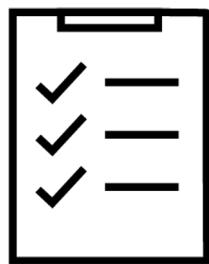


BLOCKING THREATS USING SECURITY AND NAT POLICIES



GET TRAFFIC FLOWING

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

EDU-210 Version B
PAN-OS® 10.0

An abstract graphic at the bottom left featuring several thick, curved lines in shades of orange and red. Some lines are solid, while others have a dashed or cross-hatched pattern. Two large, solid orange-red shapes resemble stylized arrows pointing towards the center. In the lower-left corner, there is a small white 'X' mark. To the right of the 'X' is the text "EDU-210 Version B" and "PAN-OS® 10.0".

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

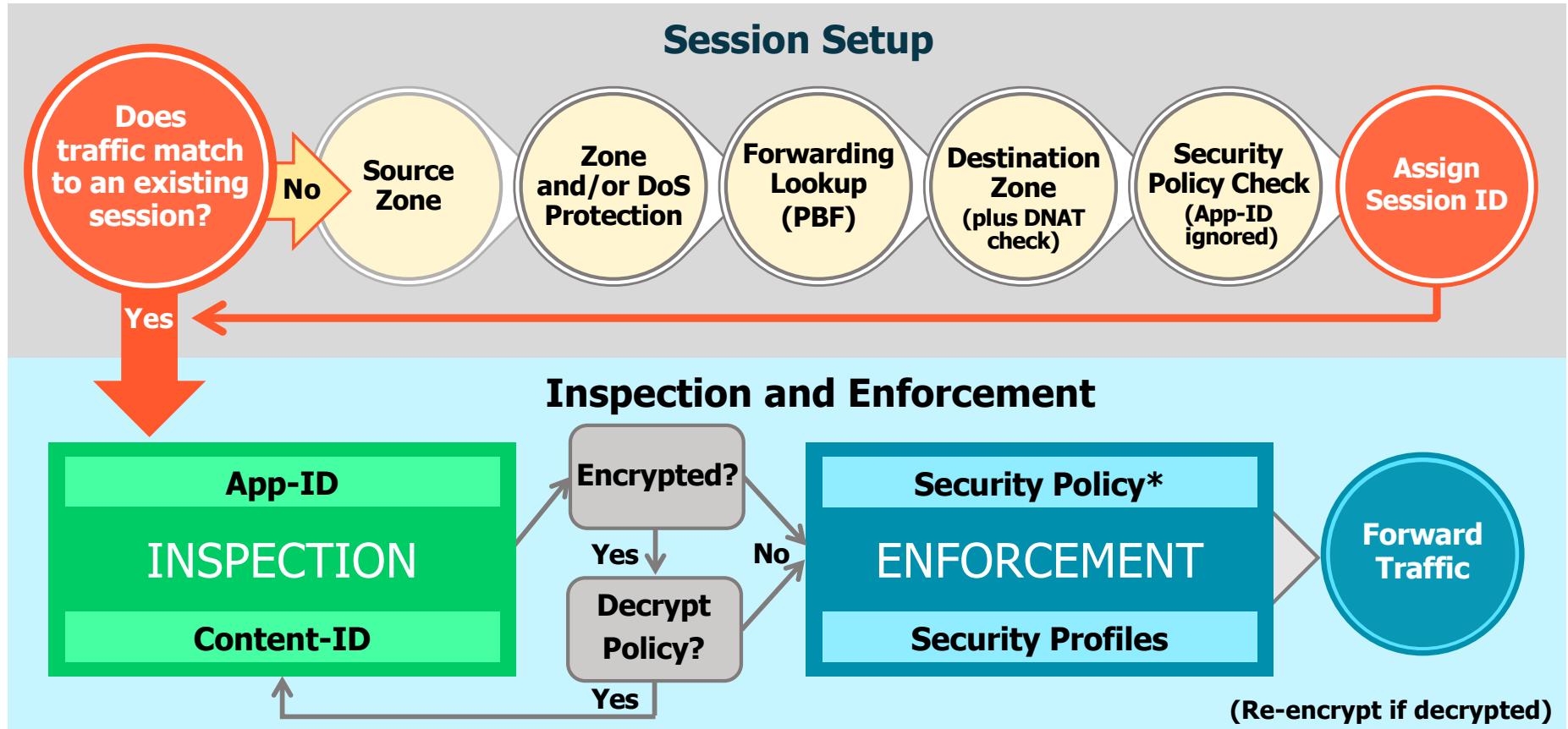
Security policy administration

Network address translation

Source NAT configuration

Destination NAT configuration

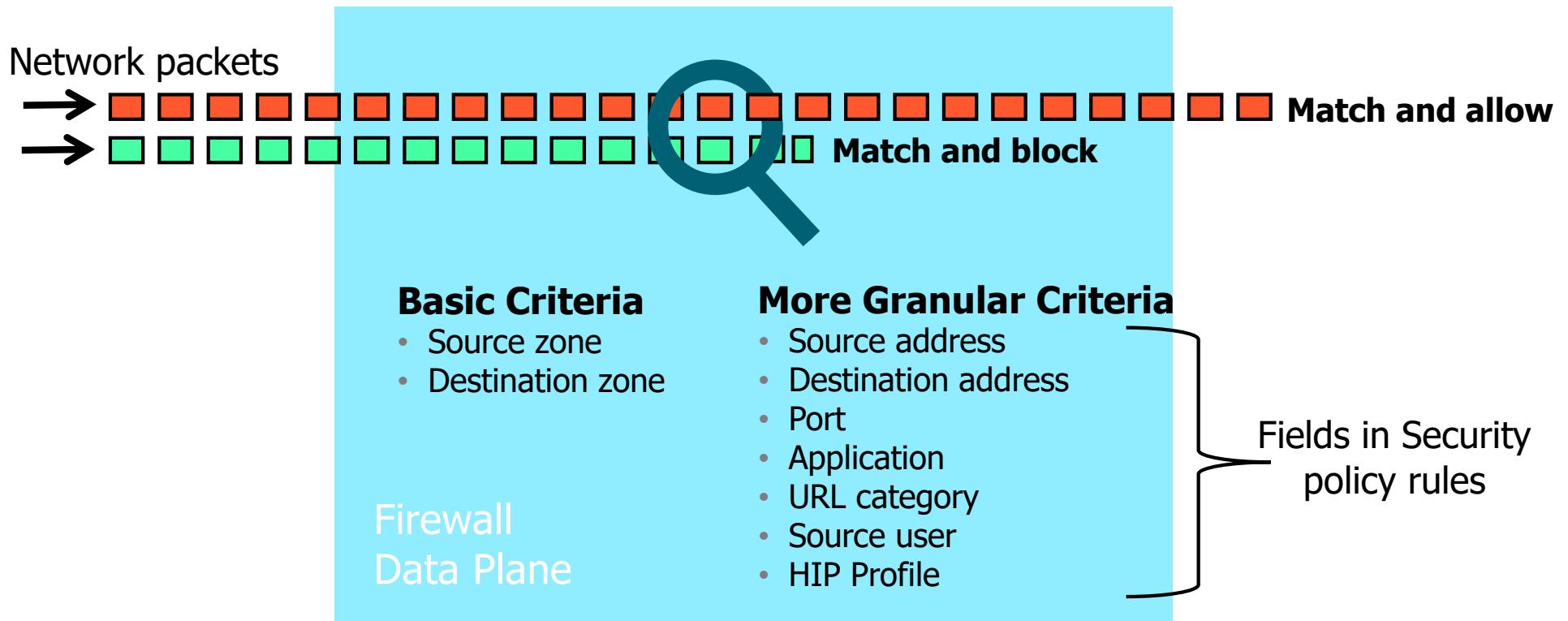
Flow Logic of the Next-Generation Firewall



