

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

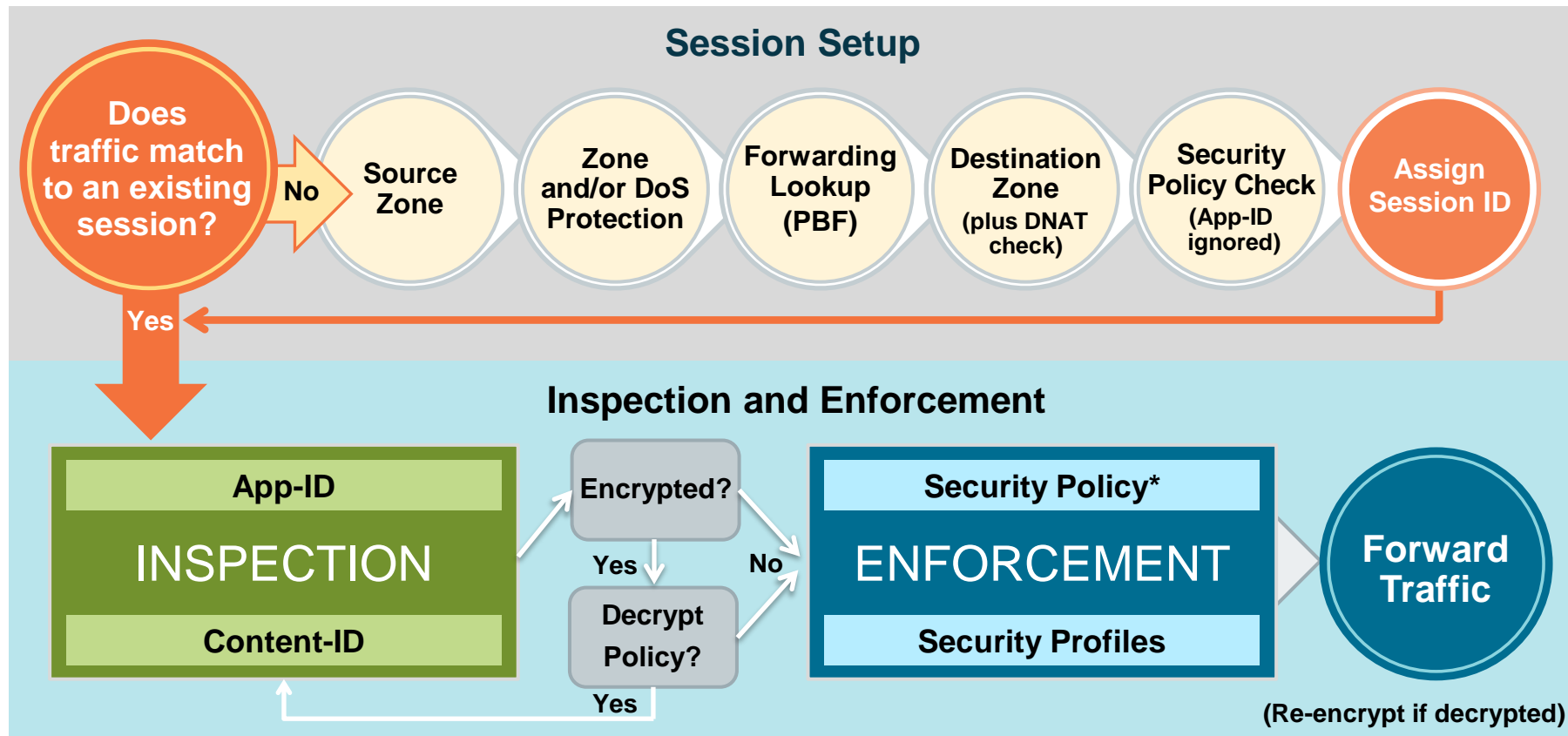
Agenda

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

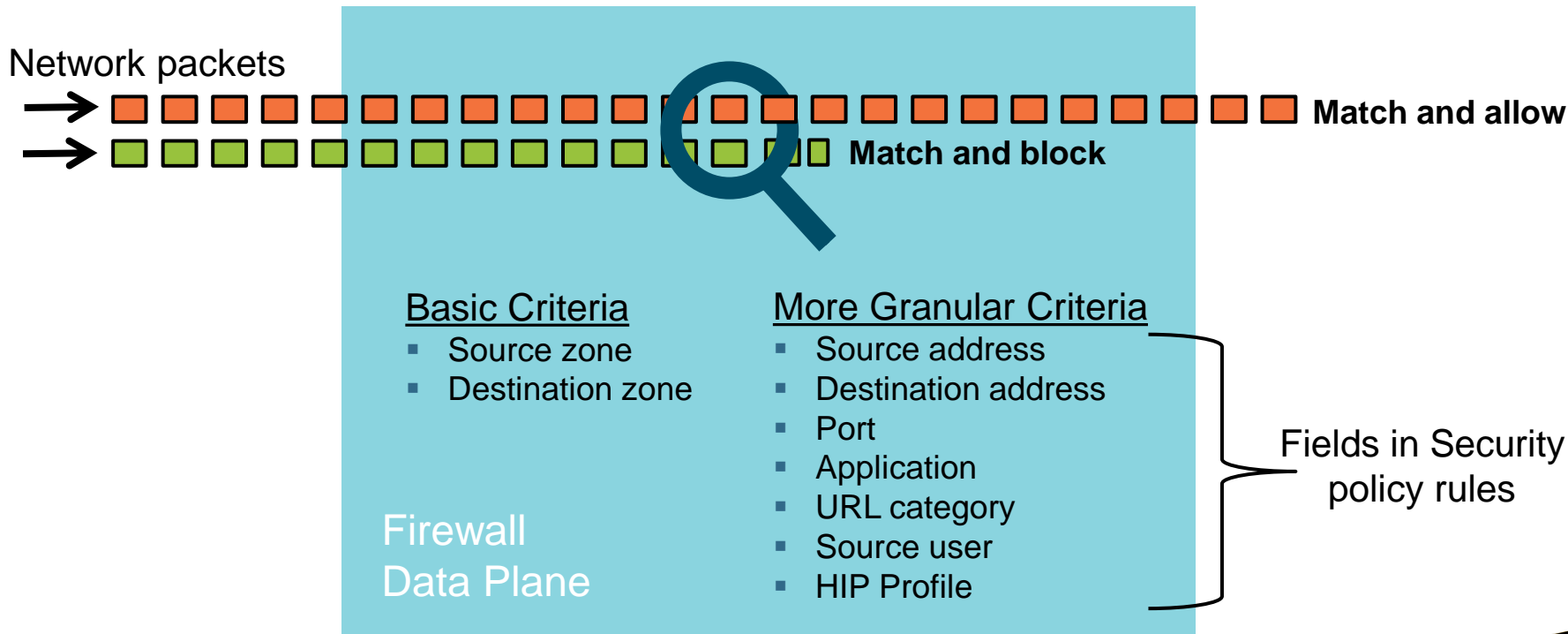
Network address translation

Source NAT configuration

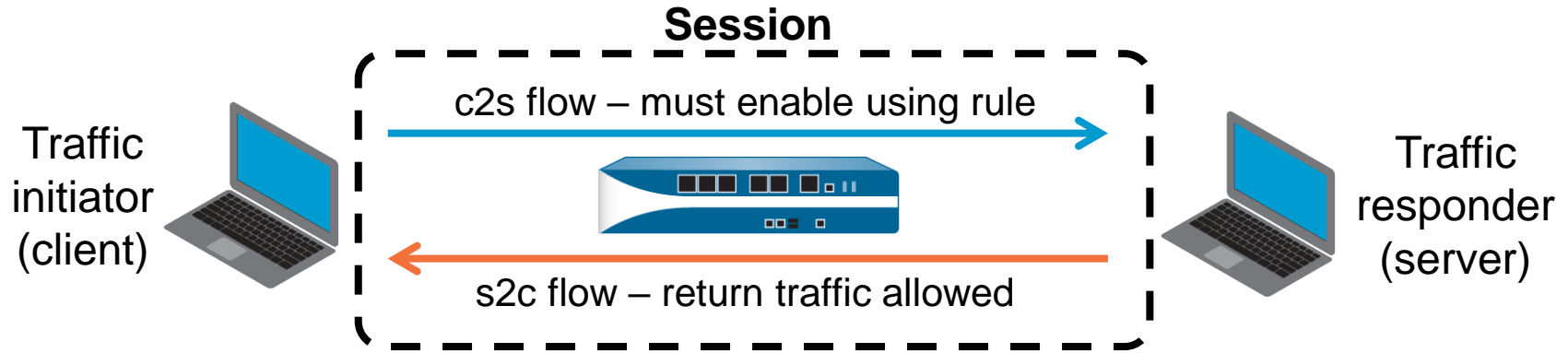
Destination NAT configuration

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

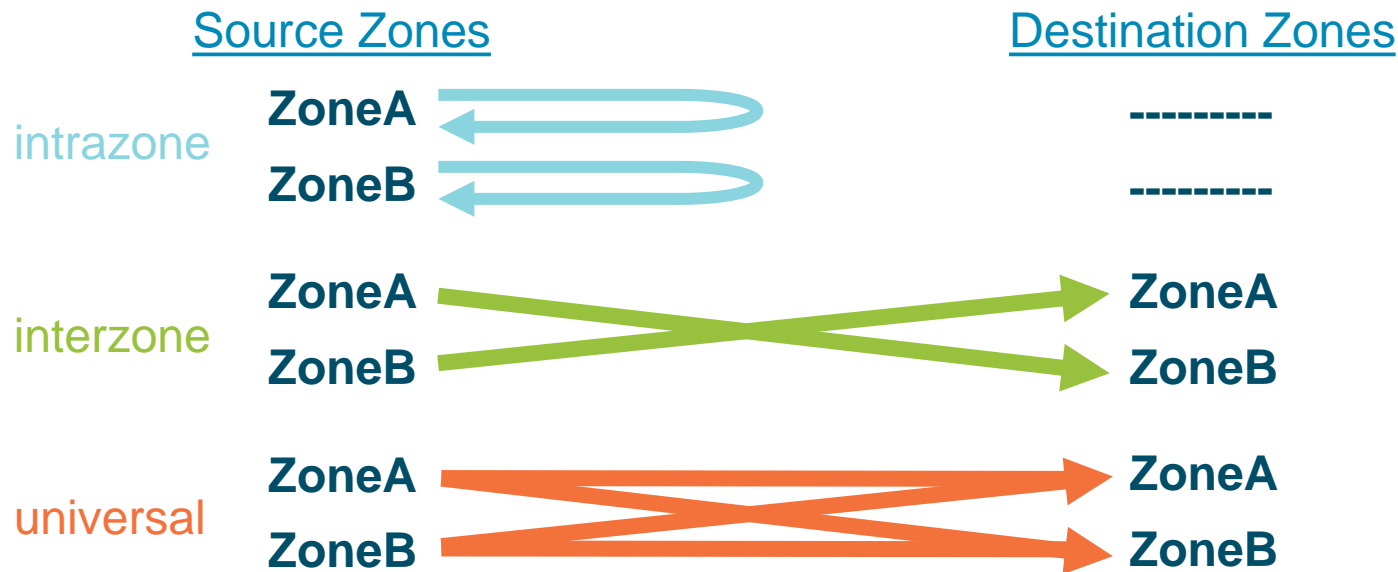
Policies > Security

	Name	Type	Source			Destination			Rule Usage		
			Zone	Address	User	Zone	Address		Hit Count	Last Hit	First Hit
1	egress-outside-app-id	universal	 inside	any	any	 outside	any	 Columns		<input checked="" type="checkbox"/> Name <input type="checkbox"/> Tags <input checked="" type="checkbox"/> Type <input checked="" type="checkbox"/> Source Zone <input checked="" type="checkbox"/> Source Address <input checked="" type="checkbox"/> Source User <input type="checkbox"/> Source HIP Profile <input checked="" type="checkbox"/> Destination Zone <input checked="" type="checkbox"/> Destination Address <input checked="" type="checkbox"/> Application <input checked="" type="checkbox"/> Service <input checked="" type="checkbox"/> URL Category <input checked="" type="checkbox"/> Action <input checked="" type="checkbox"/> Profile <input type="checkbox"/> Options <input type="checkbox"/> Description	7-10-27 20:33:03
2	egress-outside	universal	 inside	any	any	 outside	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.

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


















	Name	Tags	Type	Source				Destination		Rule Usage			Application
				Zone	Address	User	HIP Profile	Zone	Address	Hit Count	Last Hit	First Hit	
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

	Name	Tags	Type	Source				Destination		Rule Usage			Application	Service	Action
