SECURITY AND NAT POLICIES

EDU-210 Version A
PAN-OS® 9.0

GET TRAFFIC FLOWING

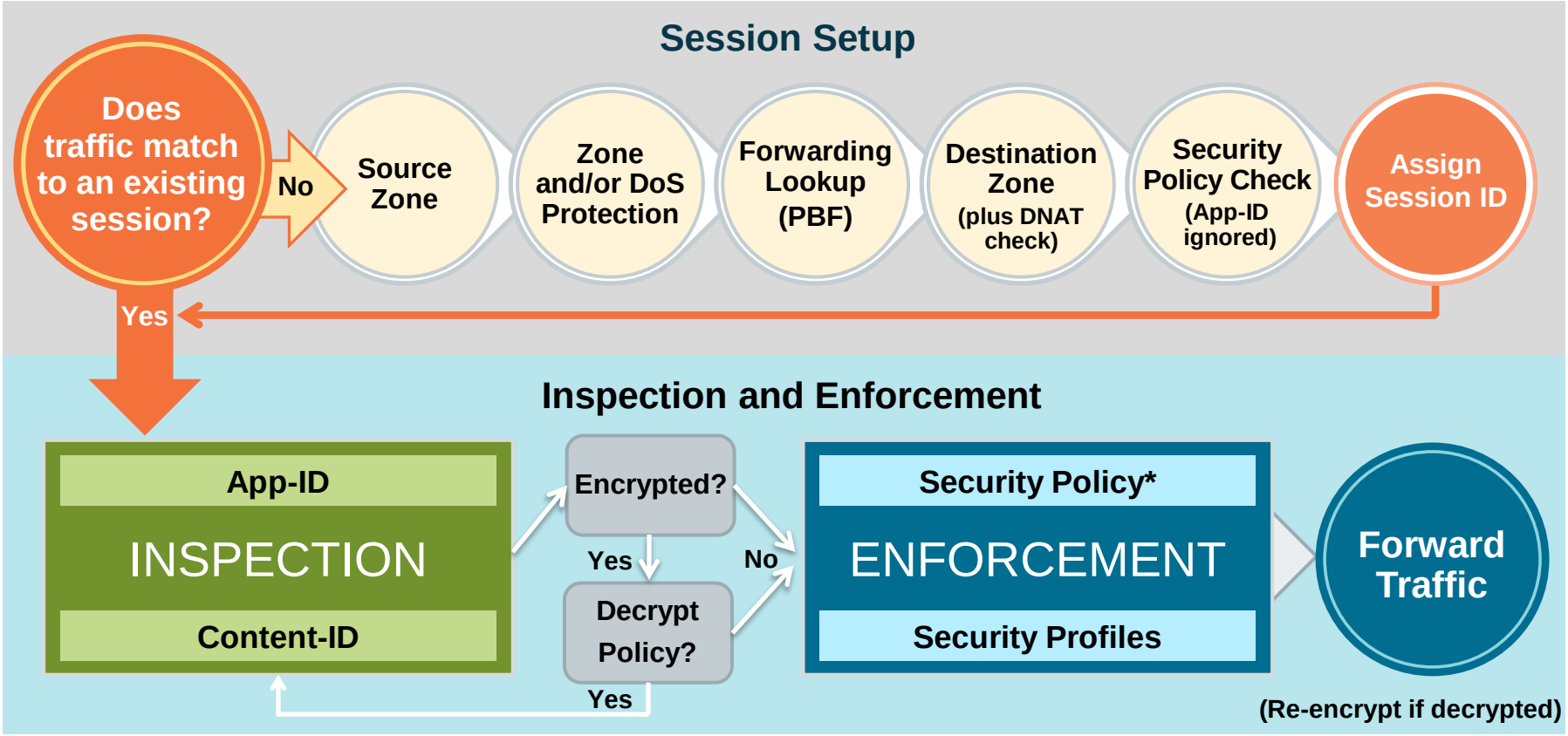
- Security policy fundamental concepts
- Security policy administration
- Network address translation
- Source NAT configuration
- Destination NAT configuration

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

Flow Logic of the Next-Generation Firewall



* Policy check relies on pre-NAT IP addresses

Security policy fundamental concepts

Security policy administration

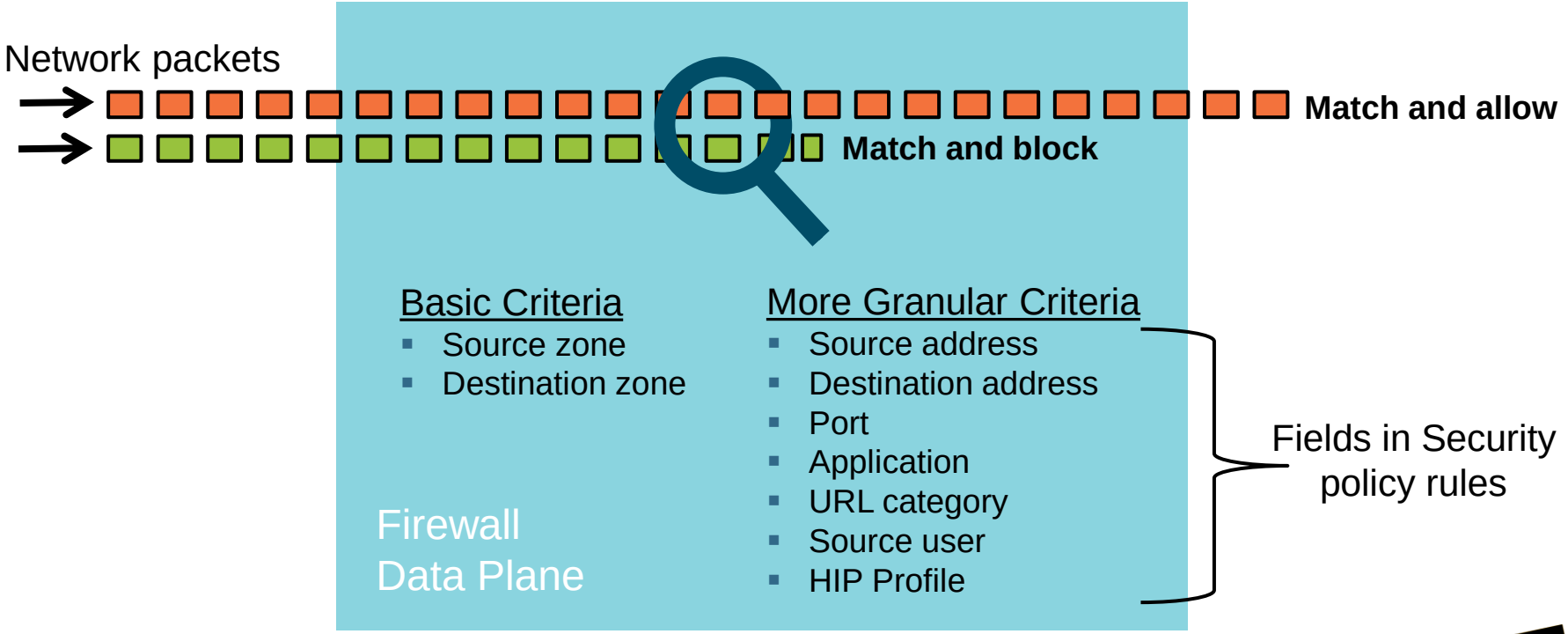
Network address translation

Source NAT configuration

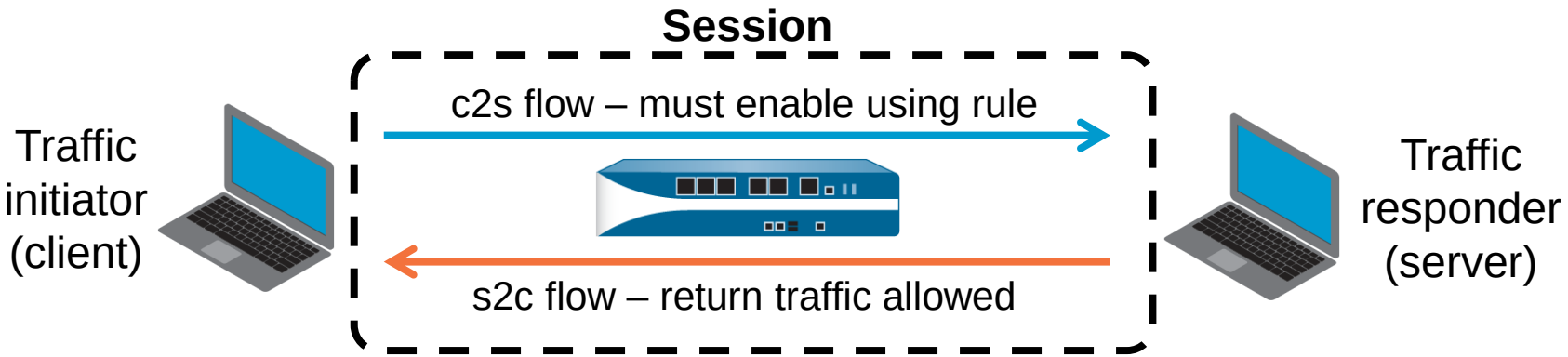
Destination NAT configuration

Controlling Network Traffic

- Multiple match criteria available to control network traffic



Sessions and Flows



- 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

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	-	-	

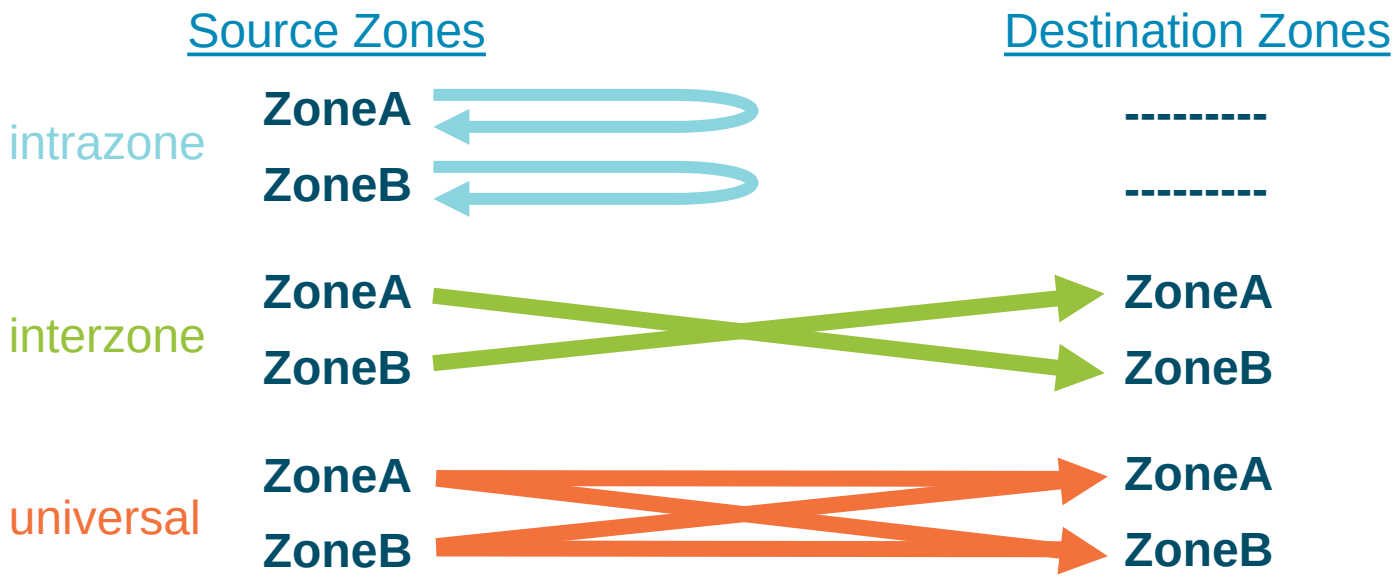
Columns
Adjust Columns

- 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.