*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 | | | | Destination | | | APPLICATION | SERVICE | ACTION |
|---|----------------------|-----------|-----------|-----------|---------|------|--------|-------------|---------|--------|-------------|----------------|--------|
| | | | | ZONE | ADDRESS | USER | DEVICE | ZONE | ADDRESS | DEVICE | | | |
| 1 | Users_to_Extranet | Users_Net | universal | Users_Net | any | any | any | Extranet | any | any | Columns | Adjust Columns | |
| 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 | | | |
| 4 | intrazone-default | none | intrazone | any | any | any | any | (intrazone) | any | any | | | |
| 5 | interzone-default | none | interzone | 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

The screenshot shows a table of policy rules with the following columns: NAME, TAGS, DEVICE, APPLICATION, SERVICE, and ACTION. The rules are numbered 1 to 5:

| | NAME | TAGS | DEVICE | APPLICATION | SERVICE | ACTION | | | | | | | |
|---|----------------------|--|-------------|-------------|---------|--------|-----|----------|-----|-----|-----|---------------------|-------|
| 1 | Users_to_Extranet | Users_Net | universal | Users_Net | any | any | any | Extranet | any | any | any | application-defa... | Allow |
| 2 | Users_to_Internet | Users_Net | universal | Users_Net | any | any | any | Internet | any | any | any | application-default | Allow |
| 3 | Extranet_to_Internet | Filter Log Viewer Move Copy UUID Global Find | universal | Extranet | any | any | any | Internet | any | any | any | application-defa... | Allow |
| 4 | intrazone-default | intrazone | (intrazone) | | any | any | any | | any | any | any | any | Allow |
| 5 | interzone-default | interzone | | | any | any | any | | any | any | any | any | Deny |

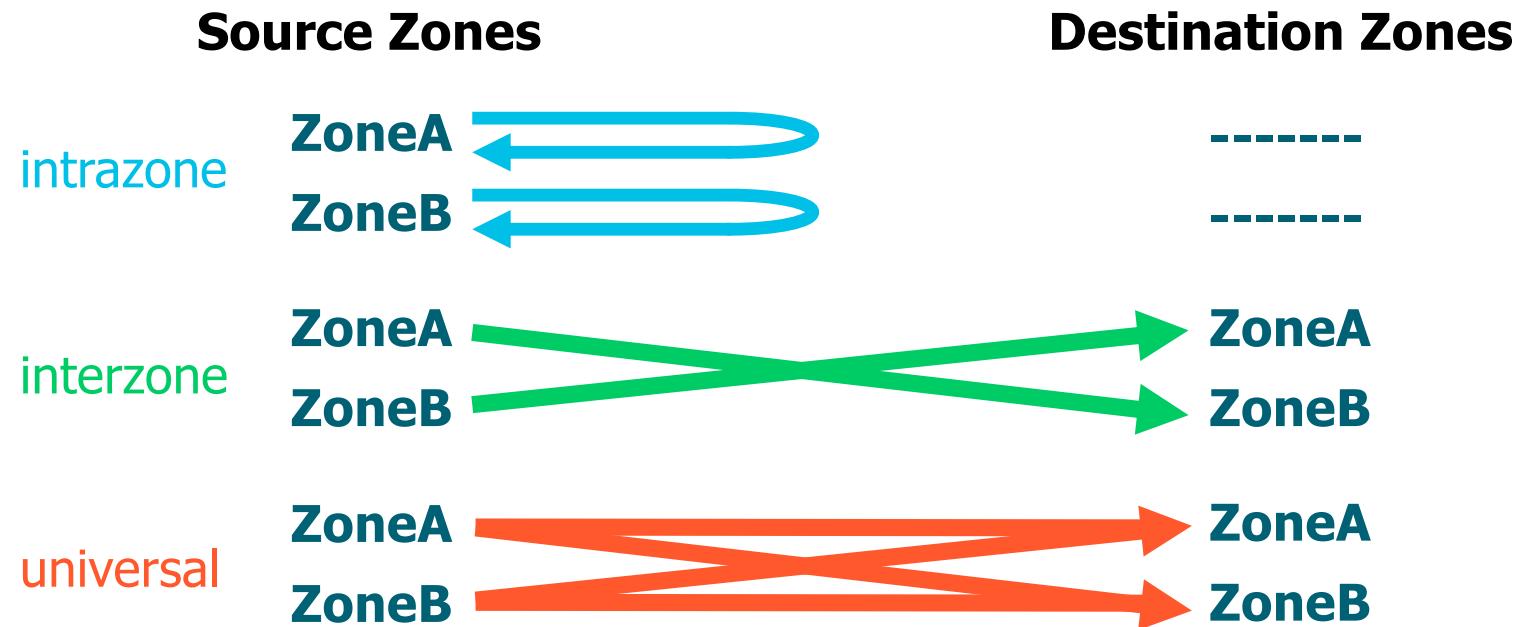
Annotations with arrows pointing to specific elements:

- A callout box points to the first rule (Users_to_Extranet) with the text: "Line numbers do not move when a rule moves."
- A callout box points to the fifth rule (interzone-default) with the text: "Disabled rules display in italics." The rule is shown in italicized text.
- A callout box points to the context menu for the third rule (Extranet_to_Internet) with the text: "Drop-down arrow displays menu options." The menu includes options like Filter, Log Viewer, Move, Copy UUID, and Global Find.
- A callout box points to the bottom navigation bar with the text: "+ Add, - Delete, ⌂ Clone, ⚙ Override, ⏪ Revert, ⚡ Enable, ⚡ Disable, ⚡ Move, PDF/CSV, ⚡ Highlight Unused Rules, ⚡ View Rulebase as Groups, Reset Rule Hit Counter, Group".

- **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.

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.

| | NAME | TAGS | TYPE | ZONE | ADDRESS | Source | Destination | DEVICE | APPLICATION | SERVICE | ACTION |
|---|----------------------|-----------|-----------|-----------|---------|--------|-------------|-------------|-------------|---------------------|---|
| 1 | Users_to_Extranet | Users_Net | universal | Users_Net | any | | | any | any | application-defa... | <input checked="" type="checkbox"/> Allow |
| 2 | Users_to_Internet | Users_Net | universal | Users_Net | any | any | any | Internet | any | any | <input checked="" type="checkbox"/> application-default |
| 3 | Extranet_to_Internet | Extranet | universal | Extranet | any | any | any | Internet | any | any | <input checked="" type="checkbox"/> application-defa... |
| 4 | intrazone-default | none | intrazone | any | any | any | any | (intrazone) | any | any | <input checked="" type="checkbox"/> Allow |
| 5 | interzone-default | none | interzone | any | any | any | any | any | any | any | <input checked="" type="checkbox"/> Deny |

Custom rule: By default, traffic is logged.

Predefined rules: By default, traffic is not logged.

Buttons at the bottom: Add, Delete, Clone, Override, Revert, Enable, Disable, Move, PDF/CSV, Highlight Unused Rules, View Rulebase as Groups, Reset Rule Hit Counter, Group.

Security Policy Rule Match

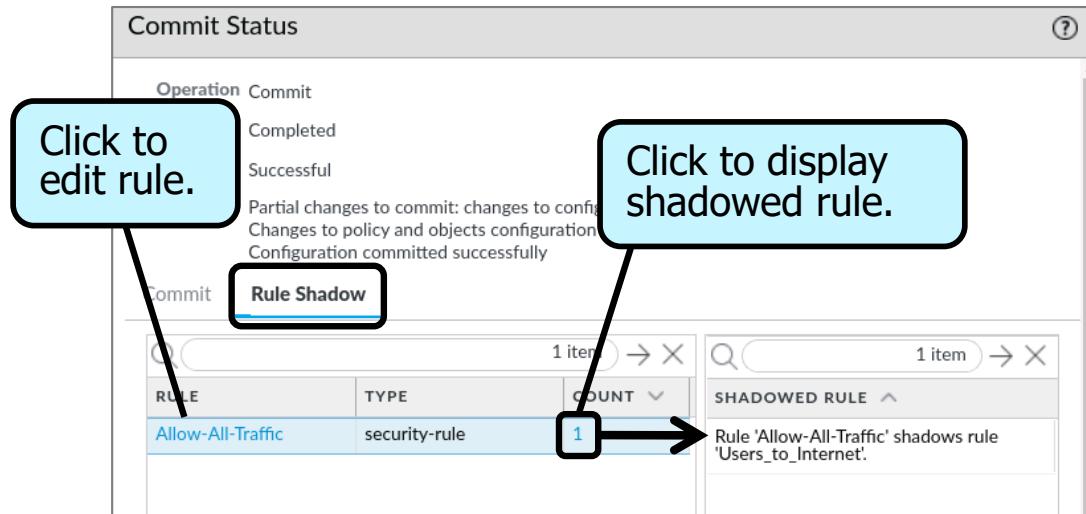
- Rules evaluated from top to bottom
- Further rules not evaluated after a rule match

| ID | 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.

