JUNIPER NETWORKS SRX SERIES AND J SERIES NAT FOR ScreenOS USERS

Understanding ScreenOS and Junos OS CLI Differences
# Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>1</td>
</tr>
<tr>
<td>Scope</td>
<td>1</td>
</tr>
<tr>
<td><strong>Design Considerations</strong></td>
<td>1</td>
</tr>
<tr>
<td>Hardware Requirements</td>
<td>1</td>
</tr>
<tr>
<td>Software Requirements</td>
<td>1</td>
</tr>
<tr>
<td><strong>Description and Deployment Scenario</strong></td>
<td>1</td>
</tr>
<tr>
<td>Source NAT</td>
<td>1</td>
</tr>
<tr>
<td>Interface-Based Source NAT</td>
<td>1</td>
</tr>
<tr>
<td>ScreenOS Configuration</td>
<td>1</td>
</tr>
<tr>
<td>Junos OS Configuration</td>
<td>2</td>
</tr>
<tr>
<td>Source NAT with IP Pool (Dynamic Internet Protocol Pool with and without Port Translation)</td>
<td>2</td>
</tr>
<tr>
<td>Source NAT with IP Pool (with Port Translation)</td>
<td>2</td>
</tr>
<tr>
<td>ScreenOS Configuration</td>
<td>2</td>
</tr>
<tr>
<td>Junos OS Configuration</td>
<td>2</td>
</tr>
<tr>
<td>ScreenOS Configuration</td>
<td>2</td>
</tr>
<tr>
<td>Junos OS Configuration</td>
<td>2</td>
</tr>
<tr>
<td>Source NAT with IP Address Shifting</td>
<td>3</td>
</tr>
<tr>
<td>ScreenOS Configuration</td>
<td>3</td>
</tr>
<tr>
<td>Junos OS Configuration</td>
<td>3</td>
</tr>
<tr>
<td>Source NAT with Loopback Group and Dynamic Internet Protocol (DIP)</td>
<td>3</td>
</tr>
<tr>
<td>ScreenOS Configuration</td>
<td>3</td>
</tr>
<tr>
<td>Junos OS Configuration</td>
<td>4</td>
</tr>
<tr>
<td>Static NAT</td>
<td>4</td>
</tr>
<tr>
<td>Static NAT to a Single Host</td>
<td>4</td>
</tr>
<tr>
<td>ScreenOS Configuration</td>
<td>4</td>
</tr>
<tr>
<td>Junos OS Configuration</td>
<td>4</td>
</tr>
<tr>
<td>Static NAT to a Subnet</td>
<td>4</td>
</tr>
<tr>
<td>ScreenOS Configuration</td>
<td>5</td>
</tr>
<tr>
<td>Junos OS Configuration</td>
<td>5</td>
</tr>
<tr>
<td>Virtual IP</td>
<td>5</td>
</tr>
<tr>
<td>ScreenOS Configuration</td>
<td>5</td>
</tr>
<tr>
<td>Junos OS Configuration</td>
<td>5</td>
</tr>
<tr>
<td><strong>Destination NAT</strong></td>
<td>6</td>
</tr>
<tr>
<td>Destination Address Translation to a Single Host</td>
<td>6</td>
</tr>
<tr>
<td>ScreenOS Configuration</td>
<td>6</td>
</tr>
<tr>
<td>Junos OS Configuration Commands</td>
<td>6</td>
</tr>
<tr>
<td>Destination Address and Port Translation to a Single Host</td>
<td>6</td>
</tr>
<tr>
<td>ScreenOS Configuration</td>
<td>7</td>
</tr>
<tr>
<td>Junos OS Configuration</td>
<td>7</td>
</tr>
</tbody>
</table>
Table of Figures

Figure 1: Source NAT ................................................................. 1
Figure 2: Source NAT with loopback group and DIP ......................... 3
Figure 3: Static NAT .................................................................. 4
Figure 4: Virtual IP (VIP) ............................................................ 5
Figure 5: Destination NAT ........................................................... 6

Destination Address Translation to a Single Host ............................... 7
ScreenOS Configuration .............................................................. 7
Junos OS Configuration ............................................................... 7
Summary ................................................................................. 8
About Juniper Networks .............................................................. 8
Introduction

Juniper Networks® SRX Series Services Gateways and J Series Services Routers use the Juniper Networks Junos® operating system command-line interface (CLI), which is unfamiliar to many current ScreenOS® users. Because of the extensive Junos OS feature set, the command sequence required to configure NAT is often slightly longer than the ScreenOS equivalent. The following CLI examples provide a starting point for ScreenOS users planning to migrate to Junos OS.

