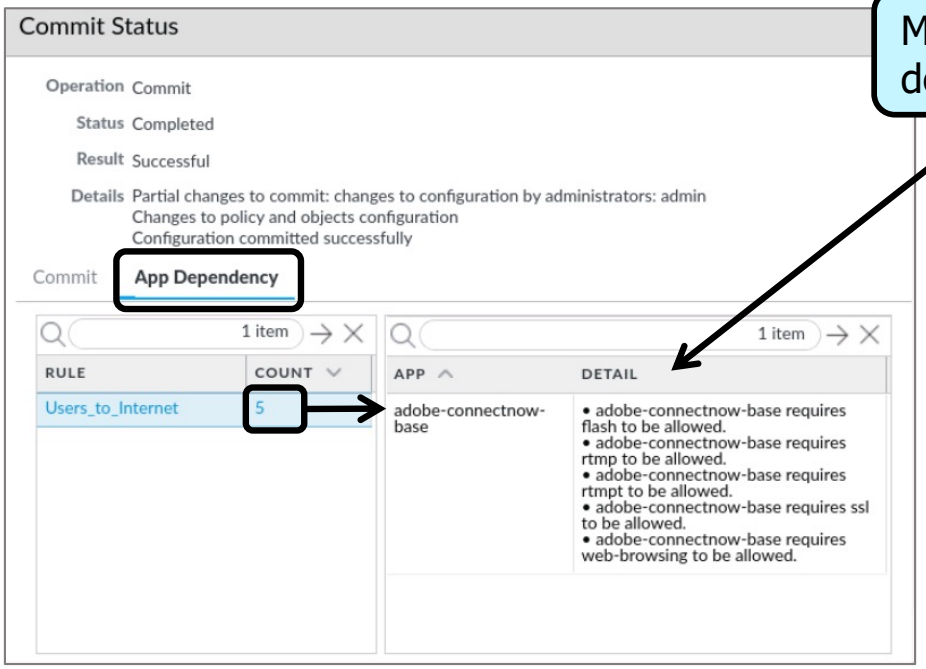
Configure a Security Policy Rule: Application Tab

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



Unresolved Dependencies Reported During a Commit

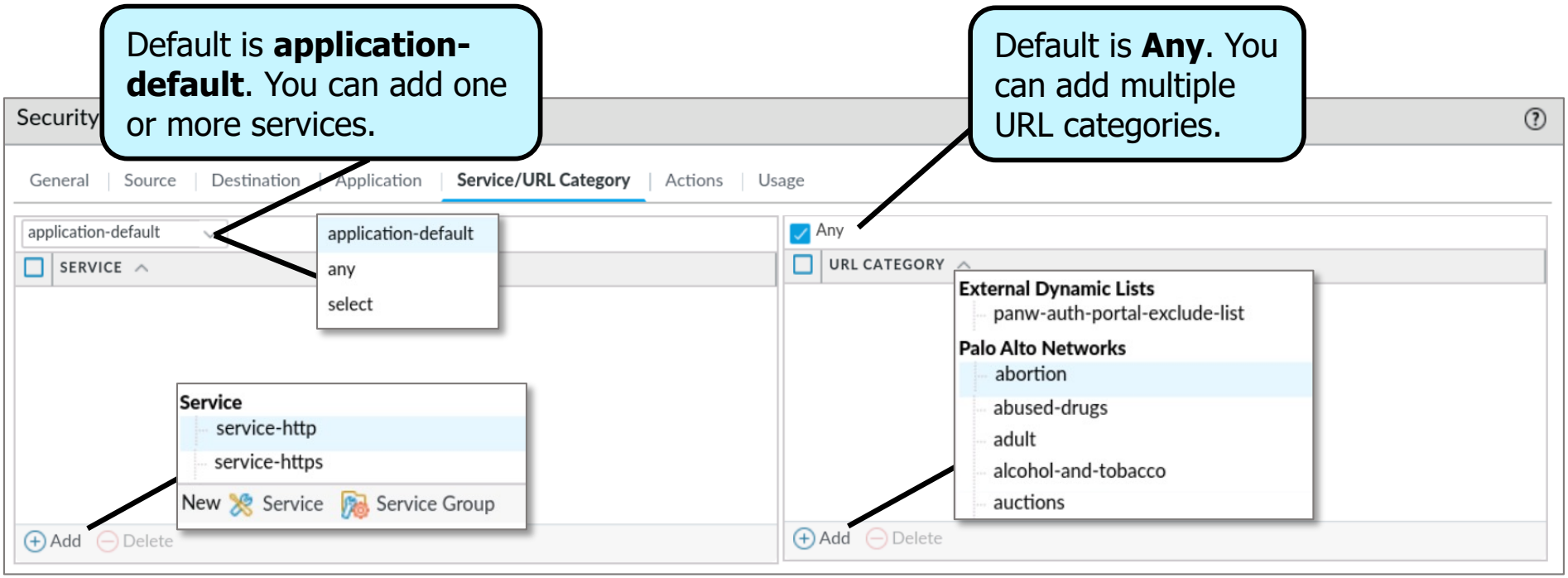
	NAME	TAGS	TYPE	Source ZONE	Source ADDRESS	Source USER	Source DEVICE	Destination ZONE	Destination ADDRESS	Destination DEVICE	APPLICATION	SERVICE	ACTION
1	Users_to_Internet	Internet	universal	Users_Net	any	any	any	Internet	any	any	adobe-connectnow-base	application-default	Allow



Missing application dependencies

- A commit determines if application dependencies in *any* rule are satisfied by *any* rule.
- Unresolved dependencies are reported per rule.
- Click rule's **Count** number to view unresolved dependencies.
- Click **<rule_name>** to open and edit rule.

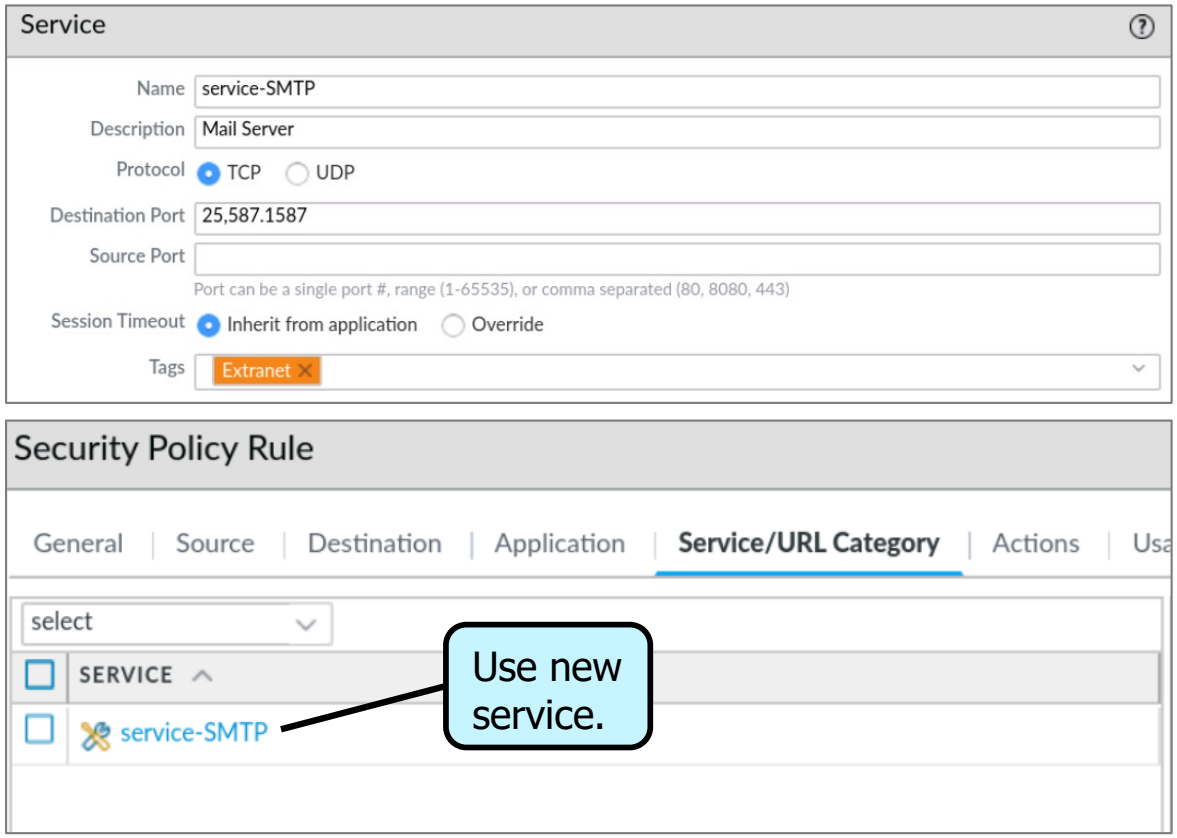
Configure a Security Policy Rule: Service/URL Category Tab



