Network Configuration Example

Junos OS NAT Configuration Examples for ScreenOS Users

Release
13.1

Published: 2013-02-11

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

Network Configuration Example Junos OS NAT Configuration Examples for ScreenOS Users
Release 13.1
NCE0073

The information in this document is current as of the date on the title page.

YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. Junos OS has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at http://www.juniper.net/support/eula.html. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Table of Contents

Introduction

This document describes how to configure the Network Address Translation (NAT) functionality on Juniper Networks® SRX Series or J Series devices using the Junos® operating system (Junos OS) command-line interface (CLI).

The instructions in this document will help ScreenOS users to migrate ScreenOS® Software on an SSG 300M-series or SSG 500M-series security device to Junos OS Software on an SRX Series Services Gateway or J Series Services Router.

Because of the extensive Junos OS feature set, the command sequence required to configure NAT is different from the ScreenOS equivalent.

The examples provided in this document compare several common ScreenOS NAT CLI command sequences with the Junos OS equivalents. These examples are a starting point for ScreenOS users planning to migrate to Junos OS. For more information about Junos OS NAT for SRX Series Services Gateways and J Series Services Routers, see Network Address Translation for Security Devices.

This document is designed for anyone who is familiar with NAT, ScreenOS, and the various NAT options available in ScreenOS.

Advantages of Using Junos OS SRX Series and J Series Devices

Junos OS is a reliable, high-performance network operating system for routing, switching, and security. It reduces the time required to deploy new services and decreases network operation costs.

Running Junos OS in a network improves the reliability, performance, and security of existing applications. It automates network operations on a streamlined system, allowing more time to focus on deploying new applications and services. Junos OS is highly scalable software that keeps up with changing needs, which, in turn, means a more cost-effective solution for your business.

The SRX Series Services Gateways based on Junos OS are high-performance security, routing, and network solutions for enterprise and service providers. SRX Series services gateways pack high port-density, advanced security, and flexible connectivity into a single, easily managed platform that supports fast, secure, and highly-available data center and branch operations.

NAT is a process to translate IP addresses. NAT configuration on SRX Series and J Series devices provides the following benefits:

- Enables multiple hosts on a private network to access the Internet using one shared globally routable IP address.
- Enhances security by shielding details about your network from the outside world.
- Supports network load sharing and traffic redirection.
- Simplifies network migration by letting you change your network topology without coordinating those changes with external networks.

Related Documentation

- Example: Configuring NAT on SRX Series and J Series Devices on page 3
- Understanding NAT on SRX Series and J Series Devices on page 2

Understanding NAT on SRX Series and J Series Devices

NAT is a technique for modifying or translating network address information, such as source or destination IP addresses or port numbers, in packet headers transparently as the packets enter or leave your protected network.

NAT is described in RFC 3022 to solve IP (version 4) address depletion problems. Since then, NAT has been found to be a useful tool for firewalls, traffic redirects, load sharing, network migrations, and so on.

The following types of NAT are supported on Juniper Networks devices:

- Static NAT
- Destination NAT
- Source NAT

Figure 1: NAT Example

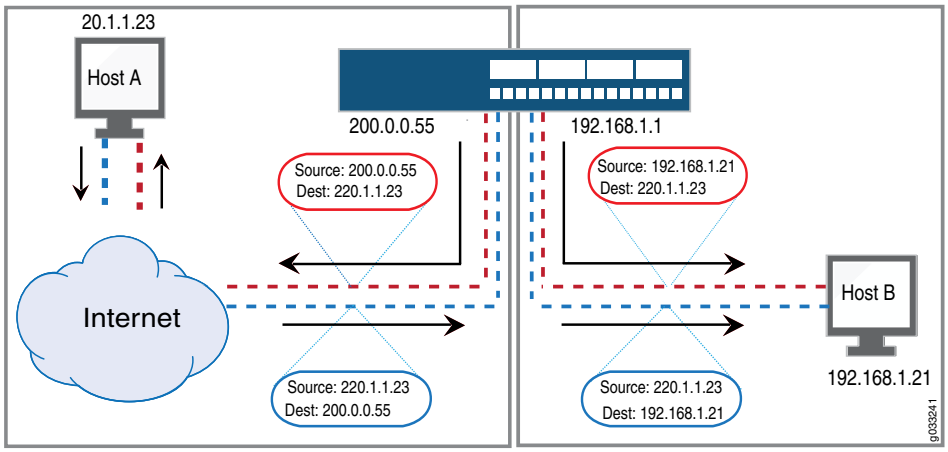


Figure 1 on page 2 illustrates how source address translation works in NAT. Host A, a computer on a protected network, uses the private IP address 196.168.1.21. When Host A communicates with Host B over the Internet, it sends out packets (light red packet flow) with source address = 192.168.1.21 and Destination Address = 220.1.1.23. When the services gateway passes each packet in this flow from the protected network to the Internet, it translates the source address in each packet header to its own external IP address (200.0.0.55). When Host B sends information back (dark blue packet flow), it sends packets to Destination Address = 200.0.0.55, and the services gateway translates this to Destination Address = 192.168.1.21 before routing the packet back to Host A.

Related Documentation

- Advantages of Using Junos OS SRX Series and J Series Devices on page 1
- Example: Configuring NAT on SRX Series and J Series Devices on page 3

Example: Configuring NAT on SRX Series and J Series Devices

This example shows how to configure NAT on SRX Series and J Series devices using the CLI.

This example compares the steps used to configure NAT on ScreenOS and provides equivalent steps required to configure NAT on Junos OS.

This topic includes the following sections:

Requirements

This example uses the following hardware and software components:

- J2320, J2350, J4350, and J6350 Services Routers
- SRX Series Services Gateways
- Junos OS Release 9.2 or later for all SRX Series Services Gateways (a more recent version might be required for all SRX Series Services Gateways released after 9.2)
- Junos OS Release 9.5 or later for all J Series Services Routers

In addition, you must do the following before configuring NAT:

- Configure network interfaces on the device
- Create security zones and assign interfaces to them

Network Topology

You must configure NAT before allowing a private network to connect to the Internet on an SRX Series Services Gateway or J Series Services Router. Procedures in these examples describe configuration of source NAT, destination NAT, and static NAT.

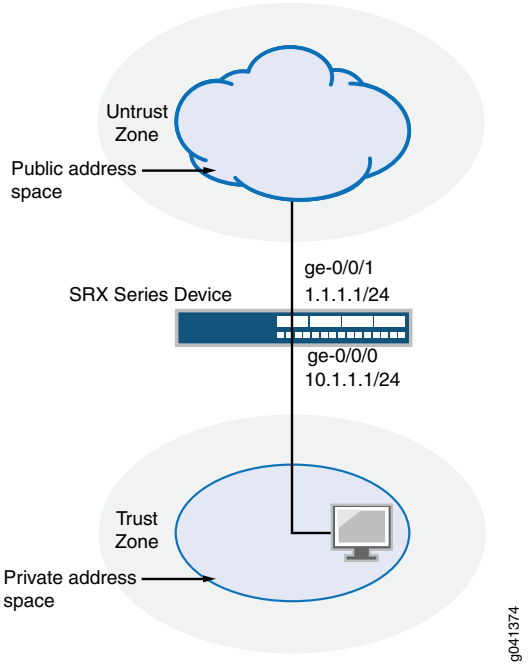
Source NAT Egress Interface Translation

Source NAT is the translation of the source IP address of a packet leaving the Juniper Networks device. Source NAT is used to allow hosts with private IP addresses to access a public network.

