Application Note:

Junos NAT Configuration Examples

January 2010

Table of Contents

Introduction

This document explains configuring Network Address Translation (NAT) on J series and SRX services gateway device for use in common network scenarios. The document assumes the reader is familiar with NAT concepts and terminology used on Juniper devices.

The examples in this document are supplemental to the examples that are included in the following application notes:

TN8 - Configuring Network Address Translation (NAT)

TN25 - Configuring Network Address Translation (NAT) on SRX and J Series devices [for ScreenOS Users]

Requirements

Hardware

- Juniper Networks J2320, J2350, J4350, and J6350 routers
- SRX series services gateways

Software

- Junos release 9.5 and later

Configuration Examples

Based on requests from the field, this application note contains CLI examples for Source NAT, Destination NAT, Double NAT (Source and Destination NAT), and Static NAT.

Source NAT

Configure Address Pools for Source NAT

This section illustrates the configuration to create different types of source NAT pools. The pools created in these examples will be used in the NAT rules of subsequent configuration examples. The entire configuration is performed under the “security nat source” hierarchy of the Junos CLI. By default, all the source IP pools will have PAT enabled. Source pools without PAT can be configured by disabling PAT on the IP pool. The IP pools are not bound to interface. Proxy ARP must be configured for the device to respond to ARP for the addresses in the IP pool.

1. Configure a source pool with a range of addresses and port translation:

```
set pool src-nat-pool-1 address 192.0.0.1 to 192.0.0.24
```

2. Configure a source pool with a range of addresses and port translation disabled:

```
set pool src-nat-pool-2 address 192.0.0.100 to 192.0.0.249
set pool src-nat-pool-2 port no-translation
```

3. Configure a source pool with a range of addresses with port translation disabled using overflow pool . Overflow pools are used as a fallback in the event that source pool without PAT runs out of free IP addresses. Overflow pools can be source IP pools with PAT or interface:

```
set pool src-nat-pool-2 address 192.0.0.100 to 192.0.0.249
set pool src-nat-pool-2 port no-translation
set pool src-nat-pool-2 overflow-pool interface
```

4. Configure a source pool with a single address and port translation:

```
set pool src-nat-pool-3 address 192.0.0.25/32
```

5. Configure a source pool with a range for both IP address and port numbers:

```
set pool src-nat-pool-4 address 192.0.0.50 to 192.0.0.59
set pool src-nat-pool-4 port range 5000 to 6000
```

Configure Source NAT using interface IP

In this example, all traffic from the trust zone to the untrust zone is translated to the egress interface, ge-0/0/2 interface IP address.

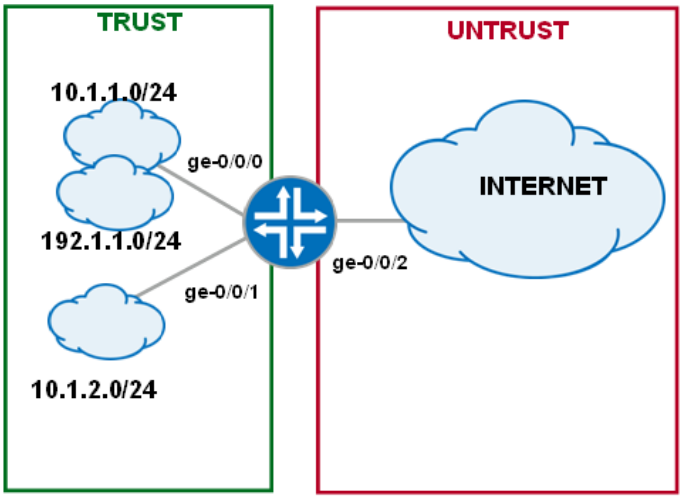


Fig1: source NAT using interface IP

```
[edit security nat source]
set rule-set rs1 from zone trust
set rule-set rs1 to zone untrust
set rule-set rs1 rule r1 match source-address 0.0.0.0/0
set rule-set rs1 rule r1 match destination-address 0.0.0.0/0
set rule-set rs1 rule r1 then source-nat interface
```

```
[edit security policies from-zone trust to-zone untrust]
set policy internet-access match source-address any destination-address any application
any
set policy internet-access then permit
```

Configure Source NAT using IP pool

In this example, all traffic from the trust zone to the untrust zone is translated to the source IP pool “src-nat-pool-1”. (The source IP pool is defined on page 4.)