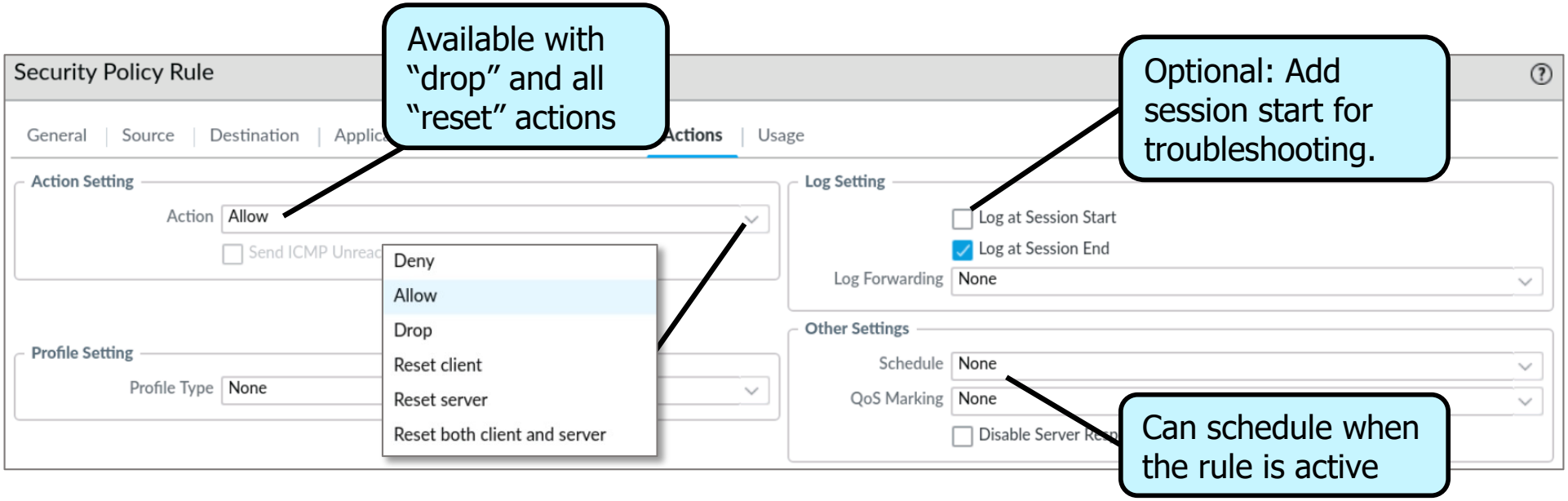
Configure a New Service Definition

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

Objects > Services > Add



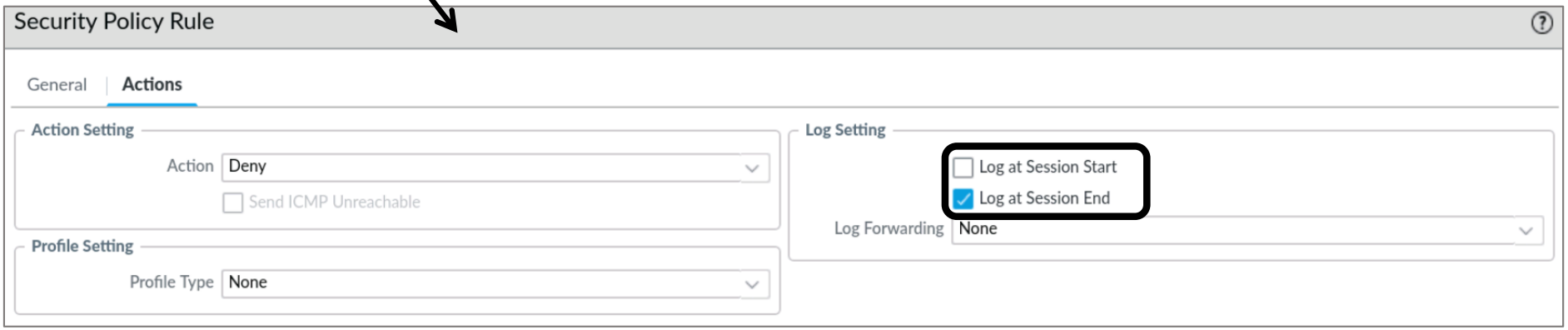
Configure a Security Policy Rule: Actions Settings



Enable Intrazone and Interzone Logging

Policies > Security > <select_default_rule>

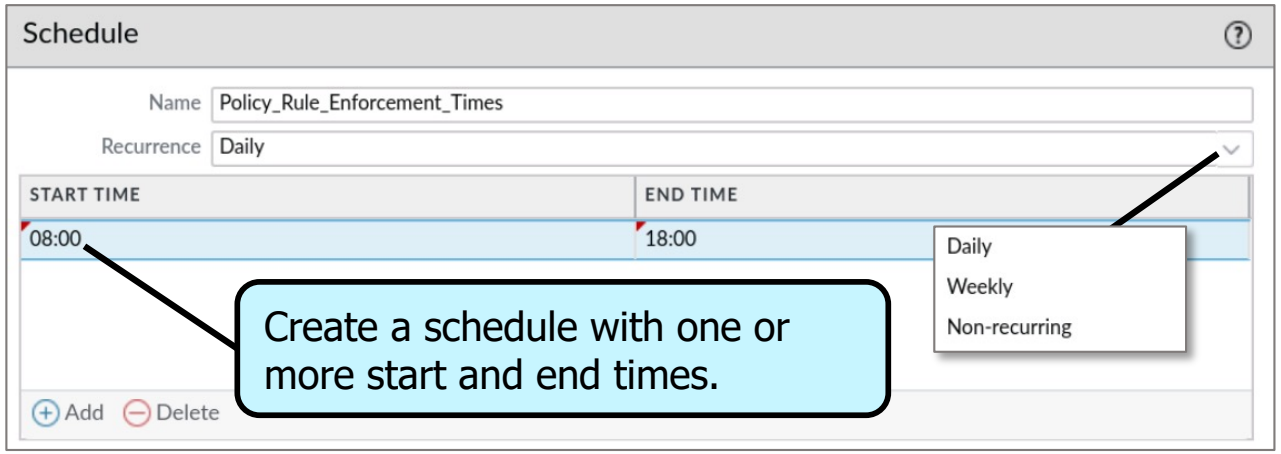
- Traffic matching default rules normally is not logged.
- Could log for visibility and troubleshooting purposes.



