

Chapter 19

Configure Network Address Translation Services

To configure Network Address Translation (NAT) services, you include statements at the [edit services] hierarchy level of the configuration:

```
[edit services]
nat {
  pool nat-pool-name {
    address (address | address-range low minimum-value high maximum-value);
    port (automatic | range low minimum-value high maximum-value);
  }
  rule rule-name {
    match-direction (input | output);
    term term-name {
      from {
        applications [ application-names ];
        application-sets [ set-names ];
        destination-address address;
        source-address address;
      }
      then {
        translated {
          destination-pool nat-pool-name;
          source-pool nat-pool-name;
          translation-type (destination type | source type);
        }
        syslog;
      }
    }
  }
  rule-set rule-set-name {
    [ rule rule-names ];
  }
}
```



Note

JUNOS software uses stateful firewall settings as a basis for performing NAT. You must commit a stateful firewall configuration in the same service set for NAT to function properly.

This chapter includes the following sections:

Configure Network Address Translation Properties on page 228

Example: Configure Network Address Translation Properties on page 232

Configure Network Address Translation Properties

This section describes the following tasks for configuring network address translation services:

Configure Address and Port Information on page 228

Configure the NAT Rule Set on page 229

Configure Rule Content on page 230

Configure Address and Port Information

The pool statement defines the address and port used for network address translation. To configure the address information, include the pool statement at the [edit services nat] hierarchy level:

```
[edit services nat]
pool nat-pool-name {
  address (address | address-range low minimum-value high maximum-value);
  port (automatic | range low minimum-value high maximum-value);
}
```

You can specify either a single specific address, a prefix, or an address range. To specify translated addresses, configure the pool statement with an identifier and include the address statement with the address, prefix, or range used in network address translation. You must configure either a specific address value or the address-range boundaries:

If you specify a specific address, it is assumed the translated address belongs to the inet.0 routing instance. The following addresses cannot be used:

```
0.0.0.0/32
127.0.0.0/8 (loopback)
224.0.0.0/4 (multicast)
240.0.0.0/4 (reserved)
255.255.255.255 (broadcast)
```

To specify an address range, include the address address-range low *minimum-value* high *maximum-value* statement at the [edit services nat pool *nat-pool-name*] hierarchy level. The low value must be a lower number than the high value. Address ranges are limited to a maximum of 32 addresses.

The port statement specifies port assignment for the translated addresses. To configure automatic assignment of ports, include the port automatic statement at the [edit services nat pool *nat-pool-name*] hierarchy level. To configure a specific range of port numbers, include the port range low *minimum-value* high *maximum-value* statement at the [edit services nat pool *nat-pool-name*] hierarchy level.

**Note**

When you include a NAT configuration that changes IP addresses, it might affect forwarding-path features elsewhere in your router configuration, such as source class usage (SCU), destination class usage (DCU), filter-based forwarding, or other features that target specific IP addresses or prefixes.

NAT configuration might also affect routing protocols operation, because the protocol peering, neighbor, and interface addresses can be altered when routing protocols packets transit the AS PIC.

Configure the NAT Rule Set

The rule-set statement defines a collection of NAT rules that determine what actions the router software performs on packets in the data stream. You define each rule by specifying a rule name and configuring terms. Then, you specify the order of the rules by including the rule-set statement at the [edit services nat] hierarchy level:

```
[edit services nat]
rule-set rule-set-name {
  rule rule-name1;
  rule rule-name2;
  rule rule-name3;
  ...
}
```

The router software processes the rules in the order in which you specify them in the configuration. If a term in a rule matches the packet, the router performs the corresponding action and the rule processing stops. If no term in a rule matches the packet, processing continues to the next rule in the rule set. If none of the rules matches the packet, the packet is dropped by default.

**Note**

After NAT processing is applied to packets, they are not subject to output service filters. The service filters affect only untranslated traffic.

Configure Rule Content

To configure a NAT rule, include the rule *rule-name* statement at the [edit services nat] hierarchy level:

```
[edit services nat]
rule rule-name {
  match-direction (input | output);
  term term-name {
    from {
      applications [ application-names ];
      application-sets [ set-names ];
      destination-address address;
      source-address address;
    }
    then {
      syslog;
      translated {
        destination-pool nat-pool-name;
        source-pool nat-pool-name;
        translation-type (destination type | source type);
      }
    }
  }
}
```

Each NAT rule consists of a set of terms, similar to a firewall filter. A term consists of the following:

from statement—Specifies the match conditions and applications that are included and excluded.

then statement—Specifies the actions and action modifiers to be performed by the router software.