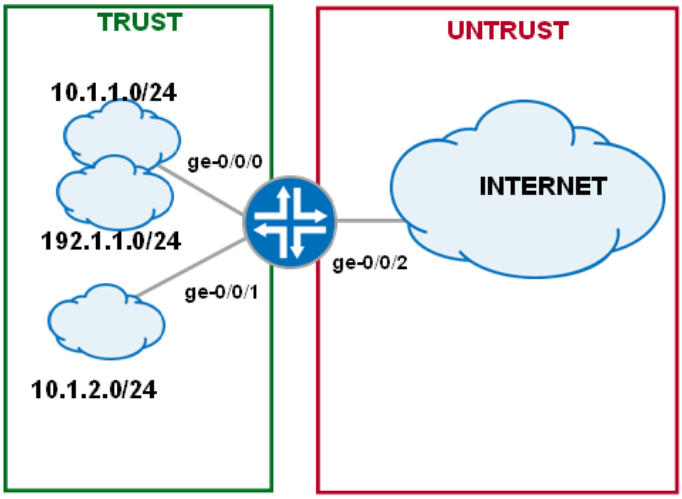


Fig2: Source NAT using IP pool

```
[edit security nat source]
set rule-set rs1 from zone trust
set rule-set rs1 to zone untrust
set rule-set rs1 rule r1 match source-address 0.0.0.0/0
set rule-set rs1 rule r1 match destination-address 0.0.0.0/0
set rule-set rs1 rule r1 then source-nat src-nat-pool-1

[edit security nat]
set proxy-arp interface ge-0/0/2.0 address 192.0.0.1 to 192.0.0.24

[edit security policies from-zone trust to-zone untrust]
set policy internet-access match source-address any destination-address any application
any
set policy internet-access then permit
```

Configure Source NAT using Multiple Rules

This example has the following requirements:

1. Traffic from the subnet 10.1.1.0/24 and 10.1.2.0/24 is translated to pool src-nat-pool-1.
2. Traffic from subnet 192.168.1.0/24 is translated to pool src-nat-pool-2.
3. Traffic from the host 192.168.1.250/24 is exempted from source NAT.

(The source IP pools are defined on page 4.)

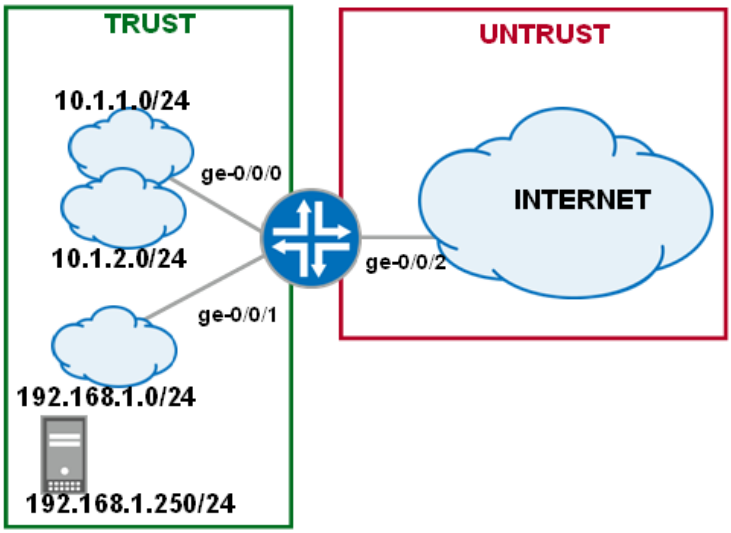


Fig 3: Source NAT using multiple rules

```
[edit security nat source]
set rule-set rs1 from zone trust
set rule-set rs1 to zone untrust

set rule-set rs1 rule r1 match source-address [10.1.1.0/24 10.1.2.0/24]
set rule-set rs1 rule r1 match destination-address 0.0.0.0/0
set rule-set rs1 rule r1 then source-nat pool src-nat-pool-1

set rule-set rs1 rule r2 match source-address 192.168.1.250/24
set rule-set rs1 rule r2 match destination-address 0.0.0.0/0
set rule-set rs1 rule r2 then source-nat off

set rule-set rs1 rule r3 match source-address 192.168.1.0/24
set rule-set rs1 rule r3 match destination-address 0.0.0.0/0
set rule-set rs1 rule r3 then source-nat pool src-nat-pool-2

[edit security nat]
set proxy-arp interface ge-0/0/2.0 address 192.0.0.1 to 192.0.0.24
set proxy-arp interface ge-0/0/2.0 address 192.0.0.100 to 192.0.0.249

[edit security policies from-zone trust to-zone untrust]
set policy internet-access match source-address any destination-address any application
any
set policy internet-access then permit
```