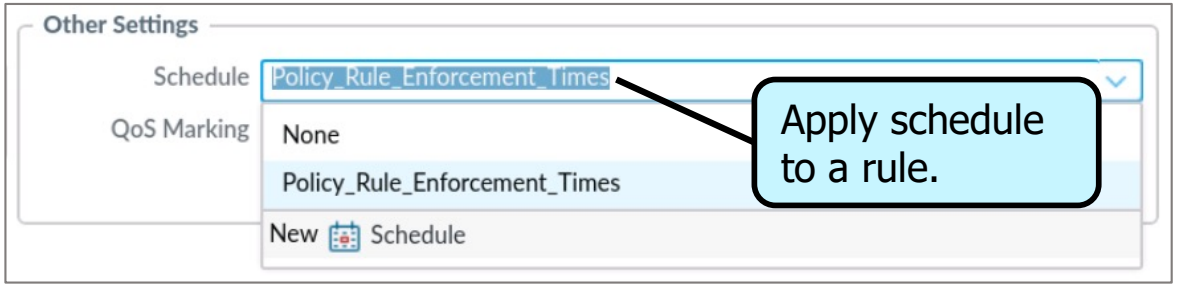
Schedule Security Policy Rules

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

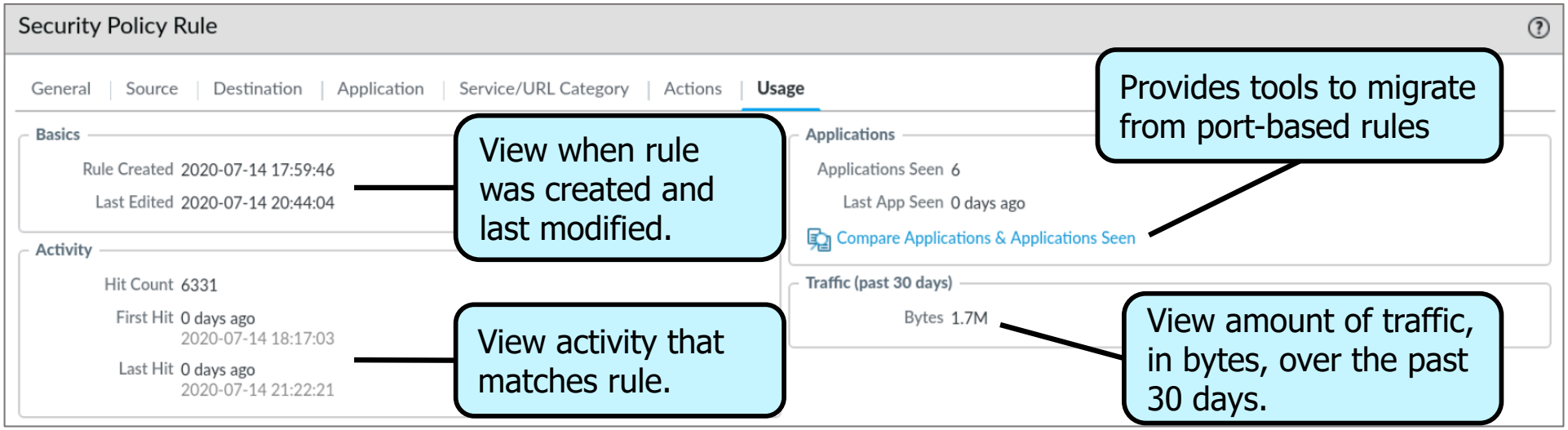
Objects > Schedules > Add



Policies > Security > <select_rule> > Actions



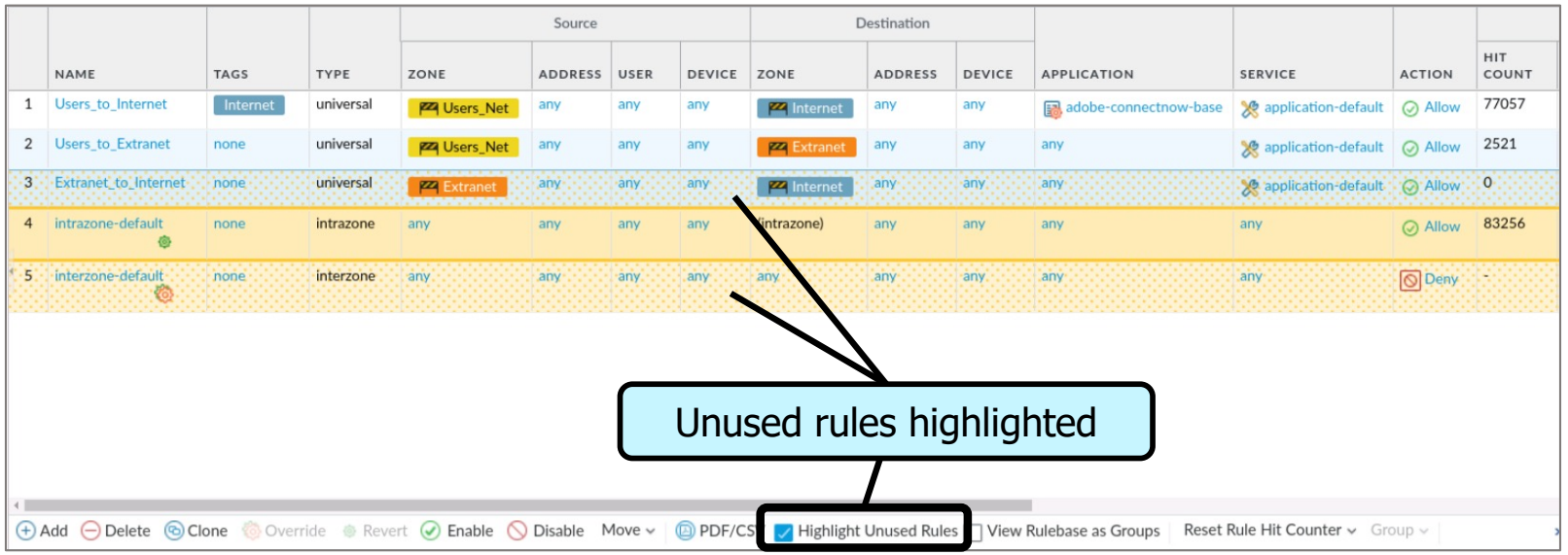
Configure a Security Policy Rule: Usage Settings



Find Unused Security Policy Rules

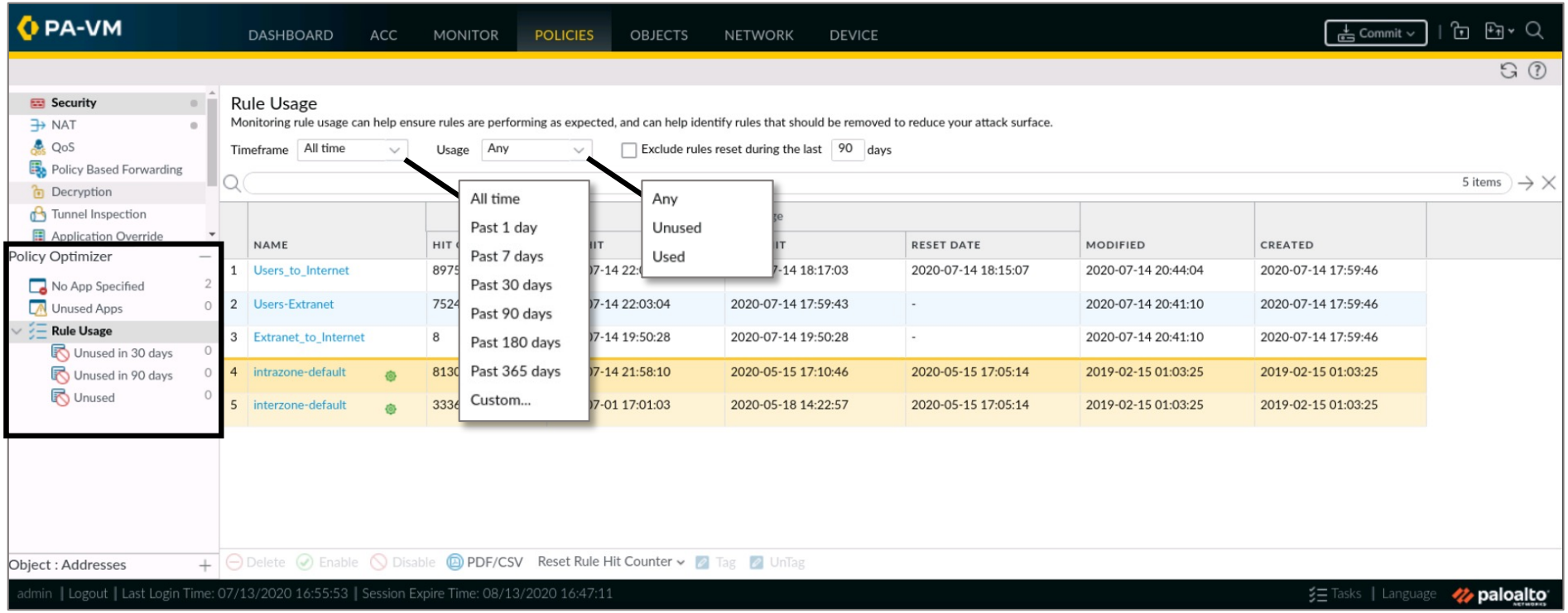
- Remove unused rules to:
  - Increase firewall operational efficiency
  - Simplify rule management
- Firewall tracks rules unused since last time the data plane restarted.

