VYATTA, INC. | Vyatta System

NAT

REFERENCE GUIDE

NAT

Vyatta
Suite 200
1301 Shoreway Road
Belmont, CA 94002
vyatta.com
650 413 7200
1 888 VYATTA 1 (US and Canada)

COPYRIGHT

PROPRIETARY NOTICES

RELEASE DATE: March 2012

DOCUMENT REVISION. R6.4 v01

RELEASED WITH: R6.4.0

PART NO. A0-0230-10-0011

Contents

Quick List of Commands

Use this list to help you quickly locate commands.

List of Examples

Use this list to help you locate examples you'd like to look at or try.

Preface

This document describes the various deployment, installation, and upgrade options for Vyatta software.

This preface provides information about using this guide. The following topics are presented:

- Intended Audience
- Organization of This Guide
- Document Conventions
- Vyatta Publications

Intended Audience

This guide is intended for experienced system and network administrators. Depending on the functionality to be used, readers should have specific knowledge in the following areas:

- Networking and data communications
- TCP/IP protocols
- General router configuration
- Routing protocols
- Network administration
- Network security
- IP services

Organization of This Guide

This guide has the following aid to help you find the information you are looking for:

- Quick List of Commands

  Use this list to help you quickly locate commands.

- List of Examples

  Use this list to help you locate examples you'd like to try or look at.

This guide has the following chapters:

Document Conventions

This guide uses the following advisory paragraphs, as follows.

WARNING *Warnings alert you to situations that may pose a threat to personal safety.*

CAUTION *Cautions alert you to situations that might cause harm to your system or damage to equipment, or that may affect service.*

NOTE *Notes provide information you might need to avoid problems or configuration errors.*

This document uses the following typographic conventions.

`Monospace`	Examples, command-line output, and representations of configuration nodes.
`bold Monospace`	Your input: something you type at a command line.
bold	Commands, keywords, and file names, when mentioned inline. Objects in the user interface, such as tabs, buttons, screens, and panes.
italics	An argument or variable where you supply a value.
<key>	A key on your keyboard, such as <Enter>. Combinations of keys are joined by plus signs ("+"), as in <Ctrl>+c.
[key1 | key2]	Enumerated options for completing a syntax. An example is [enable | disable].
num1–numN	A inclusive range of numbers. An example is 1–65535, which means 1 through 65535, inclusive.
arg1..argN	A range of enumerated values. An example is eth0..eth3, which means eth0, eth1, eth2, or eth3.
arg[*arg*...] *arg*[,*arg*...]	A value that can optionally represent a list of elements (a space-separated list and a comma-separated list, respectively).

Vyatta Publications

Full product documentation is provided in the Vyatta technical library. To see what documentation is available for your release, see the *Guide to Vyatta Documentation*. This guide is posted with every release of Vyatta software and provides a great starting point for finding the information you need.

Additional information is available on www.vyatta.com and www.vyatta.org.

Chapter 1: NAT Overview

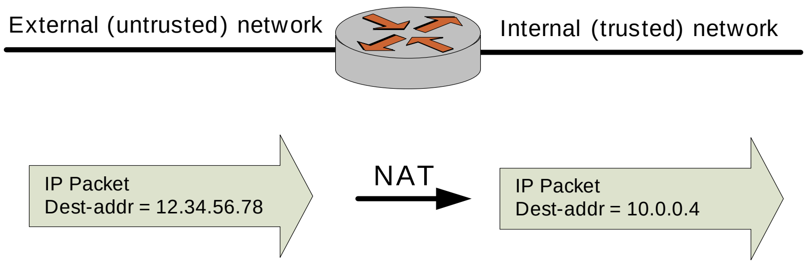
This chapter explains how to set up network address translation (NAT) on the Vyatta System.

This chapter presents the following topics:

What is NAT?

Network Address Translation (NAT) is a service that modifies address and/or port information within network packets as they pass through a computer or network device. The device performing NAT on the packets can be the source of the packets, the destination of the packets, or an intermediate device on the path between the source and destination devices.

Figure 1-1 An example of a device performing Network Address Translation (NAT)



NAT was originally designed to help conserve the number of IP addresses used by the growing number of devices accessing the Internet, but it also has important applications in network security.