In addition, each rule includes a match-direction statement that specifies the direction in which the match is applied. To configure where the match is applied, include the match-direction (input | output) statement at the [edit services nat rule *rule-name*] hierarchy level:

```
[edit services nat]
rule rule-name {
  match-direction (input | output);
}
```

Configure Match Conditions

To configure NAT match conditions, include the from statement at the [edit services nat rule *rule-name* term *term-name*] hierarchy level:

```
[edit services nat rule rule-name term term-name]
from {
  applications [ application-names ];
  application-sets [ set-names ];
  destination-address address;
  source-address address;
}
```

You can use either the source address or the destination address as a match condition, in the same way that you would configure a firewall filter; for more information, see the *JUNOS Internet Software Configuration Guide: Policy Framework*.

You can also include application protocol definitions you have configured at the [edit applications] hierarchy level; for more information, see “Configure Applications” on page 39.

To apply one or more specific application protocol definitions, include the applications statement at the [edit services nat rule *rule-name* term *term-name* from] hierarchy level.

To apply one or more sets of application protocol definitions you have defined, include the application-sets statement at the [edit services nat rule *rule-name* term *term-name* from] hierarchy level.



Note

If you include one of the statements that specifies application protocols, the router derives port and protocol information from the corresponding configuration at the [edit applications] hierarchy level; you cannot specify these properties as match conditions.

Configure Actions

To configure NAT actions, include the then statement at the [edit services nat rule *rule-name* term *term-name*] hierarchy level:

```
[edit services nat rule rule-name term term-name]
then {
  syslog;
  translated {
    destination-pool nat-pool-name;
    source-pool nat-pool-name;
    translation-type (destination type | source type);
  }
}
```

To record an alert in the system logging facility, include the syslog statement at the [edit services nat rule *rule-name* term *term-name* then] hierarchy level:

```
[edit services nat rule rule-name term term-name then]
syslog;
```

To configure NAT-specific actions for handling packets, include the translated statement at the [edit services nat rule *rule-name* term *term-name* then] hierarchy level:

```
[edit services nat rule rule-name term term-name then]
translated {
  destination-pool nat-pool-name;
  source-pool nat-pool-name;
  translation-type (destination type | source type);
}
```

The source-pool and destination-pool statements specify addressing information you define by including the pool statement at the [edit services nat] hierarchy level; for more information, see “Configure Address and Port Information” on page 228.

The translation-type statement specifies what type of network address translation is used for source or destination traffic:

destination static—Implement address translation for destination traffic without port mapping. This requires the size of the source address space to be the same as the size of the destination address space. You must specify a destination-pool name. The referenced pool must contain exactly one address and no port configuration.

source dynamic—Implement address translation for source traffic with port translation (NAPT). You must specify a source-pool name. The referenced pool must include a port configuration.

source static—Implement address translation for source traffic without port mapping. This requires the size of the source address space to be the same as the size of the destination address space. You must specify a source-pool name. The referenced pool must contain exactly one address and no port configuration.

You can configure either translation-type destination or translation-type source, but not both.

For more information on NAT methods, see RFC 2663, *IP Network Address Translator (NAT) Terminology and Considerations*.

Example: Configure Network Address Translation Properties

The following example configures an address pool containing a specified range and dynamic source translation.

```
[edit services]
nat {
  pool public {
    address-range low 112.148.2.1 high 112.148.2.32;
    port automatic;
  }
  rule Private-Public {
    match-direction input;
    term Translate {
      then {
        translated {
          source-pool public;
          translation-type source dynamic;
        }
      }
    }
  }
}
```

The following NAT service configuration includes two terms. term1 configures source address translation for traffic from any private to any public address. The translation is applied for all services. term2 performs destination address translation for HTTP traffic from any public address to the server's virtual IP address. The virtual server IP address is translated to an internal IP address.

```
[edit services nat]
rule my-nat-rule {
  match-direction input;
  term my-term1 {
    from {
      source-address private;
      destination-address public;
    }
    then {
      translated {
        source-pool my-prefix-list; # pick address from a pool
        translation-type source dynamic; # dynamic NAT functionality with port translation
      }
    }
  }
  term my-term2 {
    from {
      destination-address 202.1.137.3; # my server's virtual address
      application http;
    }
    then {
      translated {
        destination-address 162.138.3.1; # internal ip address
        translation-type destination static; # static destination NAT
      }
    }
  }
}
```