Scope

The purpose of this application note is to compare several common ScreenOS Network Address Translation (NAT) CLI command sequences with the Junos OS equivalents. This paper does not provide an overview of Junos OS next-generation NAT architecture. For more information on Junos OS NAT for Juniper Networks SRX Series Services Gateways and J Series Services Routers, please refer to the “SRX Series and J Series Network Address Translation” application note.

This paper assumes the reader is familiar with NAT, ScreenOS, and the various NAT options available in ScreenOS.

Design Considerations

Hardware Requirements

- Juniper Networks J2320, J2350, J4350, and J6350 Services Routers
- Juniper Networks SRX Series Services Gateways

Software Requirements

- Junos OS release 9.2 or later for all SRX Series Services Gateways (A more recent release will be required for all SRX Series Services Gateways released after 9.2)
- Junos OS release 9.5 or later for all Juniper Networks J Series Services Routers

Description and Deployment Scenario

By allowing a private network to connect to the Internet, configuring NAT is often the first step required to deploy an SRX Services Gateway or J Series Services Router. After reviewing the following command sequences, readers should be able to configure several common NAT variations.

The commands sequences provided can be copied exactly, but the IP addresses used are examples only and will need to be changed as appropriate to meet deployment specific addressing requirements.

Source NAT

![Source NAT Diagram]

**Interface-Based Source NAT**

<table>
<thead>
<tr>
<th>INTERFACE</th>
<th>ZONE</th>
<th>IP ADDRESS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ethernet 0/0</td>
<td>untrust</td>
<td>1.1.1.1/24</td>
</tr>
<tr>
<td>Ethernet 0/1</td>
<td>trust</td>
<td>10.1.1.1/24</td>
</tr>
</tbody>
</table>

**ScreenOS Configuration**

```
set policy id 1 from trust to untrust any any any nat src permit
```
**APPLICATION NOTE** - Juniper Networks SRX Series and J Series NAT for ScreenOS Users

**Junos OS Configuration**

- set security nat source rule-set interface-nat from zone trust
- set security nat source rule-set interface-nat to zone untrust
- set security nat source rule-set interface-nat rule rule1 match source-address 0.0.0.0/0 destination-address 0.0.0.0/0
- set security nat source rule-set interface-nat rule rule1 then source-nat interface
- set security policies from-zone trust to-zone untrust policy permit-all match source-address any destination-address any application any
- set security policies from-zone trust to-zone untrust policy permit-all then permit

**Source NAT with IP Pool (Dynamic Internet Protocol Pool with and without Port Translation)**

<table>
<thead>
<tr>
<th>INTERFACE</th>
<th>ZONE</th>
<th>IP ADDRESS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ethernet 0/0</td>
<td>untrust</td>
<td>1.1.1.1/24</td>
</tr>
<tr>
<td>Ethernet 0/1</td>
<td>trust</td>
<td>10.1.1.1/24</td>
</tr>
</tbody>
</table>

**ScreenOS Configuration (with Port Translation)**

- set int e0/0 dip 4 1.1.1.10 1.1.1.15
- set policy id 1 from trust to untrust any any any nat src dip-id 4 permit

**Junos OS Configuration (with Port Translation)**

- set security nat source pool pool-1 address 1.1.1.10 to 1.1.1.15
- set security nat source rule-set pool-nat from zone trust
- set security nat source rule-set pool-nat to zone untrust
- set security nat source rule-set pool-nat rule rule1 match source-address 0.0.0.0/0 destination-address 0.0.0.0/0
- set security nat source rule-set pool-nat rule rule1 then source-nat pool pool-1
- set security nat proxy-arp interface ge-0/0/0 address 1.1.1.10 to 1.1.1.15
- set security policies from-zone trust to-zone untrust policy permit-all match source-address any destination-address any application any
- set security policies from-zone trust to-zone untrust policy permit-all then permit