				Zone	Address	User	HIP Profile	Zone	Address	Hit Count	Last Hit	First Hit			
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

	Name	Tags	Type	Source				Destination		Hit Count	Last Hit	First Hit	Apps Seen	Data
				Zone	Addr...	User	HIP Profile	Zone	Address					
1	egress-outside-app-id	egress	universal	ins...	any	any	any	outside	any	798	2019-01-16 21:53:01	2019-01-16 21:09:01	4	
2	egress-outside	egress	universal	ins...	any	any	any	outside	any	0	-	-	-	
3	internal-dmz-ftp	internal	universal	ins...	any	any	any	dmz	192.168...	-	-	-	-	
4	intrazone-default	none	intrazone	any	any	any	any	(intrazone)	any	-	2019-01-16 21:48:43	2018-09-22 19:20:57	-	

Timestamp of first policy rule match and last policy rule match

Number of applications seen by this rule

Reset

All rules
Selected rules

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 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)

	Name	Tags	Type	Source				Destination		Rule Usage			Application	Service	Action
				Zone	Address	User	HIP Profile	Zone	Address	Hit Count	Last Hit	First Hit			
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

Security Policy Rule

General Source User Destination Application Service/URL Category Actions Usage

Name: internal-inside-dmz

Rule Type: universal (default)

Description:

Tags: internal

Group Rules By Tag: internal

Audit Comment:

Audit Comment Archive

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

universal (default)
intrazone
interzone

Creating Security Policy Rules: Source Tab

Security Policy Rule ?

General Source User Destination Application Service/URL Category Actions Usage

☐ Any

☐ Source Zone ▲

☐ inside

☒ |

Accounting

danger

Data-Center-EU

Data-Center-US

dmz

inside

☒ Marketing

Operations

outside

☒ Any

☐ Source Address ▲

☒ Add ☐ Delete

☐ Negate

Creating Security Policy Rules: User Tab

