Network Address Translation on JunOS

Course Introduction

ine.com

Piotr Kaluzny

CCIE #25665

pkaluzny@ine.com
linkedin.com/in/piotrkaluzny

CCIE Security

Course Prerequisites

+ IP Routing
+ SRX Objects & Policies series

Course Objectives

- Describe NAT
- Understand NAT operations
- Describe & explain the differences between Source, Destination & Static NAT
- Implement NAT & related features

Network Address Translation on JunOS

NAT Overview

ine.com

Module Overview

- What is NAT?
- Types of NAT
- NAT on SRX

What is NAT?

- Network Address Translation (NAT) is a data plane technology used to provide connectivity
  - Main applications
    - Typically to hide private IP addresses (RFC 1918)
    - Sometimes used for traffic redirection or overlapping subnet problems
  - NAT Operations
    - NAT rewrites IP address (and possibly port number) in a packet
      - Source and/or destination

- What NAT is not?
  - A long-term solution to IPv4 address depletion
  - Security tool

NAT Types

- NAT translations can be fixed or dynamic
  - Static NAT
    - Statically maps one IP address to another one (1-1)
      - The mapping is permanent
  - Dynamic
    - Dynamically maps one IP address to another one (1-1)
      - A new source IP address is randomly selected from a pool
      - The mapping will be removed after timeout expires

NAT Types

- Regular NAT functions can be further extended
  - Port-based NAT allows for coverage of more than one device (many-1)
    - Dynamic
      - Port Address Translation (PAT)
        - Dynamically replaces source IP address & source port number
    - Static
      - Port Redirection
        - Statically replaces source IP address & source port number
  - Policy NAT adds more criteria to better control when translations are made
    - Conditional NAT

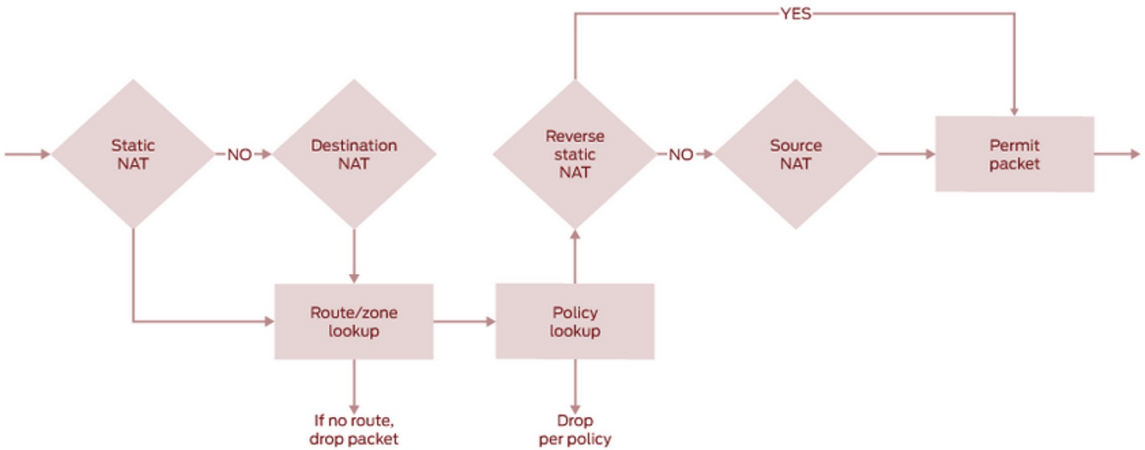
NAT on SRX

- Supported NAT Types (IPv4)
  - Static
  - Source
  - Destination

- IPv6 NAT
  - Static, Source & Destination NAT
    - Similar to IPv4 but for v6 addresses
  - Transition Mechanisms
    - NAT Protocol Translator (NAT-PT), NAT64
  - See documentation
    - User Guides -> Network Address Translation User Guide

NAT on SRX

- NAT Rule Precedence
  - NAT rules are applied in order depending on their type



source: juniper.net

Network Address Translation on JunOS

Static NAT

ine.com

Module Overview

+ Static NAT overview
+ Supported features

How does Static NAT work?