This example describes how to configure a source NAT mapping of a single private address to a public address.

In Figure 2 on page 4, a device with the private address 10.1.1.0/24 in the trust zone accesses a public network. For packets sent by the device to a destination address in the untrust zone, the Juniper Networks security device translates the source IP address to the public IP address 1.1.1.1/24.

Figure 2: Source NAT Address Translation Topology



In Table 1 on page 4, the trust security zone is configured for the private address space, and the untrust security zone is configured for the public address space.

Table 1: Interface, Zones, and IP Address Information

Interface	Zone	IP Address
Ethernet 0/0	untrust	1.1.1.1/24
Ethernet 0/1	trust	10.1.1.1/24

This example configures the following:

- Source NAT rule set *interface-nat* with a rule *rule1* to match any packet from the trust zone to the untrust zone. To match packets, the source address is translated to the IP address of the egress interface.
- Security policies to permit traffic from the trust zone to the untrust zone.

Configuring Source NAT Egress Interface Translation

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the **[edit]** hierarchy level.

Configuration in ScreenOS

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

Configuration in Junos OS

```
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
```

Step-by-Step Procedure

To configure a source NAT translation to an egress interface:

1. Create a source NAT rule set.

   ```
   [edit]
   user@host# set security nat source rule-set interface-nat from zone trust
   user@host# set security nat source rule-set interface-nat to zone untrust
   ```

2. Configure a rule that matches packets and translates the source address to the address of the egress interface.

   ```
   [edit]
   user@host# 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
   user@host# set security nat source rule-set interface-nat rule rule1 then source-nat
     interface
   ```

3. Configure a security policy that allows traffic from the trust zone to the untrust zone.

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

Verifying Source NAT Configuration

Purpose Verify the configuration of source NAT rule.

Action From operational mode, run the **show** command to verify the configuration:

```
user@host# show security nat source summary

Total port number usage for port translation pool: 0
Maximum port number for port translation pool: 268435456
Total pools: 0

Total rules: 1
Rule name          Rule set       From              To                    Action
rule1              interface-nat  trust             untrust               interface
```

Meaning The output displays information about source NAT configuration. You can verify the following information:

- Rule sets
- Rules

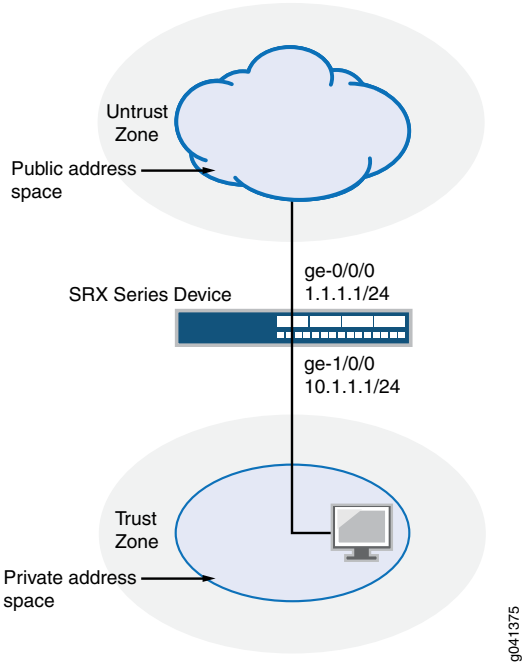
Source NAT With IP Pool (Dynamic Internet Protocol Address Pool With Port Translation)

A Dynamic Internet Protocol (DIP) address pool is a range of IP addresses from which the security device can dynamically pick addresses to use when performing NAT on the source IP address of incoming or outgoing IP packets.

This example describes how to configure a source NAT mapping of a private address block to a smaller public address block using port address translation.

In Figure 3 on page 7, the source IP address in packets sent from the trust zone to the untrust zone is mapped to a smaller block of public addresses in the range from 1.1.1.10 to 1.1.1.15. Port address translation is used, because the size of the source NAT address pool is smaller than the number of potential addresses that might need to be translated.

Figure 3: Source NAT Address Translation with IP Pool Topology



In Table 2 on page 7, the trust security zone is configured for the private address space, and the untrust security zone is configured for the public address space.

Table 2: Interface, Zones, and IP Address Information

Interface	Zone	IP Address
Ethernet 0/0	untrust	1.1.1.1/24
Ethernet 0/1	trust	10.1.1.1/24

This example configures the following:

- Source NAT pool **pool-1** that contains the IP address range 1.1.1.10 to 1.1.1.15.
- Source NAT rule set **pool-nat** to match all packets from the trust zone to the untrust zone. To match packets, the source IP address is translated to an IP address in the **pool-1** pool.
- Proxy ARP for the addresses 1.1.1.10 to 1.1.1.15 on interface ge-0/0/0. This allows the Juniper Networks security device to respond to ARP requests received on the interface for those addresses.
- Security policies to permit traffic from the trust zone to the untrust zone.

This topic includes the following sections:

Configuring Source NAT With IP Pool (Dynamic Internet Protocol Address Pool With Port Translation)

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them in a text file, remove any line breaks, change any details necessary to match your network configuration, and paste the commands into the CLI at the **[edit]** hierarchy level of your device.

Configuration in ScreenOS (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
```

Configuration in Junos OS (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
```

Step-by-Step Procedure

To configure source NAT with an IP pool (with port translation):

1. Create a source NAT pool.

   ```
   [edit]
   user@host# set security nat source pool pool-1 address 1.1.1.10 to 1.1.1.15
   ```

2. Create a source NAT rule set.

   ```
   [edit]
   user@host# set security nat source rule-set pool-nat from zone trust
   user@host# set security nat source rule-set pool-nat to zone untrust
   ```

3. Configure a rule that matches the packets and translates the source address to an address in the pool.

   ```
   [edit]
   user@host# 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
   user@host# set security nat source rule-set pool-nat rule rule1 then source-nat pool
     pool-1
   ```

4. Configure proxy ARP.

```
[edit]
user@host# set security nat proxy-arp interface ge-0/0/0 address 1.1.1.10 to 1.1.1.15
```

5. Configure a security policy that allows traffic from the trust zone to the untrust zone.

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

Verifying Source NAT With IP Pool (With Port Translation) Configuration

Purpose Verify the configuration of source NAT with an IP pool (with port translation).

Action From configuration mode, run the **show** command to verify the configuration:

```
user@host> show security nat source summary

Total port number usage for port translation pool: 18438
Maximum port number for port translation pool: 268435456
Total pools: 1
Pool                 Address                 Routing              PAT  Total
Name                 Range                   Instance                  Address
pool-1               1.1.1.10-1.1.1.15       default              yes  6

Total rules: 1
Rule name          Rule set       From             To                  Action
rule1              pool-nat       trust            untrust             pool-1
```

Meaning The output displays information about source NAT configuration. You can verify the following information:

- Rule sets
- Rules
- NAT pool
- Port address translation (PAT)

Configuring Source NAT With IP Pool (Dynamic Internet Protocol Address Pool Without Port Translation)

CLI Quick Configuration To quickly configure this example, copy the following commands, paste them in a text file, remove any line breaks, change any details necessary to match your network configuration, and paste the commands into the CLI at the **[edit]** hierarchy level of your device.