Security Policy Rule Types

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



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.

Security Policy Rule Match

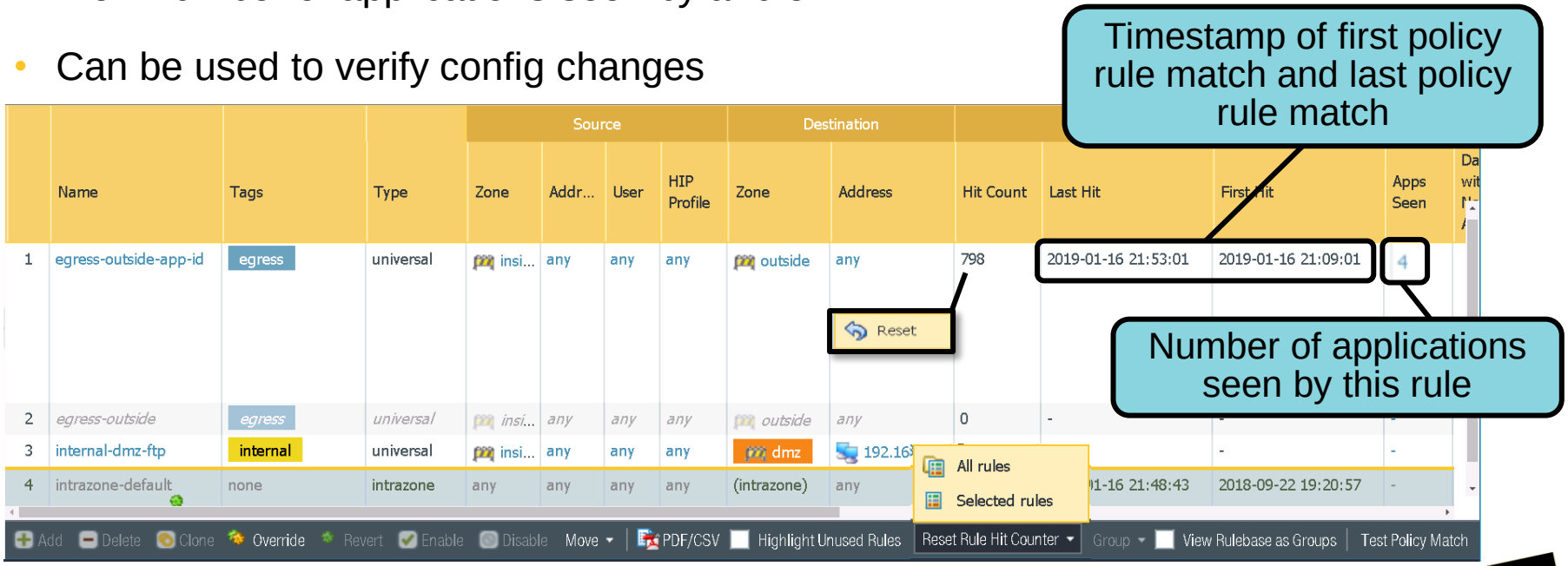
- Rules evaluated from top to bottom
- Further rules not evaluated after a rule match

				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

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



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

Security policy fundamental concepts

Security policy administration

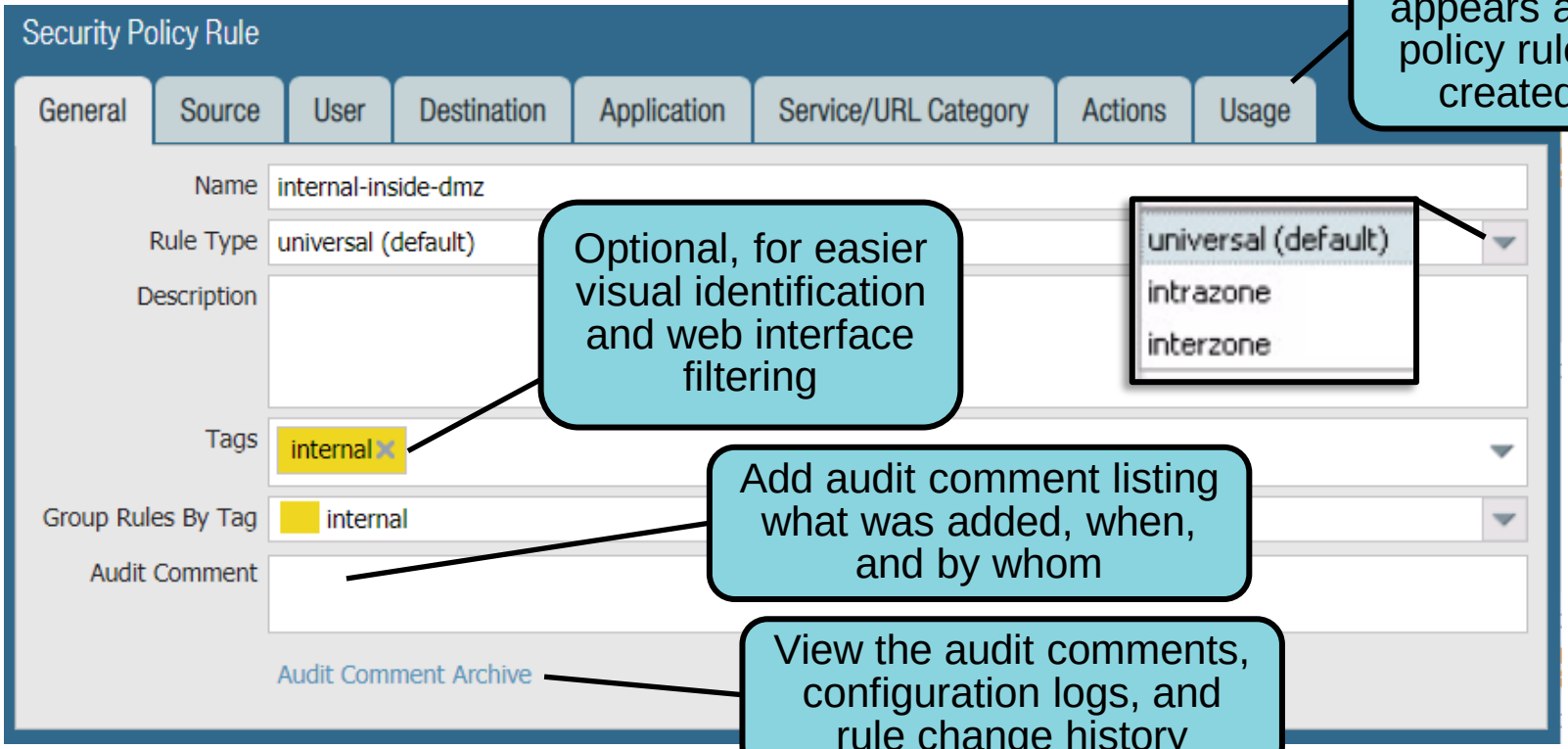
Network address translation

Source NAT configuration

Destination NAT configuration

Creating Security Policy Rules: General Tab

Policies > Security > Add



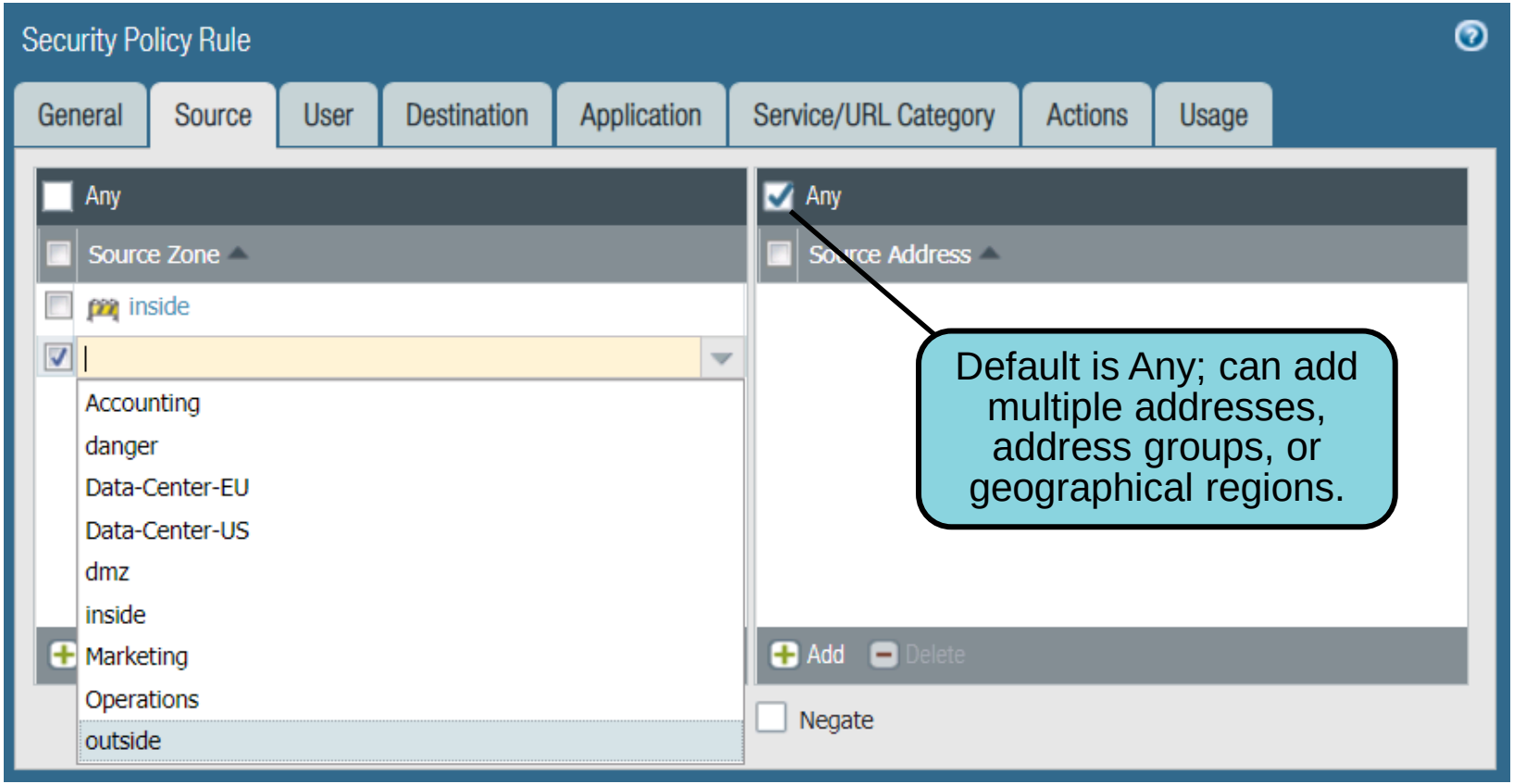
Usage tab appears after policy rule is created.