- Statically maps one IP address to another address
  - Source or destination
  - The mapping is permanent
    - No address pools are needed
  - The mapping is bidirectional

- Use Cases
  - Exposing DMZ servers
  - Overlapping subnets

Supported Features

- Subnet Mapping
  - Same-size blocks
- Port Redirection
  - IP address & port mapping

Network Address Translation on JunOS

Source NAT

ine.com

Module Overview

+ Source NAT overview
+ Supported features

How does Source NAT work?

- Dynamically maps a source IP address to another address
  - The mapping is undirectional
  - Requires an address pool
    - Except for translations involving egress interface

- Use Cases
  - Internet connectivity for LAN clients (RFC 1918)
  - Overlapping addresses
  - Routing simplification

Supported Features

- Address Block Mapping
  - Same-size blocks
  - Different-size blocks
- Port Address Translation (PAT)
  - Allows for hiding many addresses behind one
    - Changes source IP address & port number
  - The translated address can belong to the egress interface
    - Interface NAT

Supported Features

- Port Allocation Mode
  - Port Randomization
    - Sequential address, random port number
    - Default setting
  - Round-Robin
    - Sequential address & port number
    - Activated by disabling Port Randomization
      - security nat source port-randomization disable

Supported Features

- Address Sharing (no PAT)
  - Hides different clients behind a single IP address when PAT is not enabled
    - Requires traffic to come from different source ports
  - Enabled with **address-shared**
- Address Pooling (PAT)
  - Ensures all client sessions are mapped to the same IP address
  - Enabled with **address-pooling paired**
- Address Persistence (PAT)
  - Always allocates the same IP address for the same client
  - Enabled with **address-persistent**

Network Address Translation on JunOS

Destination NAT

ine.com

Module Overview

- Destination NAT overview
- Supported features

How does Destination NAT work?

- Dynamically maps a destination IP address to another address
  - The mapping is undirectional
  - Requires an address pool

- Use Cases
  - Traffic redirection
  - Load sharing

Supported Features

- Address Block Mapping
  - Same-size blocks
  - Different-size blocks
- Port Address Translation (PAT)
  - Allows for hiding many addresses behind one
    - Changes destination IP address & port number

Network Address Translation on JunOS

Using Source NAT

ine.com

Module Overview

- Configuration syntax
- Deploying source NAT

Source NAT Configuration

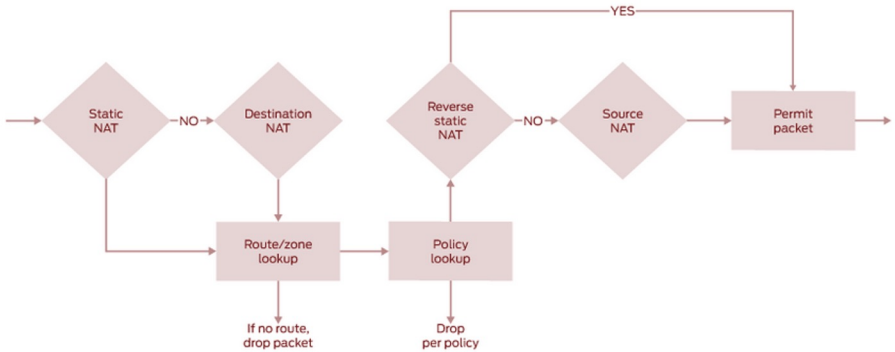
- NAT Pool
  - Pool range
    - security nat source pool address
  - PAT & related options
    - security nat source pool
      - port [no-translation]
      - address-persistent, address-pooling, address-shared
- Proxy ARP / Neighbor Discovery
  - Local subnets only
    - security nat [proxy-arp | proxy-ndp]

Source NAT Configuration

- NAT Rules
  - Context
    - security nat source rule-set [from | to]
      - zone
      - interface
      - routing-instance
  - NAT criteria
    - security nat source rule-set rule
      - match [source-address] [*options*]
      - then source-nat [*options*]