The computers on an internal network can use any of the addresses set aside by the Internet Assigned Numbers Authority (IANA) for private addressing (see also RFC 1918). These reserved IP addresses are not in use on the Internet, so an external machine will not directly route to them. The following addresses are reserved for private use:

- 10.0.0.0 to 10.255.255.255 (CIDR: 10.0.0.0/8)
- 172.16.0.0 to 172.31.255.255 (CIDR: 172.16.0.0/12)
- 192.168.0.0 to 192.168.255.255 (CIDR: 192.268.0.0/16)

To this end a NAT-enabled router can hide the IP addresses of an internal network from the external network, by replacing the internal, private IP addresses with public IP addresses that have been provided to it. These public IP addresses are the only addresses that are ever exposed to the external network. The router can manage a pool of multiple public IP addresses, from which it can dynamically choose when performing address replacement.

Be aware that, although NAT can minimize the possibility that internal computers make unsafe connections to the external network, it provides no protection to a computer that, for one reason or another, connects to an untrusted machine. Therefore, you should always combine NAT with packet filtering and other features of a complete security policy to fully protect your network.

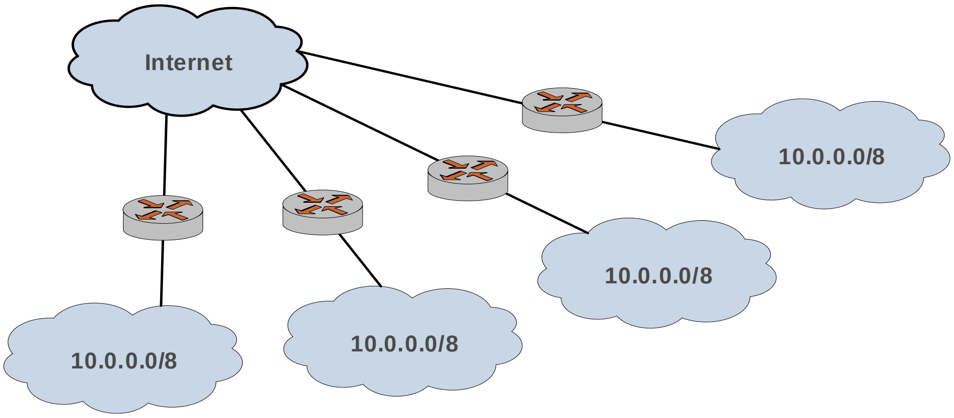
Benefits of NAT

NAT confers several advantages:

- NAT conserves public Internet address space.

  Any number of hosts within a local network can use private IP addresses, instead of consuming public IP addresses. The addresses of packets that are transmitted from this network to the public Internet are translated to the appropriate public IP address. This means that the same private IP address space can be re-used within any number of private networks, as shown in Reusing private address space Figure 1-2.

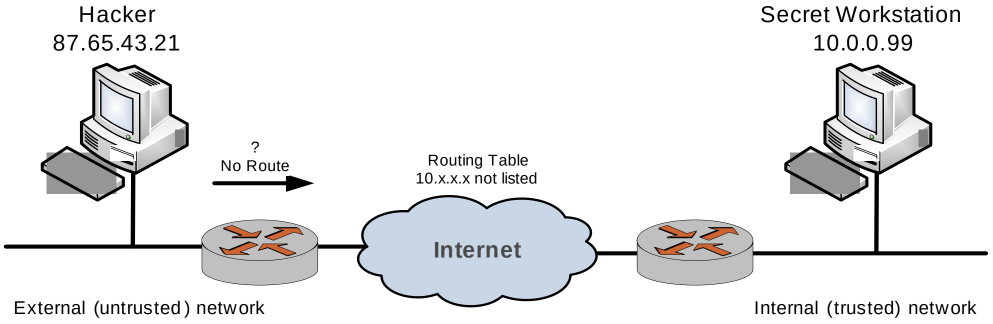
Figure 1-2 Reusing private address space



- NAT enhances security.

  IP addresses within a private (internal) network are hidden from the public (external) network. This makes it more difficult for hackers to initiate an attack on an internal host. However, private network hosts are still vulnerable to attack, and therefore NAT is typically combined with firewall functionality.

Figure 1-3 NAT combined with firewall



- NAT is seamless.

  Standard client/server network services work without modification through a NAT-enabled device.

- NAT facilitates network migration from one address space to another.

  The address space within a NATted private network is independent of the public IP address. This means that the private network can be moved to a new public IP address without changing network configurations within the private network. Likewise, the addressing within the private network can change without affecting the public IP address.