Policies > Security



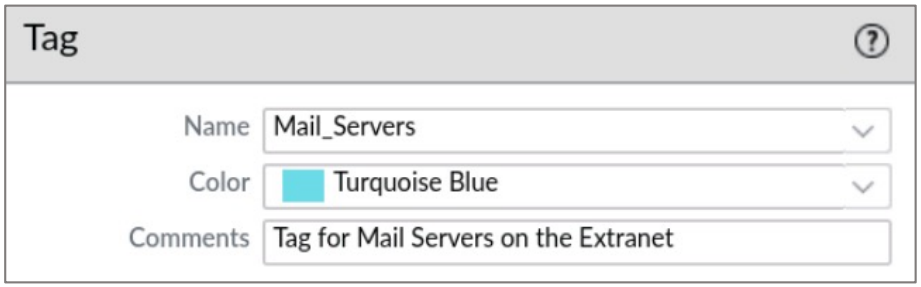
Rule Usage Filter

Policies > Security > Policy Optimizer > Rule Usage

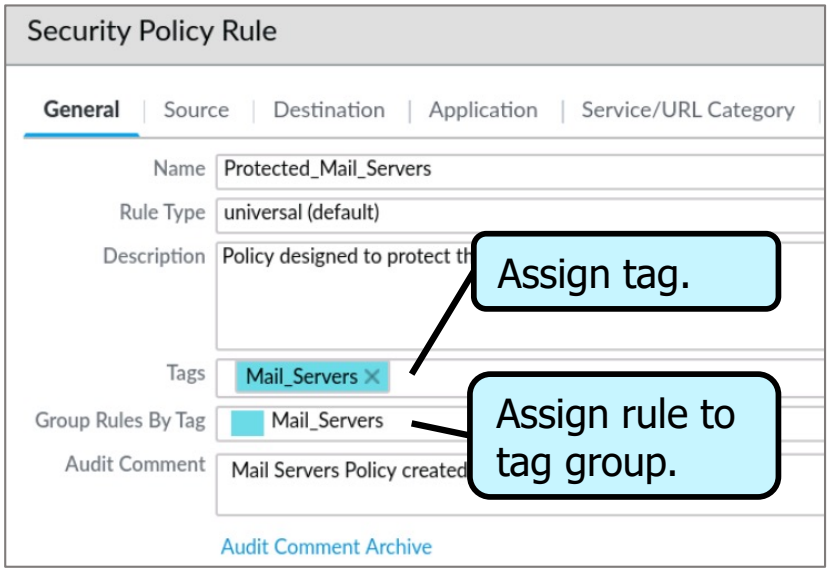


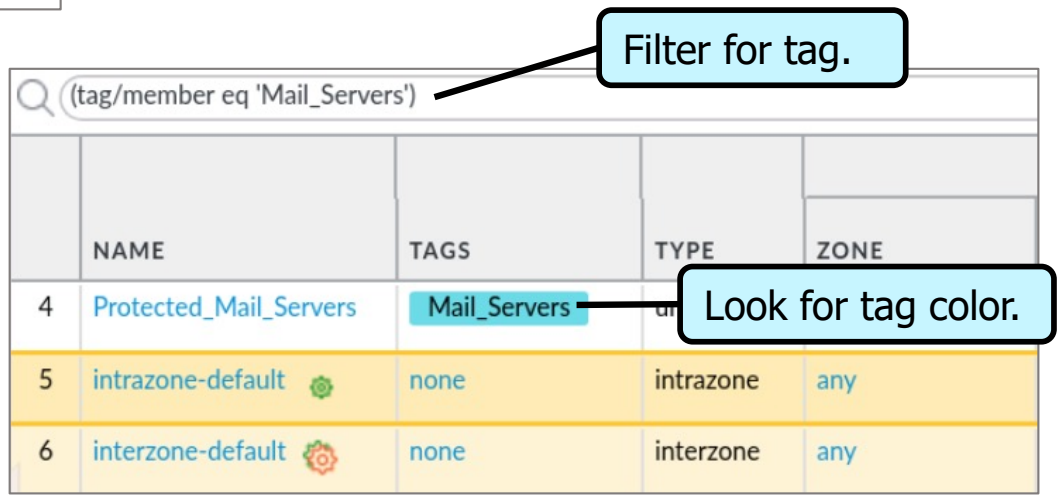
Tags

Objects > Tags > Add



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

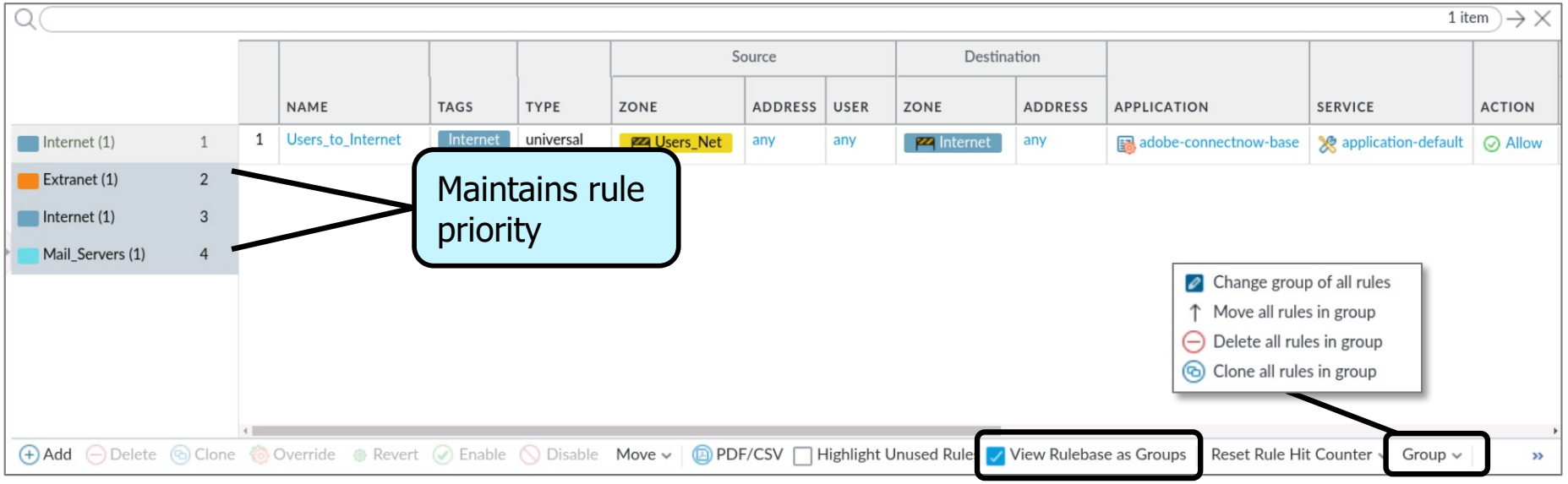




Tag-Based Rule Groups

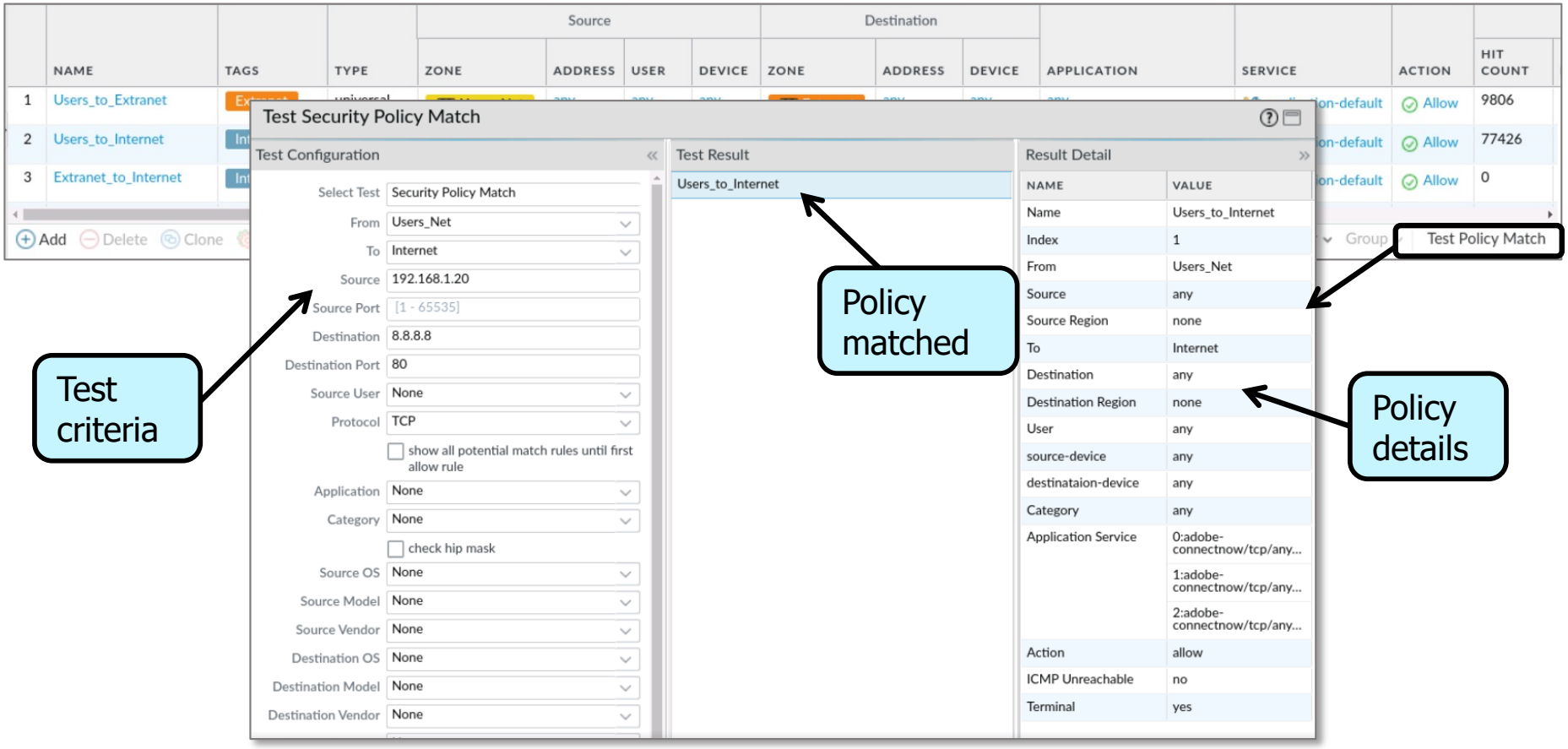
- Visually group rules based on tagging structure
- Can perform operational procedures within the selected tag group