Optional, for easier visual identification and web interface filtering

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

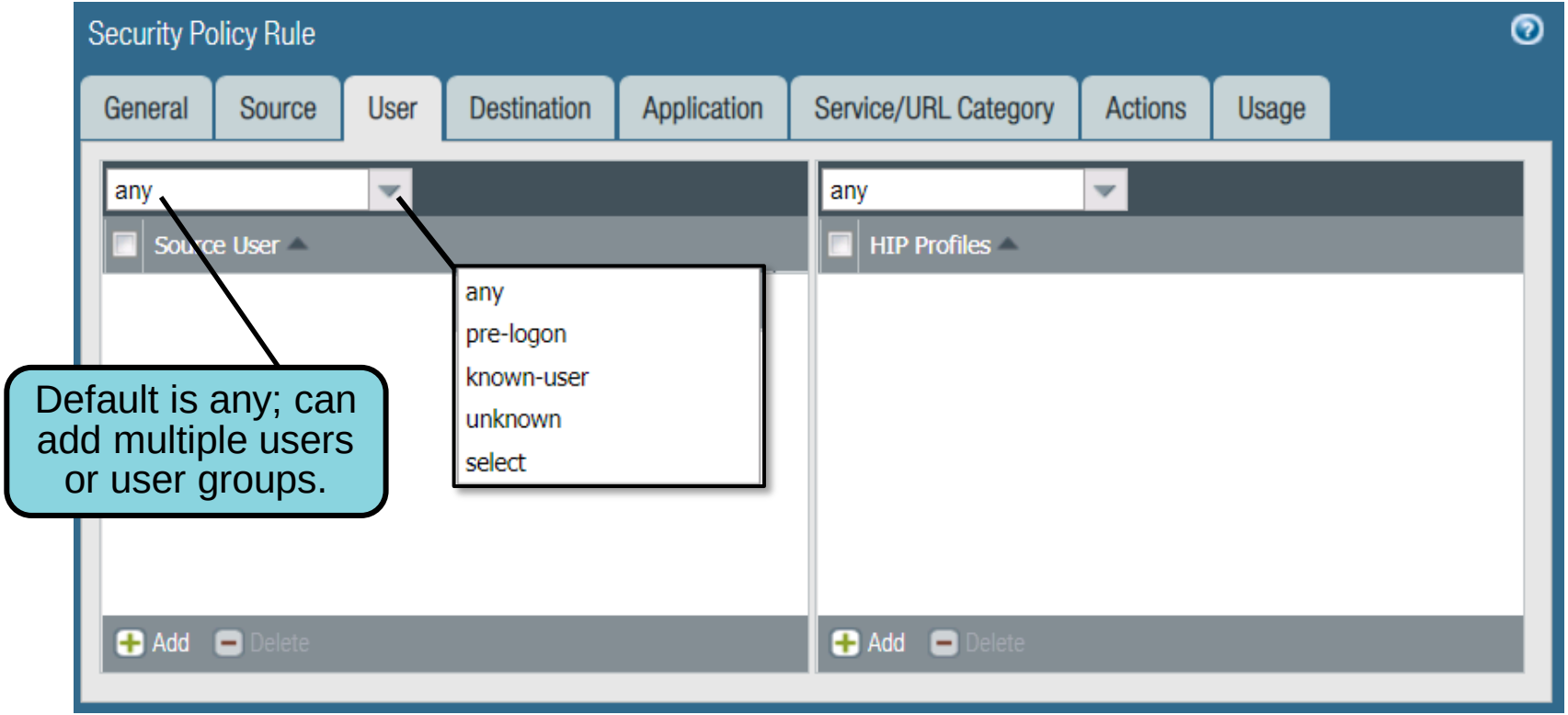
View the audit comments, configuration logs, and rule change history

Creating Security Policy Rules: Source Tab

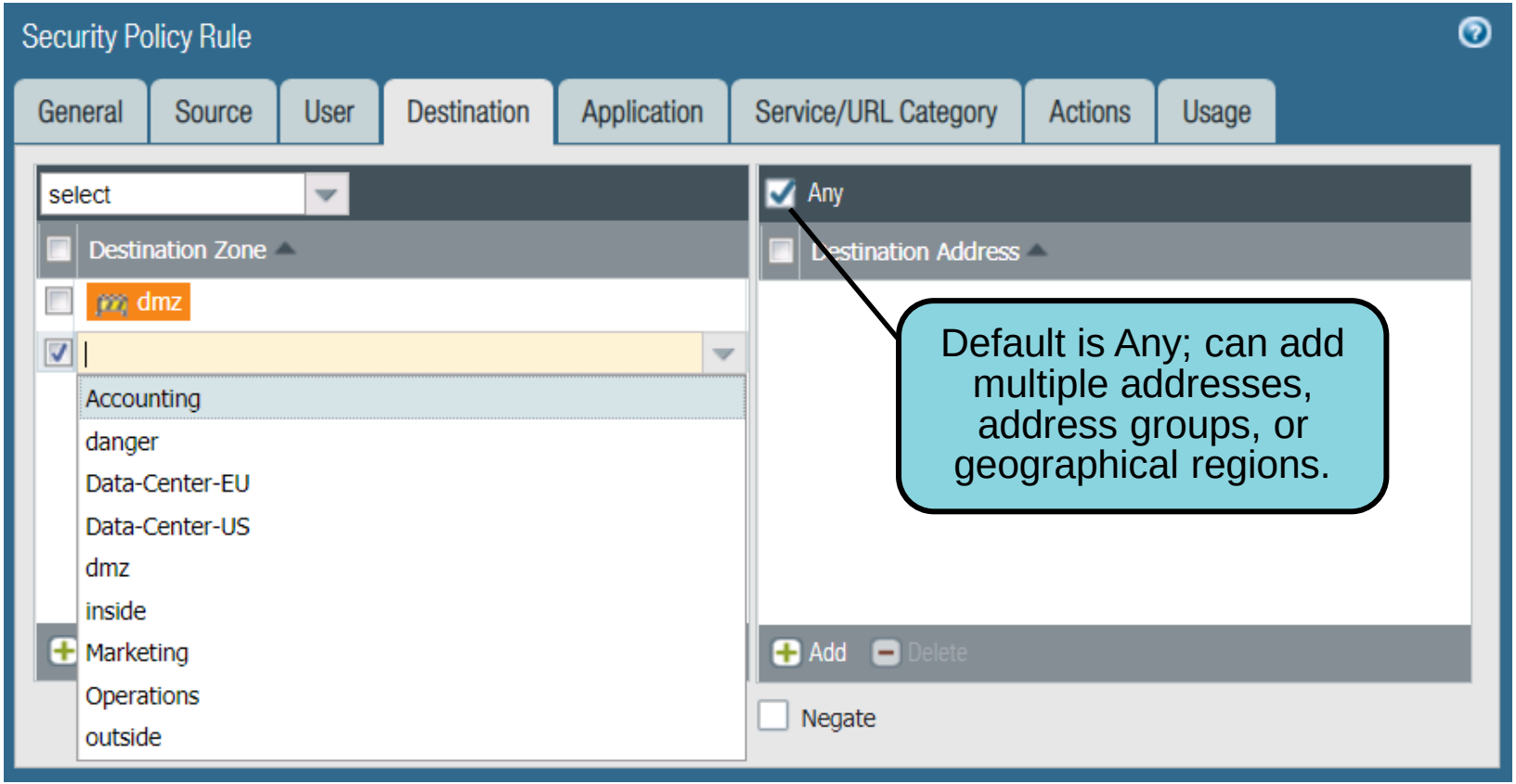


Creating Security Policy Rules: User Tab

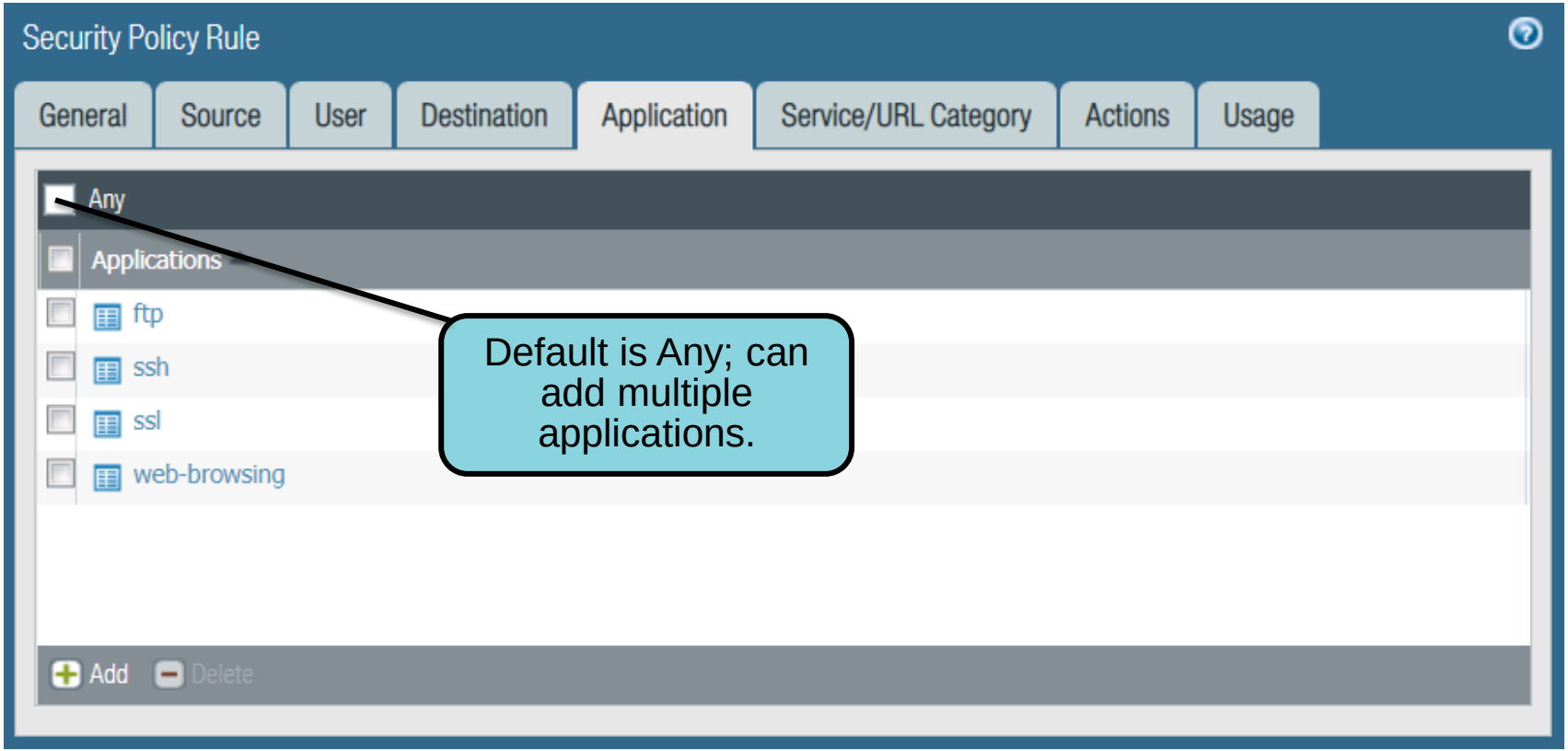
- The User-ID feature is mandatory to use source user as a match criterion.