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

Security Policy Rule

General Source **User** Destination Application Service/URL Category Actions Usage

any

Source User ▲

any
pre-logon
known-user
unknown
select

any

HIP Profiles ▲

+ Add - Delete

+ Add - Delete

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

Creating Security Policy Rules: Destination Tab

Security Policy Rule

General Source User Destination Application Service/URL Category Actions Usage

select

☐ Destination Zone ▲

☐ dmz

☒ |

Accounting

danger

Data-Center-EU

Data-Center-US

dmz

inside

+ Marketing

Operations

outside

☒ Any

☐ Destination Address ▲

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

+ Add - Delete

☐ Negate

Creating Security Policy Rules: Application Tab

Security Policy Rule ?

General Source User Destination Application Service/URL Category Actions Usage

☒ Any

☐ Applications

- ☐ ftp
- ☐ ssh
- ☐ ssl
- ☐ web-browsing

Default is Any; can add multiple applications.

+ Add - Delete

Creating Security Policy Rules: Service/URL Category Tab

Security Policy Rule

General Source User Destination Application Service/URL Category Actions Usage

application-default

☐ Service

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

☒ Any

☐ URL Category

Default is Any; can add multiple URL categories.

+ Add - Delete

+ Add - Delete

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

Log Setting

☐ Log at Session Start

☒ Log at Session End

Log Forwarding: None

Other Settings

Schedule: None

QoS Marking: None

☐ Disable Server Response Inspection

Profile Setting

Profile Type: None

Deny

Allow

Drop

Reset client

Reset server

Reset both client and server

Available with "drop" and all "reset" actions

Optional; add session start for troubleshooting.

Can schedule when the rule is active.