Policies > Security



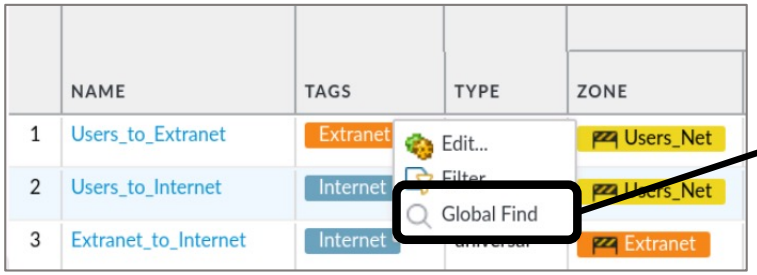
Test Policy Functionality

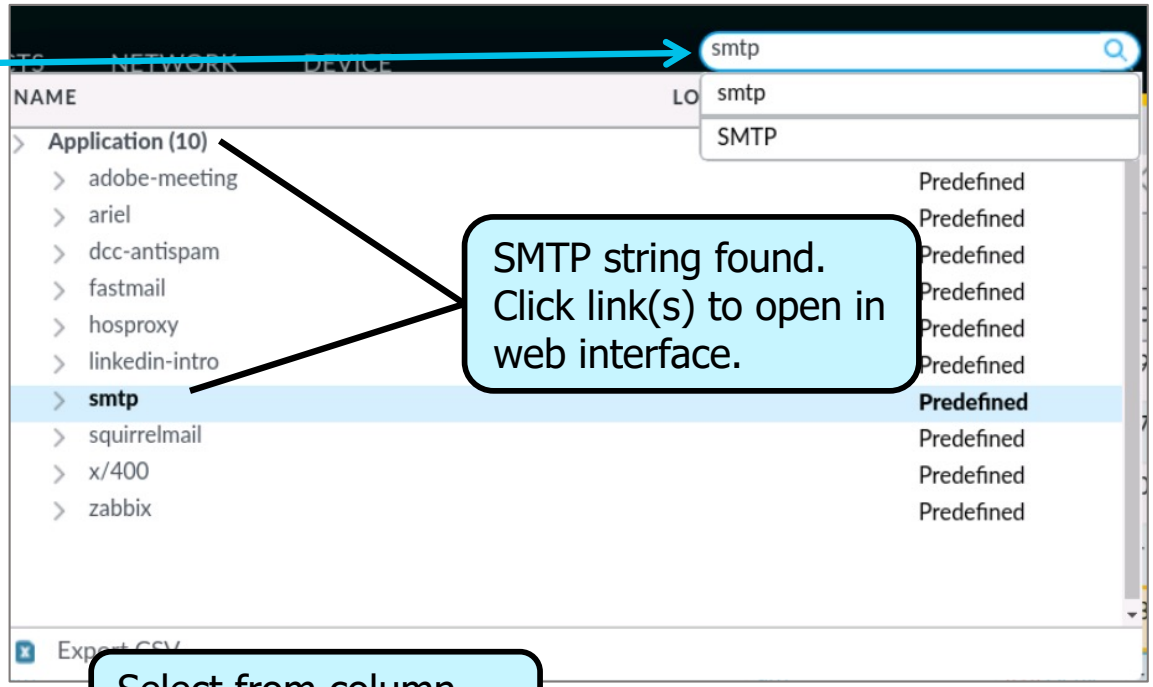
Policies > Security



Use Global Find

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





Security policy fundamental concepts

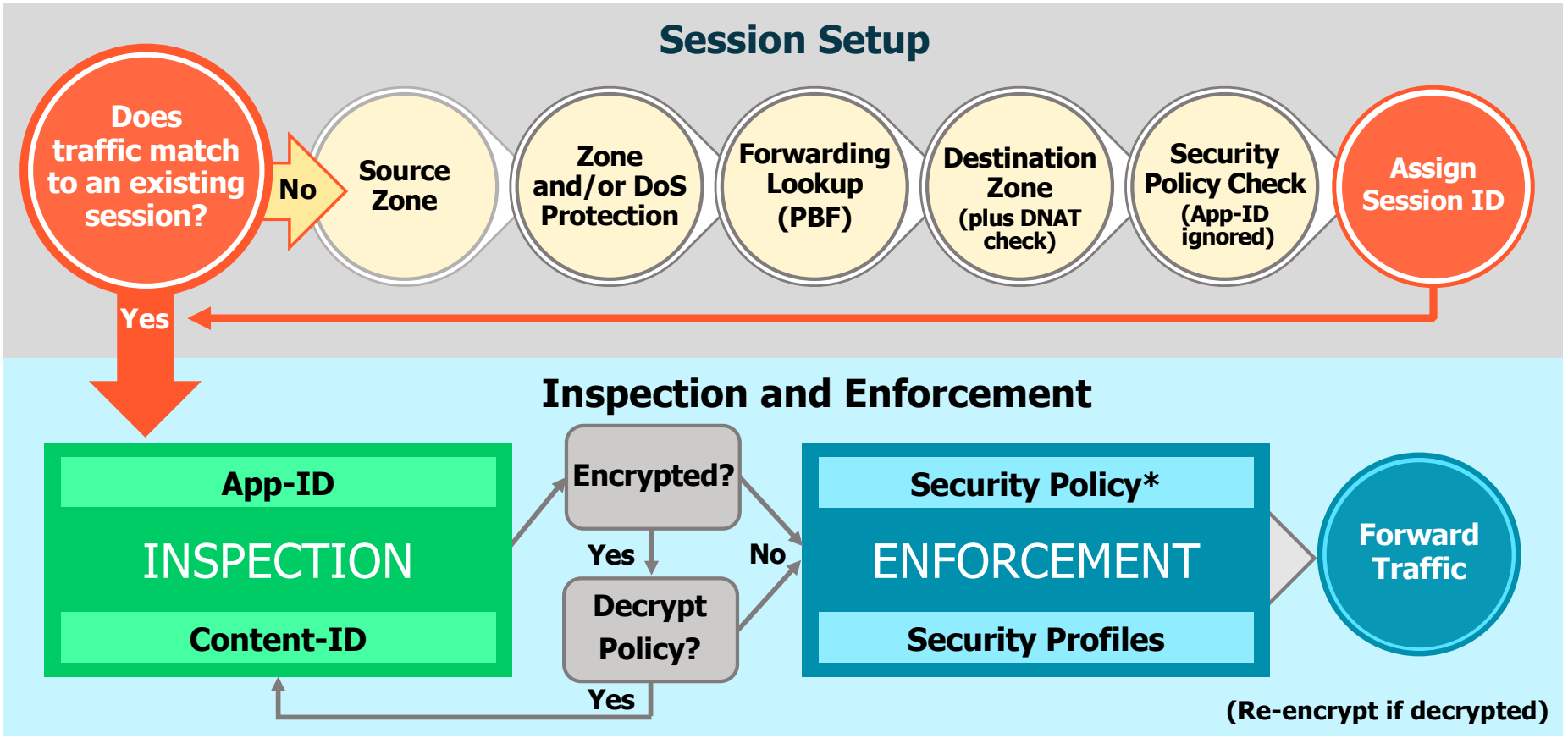
Security policy administration

Network address translation

Source NAT configuration

Destination NAT configuration

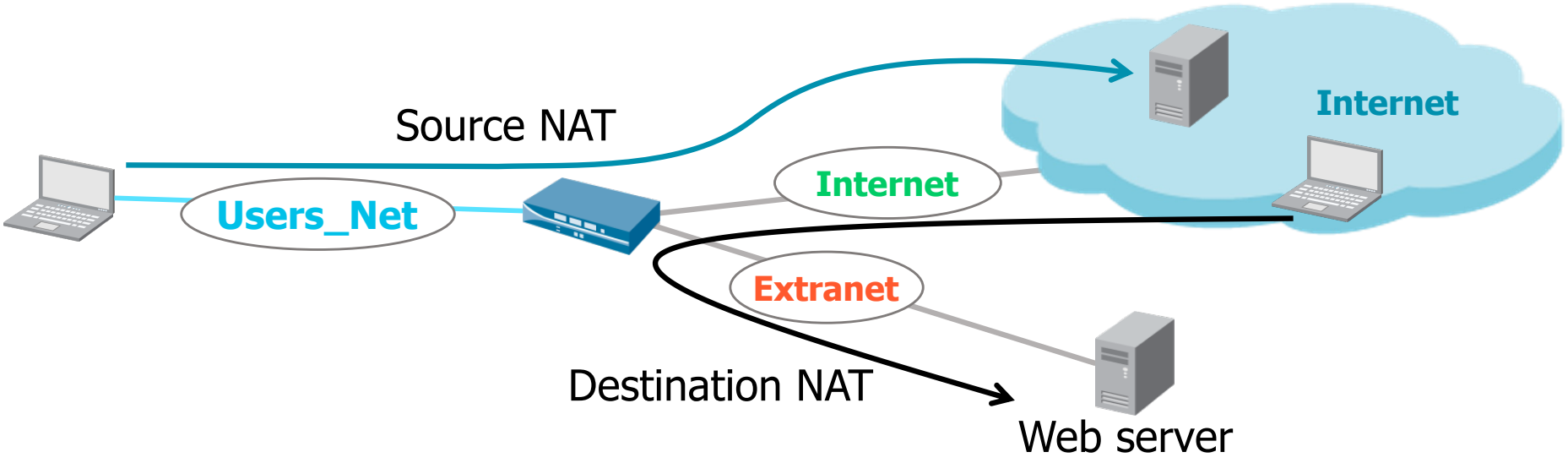
Flow Logic of the Next-Generation Firewall



*Policy check relies on pre-NAT IP addresses

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.



Security policy fundamental concepts

Security policy administration

Network address translation

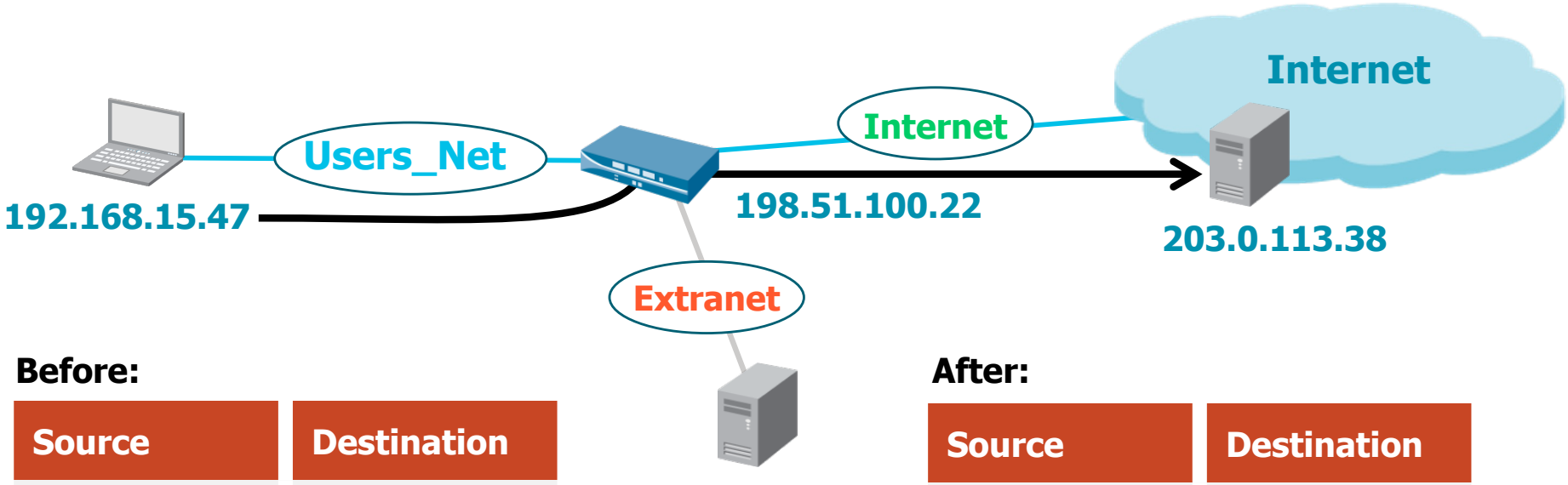
Source NAT configuration

Destination NAT configuration

paloalto NETWORKS

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
Users_Net	Internet

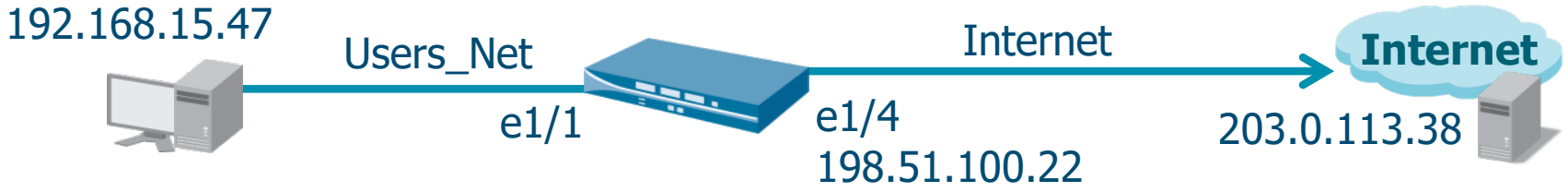
After:

Source	Destination
198.51.100.22	203.0.113.38
Internet	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 and Security Policies



Policies > NAT

	NAME	TAGS	Original Packet: SOURCE ZONE	DESTINATION ZONE	DESTINATION INTERFACE	SOURCE ADDRESS	DESTINATION ADDRESS	SERVICE	Translated Packet: SOURCE TRANSLATION	DESTINATION TRANSLATION	HIT COUNT
1	Source_Users_Net_to_Internet	Internet	Users_Net	Internet	any	192.168.15.0/24	any	any	dynamic-ip-and-port ethernet1/1 198.51.100.22	none	283983

Pre-NAT zones

Pre-NAT addresses

Policies > Security

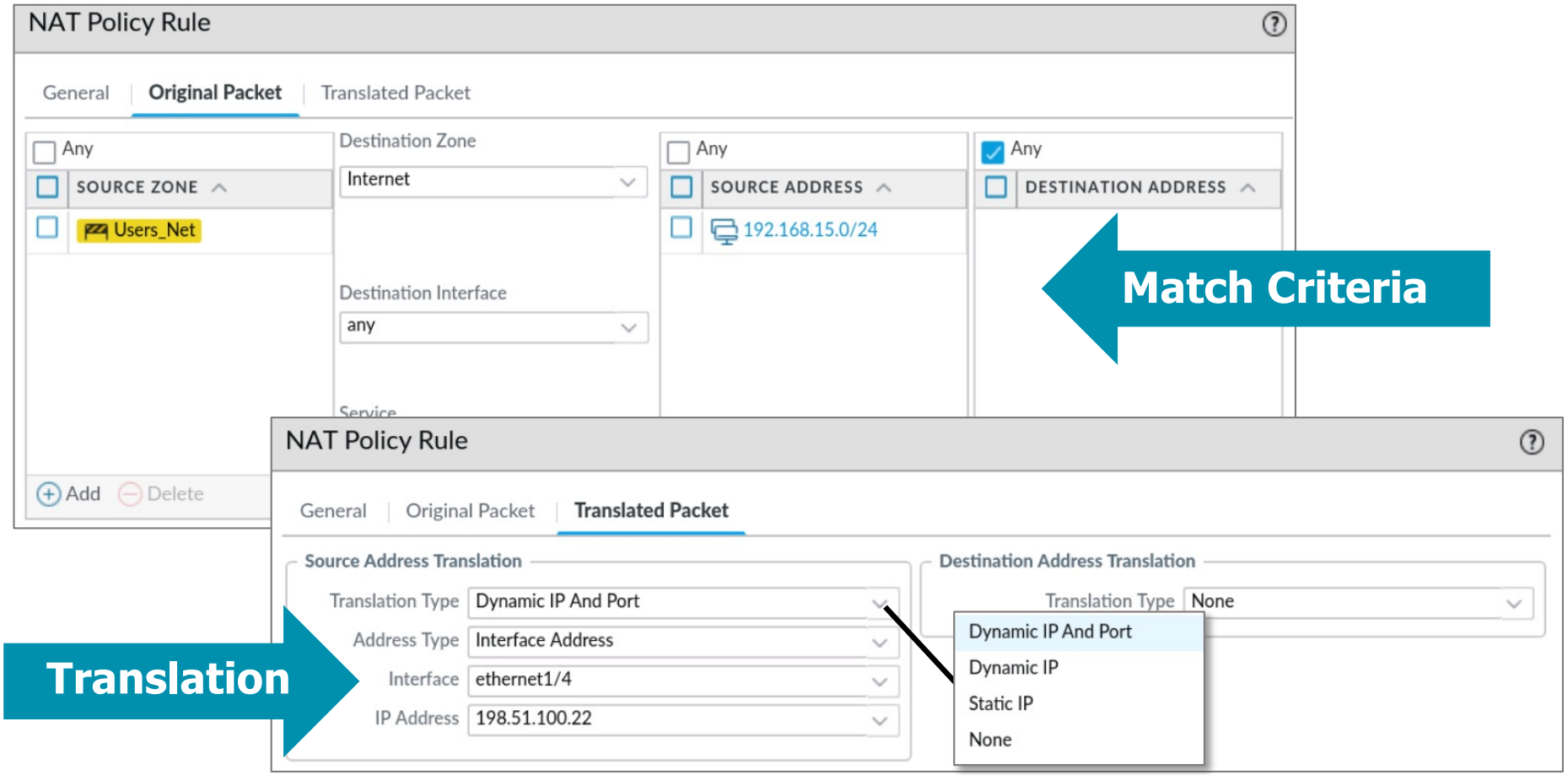
	NAME	TAGS	TYPE	Source: ZONE	Source: ADDRESS	Destination: ZONE	Destination: ADDRESS	APPLICATION	SERVICE	ACTION
1	Users_to_Internet	Internet	universal	Users_Net	192.168.15.0/24	Internet	any	ssl web-browsing	application-default	Allow

Pre-NAT address

Post-NAT zone

Pre-NAT address

Configure Source NAT



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
1	Source_Users_Net_to_Internet	Internet	Users_Net	Internet	any	192.168.15.47	any	any	static-ip 198.51.100.22 bi-directional: yes	none

Dynamic IP Translation

Policies > NAT

			Original Packet						Translated Packet	
	NAME	TAGS	SOURCE ZONE	DESTINATION ZONE	DESTINATION INTERFACE	SOURCE ADDRESS	DESTINA... ADDRESS	SERVICE	SOURCE TRANSLATION	DESTINATION TRANSLATION
1	Source_Users_Net_to_Internet	Internet	Users_Net	Internet	any	192.168.15.2-192.168.15.50	any	any	dynamic-ip 198.51.100.102-198.51.100.150	none

Source NAT Examples (Cont.)

Dynamic IP and Port Translation

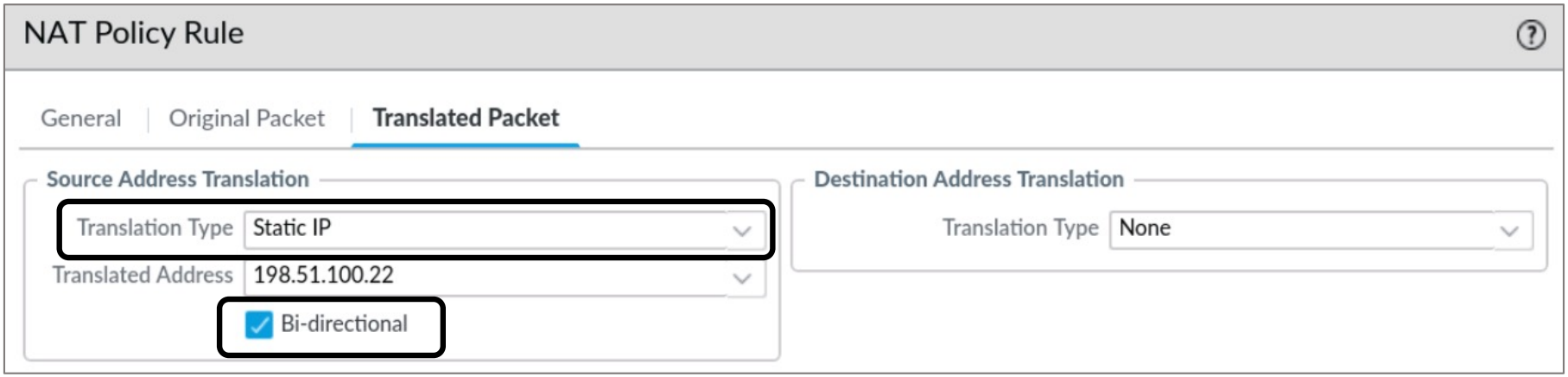
Policies > NAT

	NAME	TAGS	Original Packet						Translated Packet	
			SOURCE ZONE	DESTINATION ZONE	DESTINATION INTERFACE	SOURCE ADDRESS	DESTINA... ADDRESS	SERVICE	SOURCE TRANSLATION	DESTINATION TRANSLATION
1	Source_Users_Net_to_Internet	Internet	Users_Net	Internet	any	192.168.15.0/24	any	any	dynamic-ip-and-port 198.51.100.22-198.51.100.23	none

Configure Bidirectional Source NAT

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

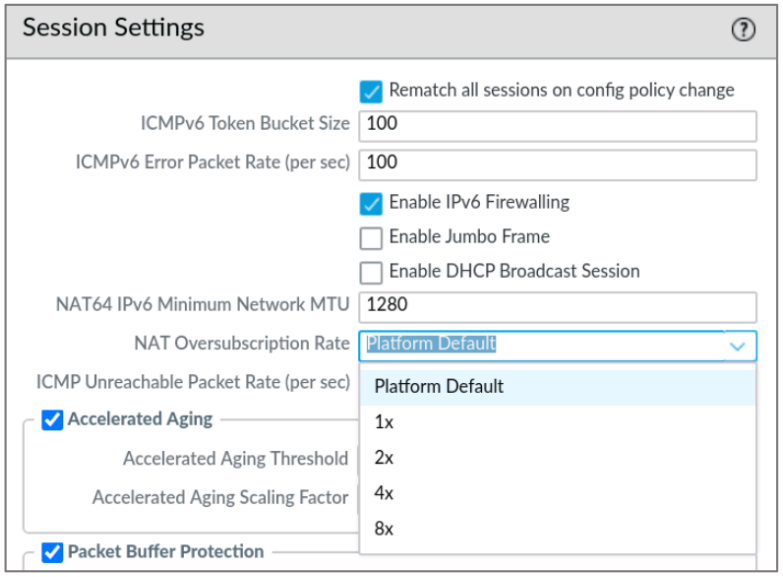
Policies > NAT



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



Internal Source Port	Firewall Source Port	Destination Address
26435	198.51.100.22:25661	51.6.33.12
35435	198.51.100.22:25661	161.8.55.4
21569	198.51.100.22:25661	201.55.45.1
51043	198.51.100.22:25661	17.39.25.6