Destination NAT

Many to many translation

This example has the following requirements:

1. Traffic to destination 1.1.1.100 is translated to 192.168.1.100
2. Traffic to destination 1.1.1.101 on port 80 is translated to 192.168.1.200 and port 8000

The real IP address and port numbers of the hosts are configured as the destination IP pool. Proxy ARP must be configured for the device to respond to ARP for the addresses in the IP pool.

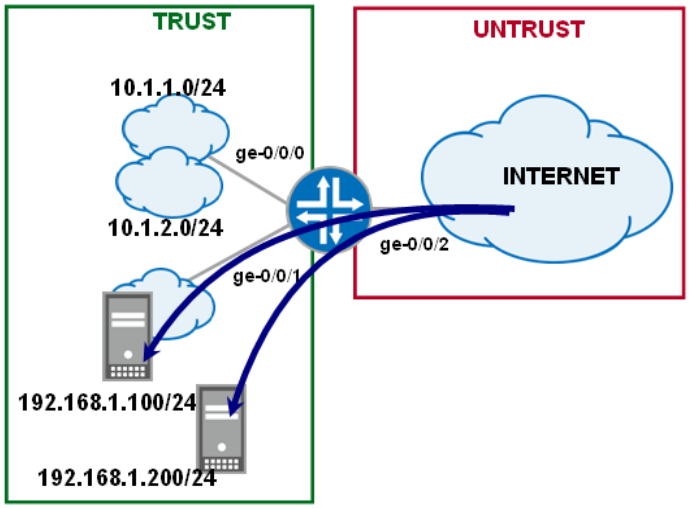


Fig 4: Destination NAT – Many to Many

Security policies to permit traffic from untrust zone to trust zone must be created. Since the destination NAT rule-sets are evaluated before a security policy, the addresses referred in the security policy must be the real IP address of the end host.

```
[edit security]
set zones security-zone trust address-book address server-1 192.168.1.100/32
set zones security-zone trust address-book address server-2 192.168.1.200/32

[edit security policies from-zone untrust to-zone trust]
set policy server-access match source-address any destination-address [server-1 server-2]
application any
set policy server-access then permit

[edit security nat destination]
set pool dst-nat-pool-1 address 192.168.1.100
set pool dst-nat-pool-2 address 192.168.1.200 port 8000

set rule-set rs1 from zone untrust
set rule-set rs1 rule r1 match destination-address 1.1.1.100
set rule-set rs1 rule r1 then destination-nat pool dst-nat-pool-1

set rule-set rs1 rule r2 match destination-address 1.1.1.101
set rule-set rs1 rule r2 match destination-port 80
set rule-set rs1 rule r2 then destination-nat pool dst-nat-pool-2
```

```
[edit security nat]
set proxy-arp interface ge-0/0/2.0 address 1.1.1.100 to 1.1.1.101
```

One to many translation

This example has the following requirements:

1. Traffic to destination 1.1.1.100 on port 80 is translated to 192.168.1.100 and port 80.
2. Traffic to destination 1.1.1.100 on port 8000 is translated to 192.168.1.200 and port 8000.