NOTE: By default, port address translation is executed with source NAT. If you specify the port no-translation option, the number of hosts that the source NAT pool can support is limited to the number of addresses in the pool.

Configuration in ScreenOS (Without 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
```

Configuration in Junos OS (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 10.1.1.1/24
  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
```

Step-by-Step Procedure

To configure source NAT with IP pool (without port translation):

1. Create a source NAT pool.

   ```
   [edit]
   user@host# set security nat source pool pool-1 address 1.1.1.10 to 1.1.1.15
   user@host# set security nat source pool pool-1 port no-translation
   ```

2. Create a source NAT rule set.

   ```
   [edit]
   user@host# set security nat source rule-set pool-nat from zone trust
   user@host# set security nat source rule-set pool-nat to zone untrust
   ```

3. Configure a rule that matches packets and translates the source address to an address in the pool.

   ```
   [edit]
   user@host# set security nat source rule-set pool-nat rule rule1 match source-address
     10.1.1.1/24 destination-address 0.0.0.0/0
   user@host# set security nat source rule-set pool-nat rule rule1 then source-nat pool
     pool-1
   ```

4. Configure proxy ARP.

   ```
   [edit]
   user@host# set security nat proxy-arp interface ge-0/0/0 address 1.1.1.10 to 1.1.1.15
   ```

5. Configure a security policy that allows traffic from the trust zone to the untrust zone.

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

Verifying Source NAT With IP Pool (Without Port Translation) Configuration

Purpose Verify the configuration of the source NAT with an IP pool (without port translation).

Action From configuration mode, run the **show** command to verify the configuration:

```
user@host> show security nat source summary

Total port number usage for port translation pool: 0
Maximum port number for port translation pool: 268435456
Total pools: 1
Pool                 Address                 Routing              PAT  Total
Name                 Range                   Instance                  Address
pool-1               1.1.1.10-1.1.1.15       default              no   6

Total rules: 1
Rule name          Rule set       From             To                  Action
rule1              pool-nat       trust            untrust             pool-1
```

Meaning The output displays information about source NAT configuration. You can verify the following information:

- Rule sets
- Rules
- NAT pool
- Port address translation (PAT)

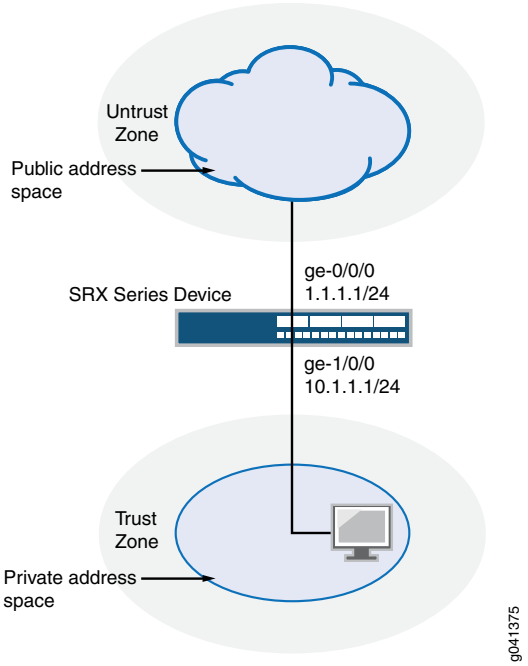
Source NAT with IP Address Shifting

A range of original source IP addresses can be mapped to another range of IP addresses by shifting the IP addresses.

This example describes how to configure a source NAT mapping of a private address range to public addresses, with optional address shifting. This mapping is one-to-one between the original source IP addresses and the translated IP addresses.

In Figure 4 on page 12, a range of private addresses in the trust zone is mapped to a range of public addresses in the untrust zone. For packets sent from the trust zone to the untrust zone, a source IP address in the range of 192.168.1.10/32 to 192.168.1.20/32 is translated to a public address in the range of 1.1.1.100 to 1.1.1.109.

Figure 4: Source NAT with IP Address Shifting Topology



In Table 3 on page 12, the trust security zone is configured for the private address space, and the untrust security zone is configured for the public address space.

Table 3: Interface, Zones, and IP Address Information

Interface	Zone	IP Address
Ethernet 0/0	untrust	1.1.1.1/24
Ethernet 0/1	trust	10.1.1.1/24

This example configures the following:

- Source NAT pool **pool-1** that contains the IP address range 1.1.1.100 to 1.1.1.109.
- Source NAT rule set **pool-nat** to match all packets from the trust zone to the untrust zone. For matching packets, the source IP address is translated to an IP address in the **pool-1** pool.
- Proxy ARP for the addresses 1.1.1.100 to 1.1.1.109 on interface ge-0/0/0. This allows the Juniper Networks security device to respond to ARP requests received on the interface for those addresses.
- Security policies to permit traffic from the trust zone to the untrust zone.

This topic includes the following sections:

- Configuring Source NAT with IP Address Shifting on page 13
- Verifying Source NAT with IP Address Shifting Configuration on page 14

Configuring Source NAT with IP Address Shifting

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them in a text file, remove any line breaks, change any details necessary to match your network configuration, and paste the commands into the CLI at the **[edit]** hierarchy level of your device.

Configuration in ScreenOS

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

Configuration in Junos OS

```
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 nat proxy-arp interface ge-0/0/0 address 1.1.1.100 to 1.1.1.109
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
```

Step-by-Step Procedure

To configure source NAT with IP address shifting:

1. Create a source NAT pool.

   ```
   [edit]
   user@host# set security nat source pool pool-1 address 1.1.1.100 to 1.1.1.109
   ```

2. Specify the beginning of the original source IP address range.

   ```
   [edit]
   user@host# set security nat source pool pool-1 host-address-base 10.1.1.100
   ```

3. Create a source NAT rule set.

   ```
   [edit]
   user@host# set security nat source rule-set pool-nat from zone trust
   user@host# set security nat source rule-set pool-nat to zone untrust
   ```

4. Configure a rule that matches packets and translates the source address to an address in the pool.

   ```
   [edit]
   user@host# 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
   user@host# set security nat source rule-set pool-nat rule rule1 then source-nat pool
     pool-1
   ```

5. Configure proxy ARP.

   ```
   [edit]
   user@host# set security nat proxy-arp interface ge-0/0/0 address 1.1.1.100 to 1.1.1.109
   ```

6. Configure a security policy that allows traffic from the trust zone to the untrust zone.

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

```
user@host# set security policies from-zone trust to-zone untrust policy permit-all
    then permit
```

Verifying Source NAT with IP Address Shifting Configuration

Purpose Verify the configuration of source NAT with IP address shifting.