Timestamp of first policy rule match and last policy rule match

Number of applications seen by this rule

All rules
Selected rules

Rule Usage

| NAME | TAGS | TYPE | Source | | Destination | | APPLICATION | SERVICE | ACTION | HIT COUNT | LAST HIT | FIRST HIT | APPS SEEN |
|------|----------------------|----------|-----------|-------------|-------------|-------------|-------------|----------------|---------------------|-----------|----------|---------------------|---------------------|
| | | | ZONE | ADDRESS | ZONE | ADDRESS | | | | | | | |
| 1 | Users_to_Internet | Internet | universal | [Users_Net] | any | [Internet] | any | [dns] | application-default | Allow | 386 | 2020-07-14 18:12:31 | 2020-07-14 17:58:58 |
| | | | | | | | | [google-base] | | | | | |
| | | | | | | | | [shutterfly] | | | | | |
| | | | | | | | | [ssl] | | | | | |
| | | | | | | | | [web-browsing] | | | | | |
| 2 | Users-Extranet | Extranet | universal | [Users_Net] | any | [Extranet] | any | any | application-default | Allow | 401 | 2020-07-14 18:12:21 | 2020-07-14 17:59:43 |
| 3 | Extranet_to_Internet | none | universal | [Extranet] | any | [Internet] | any | any | application-default | | | | 1 |
| 4 | intrazone-default | none | intrazone | any | any | (intrazone) | any | any | any | | | | 7:10:46 |
| 5 | interzone-default | none | interzone | any | any | any | any | any | any | | | | - |

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

View the Traffic Log

Monitor > Logs > Traffic

The screenshot shows the Palo Alto Networks Traffic Log interface. At the top, there is a table listing traffic sessions with columns for Receive Time, Type, From Zone, To Zone, Source, Destination, To Port, Application, Action, Rule, Session End Reason, and Bytes. Two sessions are selected, both labeled 'end' and 'allow'. A callout box points to the first session with the text 'View details.' Below the table is a detailed log view window. The 'General' tab is selected, showing session details like Session ID (127457), Action (allow), and Rule (Users_to_Internet). The 'Source' tab shows details like Source User (192.168.1.20), Source DAG, Country (192.168.0.0-192.168.255.255), Port (55648), Zone (Users_Net), Interface (ethernet1/2), NAT IP (203.0.113.20), NAT Port (28419), and X-Forwarded-For IP (0.0.0.0). The 'Destination' tab shows Destination User (172.217.9.14), Destination DAG, Country (United States), Port (80), Zone (Internet), Interface (ethernet1/1), NAT IP (172.217.9.14), and NAT Port (80). The 'Flags' tab indicates no Captive Portal. At the bottom, there is a table header for PCAP, RECEIVE TIME, TYPE, APPLICATION, ACTION, RULE, RULE UUID, BY..., SEVERI..., CATEG..., URL CATEG..., VERDI..., URL, and FILE NAME.

- 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

Configure a Security Policy Rule: General Tab

Policies > Security > Add

The screenshot shows the 'Policies > Security > Add' interface for creating a 'Security Policy Rule'. The 'General' tab is selected. The rule is named 'Users_to_Internet' with a 'universal (default)' rule type. The description is 'Allows hosts in Users_Net zone to access Internet'. It has a single tag 'Internet'. The audit comment is 'Policy initially created by admin-bob on 7/24'. A dropdown menu for 'Rule Type' shows options: 'universal (default)', 'intrazone', and 'interzone'. A link labeled 'Audit Comment Archive' is visible at the bottom left.

Usage tab appears after policy rule is created.

Optional, for easier visual identification and web interface filtering

Add audit comment describing what was added, when, and by whom.

Rule Changes Archive

Security Policy Rule

General | Source | Destination | Application | Service/IPLC | Audit Comments | Config Logs (between commits) | Rule Changes

Name: Users_to_Internet
Rule Type: universal (default)
Description: Allows hosts in Users_Net
Tags: Internet
Group Rules By Tag: Internet
Audit Comment: Added A/V, A/S, and URL filtering

Audit Comment Archive

Audit Comment Archive for Security Rule Users_to_Internet

219 Committed On 2020/07/14 20:41:12 by admin

Select a rule config version... Go

category any ;
application [dns google-base shutterfly ;
service application-default ;
source-hip any ;
destination-hip any ;
action allow ;
rule-type universal ;
description "Allows hosts in Users_Net zone"
tag Internet ;
profile-setting {
 profiles {
 url-filtering default ;
 virus default ;
 spyware default ;
 }
}
group-tag Internet ;

category any ;
application [dns google-base shutterfly ;
service application-default ;
source-hip any ;
destination-hip any ;
action allow ;
rule-type universal ;
description "Allows hosts in Users_Net zone"
tag Internet ;
profile-setting {
 profiles {
 url-filtering Corp URL Filter ;
 virus Corp AV ;
 spyware Corp AS ;
 }
}
group-tag Internet ;

Displays audit comment history
Compare changes between configuration versions.
Displays configuration logs

The screenshot shows the 'Security Policy Rule' interface. On the left, a 'General' tab displays a rule named 'Users_to_Internet' with a description 'Allows hosts in Users_Net'. It includes tags like 'Internet' and an audit comment 'Added A/V, A/S, and URL filtering'. On the right, an 'Audit Comment Archive' window is open, showing a commit history for the rule. The most recent commit (commit 219) is selected, showing the rule's configuration. The configuration includes various service definitions, source and destination IP ranges, and profile settings. Two specific sections of the configuration are highlighted with yellow boxes and labeled with callout bubbles: 'Display audit comment history' points to the audit comment in the general tab, and 'Display configuration logs' points to the configuration code in the archive window. Another callout bubble 'Compare changes between configuration versions.' points to the 'Rule Changes' tab in the archive window.

Configure a Security Policy Rule: Source Tab

The screenshot shows the 'Source' tab of a 'Security Policy Rule' configuration window. The top navigation bar includes tabs for General, Source, Destination, Application, Service/URL Category, Actions, and Usage. The 'Source' tab is selected.

The main area displays four source selection fields:

- SOURCE ZONE:** A dropdown menu showing 'Any' (selected), 'SOURCE ZONE' (disabled), and a list of zones: Danger, Extranet, Internet, and Users_Net. A blue callout box points to the 'Any' option with the text: "Default is **Any**. You can add multiple addresses, address groups, external dynamic lists, or geographical regions."
- SOURCE ADDRESS:** A dropdown menu showing 'Any' (selected), 'SOURCE ADDRESS' (disabled), and a list of options: External Dynamic List and Region. A blue callout box points to the 'Any' option with the text: "Policy will match all source addresses that are not listed."
- SOURCE USER:** A dropdown menu showing 'any' (selected), 'SOURCE USER' (disabled), and a list of user types: any, pre-logon, known-user, unknown, and select.
- SOURCE DEVICE:** A dropdown menu showing 'any' (selected), 'SOURCE DEVICE' (disabled), and a list of device types: any, no-hip, quarantine, and select.

At the bottom of the interface, there are 'Add' and 'Delete' buttons for each category, and a 'Negate' checkbox.

Configure a Security Policy Rule: Destination Tab

The screenshot shows the 'Destination' tab of a 'Security Policy Rule' configuration window. The interface includes tabs for General, Source, Destination, Application, Service/URL Category, Actions, and Usage. The Destination tab is active.