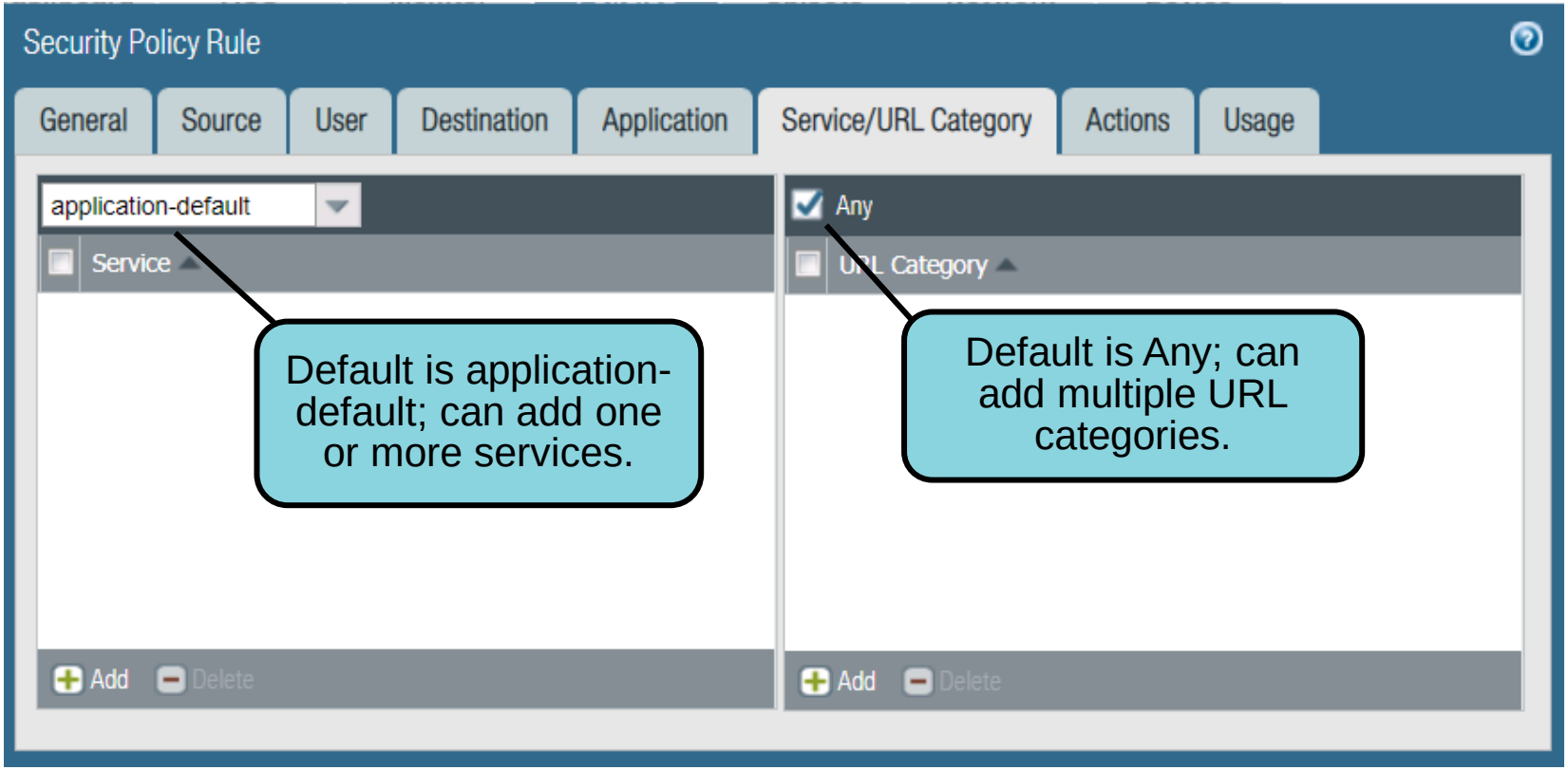
Creating Security Policy Rules: Destination Tab



Creating Security Policy Rules: Application Tab



Creating Security Policy Rules: Service/URL Category Tab



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

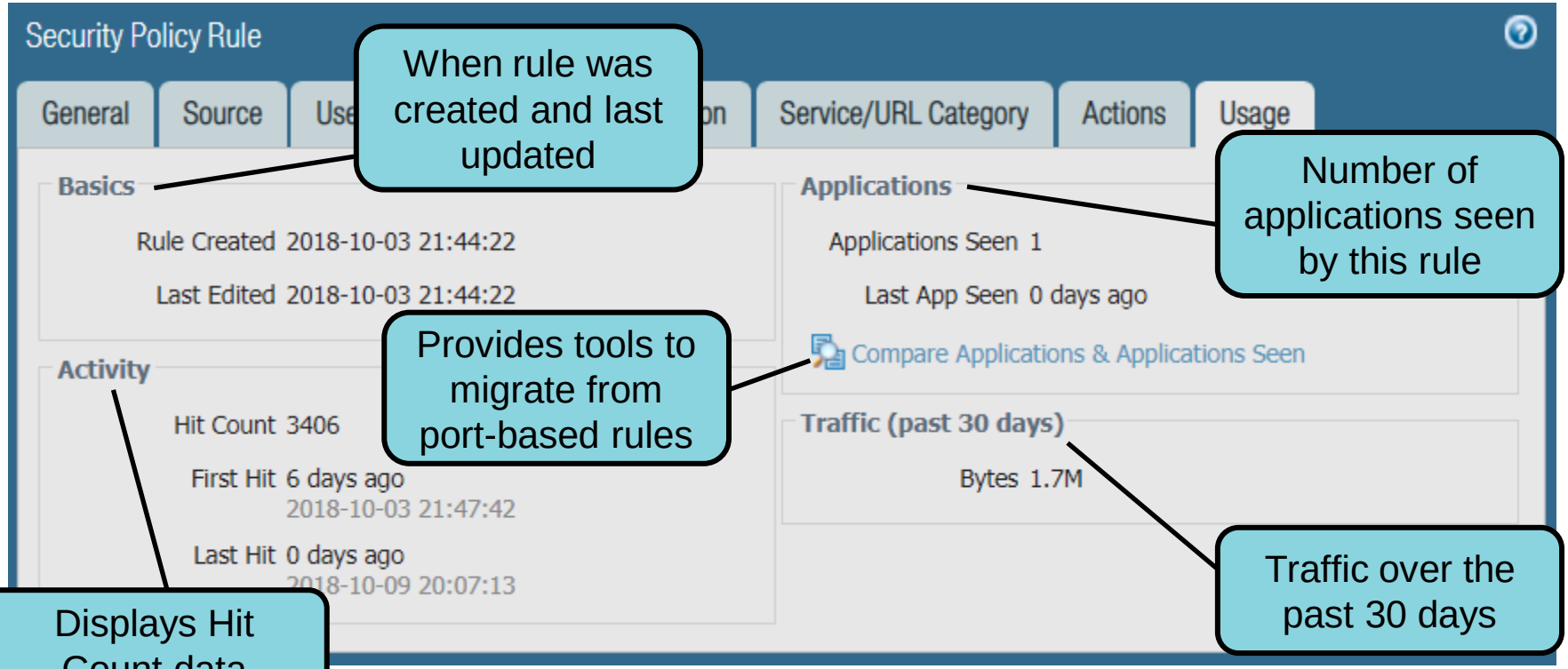
Disable Server Response Inspection

Optional; add session start for troubleshooting.

Available with "drop" and all "reset" actions

Can schedule when the rule is active.

Creating Security Policy Rules: Usage Settings



When rule was created and last updated

Number of applications seen by this rule

Provides tools to migrate from port-based rules

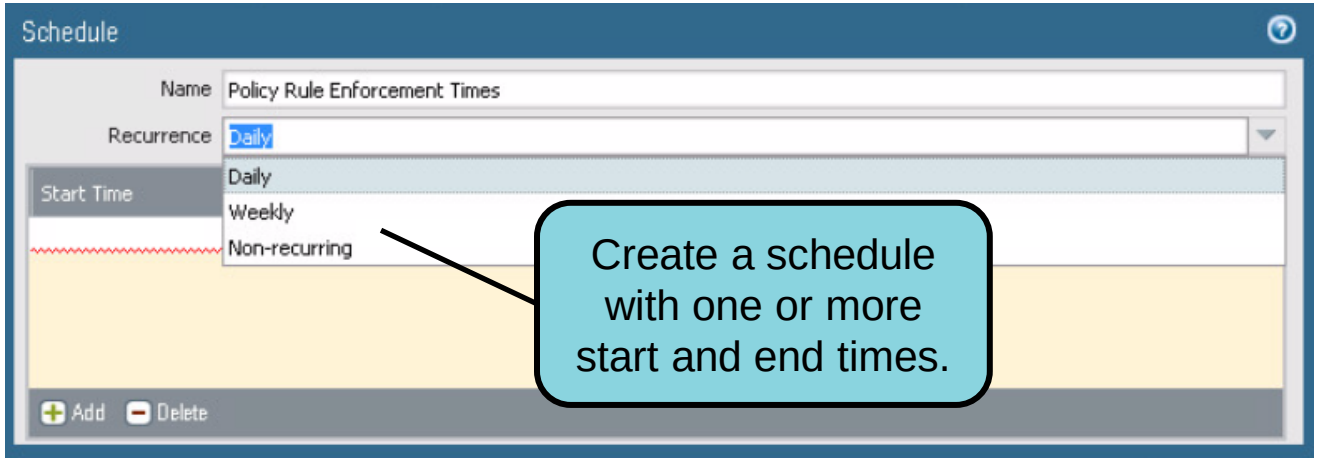
Displays Hit Count data

Traffic over the past 30 days

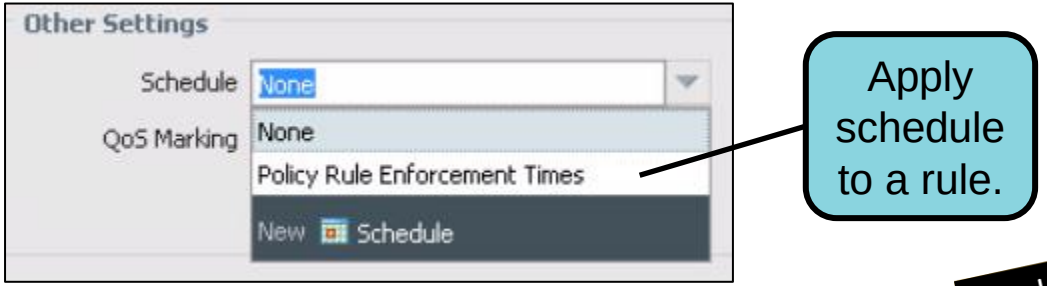
Scheduling Security Policy Rules

- 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



Policies > Security > <select_rule> > Actions



Managing the Policy Ruleset

Policies > Security

Line numbers do not move when a rule moves.

Disabled rules display in italics.

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

Filter
Log Viewer
Move
Copy UUID
Global Find

Add | Delete | Clone | Override | Revert | Enable | Disable | Move | PDF/CSV | Highlight Unused Rules | Reset Rule Hit Counter | Group | View Rulebase as Groups | Test Policy Match

- **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.