Creating Security Policy Rules: Usage Settings

The screenshot displays the 'Security Policy Rule' configuration interface. The 'Usage' tab is selected, showing the following sections and data:

- 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

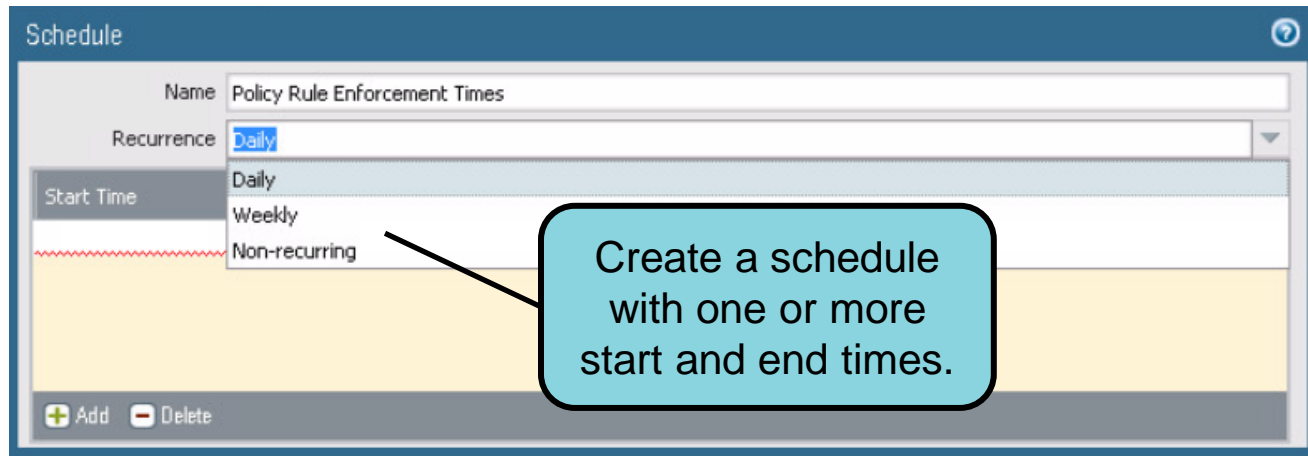
Callouts provide additional context for these sections:

- When rule was created and last updated:** Points to the 'Basics' section.
- Number of applications seen by this rule:** Points to the 'Applications' section.
- Provides tools to migrate from port-based rules:** Points to the 'Compare Applications & Applications Seen' link.
- Displays Hit Count data:** Points to the 'Activity' section.
- Traffic over the past 30 days:** Points to the 'Traffic (past 30 days)' section.

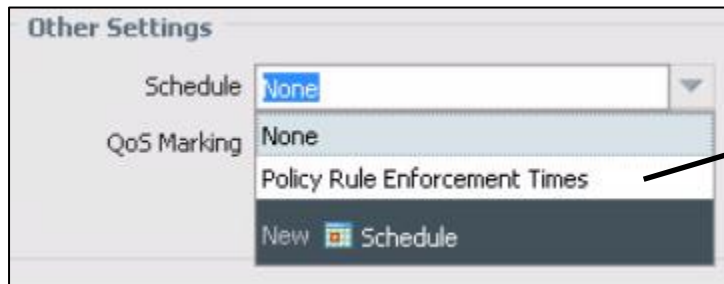
Scheduling Security Policy Rules

Objects > Schedules > Add

- 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



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	Tag	Action	Ad	Profile	Zone	Destination		Application
							Address	Application	
1	egress-outside-app-id	egress	universal	any	any	any	any	any	any
2	egress-outside	egress	universal	any	any	any	any	any	any
3	internal-dmz-ftp	Filter	universal	any	any	any	any	any	any
4	intrazone-default	Log Viewer	intrazone	any	any	any	any	any	any
5	interzone-default	Move	interzone	any	any	any	any	any	any

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

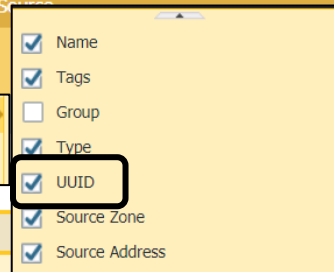
Test Policy Match

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

Universally Unique Identifiers (UUIDs)

Policies > Security

	Name	Tags	Type	UUID	Source		Destination
					Zone	Address	
1	egress-outside-app-id	egress	universal	d8982b29-22ae-4d63-b287-...	inside		outside
2	egress-outside	egress	universal	1e24dfe0-3e31-4ed9-af3a-3...	inside		outside
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)
5	interzone-default	none	interzone	c4673d56-b372-4855-9126-1993cd6dfef8		any	any



- 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			Source			Destination		
	Name	Tags	Type	Zone	Address	User	HIP Profile	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

Buttons: 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

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

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

Object : Addresses PDF/CSV Reset Rule Hit Counter

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

Tags internal

IP Netmask
IP Range
IP Wildcard Mask
FQDN

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)

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

Use new Address object.

Tags

Objects > Tags > Add

Tag

Name: Mail Servers Rule

Color: Cyan

Comments:

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

Security Policy Rule

General | Source | User | Destination | Application

Name: Protect Mail

Rule Type: universal (default)

Description:

Tags: Mail Servers Rule

Group Rules By Tag: Mail Servers Rule

Audit Comment:

Audit Comment Archive

Assign tag.

Assign rule to tag group.

(tag/member eq 'Mail Servers Rule')

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

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

		Name	Tags	Type	Source				Destination		Hit Count	
					Zone	Address	User	HIP Profile	Zone	Address		
internal (1)	1	2	egress-outside-app-id	egress	universal	inside	any	any	any	outside	any	14002
egress (2)	2-3											
internal (1)	4											
egress (1)	5											
none (1)	6	3	egress-outside	egress	universal	inside	any	any	any	outside	any	16956

Maintains rule priority

Change group of all rules
Delete all rules in group
Clone all rules in group

Hit Counter ▾ Group ▾ ☒ View Rulebase as Groups

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

Security Policy Rule

General Source User Destination Application Service/URL Category

select

☐ Service

☒ SMTP

☒ Any

☐ URL Category

Use new service.