DESTINATION ZONE: Set to 'any'. A tooltip indicates: "Default is Any. You can add multiple addresses, address groups, external dynamic lists, or geographical regions."

DESTINATION ADDRESS: Set to 'Any'. A tooltip indicates: "Policy will match all source addresses that are not listed." Below this, there are two dropdown menus: 'External Dynamic List' and 'Region'.

- External Dynamic List:** Includes options like 'Palo Alto Networks - Bulletproof IP addresses', 'Palo Alto Networks - High risk IP addresses', and 'Palo Alto Networks - Known malicious IP address'.
- Region:** Lists IP ranges: '0.0.0.0-255.255.255 (Reserved(0.0.0.0-255.255.255.255))', '10.0.0.0-10.255.255.255 (Reserved(10.0.0.0-10.255.255.255))', '100.64.0.0-100.127.255.255 (Reserved(100.64.0.0-100.127.255.255))', '127.0.0.0-127.255.255.255 (Reserved(127.0.0.0-127.255.255.255))', and '169.254.0.0-169.254.255.255 (Reserved(169.254.0.0-169.254.255.255))'.

DESTINATION DEVICE: Set to 'any'. A tooltip indicates: "any quarantine select".

Action Buttons: '+ Add' and '- Delete' buttons are visible at the bottom of each section.

Configure a Security Policy Rule: Application Tab

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

The screenshot shows the 'Application' tab of a 'Security Policy Rule' configuration page. On the left, there's a list of selected applications: 'adobe-connectnow-base' (checked) and 'Any'. Below this is a search bar and a dependency list titled 'DEPENDS ON' containing 'flash', 'rtmp', 'rtmpt', 'ssl', and 'web-browsing', all of which are checked. At the bottom are 'Add' and 'Delete' buttons, and two action buttons: 'Add To Current Rule' and 'Add To Existing Rule'. A callout box with a black border and rounded corners contains the text: 'Add application, then check for/add application dependencies.' Two arrows point from this callout to the 'adobe-connectnow-base' entry in the application list and to the 'DEPENDS ON' dependency list respectively.

Security Policy Rule

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

Any

APPLICATIONS ▾

adobe-connectnow-base

Add application, then check for/add application dependencies.

DEPENDS ON ▾

flash

rtmp

rtmpt

ssl

web-browsing

+ Add - Delete

Add To Current Rule Add To Existing Rule

Unresolved Dependencies Reported During a Commit

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

Commit Status

Operation Commit

Status Completed

Result Successful

Details Partial changes to commit: changes to configuration by administrators: admin
Changes to policy and objects configuration
Configuration committed successfully

Commit [App Dependency](#)

| RULE | COUNT |
|-------------------|-------|
| Users_to_Internet | 5 |

1 item → X

| APP | DETAIL |
|-----------------------|---|
| adobe-connectnow-base | <ul style="list-style-type: none">adobe-connectnow-base requires flash to be allowed.adobe-connectnow-base requires rtmp to be allowed.adobe-connectnow-base requires rttmp to be allowed.adobe-connectnow-base requires ssl to be allowed.adobe-connectnow-base requires web-browsing to be allowed. |

1 item → X

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

The screenshot shows the 'Service/URL Category' tab selected in a security policy rule configuration interface. On the left, under 'SERVICE', there is a dropdown menu with options: 'application-default', 'any', and 'select'. A callout box with a black border and rounded corners contains the text: 'Default is **application-default**. You can add one or more services.' An arrow points from this box to the 'application-default' option in the dropdown. Below the dropdown is a list of services: 'service-http' and 'service-https'. At the bottom of this section are 'Add' and 'Delete' buttons. On the right, under 'URL CATEGORY', there is a checkbox labeled 'Any' which is checked. Another callout box with a black border and rounded corners contains the text: 'Default is **Any**. You can add multiple URL categories.' An arrow points from this box to the 'Any' checkbox. Below the checkbox is a list of URL categories: 'External Dynamic Lists' (panw-auth-portal-exclude-list), 'Palo Alto Networks' (abortion, abused-drugs, adult, alcohol-and-tobacco, auctions). At the bottom of this section are 'Add' and 'Delete' buttons.

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

Default is **Any**. You can add multiple URL categories.

application-default

any

select

Service

service-http

service-https

New Service Service Group

Add Delete

Any

External Dynamic Lists

panw-auth-portal-exclude-list

Palo Alto Networks

abortion

abused-drugs

adult

alcohol-and-tobacco

auctions

Add Delete

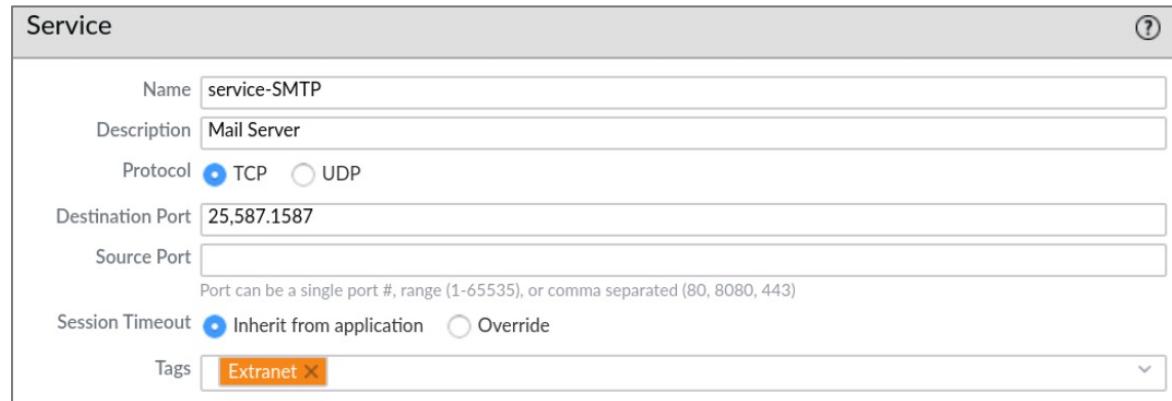
Configure a New Service Definition

- 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

Service

Name: service-SMTP
Description: Mail Server
Protocol: TCP UDP
Destination Port: 25,587,1587
Source Port:
Session Timeout: Inherit from application Override
Tags: Extranet

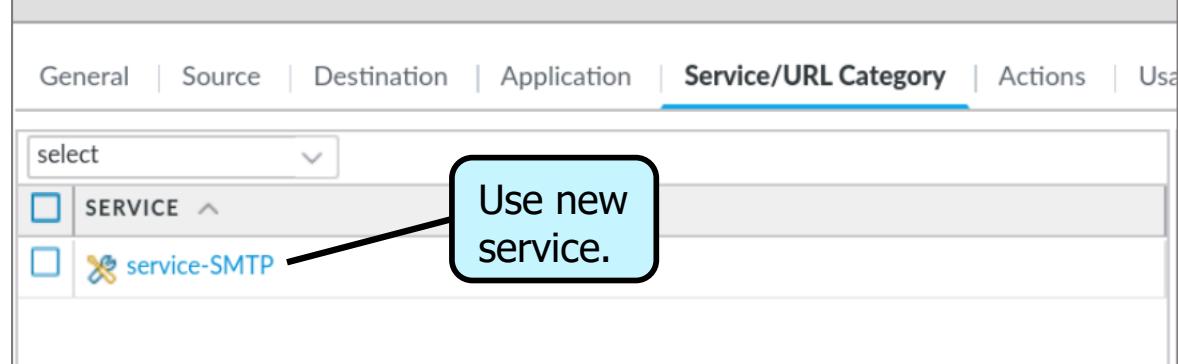


Security Policy Rule

General | Source | Destination | Application | **Service/URL Category** | Actions | Used

select

SERVICE ▾
 service-SMTP



Use new service.