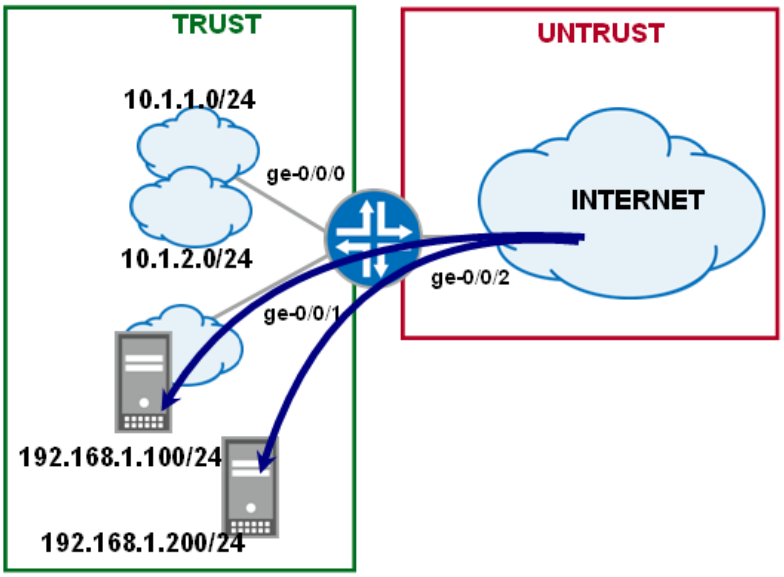


Fig 5: Destination NAT – One to many

```
[edit security nat destination]
set pool dst-nat-pool-1 address 192.168.1.100 port 80
set pool dst-nat-pool-2 address 192.168.1.200 port 8000

set rule-set rs1 from zone untrust
set rule-set rs1 rule r1 match destination-address 1.1.1.100
set rule-set rs1 rule r1 match destination-port 80
set rule-set rs1 rule r1 then destination-nat pool dst-nat-pool-1

set rule-set rs1 rule r2 match destination-address 1.1.1.100
set rule-set rs1 rule r2 match destination-port 8000
set rule-set rs1 rule r2 then destination-nat pool dst-nat-pool-2
[edit security nat]
set proxy-arp interface ge-0/0/2.0 address 1.1.1.100

[edit security]
set zones security-zone trust address-book address server-1 192.168.1.100/32
set zones security-zone trust address-book address server-2 192.168.1.200/32
```

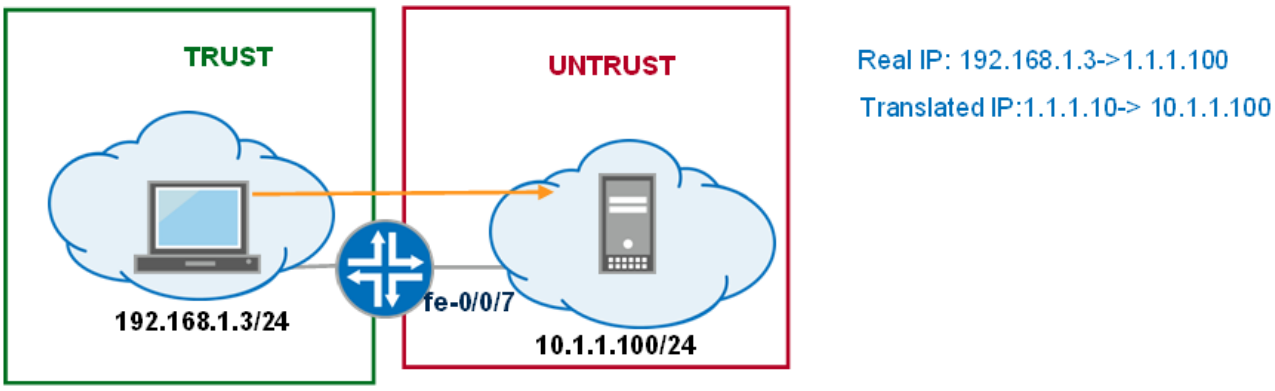
```
[edit security policies from-zone untrust to-zone trust]
set policy server-access match source-address any destination-address [server-1 server-2]
application any
set policy server-access then permit

[edit security]
set zones security-zone trust address-book address server-1 192.168.1.100/32
set zones security-zone trust address-book address server-2 192.168.1.200/32

[edit security policies from-zone untrust to-zone trust]
set policy server-access match source-address any destination-address [server-1 server-2]
application any
set policy server-access then permit
```

Double NAT

Source and destination translation

In this example, the source and destination IP address of the packet is translated. The destination host 10.1.1.100 is accessed by the source 192.168.1.3 using the IP address 1.1.1.100. As the packet traverses the SRX device, both the source and destination IP addresses are translated.