- NAT simplifies routing.

  NAT reduces the need to implement more complicated routing schemes within larger local networks.

Types of NAT

There are three main types of NAT:

- Source NAT. This is also called SNAT. “Masquerade” NAT is a special type of SNAT.
- Destination NAT. This is also called DNAT.
- Bidirectional NAT. When both SNAT and DNAT are configured, the result is bidirectional NAT.

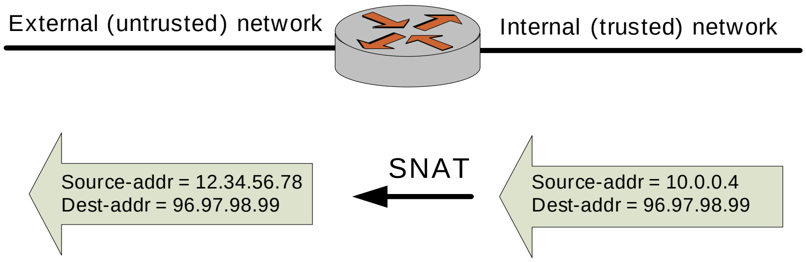
Source NAT (SNAT)

Tip: SNAT is performed after the routing decision is made.

SNAT is the most common form of NAT. SNAT changes the source address of the packets passing through the Vyatta system. SNAT is typically used when an internal (private) host needs to initiate a session to an external (public) host; in this case, the NATting device changes the source host's private IP address to some public IP address, as shown in Figure 1-4. In "masquerade" NAT (a common type of SNAT), the source address of the outgoing packet is replaced with the primary IP address of the outbound interface. The destination address of return packets is automatically translated back to the source host's IP address.

The NATting device tracks information about the traffic flow so that traffic from the flow can be correctly forwarded to and from the source host.

Figure 1-4 Source NAT (SNAT)

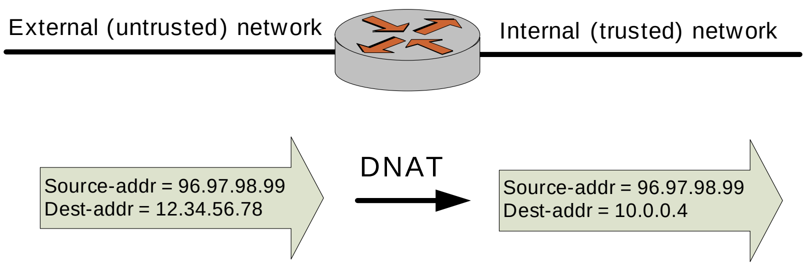

External (untrusted) network
Internal (trusted) network
Source-addr = 12.34.56.78
Dest-addr = 96.97.98.99
SNAT
Source-addr = 10.0.0.4
Dest-addr = 96.97.98.99

Destination NAT (DNAT)

Tip: DNAT is performed before the routing decision is made.

While SNAT changes the source address of packets, DNAT changes the destination address of packets passing through the Vyatta system. DNAT is typically used when an external (public) host needs to initiate a session with an internal (private) host; for example, when a subscriber accesses a news service, as shown in Figure 1-5. The source address of return packets is automatically translated back to the source host's IP address.

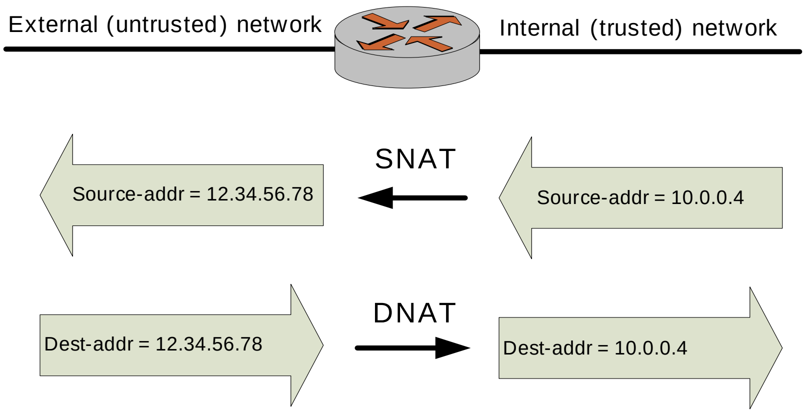
Figure 1-5 Destination NAT (DNAT)


External (untrusted) network
Internal (trusted) network
Source-addr = 96.97.98.99
Dest-addr = 12.34.56.78
DNAT
Source-addr = 96.97.98.99
Dest-addr = 10.0.0.4

Bidirectional NAT

Bidirectional NAT is just a scenario where both SNAT and DNAT are configured at the same time. Bidirectional NAT is typically used when internal hosts need to initiate sessions with external hosts AND external hosts need to initiate sessions with internal hosts. Figure 1-6 shows an example of bidirectional NAT.