Using Global Find

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

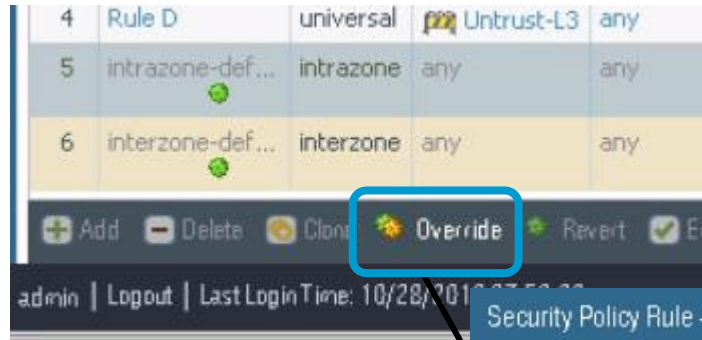
	Name	Tags	Type	Zone
1	Protect Mail	Mail Servers Rule	universal	T
5	intrazone-def...	none	Edit...	
6	interzone-def...	none	Filter	
			Global Find	

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		
Service (1)		
SMTP		
Security Rule (1)		
Protect Mail	VSYS	vsys1
Virus (1)		
Vulnerability (28)		

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

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

admin | Logout | LastLoginTime: 10/28/2018 07:53:00

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

Security Policy Rule - predefined

General Actions

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

Rule Changes Archive

The screenshot displays the Palo Alto Networks Security Policy Rule configuration interface. The left sidebar shows the rule configuration for 'egress-outside', including its name, type, description, tags, and group rules. The main area is titled 'Audit Comment Archive for Security Rule egress-outside' and contains three tabs: 'Audit Comments', 'Config Logs (between commits)', and 'Rule Changes'. The 'Audit Comments' tab is active, showing a list of comments. The 'Rule Changes' tab is also visible, showing a comparison of configuration logs between two commits. Callouts highlight specific features: 'Displays audit comment history' points to the 'Audit Comments' tab; 'Compare changes between configuration versions.' points to the 'Rule Changes' tab; 'Displays configuration logs' points to the configuration logs in the 'Rule Changes' tab; and 'Add A/V and A/S profiles' points to the 'Audit Comment' field in the left sidebar.

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

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

60

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 }

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

	Name	Tags	Type	Source				Destination		Rule Usage			
				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

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

Test Policy Match

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
	02/25 21:46:31	aged-out	any	inside	outside	192.168.1.254		4.2.2.2	53	dns	allow	egress-outside-content-id	aged-out
	02/25 21:46:01	aged-out	any	inside	outside	192.168.1.254		4.2.2.2	53	dns	allow	egress-outside-content-id	aged-out

View details

Detailed Log View

General	Source	Destination
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 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 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	Flags
	Type end	Captive Portal <input type="checkbox"/> Proxy Transaction <input type="checkbox"/> Decrypted <input type="checkbox"/>

PCAP	Receive Time	Type	Application	Action	Rule	Rule UUID	Byt...	Severity	Categ...	URL Categ...	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

