APPLICATION NOTE

JUNIPER NETWORKS SRX SERIES AND J SERIES NAT FOR ScreenOS USERS

Understanding ScreenOS and JUNOS Software CLI Differences

Copyright © 2009, Juniper Networks, Inc.

Table of Contents

Introduction . . . 1
Scope. . . . 1
Design Considerations . . . 1
Hardware Requirements . . . 1
Software Requirements . . . 1
Description and Deployment Scenario . . . 1
Source NAT . . . 1
Interface-Based Source NAT . . . 1
ScreenOS Configuration . . . 1
JUNOS Configuration . . . 2
Source NAT with IP Pool (Dynamic Internet Protocol Pool with and without Port Translation) . . . 2
ScreenOS Configuration (with Port Translation) . . . 2
JUNOS Configuration (with Port Translation) . . . 2
ScreenOS Configuration (without Port Translation) . . . 2
JUNOS Configuration (without Port Translation) . . . 2
Source NAT with IP Address Shifting . . . 3
ScreenOS Configuration . . . 3
JUNOS Configuration . . . 3
Source NAT with Loopback Group and Dynamic Internet Protocol (DIP) . . . 3
ScreenOS Configuration . . . 3
JUNOS Configuration . . . 4
Static NAT . . . 4
Static NAT to a Single Host. . . . 4
ScreenOS Configuration . . . 4
JUNOS Configuration . . . 4
Static NAT to a Subnet . . . 4
ScreenOS Configuration . . . 5
JUNOS Configuration . . . 5
Virtual IP. . . . 5
ScreenOS Configuration . . . 5
JUNOS Configuration . . . 5
Destination NAT . . . 6
Destination Address Translation to a Single Host . . . 6
ScreenOS Configuration . . . 6
JUNOS Configuration Commands . . . 6
Destination Address and Port Translation to a Single Host . . . 6
ScreenOS Configuration . . . 7
JUNOS Configuration . . . 7

Copyright © 2009, Juniper Networks, Inc.

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

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

Copyright © 2009, Juniper Networks, Inc.

Introduction

Juniper Networks® SRX Series Services Gateways and J Series Services Routers use the Juniper Networks JUNOS® Software command-line interface (CLI), which is unfamiliar to many current ScreenOS® users. Because of the extensive JUNOS 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.

Scope

The purpose of this application note is to compare several common ScreenOS Network Address Translation (NAT) CLI command sequences with the JUNOS Software equivalents. This paper does not provide an overview of JUNOS next-generation NAT architecture. For more information on JUNOS 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 Software 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 Software 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



Figure 1: Source NAT

Interface-Based Source NAT

INTERFACE	ZONE	IP ADDRESS
Ethernet 0/0	untrust	1.1.1.1/24
Ethernet 0/1	trust	10.1.1.1/24

ScreenOS Configuration

```
set policy id 1 from trust to untrust any any any nat src permit
```

Copyright © 2009, Juniper Networks, Inc.

JUNOS 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)

INTERFACE	ZONE	IP ADDRESS
Ethernet 0/0	untrust	1.1.1.1/24
Ethernet 0/1	trust	10.1.1.1/24

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 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 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
set security nat proxy-arp interface ge-0/0/0 address 1.1.1.10 to 1.1.1.15
any destination-address any application any
set security policies from-zone trust to-zone untrust policy permit-all then permit
```


Copyright © 2009, Juniper Networks, Inc.

Source NAT with IP Address Shifting

INTERFACE	ZONE	IP ADDRESS
Ethernet 0/0	untrust	1.1.1.1/24
Ethernet 0/1	trust	10.1.1.1/24

ScreenOS Configuration

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

JUNOS 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)

INTERFACE	ZONE	IP ADDRESS
Ethernet 0/0	untrust	
Ethernet 0/1	trust	
Loopback.1	untrust	1.1.1.1/24
Ethernet 0/1	trust	10.1.1.1/24



Figure 2: Source NAT with loopback group and DIP

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
```

Copyright © 2009, Juniper Networks, Inc.

JUNOS 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
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 1.1.1.10 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
any destination-address any application any
set security policies from-zone trust to-zone untrust policy permit-all then permit
```

Static NAT



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 Software.

Static NAT to a Single Host

MAPPED IP	HOST IP ADDRESS
1.1.1.100	10.1.1.100

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 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

MAPPED IP	HOST IP ADDRESS
1.1.1.0/28	10.1.1.0/28

Copyright © 2009, Juniper Networks, Inc.

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 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 nat static rule-set static-set rule rule1 then static-nat prefix 10.1.1.0/28
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

VIRTUAL IP/PORT	SERVICE	HOST IP ADDRESS
1.1.1.100/80	HTTP	10.1.1.100
1.1.1.100/110	POP3	10.1.1.200



Figure 4: Virtual IP (VIP)

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 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
```

Copyright © 2009, Juniper Networks, Inc.

```
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



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.

DESTINATION IP	REAL DESTINATION IP
2.1.1.100	10.1.1.100

ScreenOS Configuration

```
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 Configuration Commands

```
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

DESTINATION IP/PORT	REAL DESTINATION IP/PORT
2.1.1.100/80	10.1.1.100/8000

Copyright © 2009, Juniper Networks, Inc.

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 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.

DESTINATION IP	REAL DESTINATION IP
1.1.1.100	10.1.1.100

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 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
```

Copyright © 2009, Juniper Networks, Inc.

Summary

Juniper Networks SRX Series Services Gateways and J Series Services Routers use the JUNOS command-line interface, which may seem somewhat foreign to current ScreenOS users. The preceding CLI comparisons can be used by ScreenOS users to better under understand the JUNOS 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**.

Corporate and Sales Headquarters
Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089 USA
Phone: 888.JUNIPER
(888.586.4737)
or 408.745.2000
Fax: 408.745.2100

APAC Headquarters
Juniper Networks (Hong Kong)
26/F, Cityplaza One
1111 King's Road
Taikoo Shing, Hong Kong
Phone: 852.2332.3636
Fax: 852.2574.7803

EMEA Headquarters
Juniper Networks Ireland
Airside Business Park
Swords, County Dublin,
Ireland
Phone: 35.31.8903.600
Fax: 35.31.8903.601

To purchase Juniper Networks solutions, please contact your Juniper Networks representative at **1-866-298-6428** or authorized reseller.

Copyright 2009 Juniper Networks, Inc.
All rights reserved. Juniper Networks, the Juniper Networks logo, JUNOS, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. JUNOSe is a trademark of Juniper Networks, Inc. All other trademarks, service marks, registered marks, or registered service marks are the property of their respective owners. Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

3500152-002-EN June 2009

Printed on recycled paper.