**Note:** The above command sequence can be changed to create a source pool without port translation.

**ScreenOS Configuration (without Port Translation)**

- set int e0/0 dip 4 1.1.1.10 1.1.1.15 fix-port

**Junos OS Configuration (without Port Translation)**

- set security nat source pool pool-1 address 1.1.1.10 to 1.1.1.15
- set security nat source pool pool-1 port no-translation
- set security nat source rule-set pool-nat from zone trust
- set security nat source rule-set pool-nat to zone untrust
- set security nat source rule-set pool-nat rule rule1 match source-address 0.0.0.0/0 destination-address 0.0.0.0/0
- set security nat source rule-set pool-nat rule rule1 then source-nat pool pool-1
- set security policies from-zone trust to-zone untrust policy permit-all match source-address any destination-address any application any
- set security policies from-zone trust to-zone untrust policy permit-all then permit
Source NAT with IP Address Shifting

<table>
<thead>
<tr>
<th>INTERFACE</th>
<th>ZONE</th>
<th>IP ADDRESS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ethernet 0/0</td>
<td>untrust</td>
<td>1.1.1.1/24</td>
</tr>
<tr>
<td>Ethernet 0/1</td>
<td>trust</td>
<td>10.1.1.1/24</td>
</tr>
</tbody>
</table>

**ScreenOS Configuration**

set int e0/0 dip 4 shift-from 10.1.1.100 to 1.1.1.100 1.1.1.109

**Junos OS Configuration**

set security nat source pool pool-1 address 1.1.1.100 to 1.1.1.109
set security nat source pool pool-1 host-address-base 10.1.1.100
set security nat source rule-set pool-nat from zone trust
set security nat source rule-set pool-nat to zone untrust
set security nat source rule-set pool-nat rule rule1 match source-address 0.0.0.0/0
destination-address 0.0.0.0/0
set security nat source rule-set pool-nat rule rule1 then source-nat pool pool-1
set security policies from-zone trust to-zone untrust policy permit-all match source-address
set security nat proxy-arp interface ge-0/0/0 address 1.1.1.100 to 1.1.1.109
any destination-address any application any
set security policies from-zone trust to-zone untrust policy permit-all then permit

Source NAT with Loopback Group and Dynamic Internet Protocol (DIP)

<table>
<thead>
<tr>
<th>INTERFACE</th>
<th>ZONE</th>
<th>IP ADDRESS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ethernet 0/0</td>
<td>untrust</td>
<td>1.1.1.1/24</td>
</tr>
<tr>
<td>Ethernet 0/1</td>
<td>trust</td>
<td>10.1.1.1/24</td>
</tr>
<tr>
<td>Loopback.1</td>
<td>untrust</td>
<td>1.1.1.1/24</td>
</tr>
<tr>
<td>Ethernet 0/1</td>
<td>trust</td>
<td>10.1.1.1/24</td>
</tr>
</tbody>
</table>

**ScreenOS Configuration**

set int e0/0 loopback-group lo.1
set int e0/2 loopback-group lo.1
set int loopback.1 dip 4 1.1.1.10 1.1.1.15
set policy id 1 from trust to untrust any any any nat src dip-id 4 permit

Figure 2: Source NAT with loopback group and DIP
**Junos OS Configuration**

```
set security nat source pool pool-1 address 1.1.1.10 to 1.1.1.15
set security nat source rule-set pool-nat from zone trust
set security nat source rule-set pool-nat to interface ge-0/0/0 interface ge-0/0/2
set security nat source rule-set pool-nat rule rule1 match source-address 0.0.0.0/0
set security nat source rule-set pool-nat rule rule1 then source-nat pool pool-1
set security nat proxy-arp interface ge-0/0/0 address 1.1.1.10 to 1.1.1.15
set security nat proxy-arp interface ge-0/0/2 address 1.1.1.10 to 1.1.1.15
set security policies from-zone trust to-zone untrust policy permit-all match source-address
any destination-address any application any
set security policies from-zone trust to-zone untrust policy permit-all then permit
```

**Static NAT**

![Static NAT Diagram](image)

**Figure 3: Static NAT**

In ScreenOS, the interface IP address can be used for static NAT (mobile IP). This option is not currently available in Junos OS.