Figure 1-6 Bidirectional NAT


External (untrusted) network
Internal (trusted) network
Source-addr = 12.34.56.78
SNAT
Source-addr = 10.0.0.4
Dest-addr = 12.34.56.78
DNAT
Dest-addr = 10.0.0.4

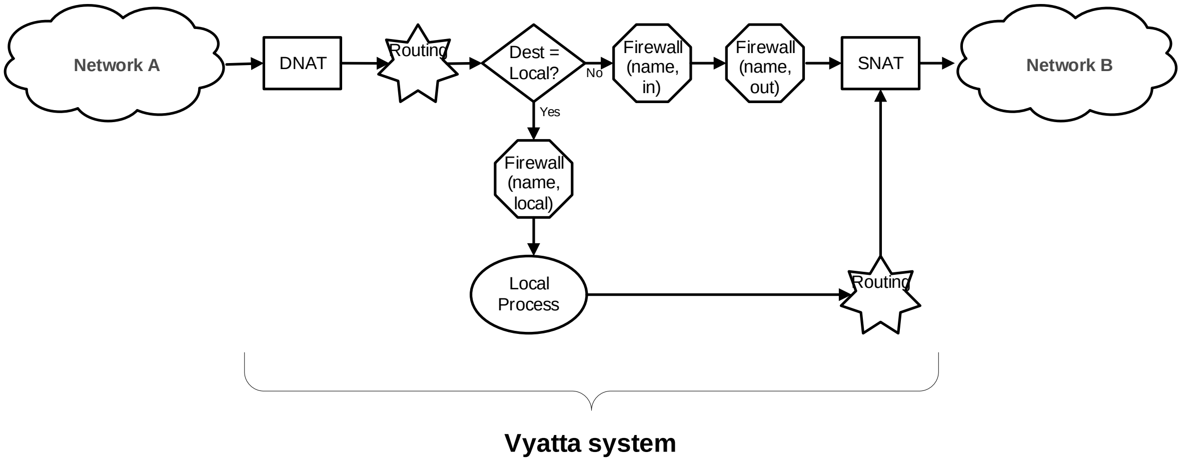
Interaction Between NAT, Routing, Firewall, and DNS

One of the most important things to understand when working with NAT is the processing order of the various services that might be configured within the Vyatta system. If processing order is not considered, the results achieved may not be as intended.

For example, if you are using DNAT you should take care not to set up the system to route packets based on particular external addresses. This routing method would not have the intended result, because the addresses of external packets would have all been changed to internal addresses by DNAT prior to routing.

Figure 1-7 shows the traffic flow relationships between NAT, routing, and firewall within the Vyatta system.

Figure 1-7 Traffic flows through the Vyatta system



Interaction Between NAT and Routing

When considering NAT in relation to routing, it is important to be aware how routing decisions are made with respect to DNAT and SNAT. The scenarios in this section illustrate this point.