Action From configuration mode, run the **show** command to verify the configuration:

```
user@host>show security nat source summary

Total port number usage for port translation pool: 0
Maximum port number for port translation pool: 268435456
Total pools: 1
Pool                 Address                 Routing              PAT  Total
Name                 Range                   Instance                  Address
pool-1               1.1.1.10-1.1.1.15
 -                   1.1.1.100-1.1.1.109     default              no   16

Total rules: 1
Rule name          Rule set       From             To                  Action
rule1              pool-nat       trust            untrust             pool-1
```

Meaning The output displays information about source NAT configuration. You can verify the following information:

- Rule sets
- Rules
- NAT pool
- Port address translation (PAT)

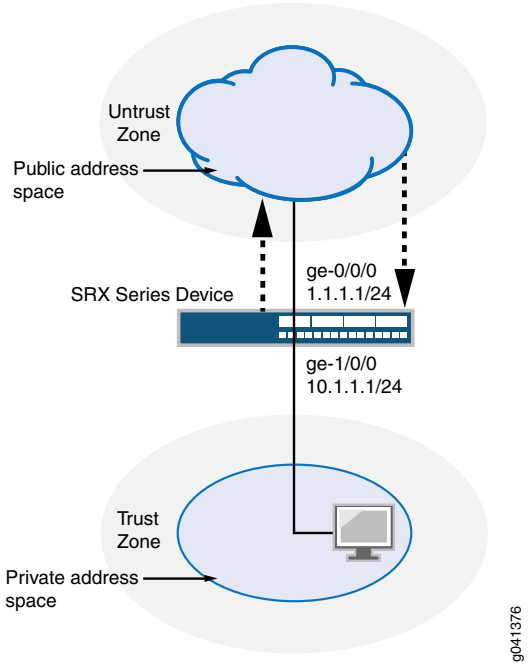
Source NAT with Loopback Group and Dynamic Internet Protocol

When performing source NAT, the security device translates the original source IP address to a different address. The translated address can come from a Dynamic Internet Protocol (DIP) pool or from the egress interface of the security device.

This example configures source NAT with a loopback group and the DIP.

In Figure 5 on page 15, packets arriving at the NAT device from the private network are translated and then looped back to the private network rather than being passed through to the public network

Figure 5: Source NAT with Loopback Group and Dynamic Internet Protocol Topology



In Table 4 on page 15, the trust security zone is configured for the private address space, and the untrust security zone is configured for the public address space.

Table 4: Interface, Zones, and IP Address Information

Interface	Zone	IP Address
Ethernet 0/0	untrust	1.1.1.1/24
Ethernet 0/1	trust	10.1.1.1/24

This example configures the following:

- Source NAT pool **pool-1** that contains the IP address range 1.1.1.10 through 1.1.1.15.
- Source NAT rule set **pool-nat** with a rule **rule1** to match any packet from the trust zone to the untrust zone. For matching packets, the source address is translated to the IP address of the egress interface.
- Security policy to allow traffic from a specific internal IP address to be mapped to the specific public IP address created.

This topic includes the following sections:

Configuring Source NAT with Loopback Group and Dynamic Internet Protocol

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them in a text file, remove any line breaks, change any details necessary to match your network configuration, and paste the commands into the CLI at the **[edit]** hierarchy level of your device.

Configuration in ScreenOS

```
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
```

Configuration in Junos OS

```
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 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
```

Step-by-Step Procedure

To configure source NAT with a loopback group and the DIP:

1. Create a source NAT pool.

   ```
   [edit]
   user@host# set security nat source pool pool-1 address 1.1.1.10 to 1.1.1.15
   ```

2. Create a source NAT rule set.

   ```
   [edit]
   user@host# set security nat source rule-set pool-nat from zone trust
   user@host# set security nat source rule-set pool-nat to interface ge-0/0/0 interface
     ge-0/0/2
   ```

3. Configure a rule that matches packets and translates the source address to an address in the pool.

   ```
   [edit]
   user@host# 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
   user@host# set security nat source rule-set pool-nat rule rule1 then source-nat pool
     pool-1
   ```

4. Configure proxy ARP.

   ```
   [edit]
   user@host# set security nat proxy-arp interface ge-0/0/0 address 1.1.1.10 to 1.1.1.15
   user@host# set security nat proxy-arp interface ge-0/0/2 address 1.1.1.10 to 1.1.1.15
   ```

5. Configure a security policy that allows traffic from the trust zone to the untrust zone.

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

```
user@host# set security policies from-zone trust to-zone untrust policy permit-all
    then permit
```

Verifying Source NAT with Loopback Group and Dynamic Internet Protocol Configuration

Purpose Verify the configuration of source NAT with loopback group and DIP.

Action From configuration mode, run the **show** command to verify the configuration:

```
user@host> show security nat source summary

Total port number usage for port translation pool: 0
Maximum port number for port translation pool: 268435456
Total pools: 1
Pool                 Address                 Routing              PAT  Total
Name                 Range                   Instance                  Address
pool-1               1.1.1.10-1.1.1.15
 -                   1.1.1.100-1.1.1.109     default              no   16

Total rules: 1
Rule name          Rule set       From             To                   Action
rule1              pool-nat       trust            ge-0/0/0.0           pool-1
rule1                                              ge-0/0/2.0
```

Meaning The output displays information about source NAT configuration. You can verify the following information:

- Rule sets
- Rules
- NAT pool
- Address range
- Port address translation (PAT)

Static NAT to a Single Host

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

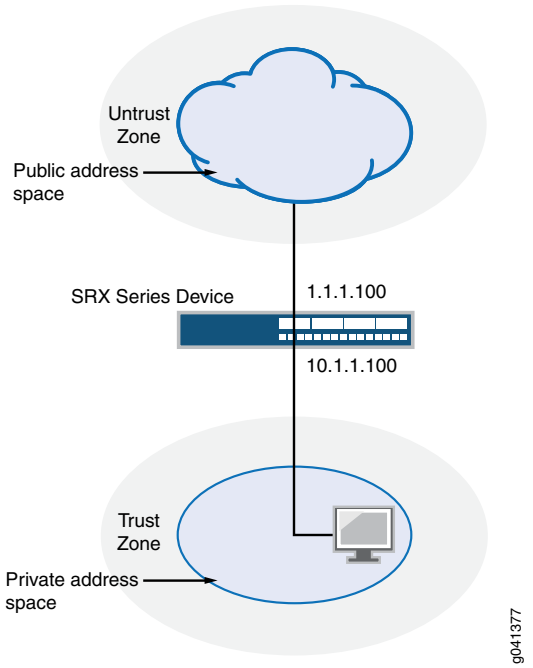
Static NAT defines a one-to-one mapping from one IP subnet to another IP subnet. The mapping includes destination IP address translation in one direction and source IP address translation in the reverse direction. From the NAT device, the original destination address is the virtual host IP address, while the mapped-to address is the real host IP address.

This example uses the trust security zone for the private address space, and the untrust security zone for the public address space.

In Figure 6 on page 18, devices in the untrust zone access a server in the trust zone by way of public address 1.1.1.100/32. For packets that enter the Juniper Networks security device from the untrust zone with the destination IP address 1.1.1.100/32, the destination

IP address is translated to the private address 10.1.1.100. For a new session originating from the server, the source IP address in the outgoing packet is translated to the public address 1.1.1.100/32.

Figure 6: Static NAT to a Single Host Topology



In Table 5 on page 18, the trust security zone is configured for the private address space, and the untrust security zone is configured for the public address space.

Table 5: Interface, Zones, and IP Address Information

Interface	Zone	IP Address
Ethernet 0/0	untrust	1.1.1.100
Ethernet 0/1	trust	10.1.1.100

This example configures the following:

- Static NAT rule set **static-nat** with rule **rule1** to match packets from the untrust zone with the destination address 1.1.1.100. For matching packets, the destination IP address is translated to the private address 10.1.1.100.
- Proxy ARP for the address 1.1.1.100/32 on interface ge-0/0/0.0. This allows the Juniper Networks security device to respond to ARP requests received on the interface for that address.
- Security policies to permit traffic to and from the 10.1.1.100 server.