Universally Unique Identifiers (UUIDs)

Policies > Security

	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

Columns
Adjust Columns

- Name
- Tags
- Group
- Type
- UUID
- Source Zone
- Source Address

Add | Delete | Clone | Override | Revert | Enable | Disable | Move | PDF/CSV | Highlight Unused Rules | Reset Rule Hit Counter | Group | View Rulebase as Groups | Test Policy Match

- 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

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

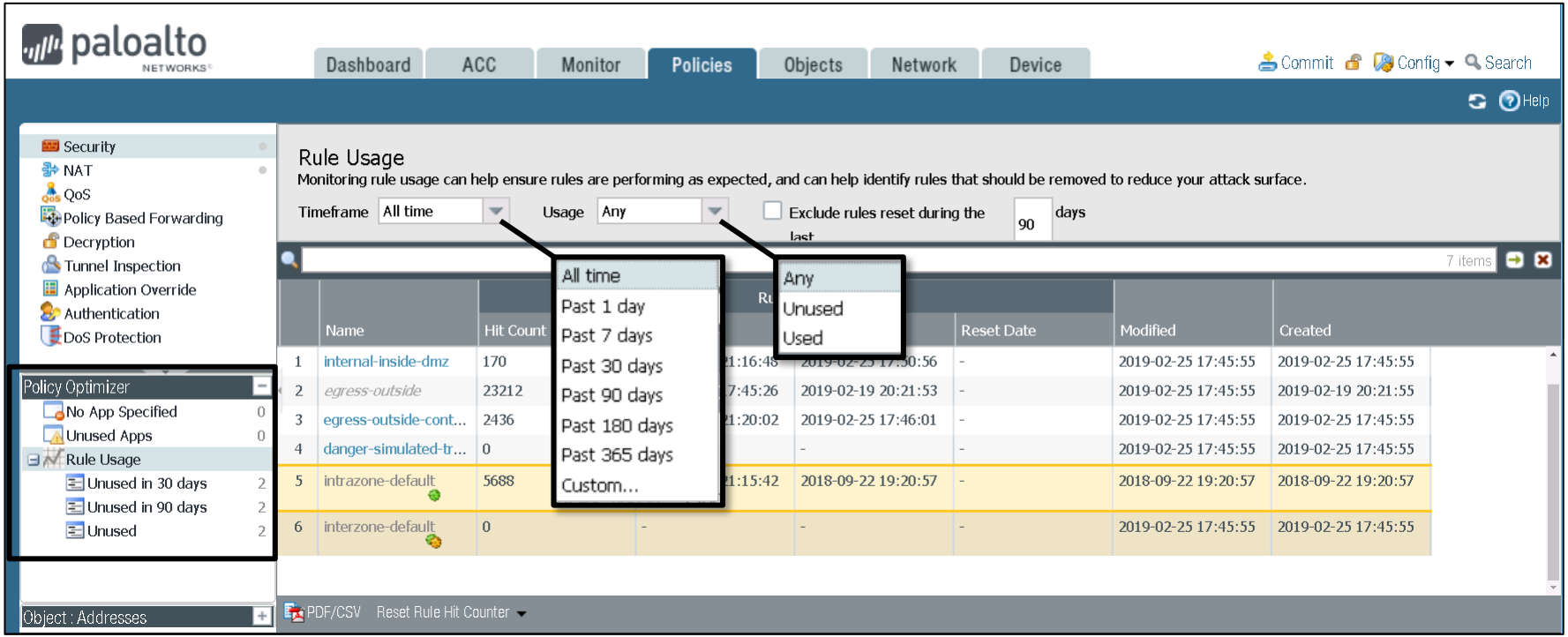
Rules highlighted

	Name	Tags	Type	Zone	Source Address	User	HIP Profile	Destination Zone	Address	Application
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

Add | Delete | Clone | Override | Revert | Enable | Disable | Move | PDF/CSV | Highlight Unused Rules | Reset Rule Hit Counter | Group | View Rulebase as Groups | Test Policy Match

Rule Usage Filter

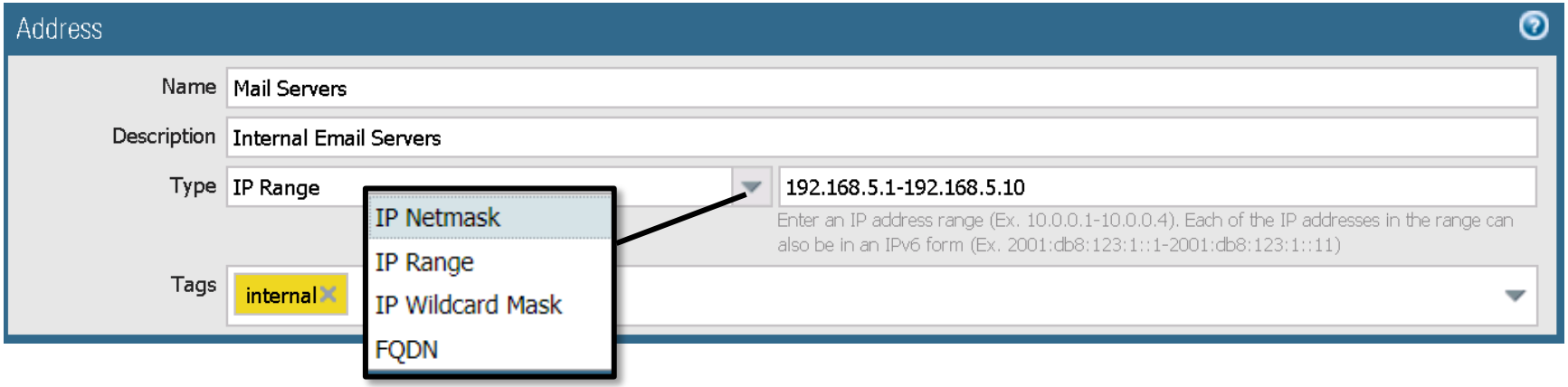
Policies > Policy Optimizer > Rule Usage



Address Objects

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

Objects > Addresses > Add



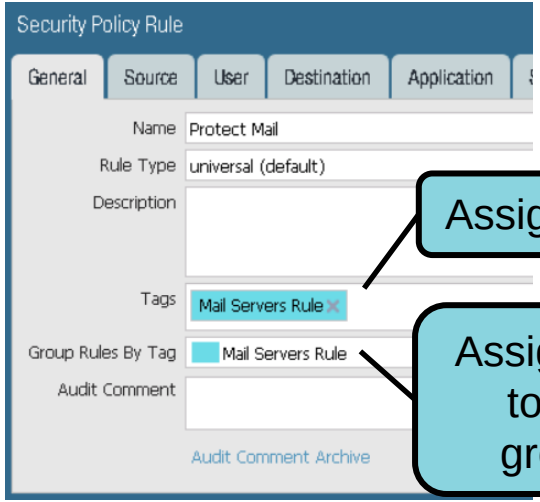
Source				Destination	
Zone	Address	User	HIP Profile	Zone	Address
inside	any	any	any	dmz	Mail Servers

Use new Address object.

Tags

Objects > Tags > Add

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



Assign tag.

Assign rule to tag group.

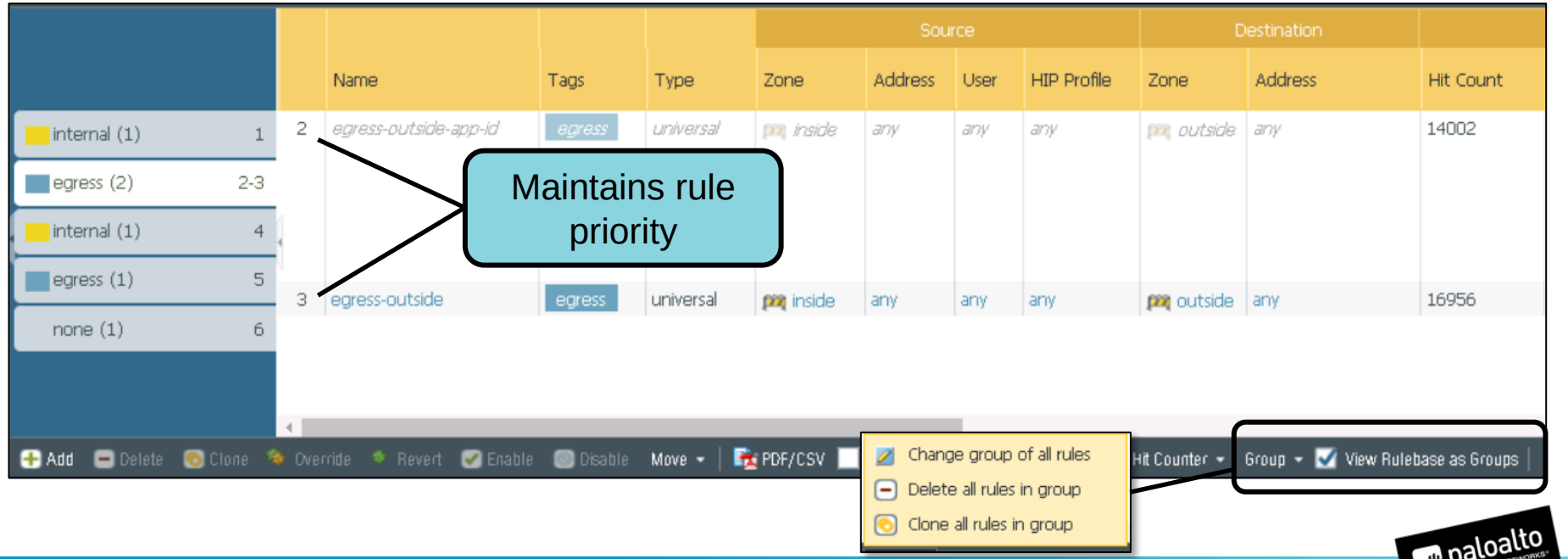
Filter for tag.

Look for tag color.

Tag-Based Rule Groups

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

Policies > Security



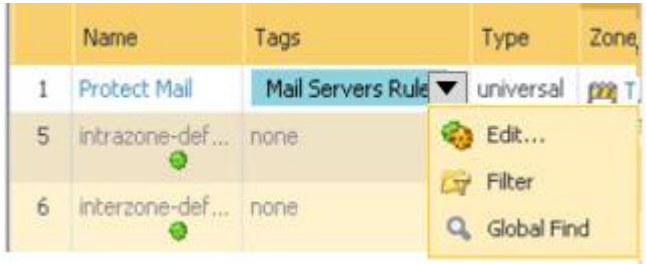
Creating a New Service Definition

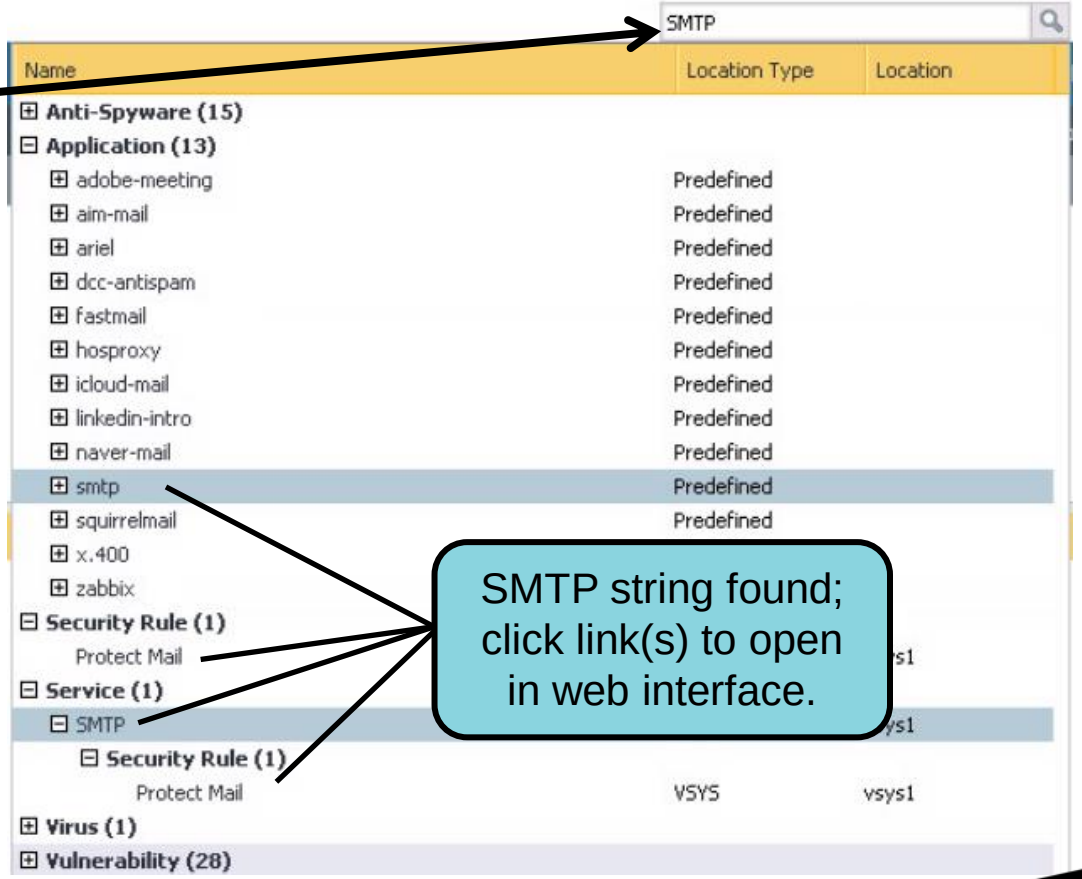
- Service definitions are assigned ports.
- Services limit ports that applications can use.
- service-http and service-https are the only predefined services.