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

Security policy fundamental concepts

Security policy administration

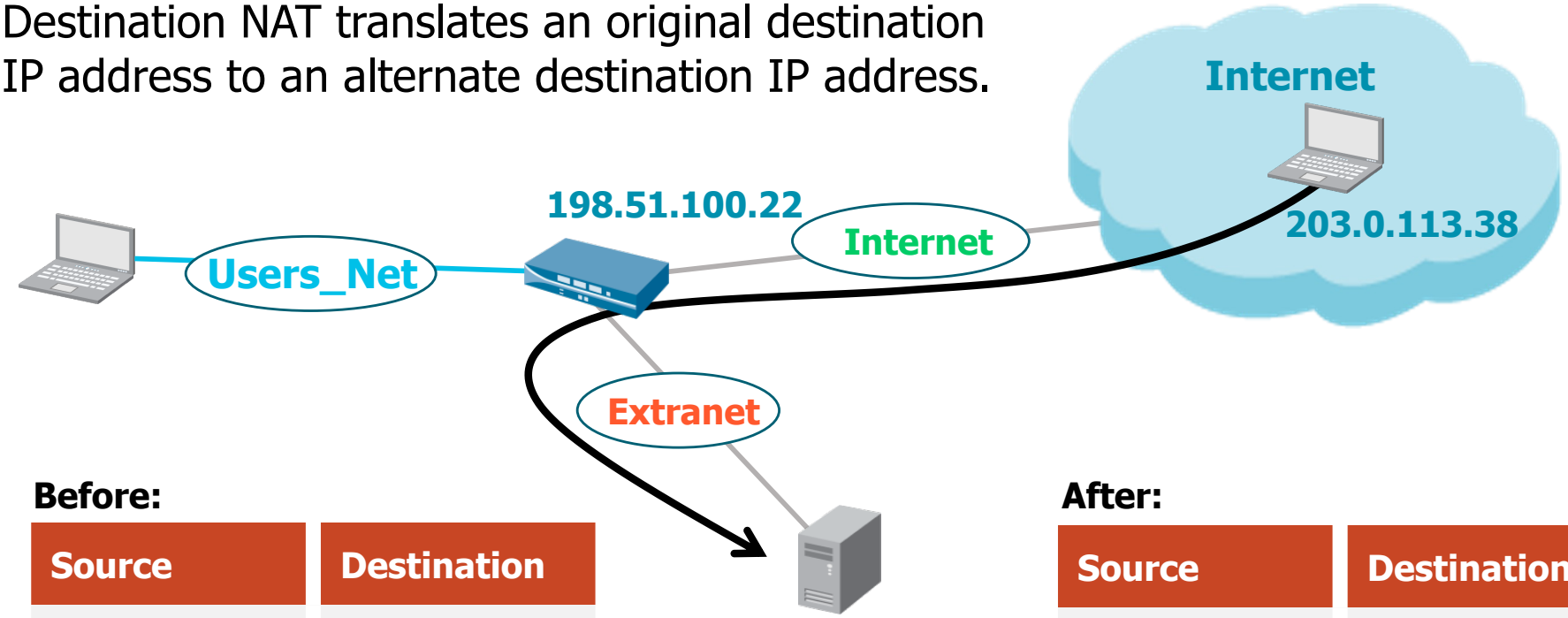
Network address translation

Source NAT configuration

Destination NAT configuration

Destination NAT

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



Before:

Source	Destination
203.0.113.38	198.51.100.22
Internet	Internet

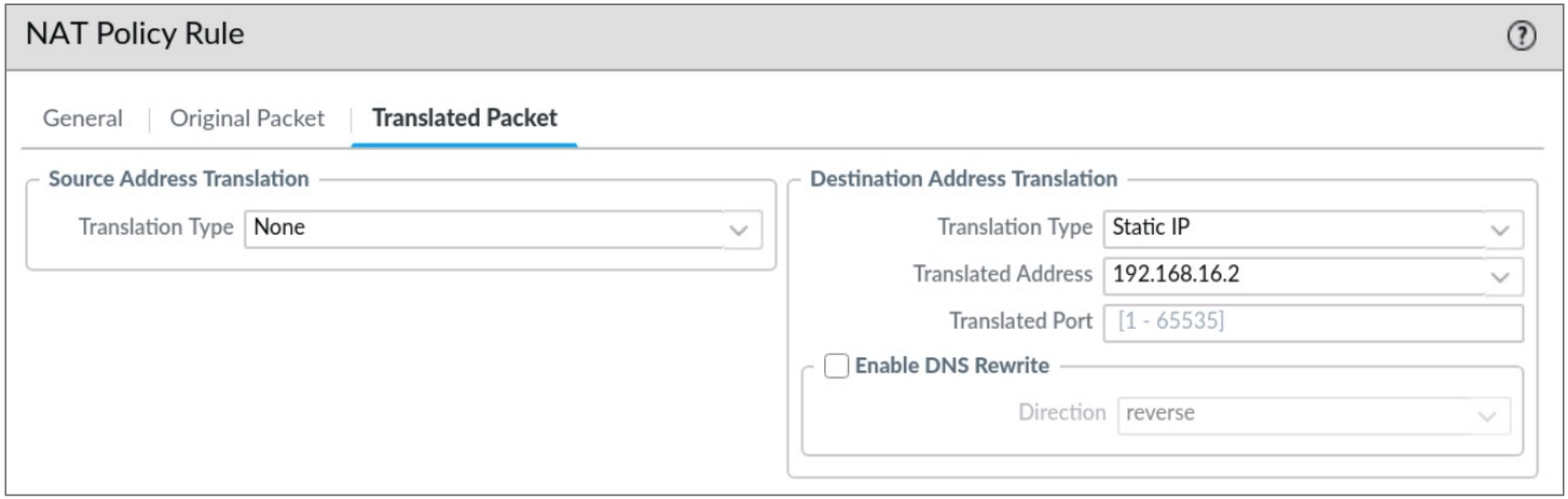
After:

Source	Destination
203.0.113.38	192.168.16.2
Internet	Extranet

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

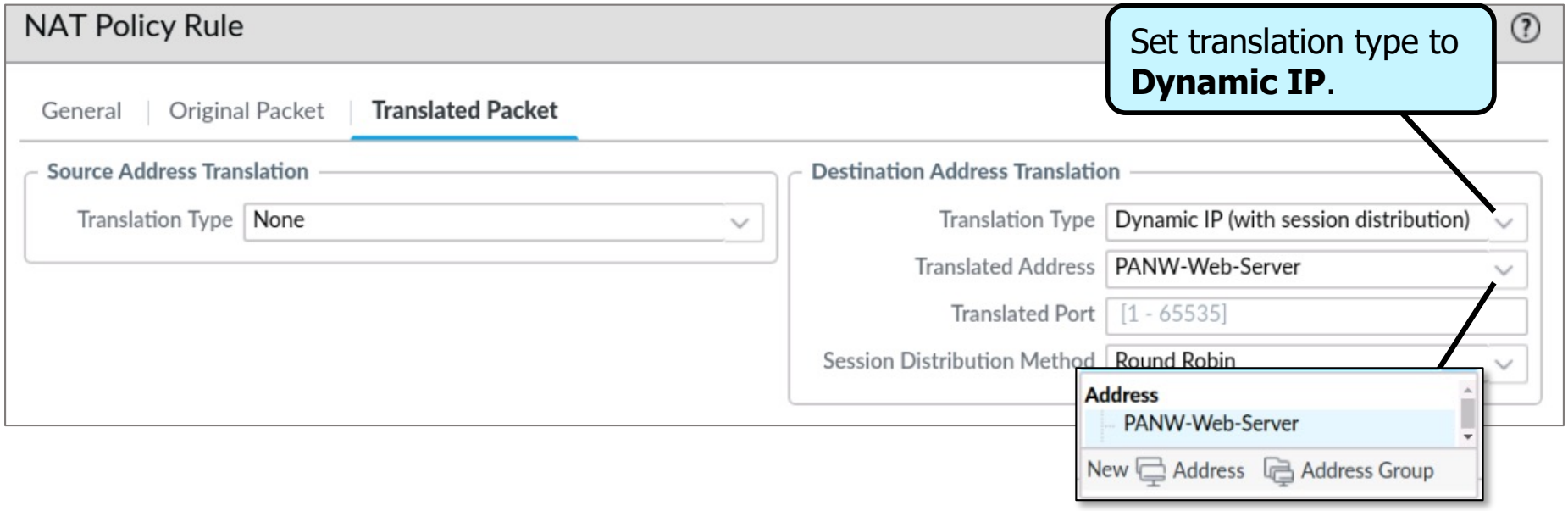
Policies > NAT > Add



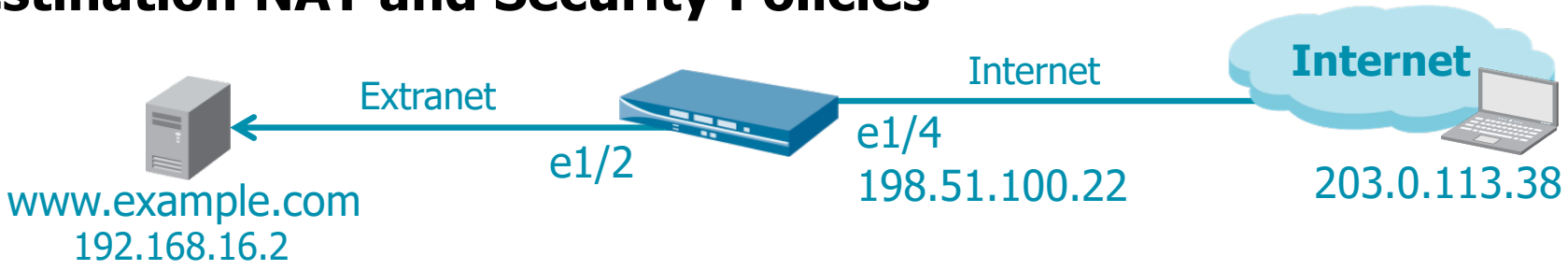
Dynamic IP Address Support for Destination NAT