This topic includes the following sections:

Configuring Static NAT to a Single Host

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them in a text file, remove any line breaks, change any details necessary to match your network configuration, and paste the commands into the CLI at the **[edit]** hierarchy level of your device.

Configuration in ScreenOS

```
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
```

Configuration in Junos OS

```
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
```

Step-by-Step Procedure

To configure static NAT to a single host configuration:

1. Configure proxy ARP.

   ```
   [edit]
   user@host# set security nat proxy-arp interface ge-0/0/0 address 1.1.1.100/32
   ```

2. Create a static NAT rule set.

   ```
   [edit]
   user@host# set security nat static rule-set static-nat from zone untrust
   ```

3. Configure a rule that matches packets and translates the destination address in the packets to a private address.

   ```
   [edit]
   user@host# set security nat static rule-set static-nat rule rule1 match
     destination-address 1.1.1.100
   user@host# set security nat static rule-set static-nat rule rule1 then static-nat prefix
     10.1.1.100
   ```

4. Configure an address in the global address book.

   ```
   [edit]
   user@host# set security zones security-zone trust address-book address webserver
     10.1.1.100
   ```

5. Configure a security policy that allows traffic from the untrust zone to the server in the trust zone.

   ```
   [edit]
   user@host# set security policies from-zone untrust to-zone trust policy static-nat
     match source-address any destination-address webserver application junos-http
   ```

```
user@host# set security policies from-zone untrust to-zone trust policy static-nat
    then permit
```

Verifying Static NAT to a Single Host Configuration

Purpose Verify the configuration of static NAT to a single host.

Action From configuration mode, run the **show** command to verify the configuration:

```
user@host> show security nat static rule all

Total static-nat rules: 1
Total referenced IPv4/IPv6 ip-prefixes: 2/0

Static NAT rule: rule1                Rule-set: static-nat
  Rule-Id                   : 1
  Rule position             : 1
  From zone                 : untrust
  Destination addresses     : 1.1.1.100
  Host addresses            : 10.1.1.100
  Netmask                   : 32
  Host routing-instance     : N/A
  Translation hits          : 0
```

Meaning The output displays information about static NAT configuration. You can verify the following information:

- Rule sets
- Rules
- Address range

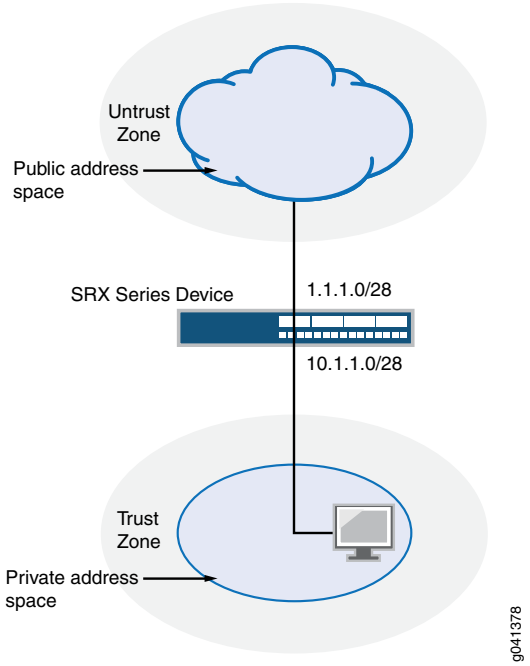
Static NAT to a Subnet

This example uses the trust security zone for the private address space, and the untrust security zone for the public address space.

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

In Figure 7 on page 21, devices in the untrust zone access devices in the trust zone by way of public subnet address 1.1.1.0/28. For packets that enter the Juniper Networks security device from the untrust zone with a destination IP address in the 1.1.1.0/28 subnet, the destination IP address is translated to a private address on the 10.1.1.0/28 subnet. For new sessions originating from the 10.1.1.0/28 subnet, the source IP address in outgoing packets is translated to an address on the public 1.1.1.0/28 subnet.

Figure 7: Static NAT to a Subnet Topology



In Table 6 on page 21, the trust security zone is configured for the private address space, and the untrust security zone is configured for the public address space.

Table 6: Interface, Zones, and IP Address Information

Interface	Zone	IP Address
Ethernet 0/0	untrust	1.1.1.0/28
Ethernet 0/1	trust	10.1.1.0/28

This example configures the following:

- Static NAT rule set **rule-set** with rule **rule1** to match packets received on interface ge-0/0/0.0 with a destination IP address in the 1.1.1.0/28 subnet. For matching packets, the destination address is translated to an address on the 10.1.1.0/28 subnet.
- Proxy ARP for the address on interface ge-0/0/0.0 is 1.1.1.0/28. This allows the Juniper Networks security device to respond to ARP requests received on the interface for those addresses.
- Security policies to permit traffic to and from the 10.1.1.0/28 subnet.

This topic includes the following sections:

- Configuring Static NAT to a Subnet on page 22
- Verifying Static NAT to a Subnet Configuration on page 23

Configuring Static NAT to a Subnet

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them in a text file, remove any line breaks, change any details necessary to match your network configuration, and paste the commands into the CLI at the **[edit]** hierarchy level of your device.

Configuration in ScreenOS

```
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
```

Configuration in Junos OS

```
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-set 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-set match source-address
    any destination-address webserver-group application junos-http
set security policies from-zone untrust to-zone trust policy static-set then permit
```

Step-by-Step Procedure

To configure static NAT to a subnet:

1. Configure an address in the global address book.

   ```
   [edit]
   user@host # set security zones security-zone trust address-book address
     webserver-group 10.1.1.0/28
   ```

2. Configure proxy ARP.

   ```
   [edit]
   user@host # set security nat proxy-arp interface ge-0/0/0 address 1.1.1.0/28
   ```

3. Create a static NAT rule set.

   ```
   [edit]
   user@host# set security nat static rule-set static-set from zone untrust
   ```

4. Configure a rule that matches packets and translates the destination address in the packets to a private address.

   ```
   [edit]
   user@host # set security nat static rule-set static-set rule rule1 match
     destination-address 1.1.1.0/28
   user@host # set security nat static rule-set static-set rule rule1 then static-nat prefix
     10.1.1.0/28
   ```

5. Configure a security policy that allows traffic from the untrust zone to the server in the trust zone.

   ```
   [edit]
   user@host# set security policies from-zone untrust to-zone trust policy static-set
     match source-address any destination-address webserver-group application
     junos-http
   user@host# set security policies from-zone untrust to-zone trust policy static-set
     then permit
   ```

Verifying Static NAT to a Subnet Configuration

Purpose Verify the configuration of static NAT to a subnet.