**Static NAT to a Single Host**

<table>
<thead>
<tr>
<th>MAPPED IP</th>
<th>HOST IP ADDRESS</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1.1.100</td>
<td>10.1.1.100</td>
</tr>
</tbody>
</table>

**ScreenOS Configuration**

```
set int e0/0 mip 1.1.1.100 host 10.1.1.100
set pol from untrust to trust any mip(1.1.1.100) http permit
```

**Junos OS Configuration**

```
set security nat proxy-arp interface ge-0/0/0 address 1.1.1.100/32
set security nat static rule-set static-nat from zone untrust
set security nat static rule-set static-nat rule rule1 match destination-address 1.1.1.100
set security nat static rule-set static-nat rule rule1 then static-nat prefix 10.1.1.100
set security zones security-zone trust address-book address webserver 10.1.1.100
set security policies from-zone untrust to-zone trust policy static-nat match source-address
any destination-address webserver application junos-http
set security policies from-zone untrust to-zone trust policy static-nat then permit
```

**Static NAT to a Subnet**

<table>
<thead>
<tr>
<th>MAPPED IP</th>
<th>HOST IP ADDRESS</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1.1.0/28</td>
<td>10.1.1.0/28</td>
</tr>
</tbody>
</table>
ScreenOS Configuration

set int e0/0 mip 1.1.1.0 host 10.1.1.0 netmask 255.255.255.240
set policy from untrust to trust any mip(1.1.1.0/28) http permit

Junos OS Configuration

set security zones security-zone trust address-book address webserver-group 10.1.1.0/28
set security nat proxy-arp interface ge-0/0/0 address 1.1.1.0/28
set security nat static rule-set static-nat from zone untrust
set security nat static rule-set static-set rule rule1 match destination-address 1.1.1.0/28
set security policies from-zone untrust to-zone trust policy static-nat match source-address
any destination-address webserver-group application junos-http
set security policies from-zone untrust to-zone trust policy static-nat then permit

Virtual IP

<table>
<thead>
<tr>
<th>VIRTUAL IP/PORT</th>
<th>SERVICE</th>
<th>HOST IP ADDRESS</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1.1.100/80</td>
<td>HTTP</td>
<td>10.1.1.100</td>
</tr>
<tr>
<td>1.1.1.100/110</td>
<td>POP3</td>
<td>10.1.1.200</td>
</tr>
</tbody>
</table>

ScreenOS Configuration

set int e0/0 vip 1.1.1.100 80 http 10.1.1.100
set int e0/0 vip 1.1.1.100 110 pop3 10.1.1.200
set policy from untrust to trust any vip(1.1.1.100) http permit

Junos OS Configuration

set security nat proxy-arp interface ge-0/0/0.0 address 1.1.1.100
set security nat destination pool dnat-pool-1 address 10.1.1.100/32
set security nat destination pool dnat-pool-2 address 10.1.1.200/32
set security nat destination rule-set dst-nat from zone untrust
set security nat destination rule-set dst-nat rule rule1 match destination-address 1.1.1.100/32
set security nat destination rule-set dst-nat rule rule1 match destination-port 80
set security nat destination rule-set dst-nat rule rule1 then destination-nat pool dnat-pool-1
set security nat destination rule-set dst-nat rule rule2 match destination-address 1.1.1.100/32
set security nat destination rule-set dst-nat rule rule2 match destination-port 110
set security nat destination rule-set dst-nat rule rule2 then destination-nat pool dnat-pool-2
set security zones security-zone trust address-book address webserver 10.1.1.100
set security zones security-zone trust address-book address mailserver 10.1.1.200
set security zones security-zone trust address-book address-set servergroup address webserver
set security zones security-zone trust address-book address-set servergroup address mailserver
set security policies from-zone untrust to-zone trust policy static-nat match source-address any
destination-address servergroup application junos-http
set security policies from-zone untrust to-zone trust policy static-nat match application
junos-pop3
set security policies from-zone untrust to-zone trust policy static-nat then permit

---

**Destination NAT**

![Diagram](image)

**Figure 5: Destination NAT**

**Destination Address Translation to a Single Host**

In this example, the destination IP and the interface IP are on different subnets.