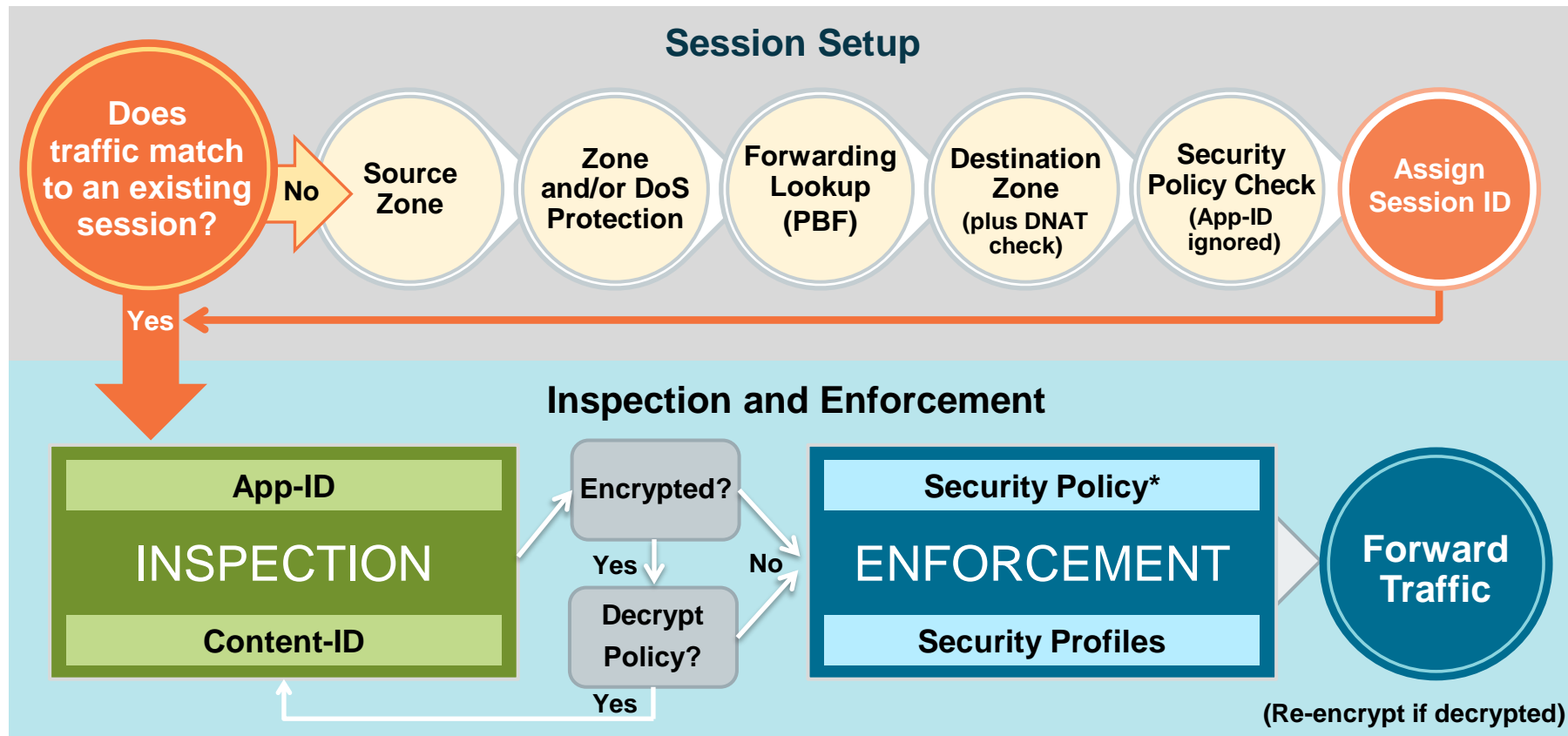
Security policy administration

Network address translation

Source NAT configuration

Destination NAT configuration

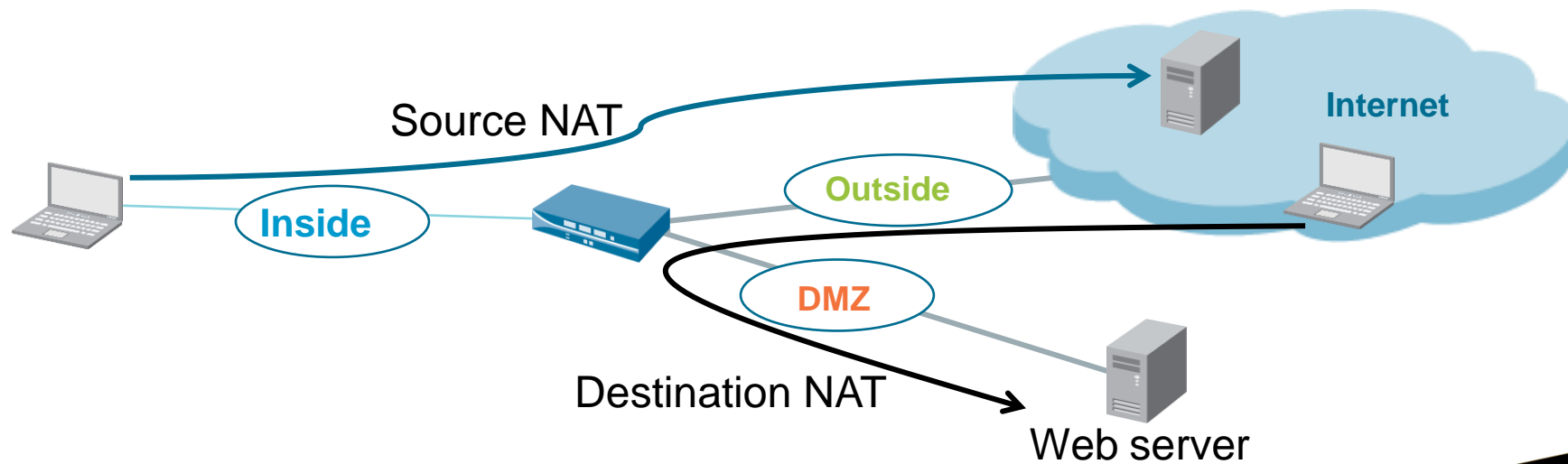
Flow Logic of the Next-Generation Firewall