Configure a Security Policy Rule: Actions Settings

The screenshot shows the 'Actions' tab of a 'Security Policy Rule' configuration page. The 'Action Setting' section has an 'Action' dropdown set to 'Allow'. Below it is a checkbox for 'Send ICMP Unread'. The 'Profile Setting' section has a 'Profile Type' dropdown set to 'None'. The 'Actions' dropdown menu is open, showing options: Deny, Allow (selected), Drop, Reset client, Reset server, and Reset both client and server. The 'Log Setting' section includes checkboxes for 'Log at Session Start' (unchecked) and 'Log at Session End' (checked). The 'Log Forwarding' dropdown is set to 'None'. The 'Other Settings' section includes dropdowns for 'Schedule' (set to 'None') and 'QoS Marking' (set to 'None'), and a checkbox for 'Disable Server Response' (unchecked).

Available with "drop" and all "reset" actions

Optional: Add session start for troubleshooting.

Can schedule when the rule is active

Enable Intrazone and Interzone Logging

Policies > Security > <select_default_rule>

| | | | | | | |
|---|-------------------|------|-----------|-----|-----|-----|
| 4 | intrazone-default | none | intrazone | any | any | any |
| 5 | interzone-default | none | interzone | any | any | any |

Add Delete Clone **Override** Revert Enable Disable Move

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

Security Policy Rule

General Actions

Action Setting

Action Deny
 Send ICMP Unreachable

Profile Setting

Profile Type None

Log Setting

Log at Session Start
 Log at Session End

Log Forwarding None

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

The screenshot shows a 'Schedule' configuration window. The 'Name' field is set to 'Policy_Rule_Enforcement_Times'. The 'Recurrence' dropdown is set to 'Daily'. Below the recurrence dropdown, there is a table with two rows: 'START TIME' (08:00) and 'END TIME' (18:00). A callout box points to this table with the text: 'Create a schedule with one or more start and end times.' To the right of the table, a dropdown menu shows options: 'Daily', 'Weekly', and 'Non-recurring'. Another callout box points to this dropdown with the text: 'Apply schedule to a rule.'

Policies > Security > <select_rule> > Actions

The screenshot shows the 'Actions' section of a policy rule configuration. Under 'Other Settings', the 'Schedule' dropdown is set to 'Policy_Rule_Enforcement_Times'. A callout box points to this dropdown with the text: 'Apply schedule to a rule.'

Configure a Security Policy Rule: Usage Settings

The screenshot shows the 'Usage' tab of a 'Security Policy Rule' configuration page. The tab is part of a navigation bar with other tabs like General, Source, Destination, Application, Service/URL Category, Actions, and Usage. The Usage tab is highlighted with a blue underline.

Basics:

- Rule Created: 2020-07-14 17:59:46
- Last Edited: 2020-07-14 20:44:04

Activity:

- Hit Count: 6331
- First Hit: 0 days ago (2020-07-14 18:17:03)
- Last Hit: 0 days ago (2020-07-14 21:22:21)

Applications:

- Applications Seen: 6
- Last App Seen: 0 days ago

Traffic (past 30 days):

- Bytes: 1.7M

Annotations with callouts explain specific features:

- A callout points to the 'Rule Created' and 'Last Edited' fields with the text: "View when rule was created and last modified."
- A callout points to the 'Compare Applications & Applications Seen' link with the text: "Provides tools to migrate from port-based rules"
- A callout points to the 'Bytes' field with the text: "View amount of traffic, in bytes, over the past 30 days."

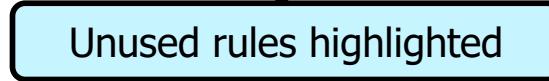
Find Unused Security Policy Rules

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

Policies > Security

| | NAME | TAGS | TYPE | Source | | | Destination | | | APPLICATION | SERVICE | ACTION | HIT COUNT | |
|---|----------------------|----------|-----------|-----------|---------|------|-------------|-------------|---------|-------------|-----------------------|---------------------|-----------|-------|
| | | | | ZONE | ADDRESS | USER | DEVICE | ZONE | ADDRESS | DEVICE | | | | |
| 1 | Users_to_Internet | Internet | universal | Users_Net | any | any | any | Internet | any | any | adobe-connectnow-base | application-default | Allow | 77057 |
| 2 | Users_to_Extranet | none | universal | Users_Net | any | any | any | Extranet | any | any | | application-default | Allow | 2521 |
| 3 | Extranet_to_Internet | none | universal | Extranet | any | any | any | Internet | any | any | | application-default | Allow | 0 |
| 4 | intrazone-default | none | intrazone | any | any | any | any | (intrazone) | any | any | any | any | Allow | 83256 |
| 5 | interzone-default | none | interzone | any | any | any | any | any | any | any | any | any | Deny | - |

Unused rules highlighted



Highlight Unused Rules

Rule Usage Filter

Policies > Security > Policy Optimizer > Rule Usage

PA-VM

DASHBOARD ACC MONITOR POLICIES OBJECTS NETWORK DEVICE

Commit ?

Security

- NAT
- QoS
- Policy Based Forwarding
- Decryption
- Tunnel Inspection
- Application Override

Policy Optimizer

- No App Specified
- Unused Apps
- Rule Usage
 - Unused in 30 days
 - Unused in 90 days
 - Unused

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 | TIMEFRAME | RESET DATE | MODIFIED | CREATED |
|------------------------|-----------|---------------|---------------------|---------------------|---------------------|
| 1 Users_to_Internet | 8975 | All time | 2020-07-14 22:00:00 | 2020-07-14 18:17:03 | 2020-07-14 20:44:04 |
| 2 Users-Extranet | 7524 | Past 1 day | 2020-07-14 22:03:04 | 2020-07-14 17:59:43 | 2020-07-14 20:41:10 |
| 3 Extranet_to_Internet | 8 | Past 7 days | 2020-07-14 19:50:28 | 2020-07-14 19:50:28 | 2020-07-14 20:41:10 |
| 4 intrazone-default | 8130 | Past 30 days | 2020-07-14 21:58:10 | 2020-05-15 17:10:46 | 2019-02-15 01:03:25 |
| 5 interzone-default | 3336 | Past 90 days | 2020-07-01 17:01:03 | 2020-05-18 14:22:57 | 2019-02-15 01:03:25 |
| | | Past 180 days | | | |
| | | Past 365 days | | | |
| | | Custom... | | | |

Object : Addresses + Delete Enable Disable PDF/CSV Reset Rule Hit Counter Tag UnTag

admin | Logout | Last Login Time: 07/13/2020 16:55:53 | Session Expire Time: 08/13/2020 16:47:11

Tasks | Language paloalto NETWORKS

Tags

Objects > Tags > Add

| | |
|----------|--------------------------------------|
| Tag | ? |
| Name | Mail_Servers |
| Color | Turquoise Blue |
| Comments | Tag for Mail Servers on the Extranet |

| | | | | |
|---|--|--|--|--|
| Security Policy Rule | | | | |
| General Source Destination Application Service/URL Category | | | | |
| Name | Protected_Mail_Servers | | | |
| Rule Type | universal (default) | | | |
| Description | Policy designed to protect the mail servers. | | | |
| Tags | Mail_Servers | | | |
| Group Rules By Tag | Mail_Servers | | | |
| Audit Comment | Mail Servers Policy created | | | |
| Audit Comment Archive | | | | |

Assign tag.

Assign rule to tag group.

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

Filter for tag.

| | NAME | TAGS | TYPE | ZONE |
|---|------------------------|--------------|-----------|------|
| 4 | Protected_Mail_Servers | Mail_Servers | universal | any |
| 5 | intrazone-default | none | intrazone | any |
| 6 | interzone-default | none | interzone | any |

Look for tag color.