Objects > Services > Add

Using Global Find

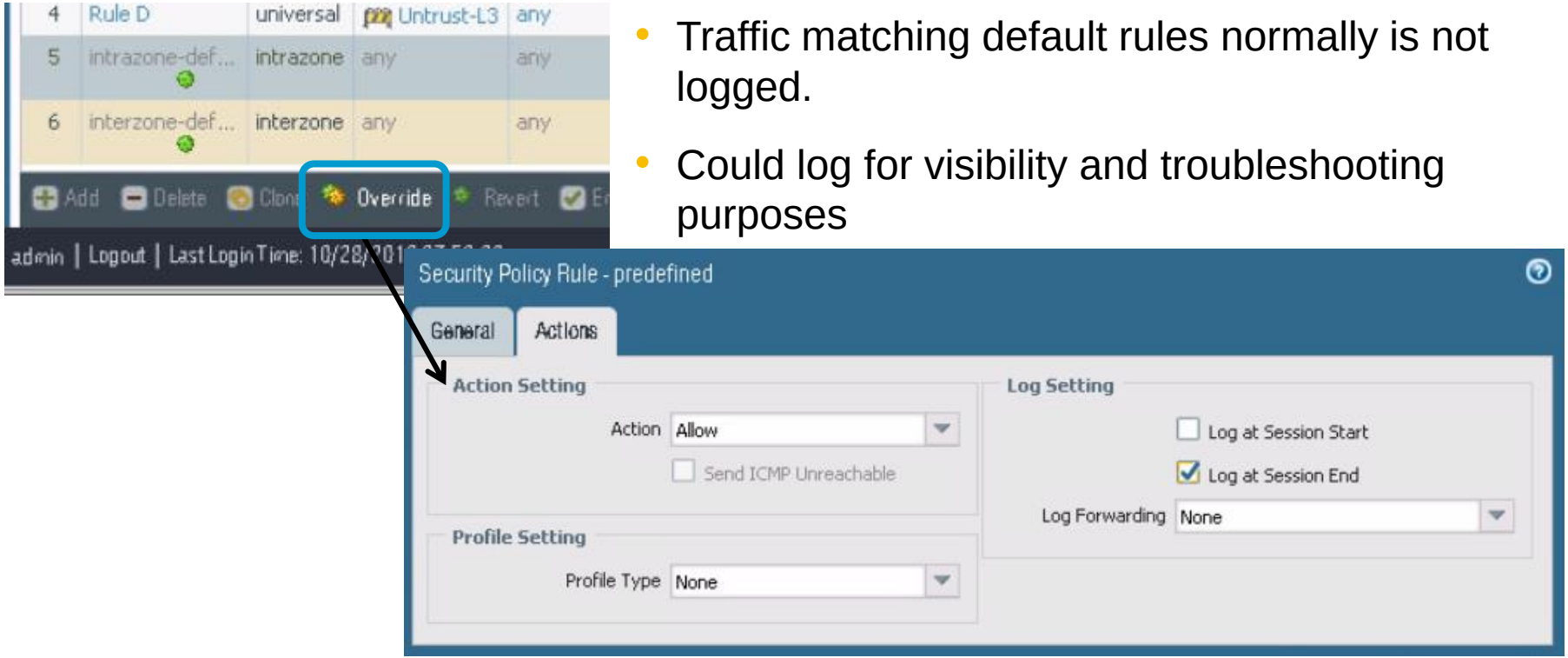
- Search candidate configuration and content databases for occurrences of a string
- Launch from Search or Context menu





Enabling Intrazone and Interzone Logging

Policies > Security > <select_default_rule>



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

Rule Changes Archive

Displays audit comment history

Compare changes between configuration versions.

Displays configuration logs

Security Policy Rule

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

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

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

```
1  egress-outside {
2    to outside ;
3    from inside ;
4    source any ;
5    destination any ;
6    source-user any ;
7    category any ;
8    application any ;
9    service application-default ;
10   hip-profiles any ;
11   tag egress ;
12   action allow ;
13   disabled no ;
14   group-tag egress ;
15   profile-setting {
16     profiles {
17       url-filtering lab-url-filtering ;
18       virus lab-av ;
19       spyware lab-as ;
20     }
21   }
22 }
23
```

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

```
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 ;
    }
  }
}
```


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

Add | Rulebase as Group | Test Policy Match

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

Execute | Reset

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

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 21:47:09	end	private-ip-addresses	inside	dmz	192.168.1.254		192.168.50.10	80	web-browsing	allow	internal-inside-dmz	tcp-fin
		02									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

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

Details

Type	end
Bytes	268

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

Security policy fundamental concepts

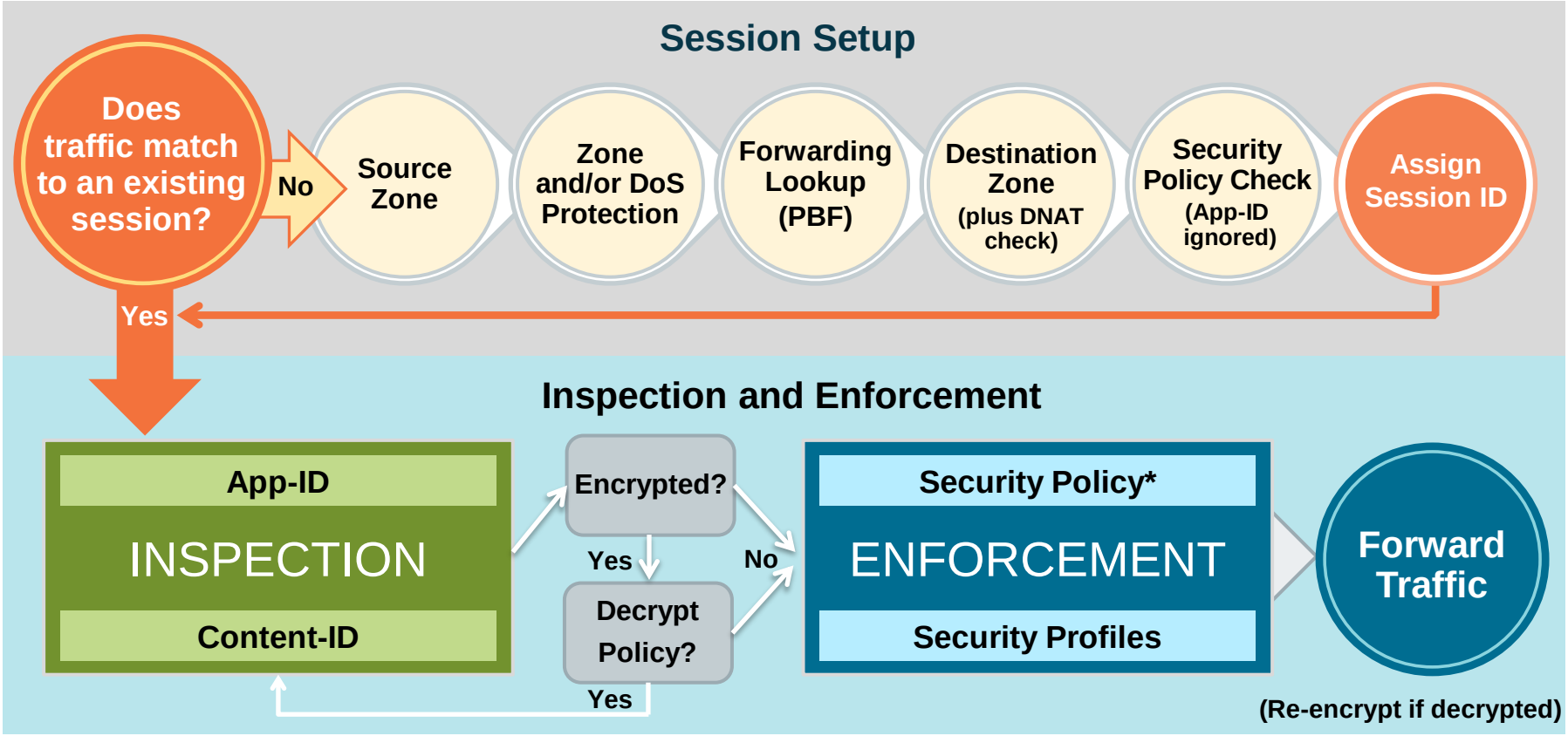
Security policy administration

Network address translation

Source NAT configuration

Destination NAT configuration

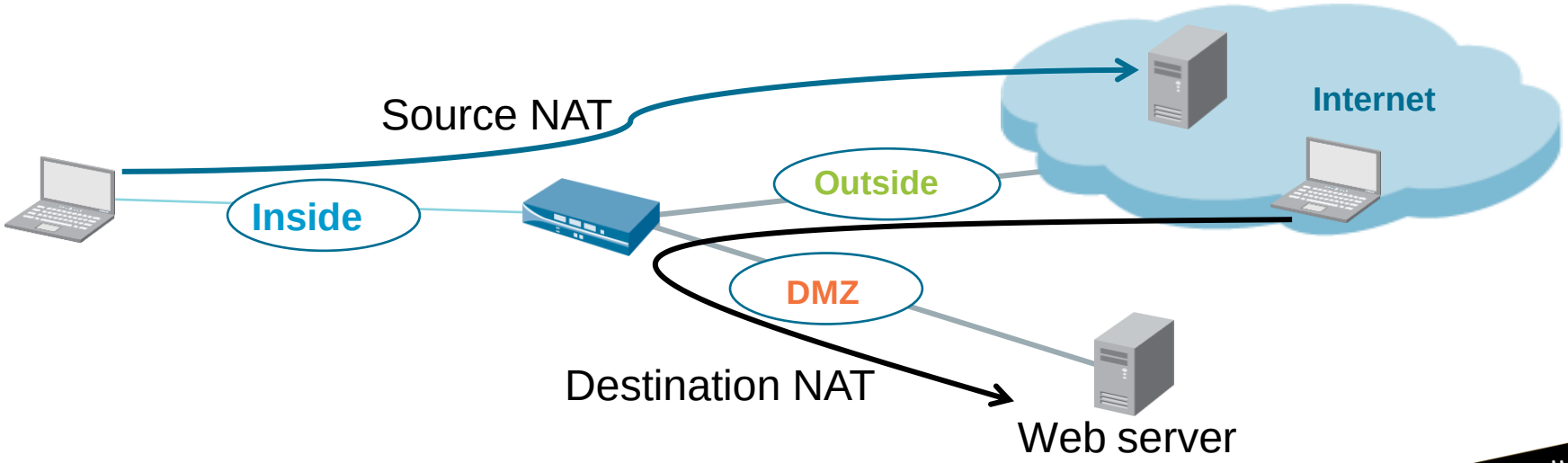
Flow Logic of the Next-Generation Firewall