Action From configuration mode, run the following **show** command to verify the configuration:

```
user@host> show security nat static rule all

Total static-nat rules: 1
Total referenced IPv4/IPv6 ip-prefixes: 2/0

Static NAT rule: rule1                Rule-set: static-set
  Rule-Id                   : 1
  Rule position             : 1
  From zone                 : untrust
  Destination addresses     : 1.1.1.0
  Host addresses            : 10.1.1.0
  Netmask                   : 28
  Host routing-instance     : N/A
  Translation hits          : 0
```

Meaning The output displays information about static NAT configuration. You can verify the following information:

- Rule sets
- Rules
- Address range

Destination NAT Pool for Virtual IP Addresses

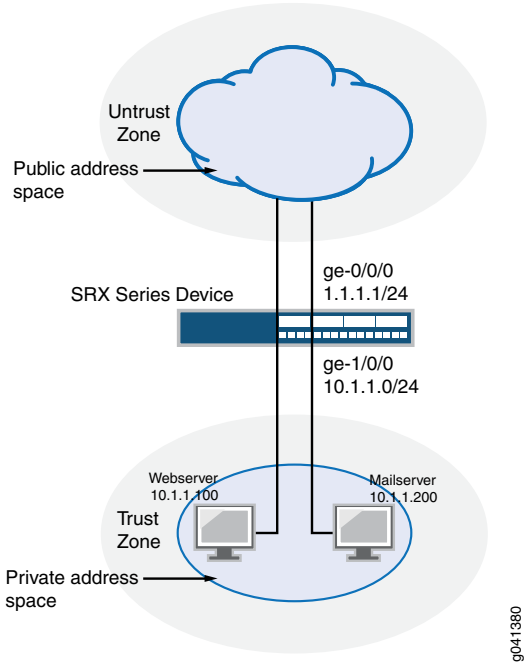
A virtual IP (VIP) is a mapping of one IP address to another IP address based on the destination port number. A single IP address defined in the same subnet as an interface can host mappings of several services—identified by various destination port numbers—to many hosts. The virtual IP address also supports port mapping.

This example uses the trust security zone for the private address space, and the untrust security zone for the public address space.

In Figure 8 on page 24, devices in the untrust zone access servers in the trust zone by way of public addresses 10.1.1.100/32 and 10.1.1.200/32. Packets entering the Juniper Networks security device from the untrust zone are mapped to the private addresses of the servers as follows:

- The destination IP address 1.1.1.100/32 and port 80 is translated to the private address 10.1.1.100/32 and port 80.
- The destination IP address 1.1.1.100/32 and port 110 is translated to the private address 10.1.1.200/32 and port 110.

Figure 8: Destination NAT Pool for Virtual IP Topology



In Table 7 on page 24, the trust security zone is configured for the private address space, and the untrust security zone is configured for the public address space.

Table 7: Interface, Zones, and IP Address Information

Interface	Zone	IP Address
Ethernet 0/0	untrust	1.1.1.1/24
Ethernet 0/1	trust	10.1.1.0/24

This example configures the following:

- Destination NAT pool **dnat-pool-1** that contains the IP address 10.1.1.100/32 port 80.
- Destination NAT pool **dnat-pool-2** that contains the IP address 10.1.1.200/32 and port 110.
- Destination NAT rule set **dst-nat** with rule **rule1** to match packets received from the untrust zone with the destination IP address 1.1.1.100/32 and destination port 80. For matching packets, the destination address is translated to the address in the **dnat-pool-1** pool.
- Destination NAT rule set **dst-nat** with rule **rule2** to match packets received from the untrust zone with the destination IP address 1.1.1.100/32 and destination port 110. For matching packets, the destination IP address and port are translated to the address and port in the **dnat-pool-2** pool.

- Proxy ARP for the address 1.1.1.100. This allows the Juniper Networks security device to respond to ARP requests received on the interface for that address.
- Security policies to permit traffic from the untrust zone to the translated destination IP addresses in the trust zone.

This topic includes the following sections:

Configuring Destination NAT Pool for Virtual IP

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them in a text file, remove any line breaks, change any details necessary to match your network configuration, and paste the commands into the CLI at the **[edit]** hierarchy level of your device.

Configuration in ScreenOS

```
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
```

Configuration in Junos OS

```
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
```

Step-by-Step Procedure

To configure a destination NAT pool for a virtual IP:

1. Configure proxy ARP.

   ```
   [edit]
   user@host# set security nat proxy-arp interface ge-0/0/0.0 address 1.1.1.100
   ```

2. Create destination NAT pools.

```
[edit]
user@host# set security nat destination pool dnat-pool-1 address 10.1.1.100/32
user@host# set security nat destination pool dnat-pool-2 address 10.1.1.200/32
```

3. Create a destination NAT rule set.

```
[edit]
user@host# set security nat destination rule-set dst-nat from zone untrust
```

4. Configure a rule that matches packets and translates the destination address to the address in the pool.

   This rule matches packets received from the untrust zone with the destination IP address 1.1.1.100 and destination port 80.

```
[edit]
user@host# set security nat destination rule-set dst-nat rule rule1 match
  destination-address 1.1.1.100/32
user@host# set security nat destination rule-set dst-nat rule rule1 match
  destination-port 80
user@host# set security nat destination rule-set dst-nat rule rule1 then
  destination-nat pool dnat-pool-1
```

5. Configure a rule that matches packets and translates the destination address to the address in the pool.

   This rule matches packets received from the untrust zone with the destination IP address 1.1.1.100 and destination port 110.

```
[edit]
user@host# set security nat destination rule-set dst-nat rule rule2 match
  destination-address 1.1.1.100/32
user@host# set security nat destination rule-set dst-nat rule rule2 match
  destination-port 110
user@host# set security nat destination rule-set dst-nat rule rule2 then
  destination-nat pool dnat-pool-2
```

6. Configure addresses in the global address book.

```
[edit]
user@host# set security zones security-zone trust address-book address webserver
  10.1.1.100
user@host# set security zones security-zone trust address-book address mailserver
  10.1.1.200
user@host# set security zones security-zone trust address-book address-set
  servergroup address webserver
user@host# set security zones security-zone trust address-book address-set
  servergroup address mailserver
```

7. Configure a security policy that allows traffic from the untrust zone to the servers in the trust zone.

```
[edit]
user@host# set security policies from-zone untrust to-zone trust policy static-nat
  match source-address any destination-address servergroup application junos-http
user@host# set security policies from-zone untrust to-zone trust policy static-nat
  match application junos-pop3
user@host# set security policies from-zone untrust to-zone trust policy static-nat
  then permit
```


Verifying Destination NAT Pool for Virtual IP Configuration

Purpose Verify the configuration of destination NAT pool for virtual IP.

Action From configuration mode, run the following **show** command to verify the configuration:

```
user@host> show security nat destination summary

Total pools: 2
Pool name            Address                          Routing        Port  Total

                    Range                            Instance            Address
dnat-pool-1          10.1.1.100     - 10.1.1.100                     0     1
dnat-pool-2          10.1.1.200     - 10.1.1.200                     0     1

Total rules: 2
Rule name            Rule set       From                               Action
rule1                dst-nat        untrust                            dnat-pool-1
rule2                dst-nat        untrust                            dnat-pool-2
```

Meaning The output displays information about destination NAT configuration. You can verify the following information:

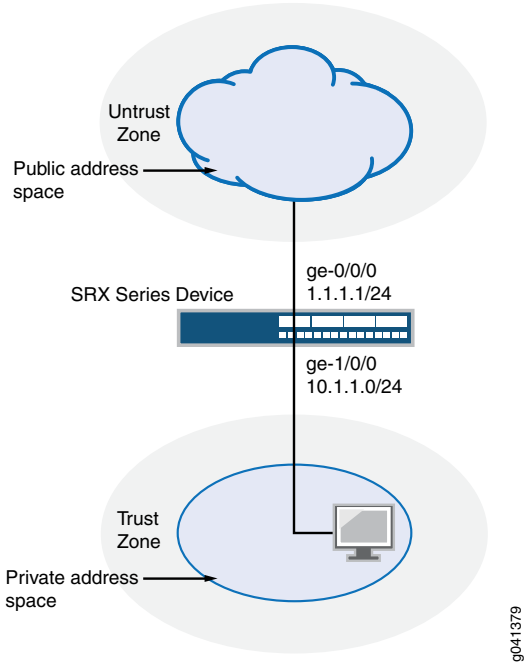
- Rule sets
- Rules
- Address range
- NAT pool
- Port details

Destination Address Translation for Subnet Translation

This example describes how to configure a destination NAT mapping of a single public address to a private address. In this example, the destination IP address and the interface IP address are on different subnets.