Source NAT Configuration

- Security Policy
  - Refer to the original IP address



- Verification
  - show security nat source [*options*]

Network Address Translation on JunOS

Using Destination NAT

ine.com

Module Overview

- Configuration syntax
- Deploying destination NAT

Destination NAT Configuration

- NAT Pool
  - Pool range
    - security nat destination pool address [port]

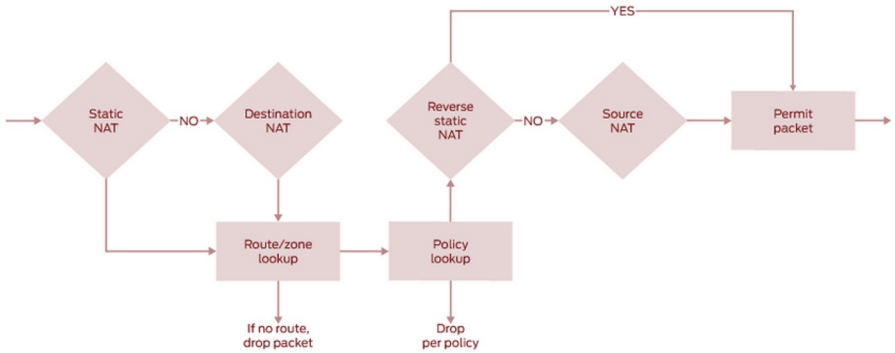
- Proxy ARP / Neighbor Discovery
  - Local subnets only
    - security nat [proxy-arp | proxy-ndp]

Destination NAT Configuration

- NAT Rules
  - Context
    - security nat destination rule-set from
      - zone
      - interface
      - routing-instance
  - NAT criteria
    - security destination rule-set rule
      - match [destination-address] [*options*]
      - then destination-nat [*options*]

Destination NAT Configuration

- Security Policy
  - Refer to the translated IP address



- Verification
  - show security nat destination [*options*]

Network Address Translation on JunOS

Using Static NAT

ine.com

Module Overview

- Configuration syntax
- Deploying static NAT

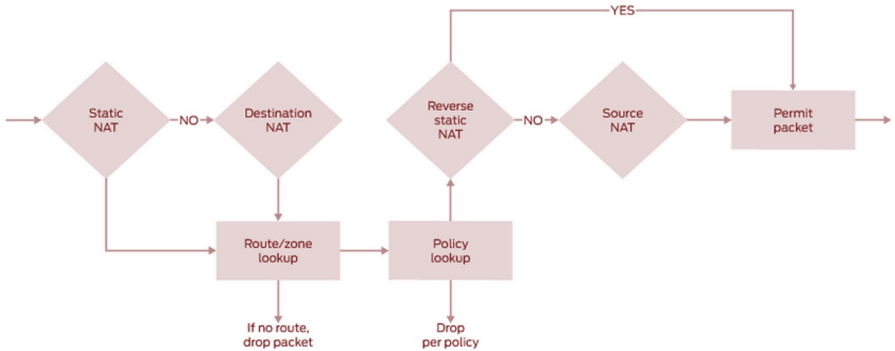
Static NAT Configuration

- NAT Rules
  - Context
    - security nat static rule-set from
      - zone, interface, routing-instance
  - NAT criteria
    - security nat static rule-set rule
      - match [destination-address] [*options*]
      - then static-nat [*options*]

- Proxy ARP / Neighbor Discovery
  - Local subnets only
    - security nat [proxy-arp | proxy-ndp]

Static NAT Configuration

- Security Policy
  - Refer to the translated IP address (destination address)
  - Refer to the original IP address (reverse/source address)



- Verification
  - show security nat static rule [*options*]

Network Address Translation on JunOS

ine.com

Course Conclusion

- NAT is a data plane technology used to provide connectivity
- Static & dynamic NAT are the main types of NAT
- Other NAT flavors include PAT or Policy NAT
- SRX distinguishes between Source, Destination & Static NAT
- SRX supports some advanced NAT features, such as Address Pairing

Thank You