* 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

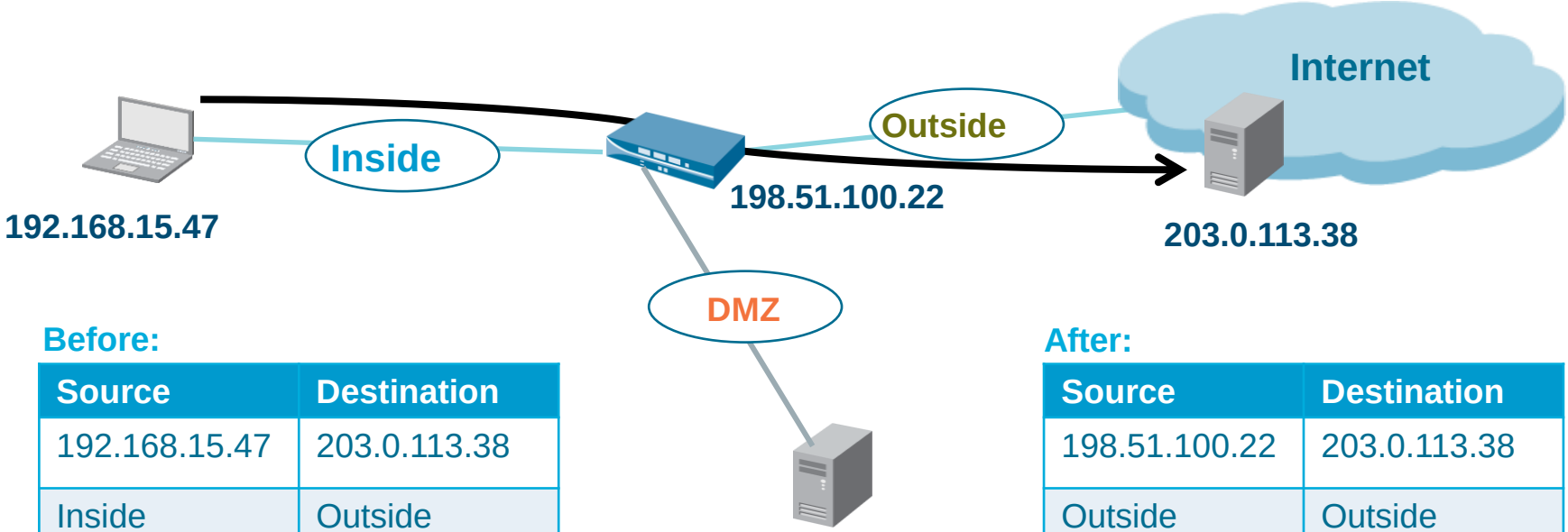
Network address translation

Source NAT configuration

Destination NAT configuration

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

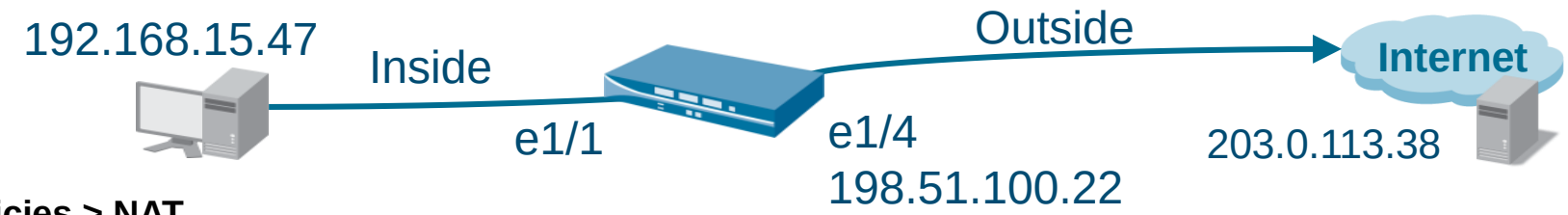
After:

Source	Destination
198.51.100.22	203.0.113.38
Outside	Outside

Source NAT 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

			Original Packet						Translated Packet			
	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			ethernet1/2	any				destination-translation address: 192.168.50.10	0	-

Pre-NAT zones

Pre-NAT addresses

Policies > Security

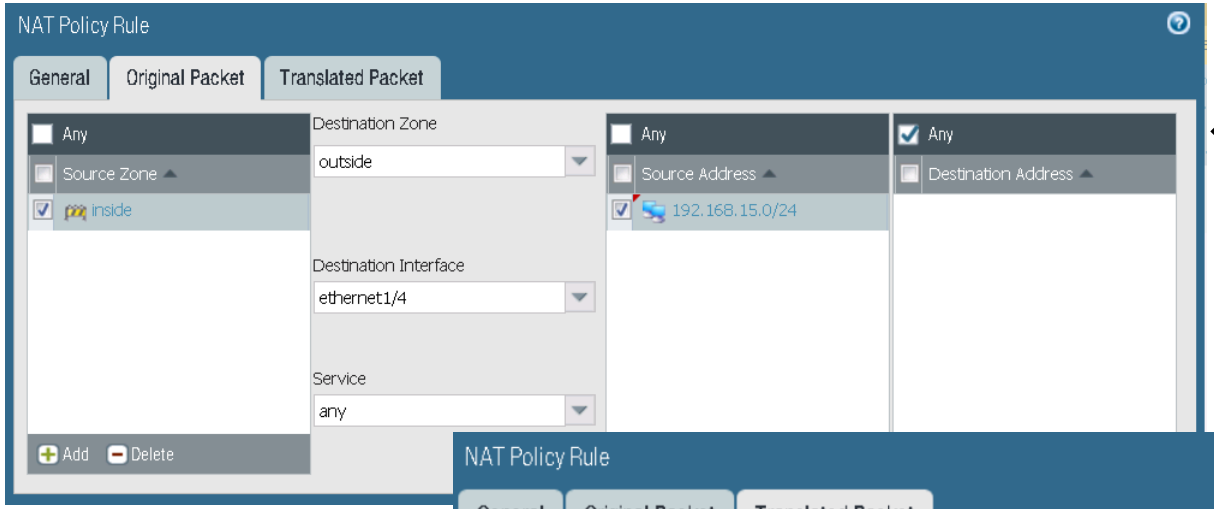
				Source				Destination		Rule Usage					
	Name	Tags	Type	Zone	Address	User	HIP Profile	Zone	Address	Hit Count	Last Hit	First Hit	Application	Service	Action
1	Internet Usage	egress	universal	inside	192.168.15.0...	any	any	outside	any	-	-	-	dns ftp web-browsing	application-de...	Allow

Pre-NAT address

Post-NAT zone

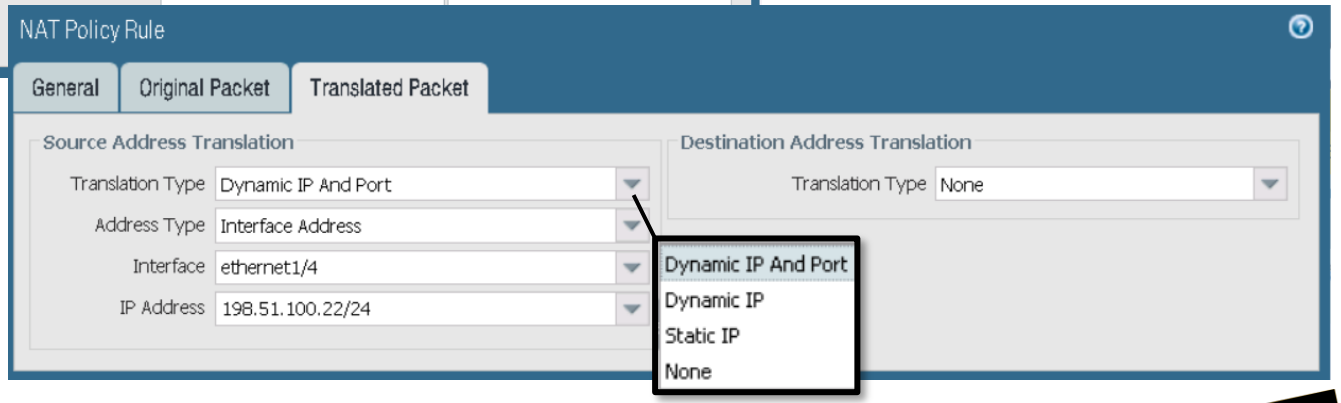
Pre-NAT address

Configuring Source NAT



Match Criteria

Translation



Source NAT Examples

Static 1:1 Translation

Policies > NAT

	Name	Tags	Original Packet						Translated Packet		
			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

	Name	Tags	Original Packet						Translated Packet		
			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

Source NAT Examples (Cont.)

Dynamic IP and Port Translation

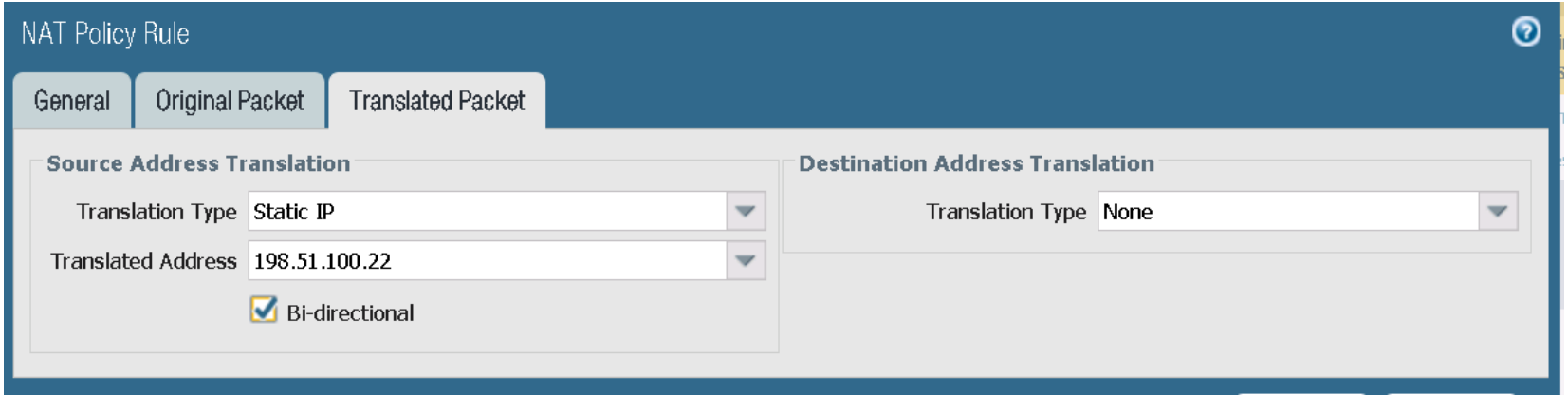
Policies > NAT

			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	-	-

Configuring Bidirectional Source NAT

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

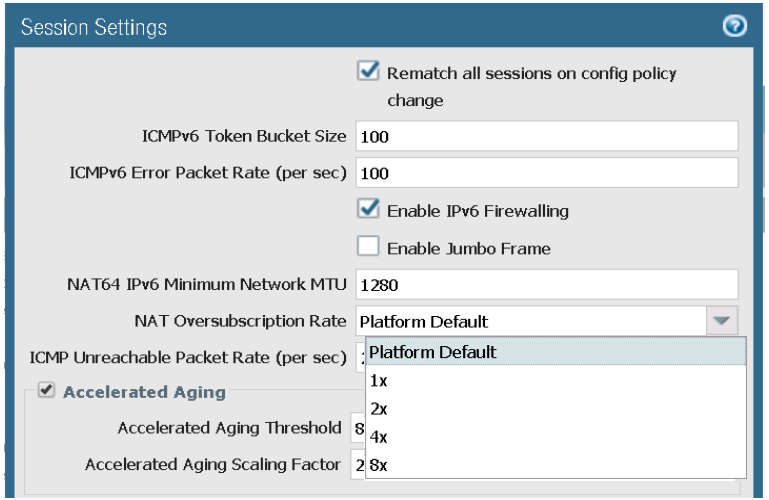
Policies > NAT



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	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