In Figure 9 on page 28, devices in the untrust zone access a server in the trust zone by way of public address 2.1.1.100. For packets that enter the Juniper Networks security device from the untrust zone with the destination IP address 2.1.1.100, the destination IP address is translated to the private address 10.1.1.100.

Figure 9: Destination Address Translation to a Single Host Topology



In Table 8 on page 28, the trust security zone is configured for the private address space, and the untrust security zone is configured for the public address space.

Table 8: Interface, Zones, and IP Address Information

Interface	Zone	IP Address
Ethernet 0/0	untrust	1.1.1.1/24
Ethernet 0/1	trust	10.1.1.0/24

This example configures the following:

- Destination NAT pool **dnat-pool-1** that contains the IP address 10.1.1.100.
- Destination NAT rule set **dst-nat** with rule **r1** to match packets received from the ge-0/0/0.0 interface with the destination IP address 2.1.1.100. For matching packets, the destination address is translated to the address in the **dnat-pool-1** pool.
- Proxy ARP for the address 2.1.1.100 on interface ge-0/0/0.0. This allows the Juniper Networks security device to respond to ARP requests received on the interface for that address.
- Security policies to permit traffic from the untrust zone to the translated destination IP address in the trust zone.

This topic includes the following sections:

Configuring Destination Address Translation to a Single Host

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them in a text file, remove any line breaks, change any details necessary to match your network configuration, and paste the commands into the CLI at the **[edit]** hierarchy level of your device.

Configuration in ScreenOS

```
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
```

Configuration in Junos OS

```
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
```

Step-by-Step Procedure

To configure destination address translation to a single host:

1. Configure proxy ARP.

   ```
   [edit]
   user@host# set security nat proxy-arp interface ge-0/0/0.0 address 2.1.1.100
   ```

2. Create destination NAT pools.

   ```
   [edit]
   user@host# set security nat destination pool dnat-pool-1 address 10.1.1.100
   ```

3. Create a destination NAT rule set.

   ```
   [edit]
   user@host# set security nat destination rule-set dst-nat from zone untrust
   ```

4. Configure a rule that matches packets and translates the destination address to the address in the pool.

   ```
   [edit]
   user@host# set security nat destination rule-set dst-nat rule r1 match
     destination-address 2.1.1.100
   user@host# set security nat destination rule-set dst-nat rule r1 then destination-nat
     pool dnat-pool-1
   ```

5. Configure the address book entry for the trust security zone.

   ```
   [edit]
   user@host# set security zones security-zone trust address-book address webserver
     10.1.1.100
   ```

6. Associate the custom application to a policy.

```
[edit]
user@host# set security policies from-zone untrust to-zone trust policy dst-nat
    match source-address any destination-address webserver application junos-http
user@host# set security policies from-zone untrust to-zone trust policy dst-nat then
    permit
```

Verifying Destination Address Translation to a Single Host Configuration

Purpose Verify the configuration of destination address translation to a single host.

Action From configuration mode, run the following **show** command to verify the configuration:

```
user@host> show security nat destination summary

Total pools: 2
Pool name            Address                          Routing        Port  Total

                    Range                           Instance            Address
dnat-pool-1          10.1.1.100     - 10.1.1.100                     0     1
dnat-pool-2          10.1.1.200     - 10.1.1.200                     0     1

Total rules: 3
Rule name            Rule set       From                               Action
rule1                dst-nat        untrust                            dnat-pool-1
rule2                dst-nat        untrust                            dnat-pool-2
r1                   dst-nat        untrust                            dnat-pool-1
```

Meaning The output displays information about destination NAT configuration. You can verify the following information:

- Rule sets
- Rules
- Address range
- NAT pool
- Port details

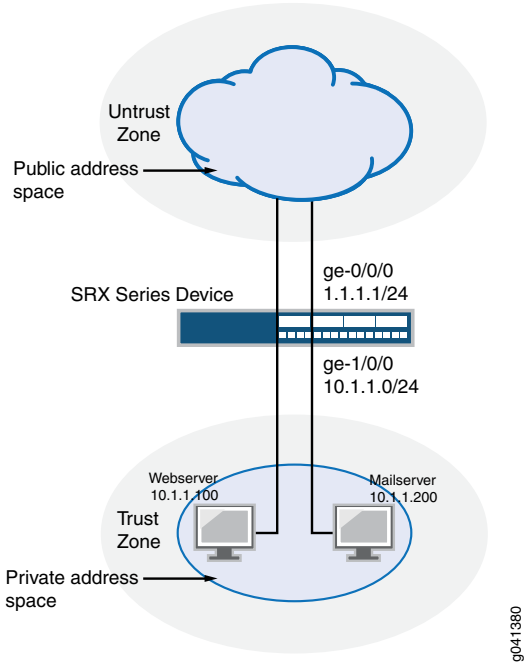
Destination Address and Port Translation to a Single Host

This example describes how to configure destination NAT mappings of a public address to private addresses, depending on the port number. This example uses the trust security zone for the private address space, and the untrust security zone for the public address space.

In Figure 10 on page 31, devices in the untrust zone access servers in the trust zone by way of public address 10.1.1.100 on port 8000. Packets entering the Juniper Networks security device from the untrust zone are mapped to the private addresses of the servers.

The destination IP address 10.1.1.100 and port 8000 are translated to the private address 2.1.1.100 on port 80.

Figure 10: Destination Address and Port Translation to a Single Host Topology



In Table 9 on page 31, the trust security zone is configured for the private address space, and the untrust security zone is configured for the public address space.

Table 9: Interface, Zones, and IP Address Information

Interface	Zone	IP Address
Ethernet 0/0	untrust	1.1.1.1/24
Ethernet 0/1	trust	10.1.1.0/24

This example configures the following:

- Destination NAT pool **dnat-pool-1** that contains the IP address 10.1.1.100 on port 8000.
- Destination NAT rule set **dst-nat** with rule **r1** to match packets received from the ge-0/0/0.0 interface with the destination IP address 2.1.1.100. For matching packets, the destination address is translated to the address in the **dnat-pool-1** pool.
- Proxy ARP for the address 2.1.1.100. This allows the Juniper Networks security device to respond to ARP requests received on the interface for that address.
- Security policies to permit traffic from the untrust zone to the translated destination IP addresses in the trust zone.
- Address book entry **webserver 10.1.1.100** and a custom application **http-8000** using TCP port 1500 are created.

This topic includes the following sections:

Configuring Destination Address and Port Translation to a Single Host

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them in a text file, remove any line breaks, change any details necessary to match your network configuration, and paste the commands into the CLI at the **[edit]** hierarchy level of your device.