* 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

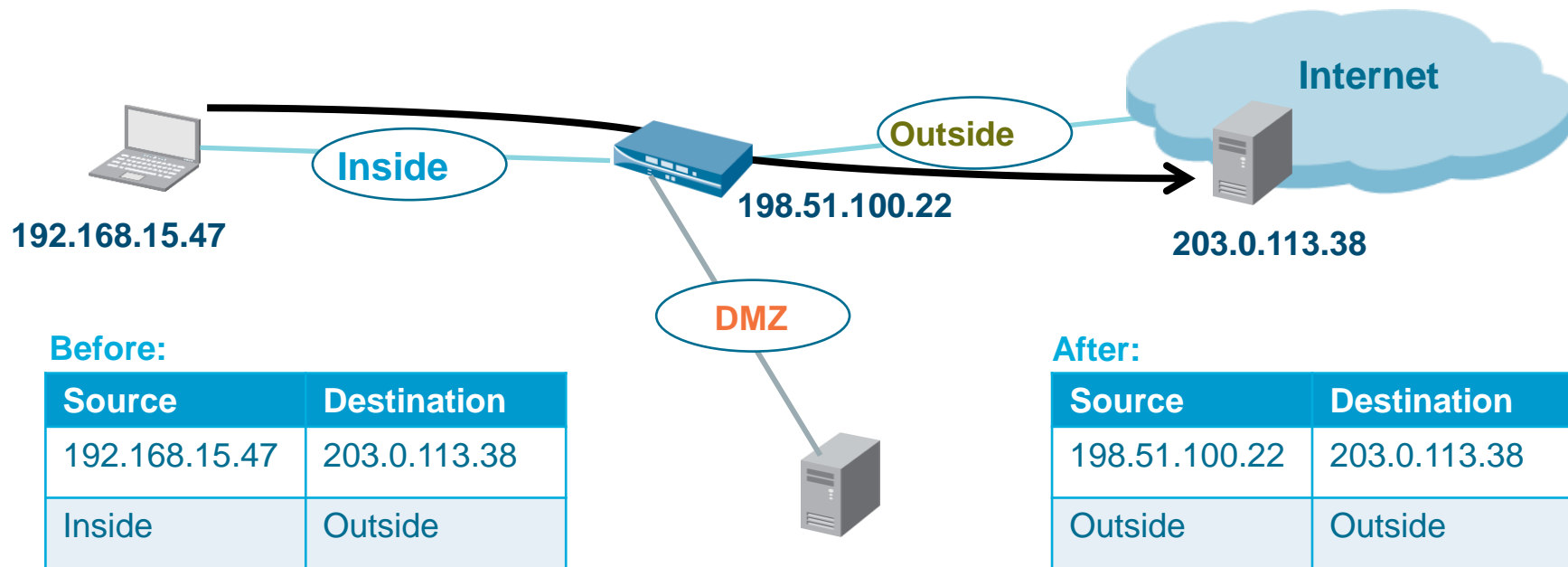
Network address translation

Source NAT configuration

Destination NAT configuration

Source NAT

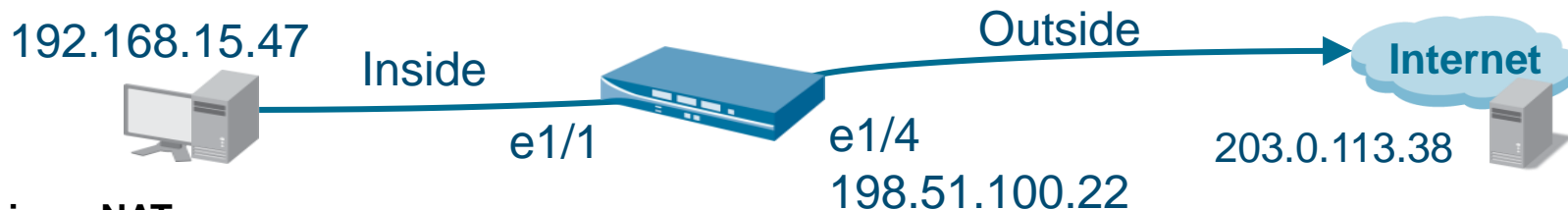
- Source NAT translates an original source IP address to an alternate source IP address.











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					Translated Packet		Rule U		
			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	internet	 any	 any	ethernet1/2	any	 192.168.15.0/24	 any	none	destination-translation address: 192.168.50.10	0	-

Pre-NAT zones

Pre-NAT addresses

Pre-NAT zones

Pre-NAT addresses

Policies > Security

	Name	Tags	Type	Source				Destination		Rule Usage			Application	Service	Action
				Zone	Address	User	HIP Profile	Zone	Address	Hit Count	Last Hit	First Hit			
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

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

+ Add - Delete

Match Criteria

Translation

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

Dynamic IP And Port

Dynamic IP




Static IP

None

Source NAT Examples




Static 1:1 Translation

Policies > NAT

	Name	Tags	Original Packet						Translated Packet		Hit Count
			Source Zone	Destination Zone	Destination Interface	Source Address	Destination Address	Service	Source Translation	Destination Translation	
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		Hit Count
			Source Zone	Destination Zone	Destination Interface	Source Address	Destination Address	Service	Source Translation	Destination Translation	
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

	Name	Tags	Original Packet						Translated Packet		Rule Usage		
			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

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 ▼

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

The screenshot shows the 'Session Settings' configuration page. Key settings include:

- ☒ 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
- ICMP Unreachable Packet Rate (per sec): Platform Default
- ☒ Accelerated Aging
- Accelerated Aging Threshold: 8
- Accelerated Aging Scaling Factor: 2.8x