Tag-Based Rule Groups

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

Policies > Security

The screenshot shows a table of security rules. A callout box points to the rule at index 1, which has a yellow 'Users_Net' tag under 'TAGS'. This rule is highlighted with a yellow background. Another callout box points to the rule at index 2, which has an orange 'Extranet' tag under 'TAGS'. The rule at index 2 is also highlighted with a yellow background. A context menu is open over the rule at index 2, listing options: 'Change group of all rules', 'Move all rules in group', 'Delete all rules in group', and 'Clone all rules in group'. The 'View Rulebase as Groups' checkbox is checked in the bottom right corner of the interface.

| | NAME | TAGS | TYPE | Source | | | Destination | | APPLICATION | SERVICE | ACTION | |
|------------------|------|---------------------|----------|-----------|-----------|------|-------------|----------|-------------|-----------------------|---------------------|-------|
| | | | | ZONE | ADDRESS | USER | ZONE | ADDRESS | | | | |
| Internet (1) | 1 | 1 Users_to_Internet | Internet | universal | Users_Net | any | any | Internet | any | adobe-connectnow-base | application-default | Allow |
| Extranet (1) | 2 | | | | | | | | | | | |
| Internet (1) | 3 | | | | | | | | | | | |
| Mail_Servers (1) | 4 | | | | | | | | | | | |

Maintains rule priority

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

View Rulebase as Groups Reset Rule Hit Counter Group

Test Policy Functionality

Policies > Security

Test criteria

Test Security Policy Match

Test Configuration

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

Test Result

Users_to_Internet

Result Detail

| NAME | VALUE |
|---------------------|---|
| Name | Users_to_Internet |
| Index | 1 |
| From | Users_Net |
| Source | any |
| Source Region | none |
| To | Internet |
| Destination | any |
| Destination Region | none |
| User | any |
| source-device | any |
| destination-device | any |
| Category | any |
| Application Service | 0:adobe-connectnow/tcp/any... 1:adobe-connectnow/tcp/any... 2:adobe-connectnow/tcp/any... |
| Action | allow |
| ICMP Unreachable | no |
| Terminal | yes |

Policy matched

Policy details

Use Global Find



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

| | NAME | TAGS | TYPE | ZONE |
|---|----------------------|----------|-------------|-----------|
| 1 | Users_to_Extranet | Extranet | Edit... | Users_Net |
| 2 | Users_to_Internet | Internet | Filter | Users_Net |
| 3 | Extranet_to_Internet | Internet | Global Find | Extranet |

smtp

| NAME | TYPE | ZONE |
|------------------|------------|------|
| Application (10) | | |
| > adobe-meeting | Predefined | |
| > ariel | Predefined | |
| > dcc-antispam | Predefined | |
| > fastmail | Predefined | |
| > hosproxy | Predefined | |
| > linkedin-intro | Predefined | |
| > smtp | Predefined | |
| > squirrelmail | Predefined | |
| > x/400 | Predefined | |
| > zabbix | Predefined | |

Export CSV

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

Security policy fundamental concepts

Security policy administration

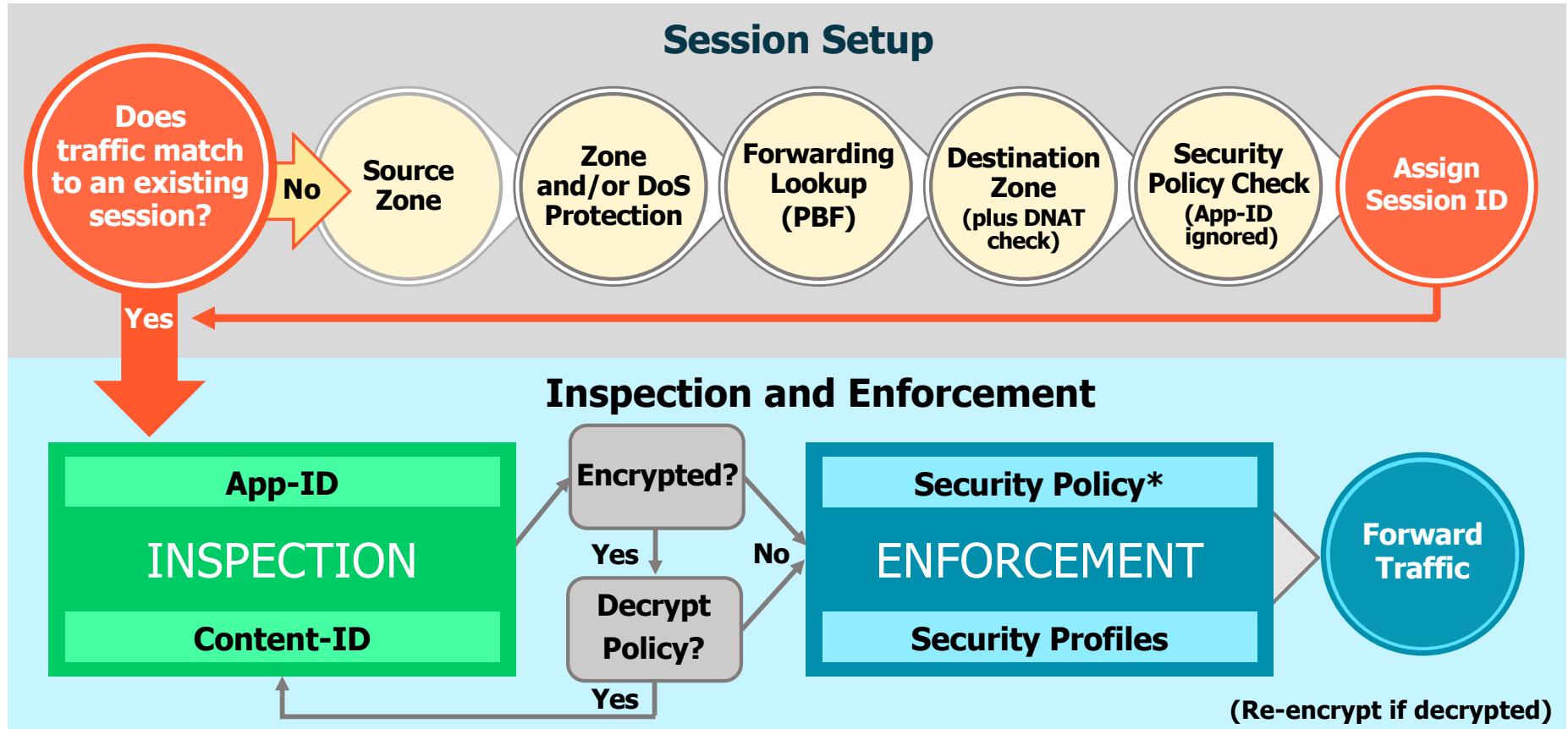


Network address translation

Source NAT configuration

Destination NAT configuration

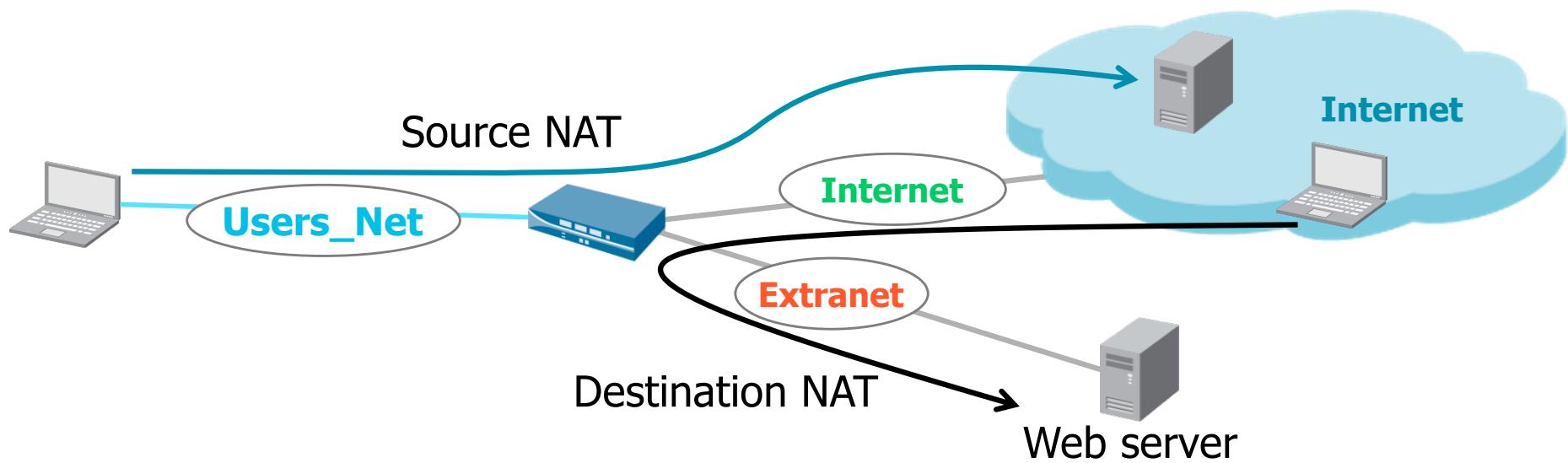
Flow Logic of the Next-Generation Firewall