(The source IP pools are defined on page 4.)




```
[edit security nat source]
set pool src-nat-pool-1 address 1.1.1.10 to 1.1.1.14

set rule-set rs1 from zone trust
set rule-set rs1 to zone untrust
set rule-set rs1 rule r1 match source-address 0.0.0.0/0
set rule-set rs1 rule r1 match destination-address 0.0.0.0/0
set rule-set rs1 rule r1 then source-nat src-nat-pool-1

[edit security nat destination]
set pool dst-nat-pool-1 address 10.1.1.100

set rule-set rs1 from zone trust
set rule-set rs1 rule r1 match destination-address 1.1.1.100
set rule-set rs1 rule r1 then destination-nat pool dst-nat-pool-1

[edit security nat]
set proxy-arp interface fe-0/0/7.0 address 1.1.1.10 to 1.1.1.14

[edit security policies from-zone trust to-zone untrust]
set policy permit-all match source-address any destination-address any application any
set policy permit-all then permit
```

The security policy above allows all outbound access from trust zone to untrust zone. As a result the server can be accessed either by its translated or untranslated address.

The session table shown below confirms this:

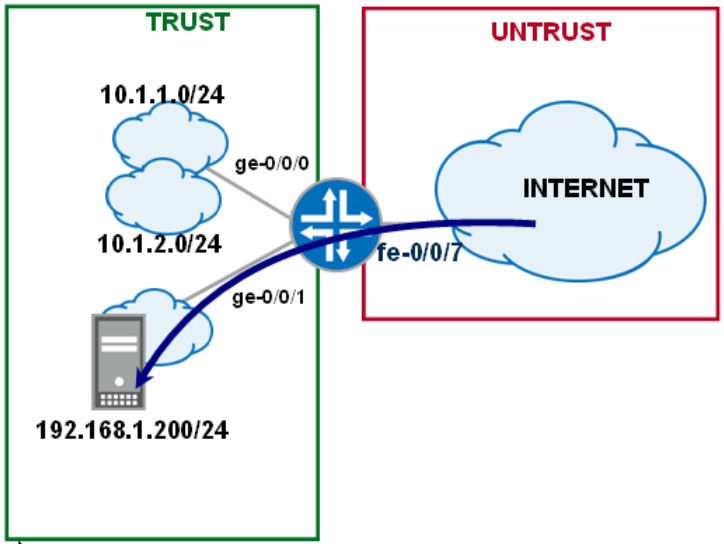
```
[edit]
root# run show security flow session source-prefix 192.168.1.3
Session ID: 60261, Policy name: permit-all/4, Timeout: 1778
  In: 192.168.1.3/48919 --> 1.1.1.100/23;tcp, If: ge-0/0/0.0
  Out: 10.1.1.100/23 --> 1.1.1.10/1046;tcp, If: fe-0/0/7.0

Session ID: 60434, Policy name: permit-all/4, Timeout: 1774
  In: 192.168.1.3/48924 --> 10.1.1.100/23;tcp, If: ge-0/0/0.0
  Out: 10.1.1.100/23 --> 1.1.1.14/1047;tcp, If: fe-0/0/7.0

2 sessions displayed
```

The security policy can be modified to allow access to the server only via the translated address. The key word “drop-untranslated” will drop all traffic to the destination address of 10.1.1.100. This will limit the access to the server using the destination address of 1.1.1.100.

```
[edit security policies from-zone trust to-zone untrust]
set policy permit-all match source-address any destination-address any application any
set policy permit-all then permit destination-address drop-untranslated
```

Static NAT

In this example, host 192.168.1.200 is assigned a static NAT mapping to IP address 1.1.1.200. Any traffic to the destination address of 1.1.1.200 will be translated to 192.168.1.200. Any new sessions originating from host 192.168.1.200 will have the source IP of the packet translated to 1.1.1.200.




```
[edit security nat static]
set rule-set rs1 from zone untrust
set rule-set rs1 rule r1 match destination-address 1.1.1.200/32
set rule-set rs1 rule r1 then static-nat prefix 192.168.1.200/32

[edit security nat]
set proxy-arp interface fe-0/0/7.0 address 1.1.1.200

[edit security]
set zones security-zone trust address-book address server-1 192.168.1.200/32

[edit security policies from-zone untrust to-zone trust]
set policy server-access match source-address any destination-address server-1application
any
set policy server-access then permit

[edit security policies from-zone trust to-zone untrust]
set policy permit-all match source-address server-1 destination-address any application
any
set policy permit-all then permit
```

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.