Security policy fundamental concepts

Security policy administration

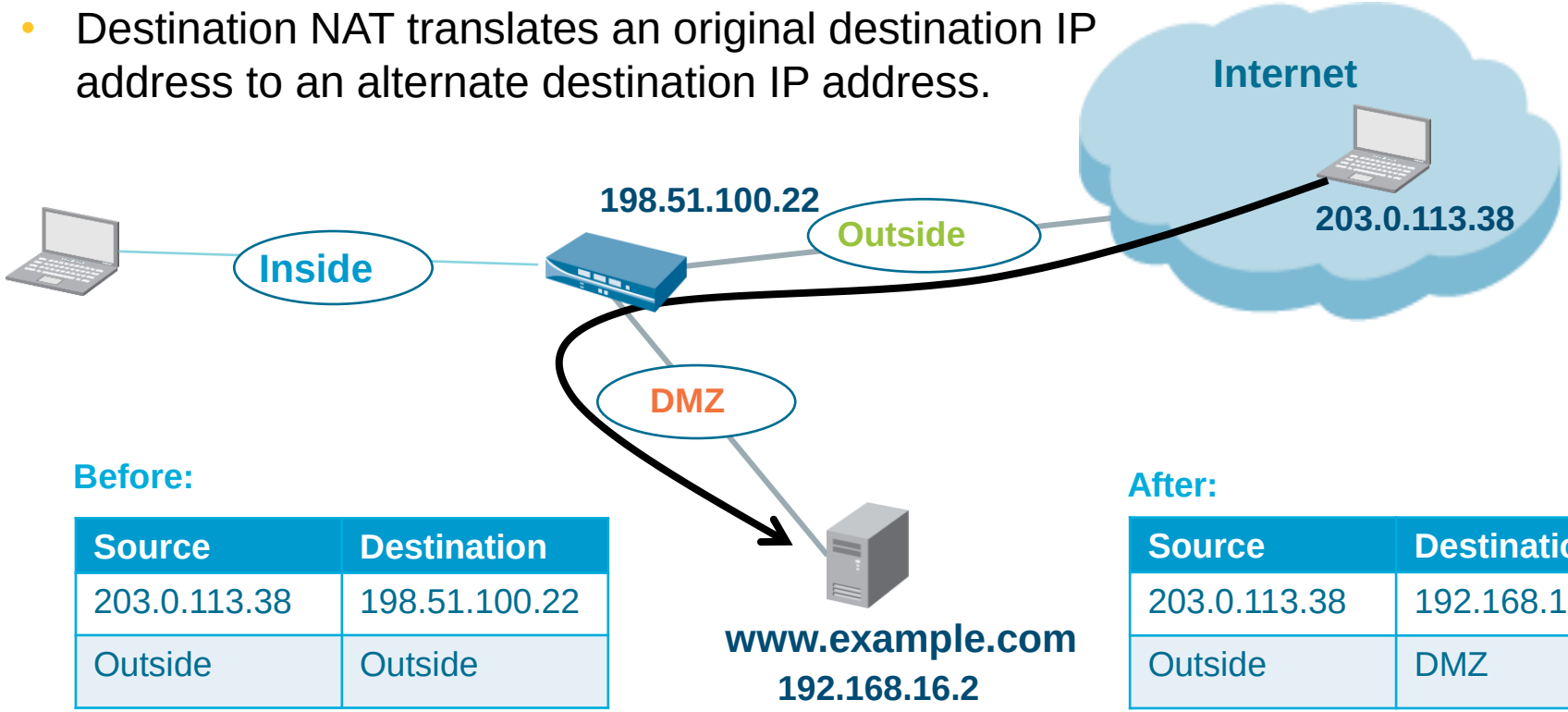
Network address translation

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
Outside	Outside

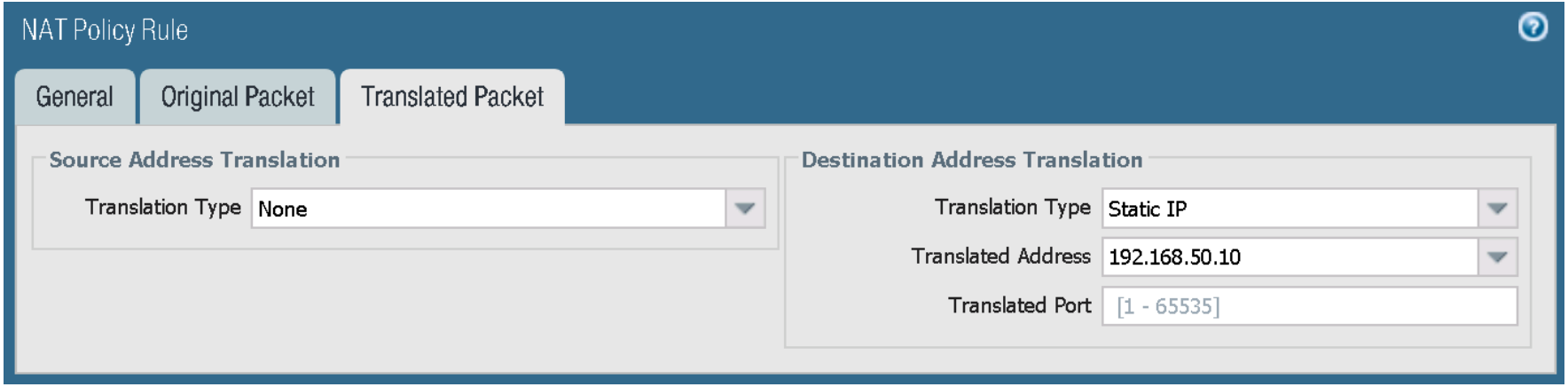
After:

Source	Destination
203.0.113.38	192.168.16.2
Outside	DMZ

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

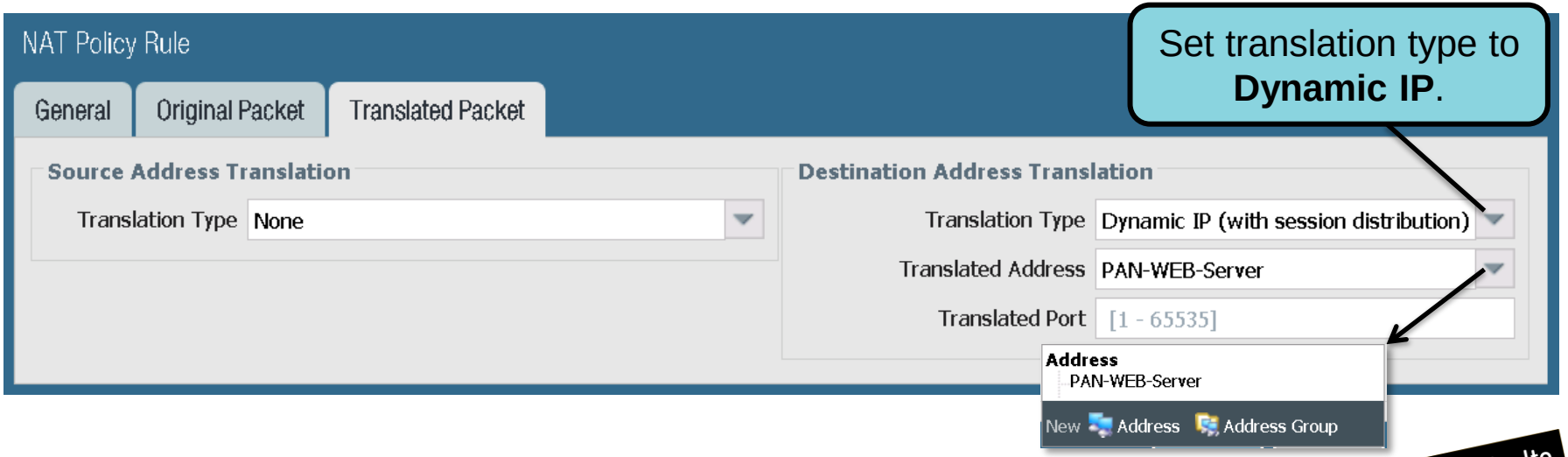
Policies > NAT > Add



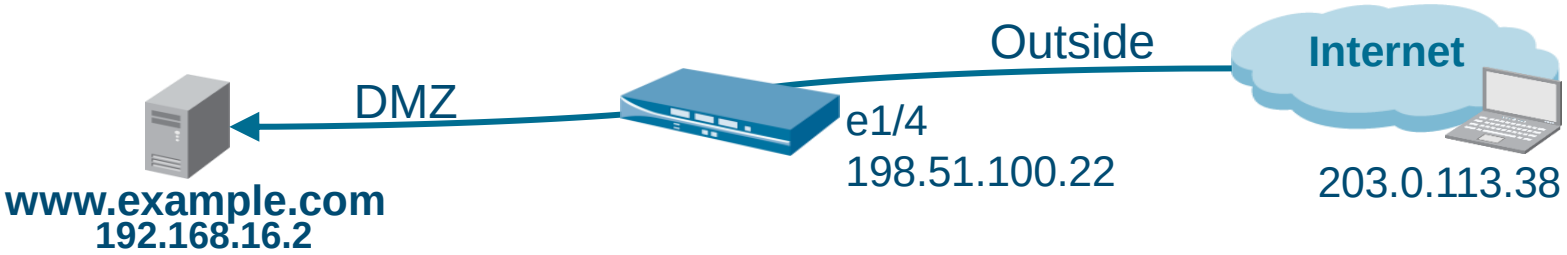
Dynamic IP Address Support for Destination NAT

- 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

			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

Pre-NAT zones

Pre-NAT address

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...

Pre-NAT addresses

Post-NAT zone

Pre-NAT addresses

Configuring Destination NAT

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

Add Delete

Match Criteria

Translation

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]

Destination NAT Port Translation Configuration

Policies > NAT

NAT Policy Rule

General | Original Packet | Translated Packet

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

	Name	Tags	Original Packet						Translated Packet	
			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

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

Questions?

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.

paloalto NETWORKS®