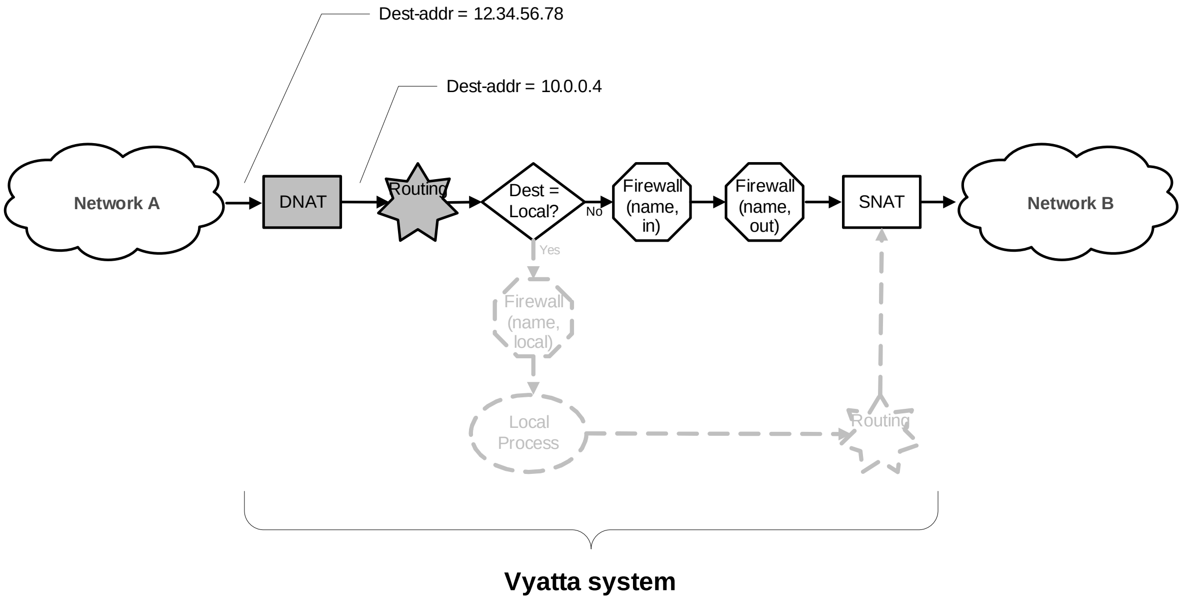
Scenario 1a: DNAT—Packets Passing Through the Vyatta System

In this scenario, packets are originated in Network A and pass through the Vyatta system. Note the following:

Tip: *DNAT—routing decisions are based on translated destination address.*

DNAT operates on the packets *prior* to the routing decision. This means that routing decisions based on the destination address are made relative to the *translated* destination address—*not* the original destination address; see Figure 1-8.

Figure 1-8 Pass-through DNAT routing decisions

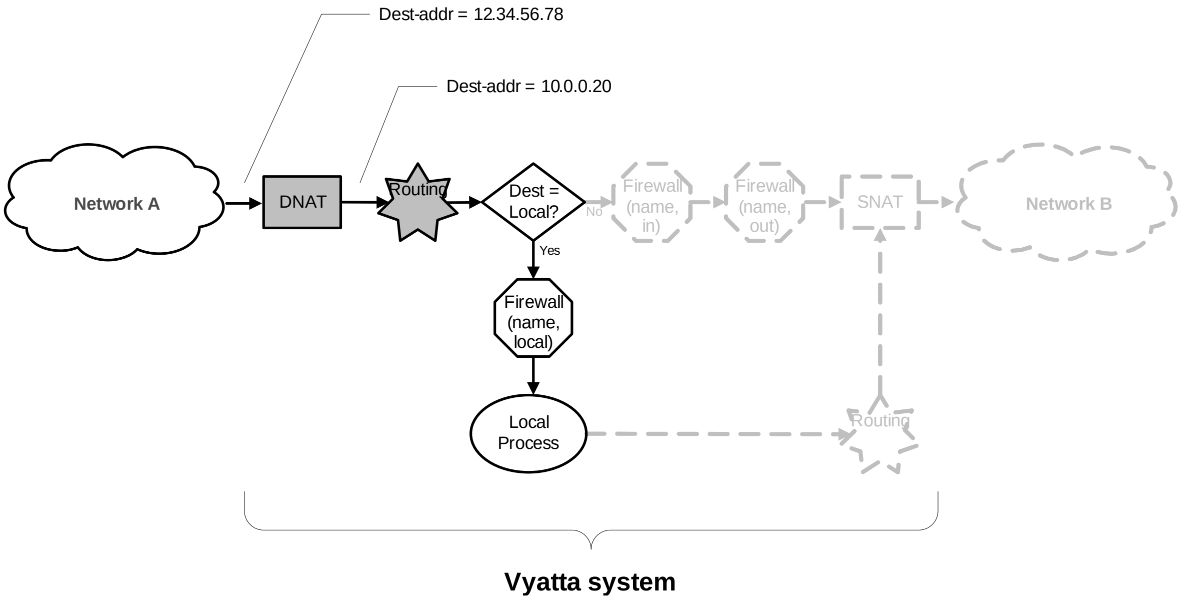


Scenario 1b: DNAT—Packets Destined for the Vyatta System

The same is true for packets destined for the Vyatta system itself. In this scenario, packets are destined for a process within the Vyatta system.