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

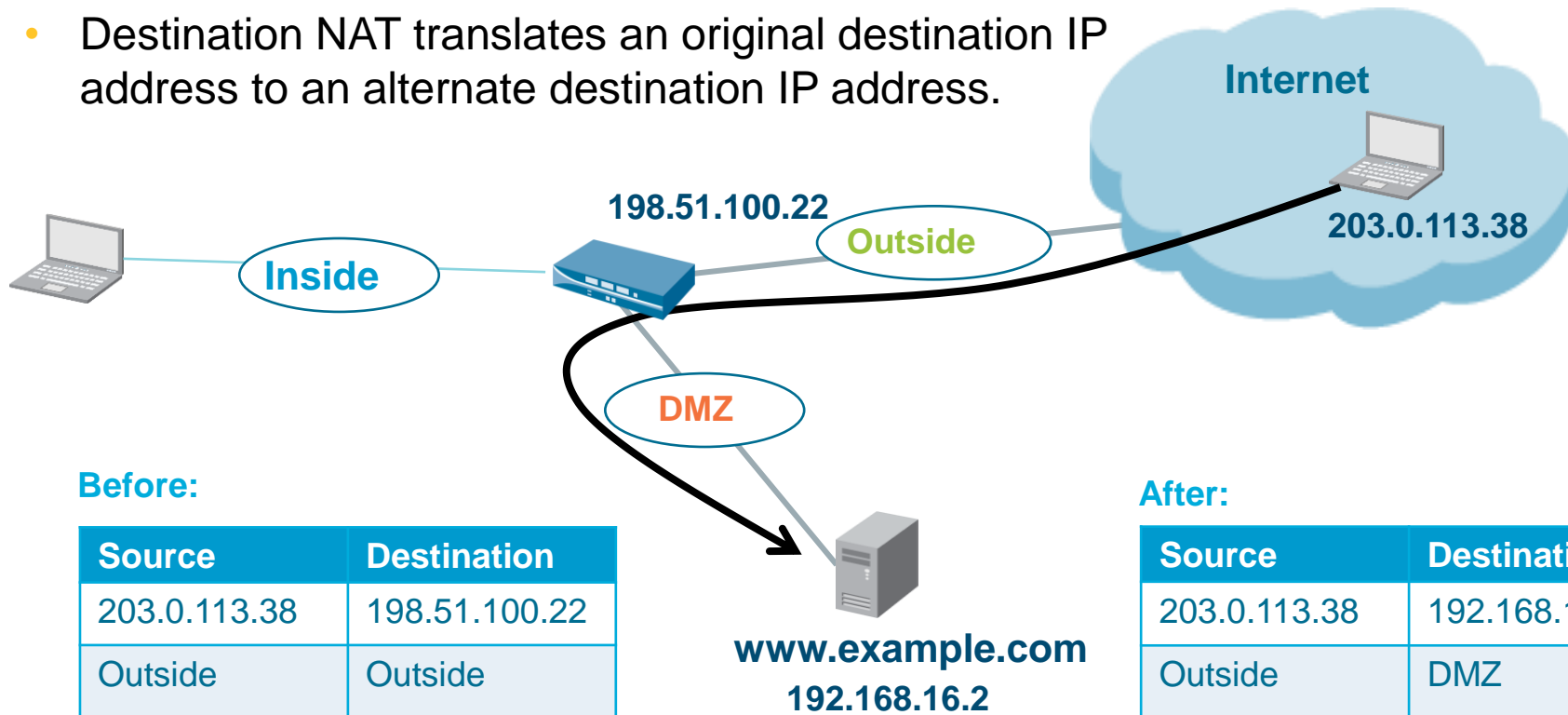
Network address translation

Source NAT configuration

Destination NAT configuration

Destination NAT


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



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 

General Original Packet Translated Packet

Source Address Translation

Translation Type

Destination Address Translation

Translation Type

Translated Address

Translated Port

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

General Original Packet Translated Packet

Source Address Translation

Translation Type

Destination Address Translation

Translation Type

Translated Address

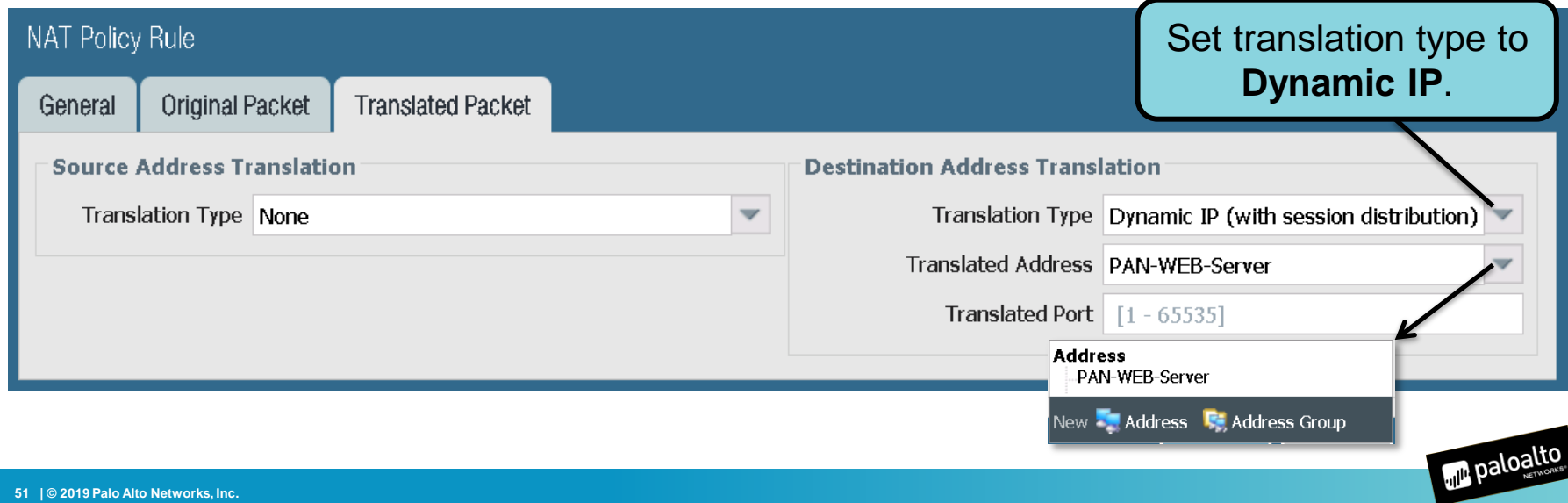
Translated Port

Address

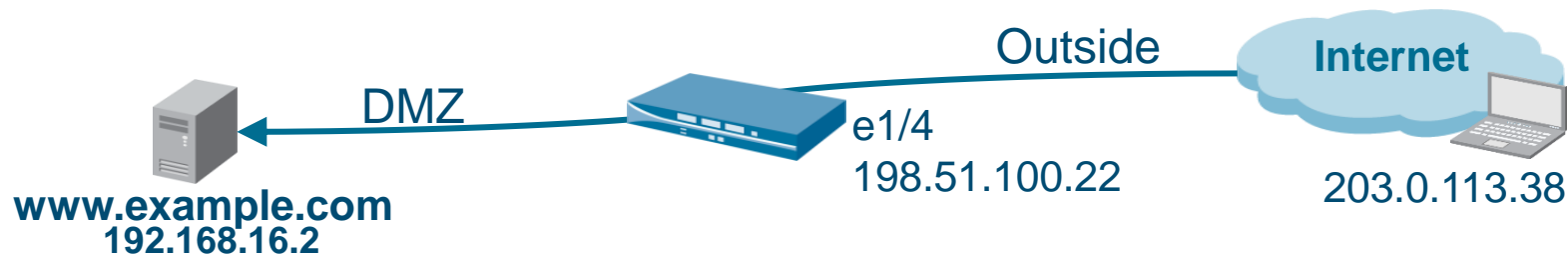
PAN-WEB-Server

New Address Address Group

Set translation type to **Dynamic IP**.



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	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

	Name	Tags	Type	Source				Destination		Rule Usage			Application	Service
				Zone	Address	User	HIP Profile	Zone	Address	Hit Count	Last Hit	First Hit		
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

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.