<table>
<thead>
<tr>
<th>DESTINATION IP</th>
<th>REAL DESTINATION IP</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.1.1.100</td>
<td>10.1.1.100</td>
</tr>
</tbody>
</table>

**ScreenOS Configuration**

```bash
set route 2.1.1.100/32 int e0/1
set address trust webserver 2.1.1.100/32
set pol from untrust to trust any webserver http nat dst ip 10.1.1.100 permit
```

**Junos OS Configuration Commands**

```bash
set security nat proxy-arp interface ge-0/0/0.0 address 2.1.1.100
set security nat destination pool dnat-pool-1 address 10.1.1.100
set security nat destination rule-set dst-nat from zone untrust
set security nat destination rule-set dst-nat rule r1 match destination-address 2.1.1.100
set security nat destination rule-set dst-nat rule r1 then destination-nat pool dnat-pool-1
set security zones security-zone trust address-book address webserver 10.1.1.100
set security policies from-zone untrust to-zone trust policy dst-nat match source-address any
destination-address webserver application junos-http
set security policies from-zone untrust to-zone trust policy dst-nat then permit
```

**Destination Address and Port Translation to a Single Host**

<table>
<thead>
<tr>
<th>DESTINATION IP/PORT</th>
<th>REAL DESTINATION IP/PORT</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.1.1.100/80</td>
<td>10.1.1.100/8000</td>
</tr>
</tbody>
</table>

---
APPLICATION NOTE - Juniper Networks SRX Series and J Series NAT for ScreenOS Users

ScreenOS Configuration

set route 2.1.1.100/32 int e0/1
set address trust webserver 2.1.1.100/32
set policy from untrust to trust any webserver http nat dst ip 10.1.1.100 port 8000 permit

Junos OS Configuration

set security nat proxy-arp interface ge-0/0/0.0 address 2.1.1.100
set security nat destination pool dnat-pool-1 address 10.1.1.100 port 8000
set security nat destination rule-set dst-nat from zone untrust
set security nat destination rule-set dst-nat rule r1 match destination-address 2.1.1.100
set security nat destination rule-set dst-nat rule r1 then destination-nat pool dnat-pool-1
set security zones security-zone trust address-book address webserver 10.1.1.100
set applications application http-8000 protocol tcp destination-port 8000
set security policies from-zone untrust to-zone trust policy dst-nat match source-address any
destination-address webserver application http-8000
set security policies from-zone untrust to-zone trust policy dst-nat then permit

Destination Address Translation to a Single Host
In this example, the destination IP and the interface IP are on the same subnet.

<table>
<thead>
<tr>
<th>DESTINATION IP</th>
<th>REAL DESTINATION IP</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1.1.100</td>
<td>10.1.1.100</td>
</tr>
</tbody>
</table>

ScreenOS Configuration

set arp nat
set address trust webserver 1.1.1.100/32
set pol from untrust to trust any webserver http nat dst ip 10.1.1.100 permit

Junos OS Configuration

set security nat destination pool dnat-pool-1 address 10.1.1.100/32
set security nat proxy-arp interface ge-0/0/0.0 address 1.1.1.100
set security nat destination rule-set dst-nat from zone untrust
set security nat destination rule-set dst-nat rule r1 match destination-address 1.1.1.100
set security nat destination rule-set dst-nat rule r1 then destination-nat pool dnat-pool-1
set security policies from-zone untrust to-zone trust policy dst-nat match source-address any
destination-address any application junos-http
set security policies from-zone untrust to-zone trust policy dst-nat then permit
Summary

Juniper Networks SRX Series Services Gateways and J Series Services Routers use the Junos OS command-line interface, which may seem somewhat foreign to current ScreenOS users. The preceding CLI comparisons can be used by ScreenOS users to better understand the Junos OS equivalents. After working through all the examples, the reader should be able to easily configure NAT for several common deployment scenarios.

About Juniper Networks

Juniper Networks, Inc. is the leader in high-performance networking. Juniper offers a high-performance network infrastructure that creates a responsive and trusted environment for accelerating the deployment of services and applications over a single network. This fuels high-performance businesses. Additional information can be found at www.juniper.net.