*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

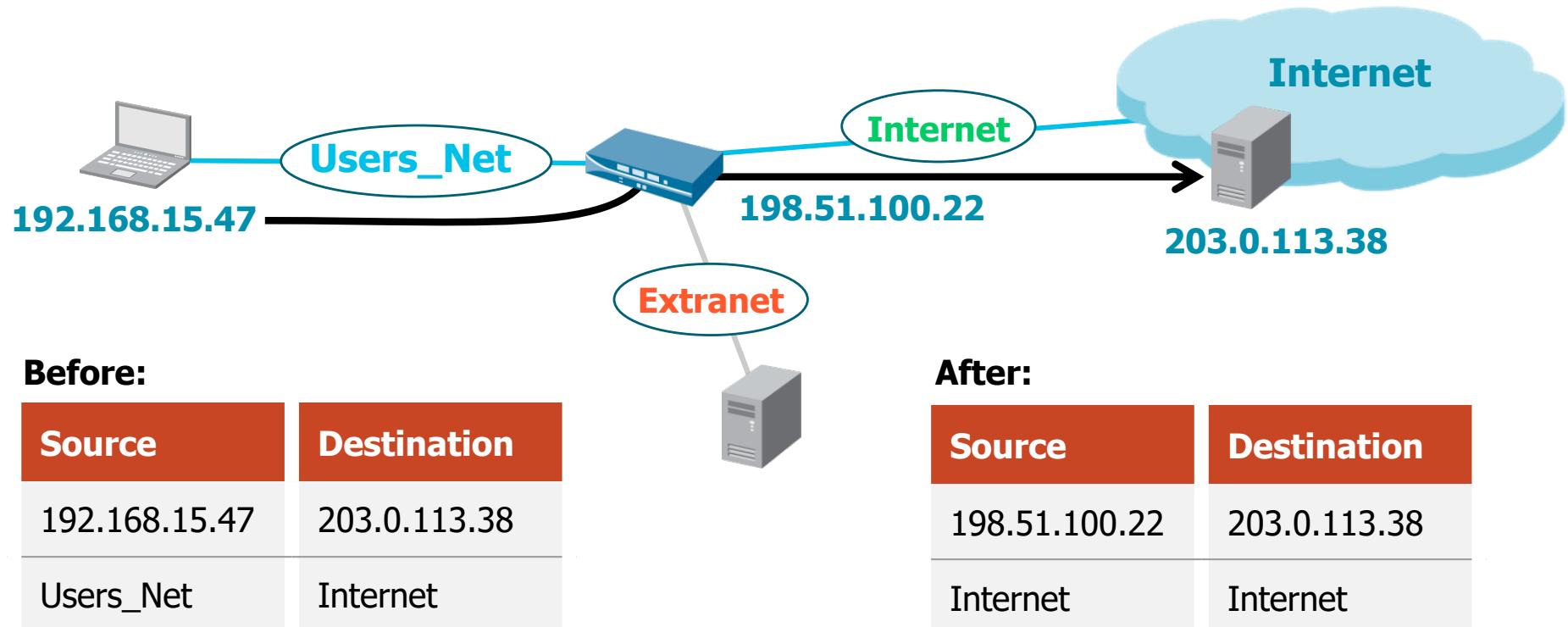


Source NAT configuration

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 | | | HIT COUNT | |
|------|------------------------------|-----------------|------------------|-----------------------|----------------|---------------------|---------|---|-----------|--------|
| | | SOURCE ZONE | DESTINATION ZONE | DESTINATION INTERFACE | SOURCE ADDRESS | DESTINATION ADDRESS | SERVICE | SOURCE TRANSLATION | | |
| 1 | Source_Users_Net_to_Internet | Internet | Users_Net | Internet | any | 192.168.15.0/24 | any | dynamic-ip-and-port ethernet1/1 198.51.100.22 | none | 283983 |

Annotations below the table highlight 'Pre-NAT zones' (covering SOURCE ZONE and DESTINATION ZONE) and 'Pre-NAT addresses' (covering SOURCE ADDRESS and DESTINATION ADDRESS).

Policies > Security

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

Annotations below the table highlight 'Pre-NAT address' (covering SOURCE ADDRESS), 'Post-NAT zone' (covering DESTINATION ZONE), and 'Pre-NAT address' (covering DESTINATION ADDRESS).

Configure Source NAT

NAT Policy Rule

Original Packet

General | Original Packet | Translated Packet

Any | SOURCE ZONE | Users_Net

Destination Zone: Internet

Any | SOURCE ADDRESS | 192.168.15.0/24

Any | DESTINATION ADDRESS

Destination Interface: any

Match Criteria

NAT Policy Rule

Translated Packet

Source Address Translation

Translation Type: Dynamic IP And Port

Address Type: Interface Address

Interface: ethernet1/4

IP Address: 198.51.100.22

Destination Address Translation

Translation Type: None

Dynamic IP And Port

Dynamic IP

Static IP

None

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 |
| 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

| | 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 | 192.168.15.2-192.168.15.50 | 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

The screenshot shows the 'NAT Policy Rule' configuration page. The 'Translated Packet' tab is selected. Under 'Source Address Translation', the 'Translation Type' is set to 'Static IP' (highlighted with a black box) and the 'Translated Address' is '198.51.100.22'. A checkbox labeled 'Bi-directional' is checked and highlighted with a black box. Under 'Destination Address Translation', the 'Translation Type' is set to '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

Session Settings

| |
|--|
| <input checked="" type="checkbox"/> Rematch all sessions on config policy change |
| ICMPv6 Token Bucket Size <input type="text" value="100"/> |
| ICMPv6 Error Packet Rate (per sec) <input type="text" value="100"/> |
| <input checked="" type="checkbox"/> Enable IPv6 Firewalling |
| <input type="checkbox"/> Enable Jumbo Frame |
| <input type="checkbox"/> Enable DHCP Broadcast Session |
| NAT64 IPv6 Minimum Network MTU <input type="text" value="1280"/> |
| NAT Oversubscription Rate <input type="text" value="Platform Default"/> |
| ICMP Unreachable Packet Rate (per sec) |
| <input checked="" type="checkbox"/> Accelerated Aging |
| Accelerated Aging Threshold |
| Accelerated Aging Scaling Factor |
| <input checked="" type="checkbox"/> Packet Buffer Protection |