Configuration in ScreenOS

```
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
```

Configuration in Junos OS

```
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
```

Step-by-Step Procedure

To configure the destination address and port translation to a single host:

1. Configure proxy ARP.

   ```
   [edit]
   user@host# set security nat proxy-arp interface ge-0/0/0.0 address 2.1.1.100
   ```

2. Create destination NAT pools.

   ```
   [edit]
   user@host# set security nat destination pool dnat-pool-1 address 10.1.1.100 port
     8000
   ```

3. Create a destination NAT rule set.

   ```
   [edit]
   user@host# set security nat destination rule-set dst-nat from zone untrust
   ```

4. Configure a rule that matches packets and translates the destination address to the address in the pool.

   ```
   [edit]
   user@host# set security nat destination rule-set dst-nat rule r1 match
     destination-address 2.1.1.100
   user@host# set security nat destination rule-set dst-nat rule r1 then destination-nat
     pool dnat-pool-1
   ```

5. Configure the address book entry for the trust security zone.

   ```
   [edit]
   ```

```
user@host# set security zones security-zone trust address-book address webserver
  10.1.1.100
```

6. Configure a custom application.

```
[edit]
user@host# set applications application http-8000 protocol tcp destination-port
  8000
```

7. Associate the custom application to a policy.

```
[edit]
user@host# set security policies from-zone untrust to-zone trust policy dst-nat
  match source-address any destination-address webserver application http-8000
user@host# set security policies from-zone untrust to-zone trust policy dst-nat then
  permit
```

Verifying Destination Address and Port Translation to a Single Host Configuration

Purpose Verify the configuration of destination address and port translation to a single host.

Action From configuration mode, run the following **show** command to verify the configuration:

```
user@host> show security nat destination summary

Total pools: 2
Pool name            Address                          Routing        Port  Total

                    Range                           Instance            Address
dnat-pool-1          10.1.1.100     - 10.1.1.100                     8000  1
dnat-pool-2          10.1.1.200     - 10.1.1.200                     0     1

Total rules: 3
Rule name            Rule set       From                               Action
rule1                dst-nat        untrust                            dnat-pool-1
rule2                dst-nat        untrust                            dnat-pool-2
r1                   dst-nat        untrust                            dnat-pool-1
```

Meaning The output displays information about destination NAT configuration. You can verify the following information:

- Rule sets
- Rules
- Address range
- NAT pool
- Port details

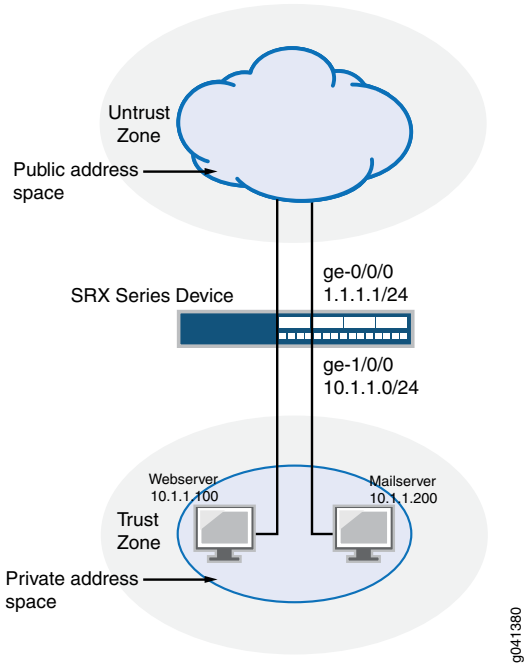
Destination Address Translation to a Single Host

This example describes how to configure NAT proxy ARP entries for IP addresses in the same subnet of the ingress interface. In this example, the destination IP address and the interface IP address are on the same subnet.

This example uses the trust security zone for the private address space, and the untrust security zone for the public address space.

In Figure 11 on page 34, devices in the untrust zone access a server in the trust zone by using public address 1.1.1.100. For packets that enter the security device from the untrust zone with the destination IP address 1.1.1.100, the destination IP address is translated to the private address 10.1.1.100/32.

Figure 11: Destination Address Translation to a Single Host Topology



In Table 10 on page 34, the trust security zone is configured for the private address space, and the untrust security zone is configured for the public address space.

Table 10: Interface, Zones, and IP Address Information

Interface	Zone	IP Address
Ethernet 0/0	untrust	1.1.1.1/24
Ethernet 0/1	trust	10.1.1.0/24

This example configures the following:

- Destination NAT pool **dnat-pool-1** that contains the IP address 10.1.1.100/32.
- Destination NAT rule set **dst-nat** with rule **r1** to match packets received from the ge-0/0/0.0 interface with the destination IP address 1.1.1.100. For matching packets, the destination address is translated to the address in the **dnat-pool-1** pool.

- Proxy ARP for the address 1.1.1.100 on interface ge-0/0/0.0. This allows the Juniper Networks security device to respond to ARP requests received on the interface for that address.
- Security policies to permit traffic from the untrust zone to the translated destination IP address in the trust zone.

This topic includes the following sections:

Configuring Destination Address Translation to a Single Host

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them in a text file, remove any line breaks, change any details necessary to match your network configuration, and paste the commands into the CLI at the **[edit]** hierarchy level of your device.

Configuration in ScreenOS

```
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
```

Configuration in Junos OS

```
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
```

Step-by-Step Procedure

To configure destination address translation to a single host:

1. Create the destination NAT pool.

   ```
   [edit]
   user@host# set security nat destination pool dnat-pool-1 address 10.1.1.100/32
   ```

2. Configure proxy ARP.

   ```
   [edit]
   user@host# set security nat proxy-arp interface ge-0/0/0.0 address 1.1.1.100
   ```

3. Create a destination NAT rule set.

   ```
   [edit]
   user@host# set security nat destination rule-set dst-nat from zone untrust
   ```

4. Configure a rule that matches packets and translates the destination address to the address in the pool.

   ```
   [edit]
   user@host# set security nat destination rule-set dst-nat rule r1 match
     destination-address 1.1.1.100
   user@host# set security nat destination rule-set dst-nat rule r1 then destination-nat
     pool dnat-pool-1
   ```

5. Configure a security policy that allows traffic from the untrust zone to the server in the trust zone.

```
[edit]
user@host# set security policies from-zone untrust to-zone trust policy dst-nat
    match source-address any destination-address any application junos-http
user@host# set security policies from-zone untrust to-zone trust policy dst-nat then
    permit
```

Verifying Destination Address Translation to a Single Host Configuration

Purpose Verify the configuration of destination address translation to a single host.

Action From configuration mode, run the following **show** command to verify the configuration:

```
user@host> show security nat destination summary

Total pools: 2
Pool name            Address                          Routing        Port  Total

                    Range                           Instance            Address
dnat-pool-1          10.1.1.100     - 10.1.1.100                     8000  1
dnat-pool-2          10.1.1.200     - 10.1.1.200                     0     1

Total rules: 3
Rule name            Rule set       From                               Action
rule1                dst-nat        untrust                            dnat-pool-1
rule2                dst-nat        untrust                            dnat-pool-2
r1                   dst-nat        untrust                            dnat-pool-1
```

Meaning The output displays information about destination NAT configuration. You can verify the following information:

- Rule sets
- Rules
- Address range
- NAT pool
- Port details

Related Documentation

- Advantages of Using Junos OS SRX Series and J Series Devices on page 1
- Understanding NAT on SRX Series and J Series Devices on page 2