Again, because DNAT operates on the packets *prior* to the routing decision, routing decisions based on destination address are made on the *translated* destination address—*not* the original destination address; see Figure 1-9.

Figure 1-9 Vyatta system-destined DNAT routing decisions

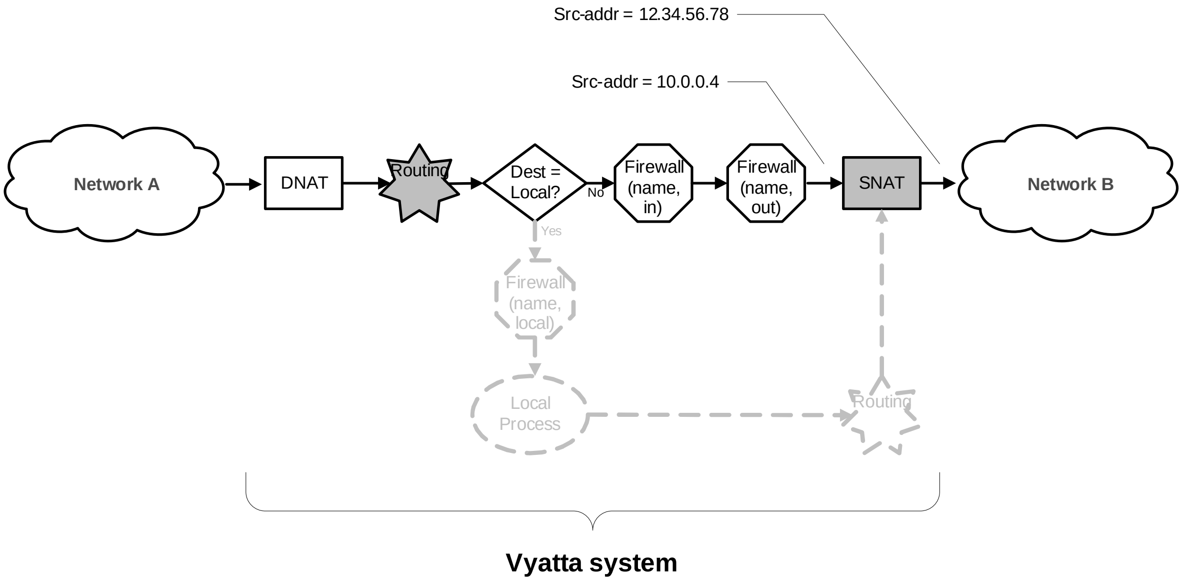


Scenario 2a: SNAT—Packets Passing Through the Vyatta System

Tip: *SNAT routing decisions are based on original source address.*

On the other hand, routing decisions are made *prior* to SNAT. This means that routing decisions based on source address are made on the *original* source address—*not* the translated source address; see Figure 1-10.