| 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

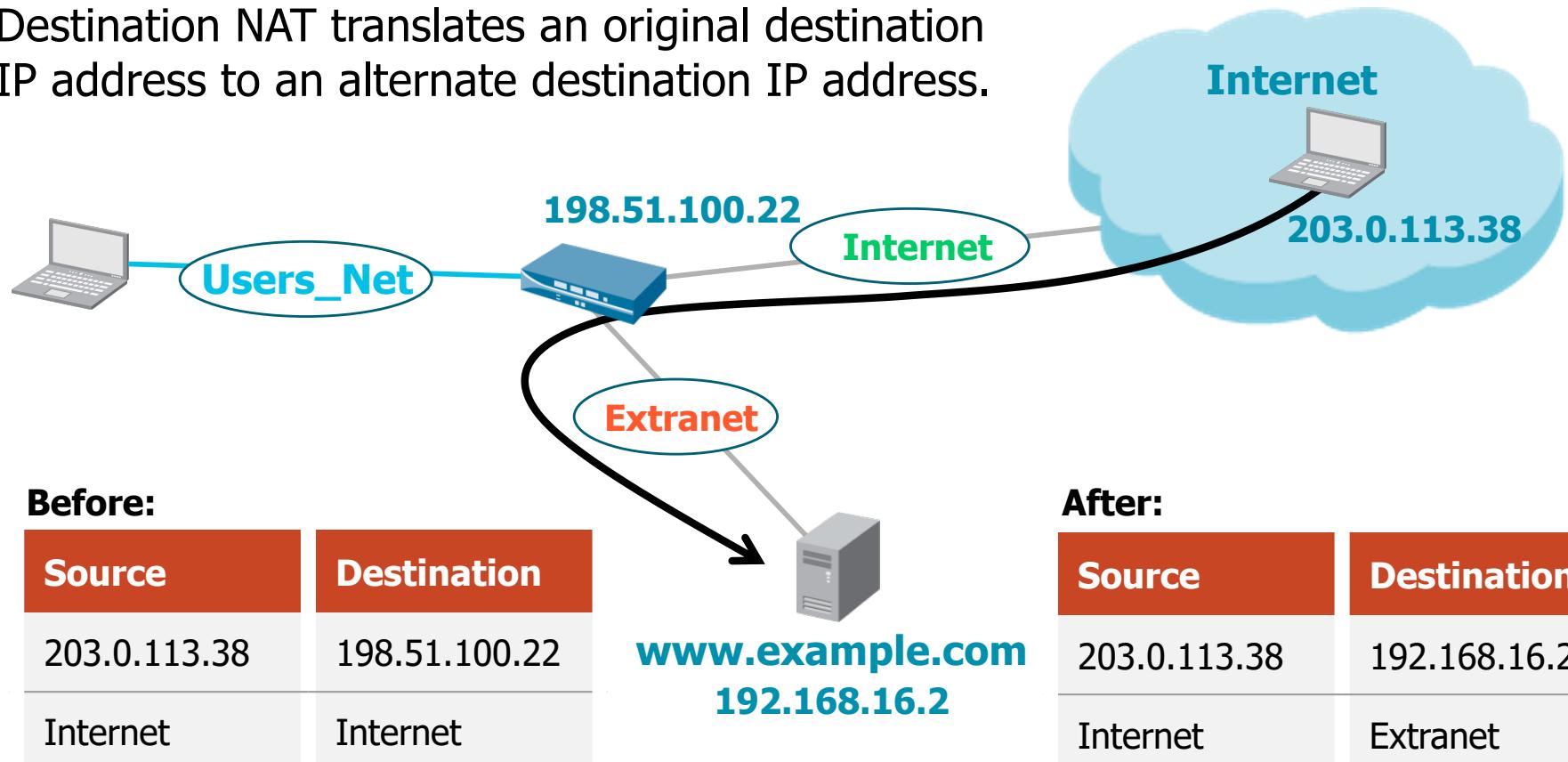
Network address translation

Source NAT configuration

▶ **Destination NAT configuration**

Destination NAT

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



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

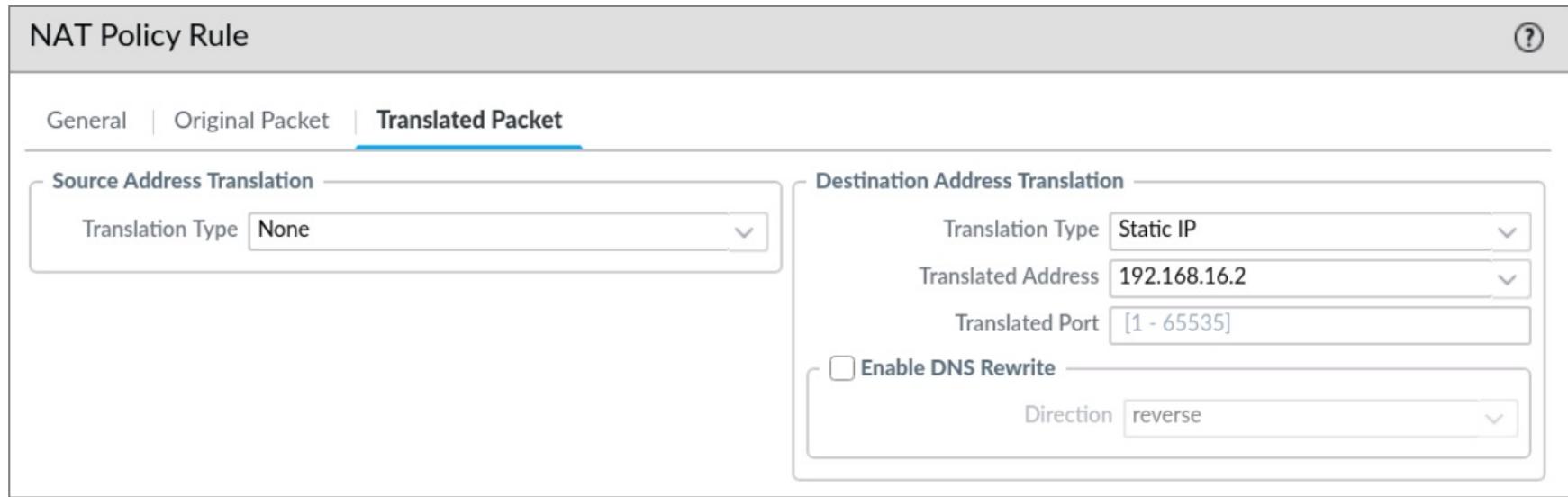
Translation Type

Translated Address

Translated Port

Enable DNS Rewrite

Direction



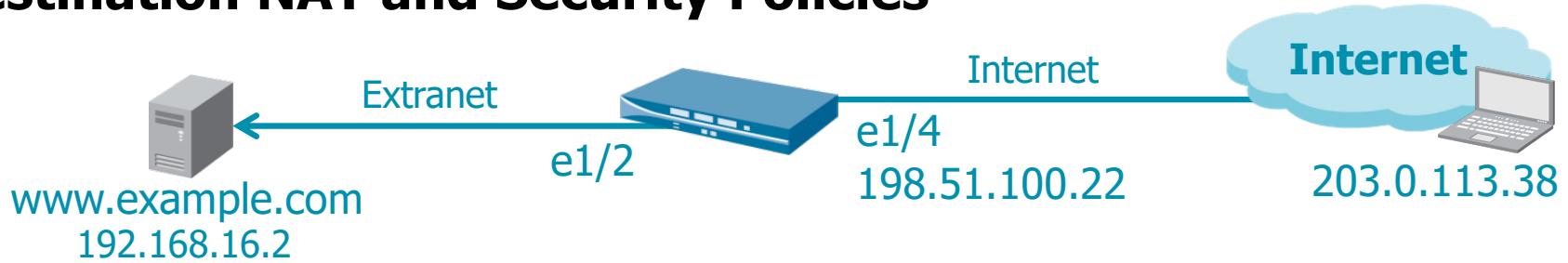
Dynamic IP Address Support for Destination NAT

- 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

The screenshot shows the 'NAT Policy Rule' configuration interface. The 'Translated Packet' tab is selected. In the 'Source Address Translation' section, the 'Translation Type' dropdown is set to 'None'. In the 'Destination Address Translation' section, the 'Translation Type' dropdown is set to 'Dynamic IP (with session distribution)'. The 'Translated Address' dropdown is set to 'PANW-Web-Server'. The 'Translated Port' dropdown is set to '[1 - 65535]'. The 'Session Distribution Method' dropdown is set to 'Round Robin'. A callout bubble points to the 'Dynamic IP (with session distribution)' option with the text: 'Set translation type to Dynamic IP.' Another callout bubble points to the 'PANW-Web-Server' entry in the 'Translated Address' dropdown with the text: 'Address PANW-Web-Server'.

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

Pre-NAT addresses

Post-NAT zone

Pre-NAT addresses

Configure Destination NAT

NAT Policy Rule

General | **Original Packet** | Translated Packet

Any
 SOURCE ZONE ▾
 Internet

Destination Zone: Internet

Any
 SOURCE ADDRESS ▾
 198.51.100.22

Destination Interface: any

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]
 Enable DNS Rewrite
Direction: reverse

Match Criteria

Translation

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: 192.168.16.2
Translated Port: 8000

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

Direction: reverse

| 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 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.