- 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



Destination NAT and Security Policies



Policies > NAT

	NAME	TAGS	Original Packet						Translated Packet	
			SOURCE ZONE	DESTINATION ZONE	DESTINATION INTERFACE	SOURCE ADDRESS	DESTINATION ADDRESS	SERVICE	SOURCE TRANSLATION	DESTINATION TRANSLATION
1	Dest_NAT_From_Internet	Internet	Internet	Internet	any	any	198.51.100.22	service-http	none	destination-translation address: 192.168.16.2

Pre-NAT zones

Pre-NAT address

Policies > Security

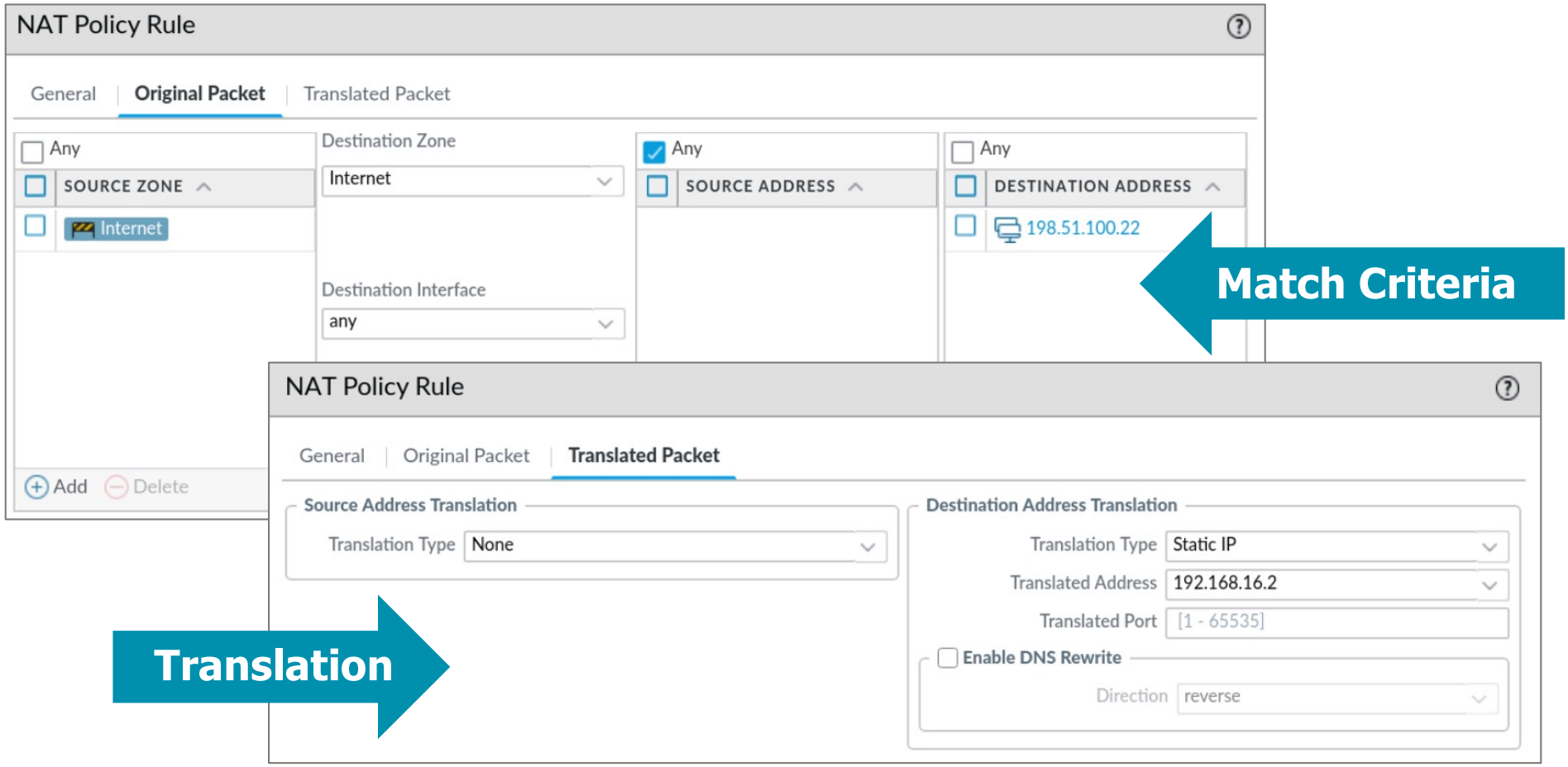
	NAME	TAGS	TYPE	Source		Destination		APPLICATION	SERVICE	ACTION
				ZONE	ADDRESS	ZONE	ADDRESS			
1	Web_Server_Access	Internet	universal	Internet	any	Extranet	198.51.100.22	web-browsing	application-default	Allow

Pre-NAT addresses

Post-NAT zone

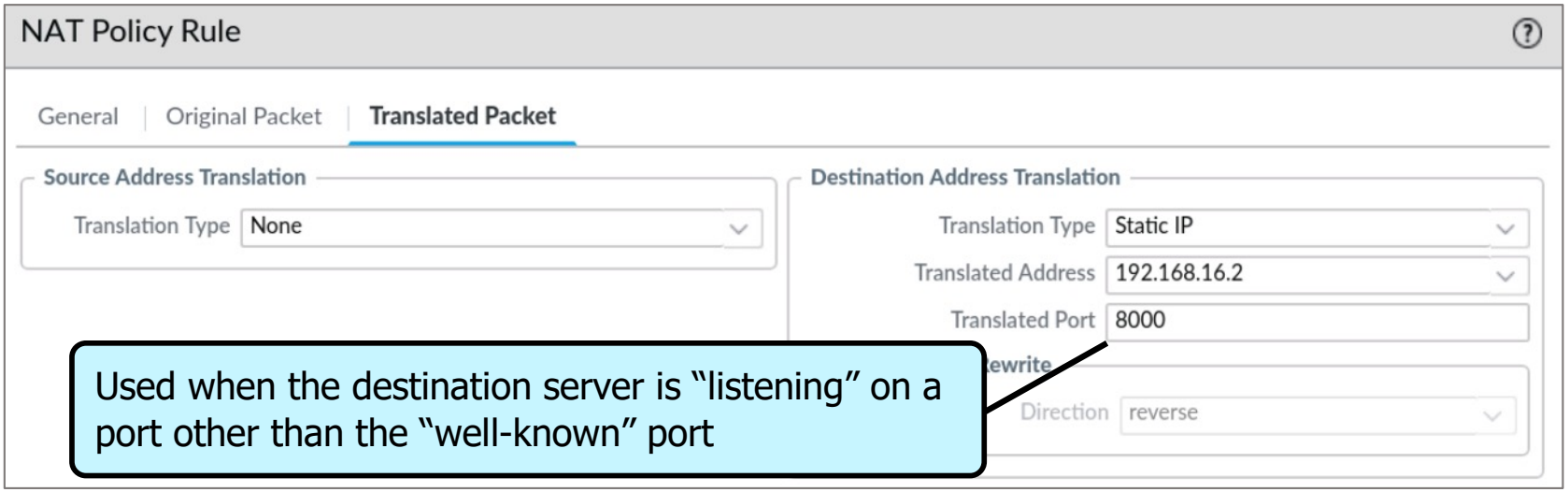
Pre-NAT addresses

Configure Destination NAT



Destination NAT Port Translation Configuration

Policies > NAT



	NAME	TAGS	Original Packet: SOURCE ZONE	DESTINATION ZONE	DESTINATION INTERFACE	SOURCE ADDRESS	DESTINATION ADDRESS	SERVICE	Translated Packet: SOURCE TRANSLATION	DESTINATION TRANSLATION
1	Dest_NAT_From_Internet	Internet	Internet	Internet	any	any	198.51.100.22	service-http	none	destination-translation address: 192.168.16.2 port: 8000

The service-http option includes TCP port 80 and TCP port 8080.

Module Summary

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

- Describe Security policy concepts and operation
- Configure a Security policy rule
- Manage a Security policy
- Create and use tags and custom services in a Security policy
- Configure a NAT policy to implement source NAT
- Configure a NAT policy to implement destination NAT

Questions

Lab 7: Configuring Security Policy Rules and NAT Policy Rules

- Create and Test Security Policy Rules
- Modify Security Policy Table Columns
- Examine Rule Hit Count
- Reset the Rule Hit Counter
- Examine the Traffic Log
- Enable Logging for Default Rules
- Create and Test a Source NAT Policy
- Create and Test a Destination NAT Policy

Protecting our digital way of life.

This page intentionally left blank.