Figure 1-10 Pass-through SNAT routing decisions

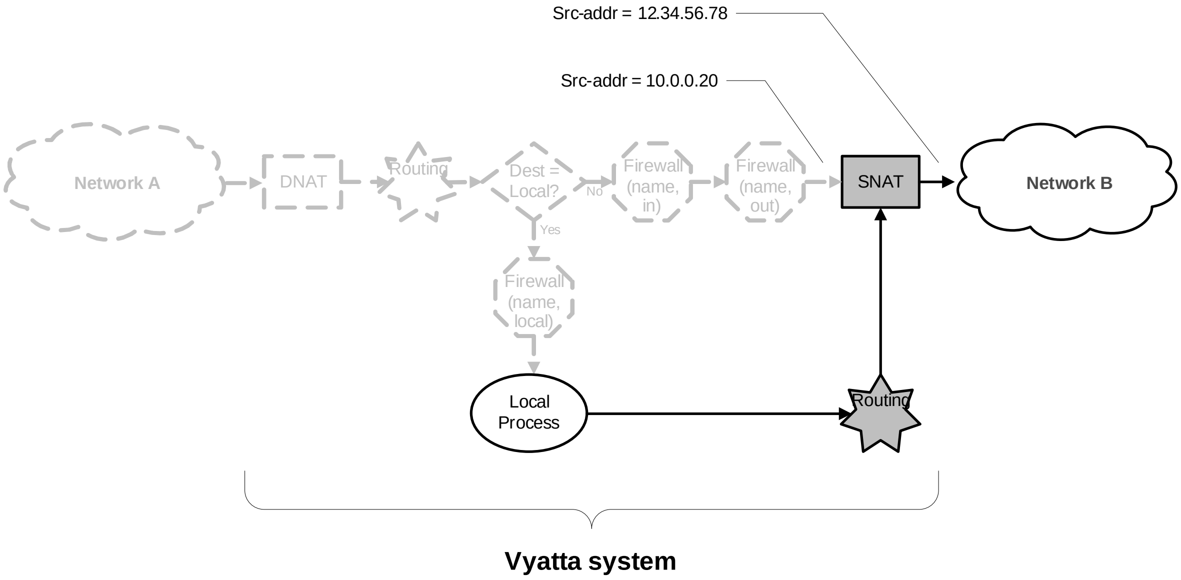


Scenario 2b: SNAT—Packets Originating From the Vyatta System

In this scenario, packets are originated by a process within the Vyatta system.

Again, because routing decisions are made prior to SNAT, operations based on source address are made on the *original* source *address*—*not* the translated source address; see Figure 1-11.

Figure 1-11 Vyatta system-originated SNAT routing decisions



Interaction Between NAT and Firewall

When considering NAT in relation to the firewall, it is important to understand the traffic flow relationship between NAT and firewall. In particular, it is important to keep in mind that firewall rule sets are evaluated at different points in the traffic flow. The scenarios in this section illustrate this point.

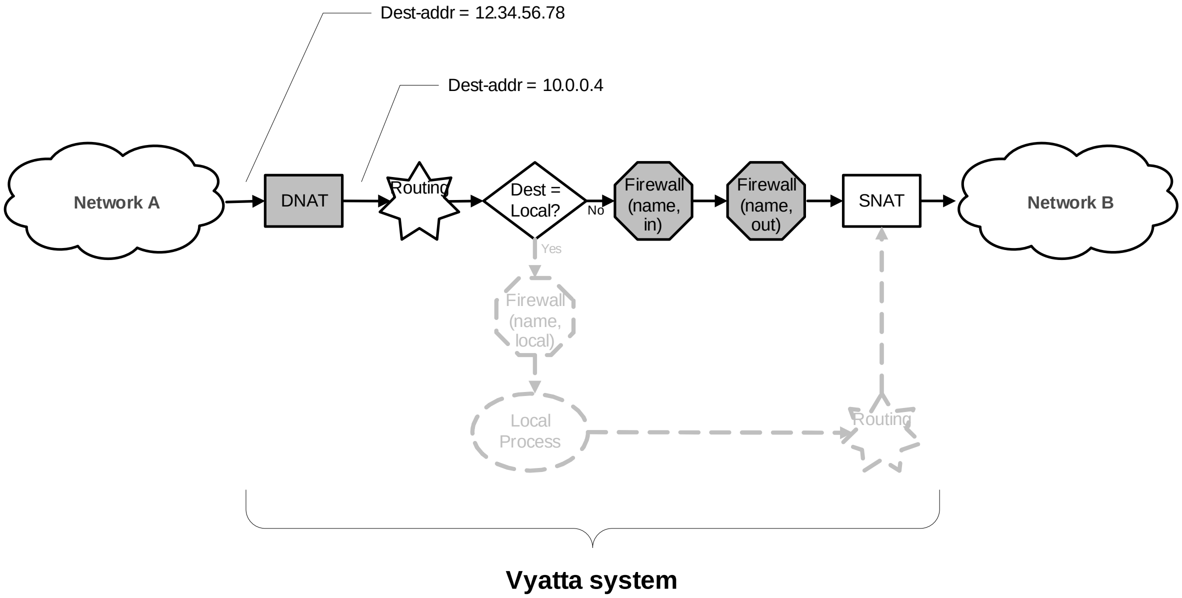
Scenario 1a: DNAT—Packets Passing Through the Vyatta System

In this scenario, packets are originated in Network A and pass through the Vyatta system. Note the following:

For firewall rule sets applied to inbound packets on an interface, the firewall rules are applied *after* DNAT (that is, on the *translated* destination address).

For rule sets applied to outbound packets on an interface, the firewall rules are applied *after* DNAT (that is, on the *translated* destination address); see Figure 1-12.

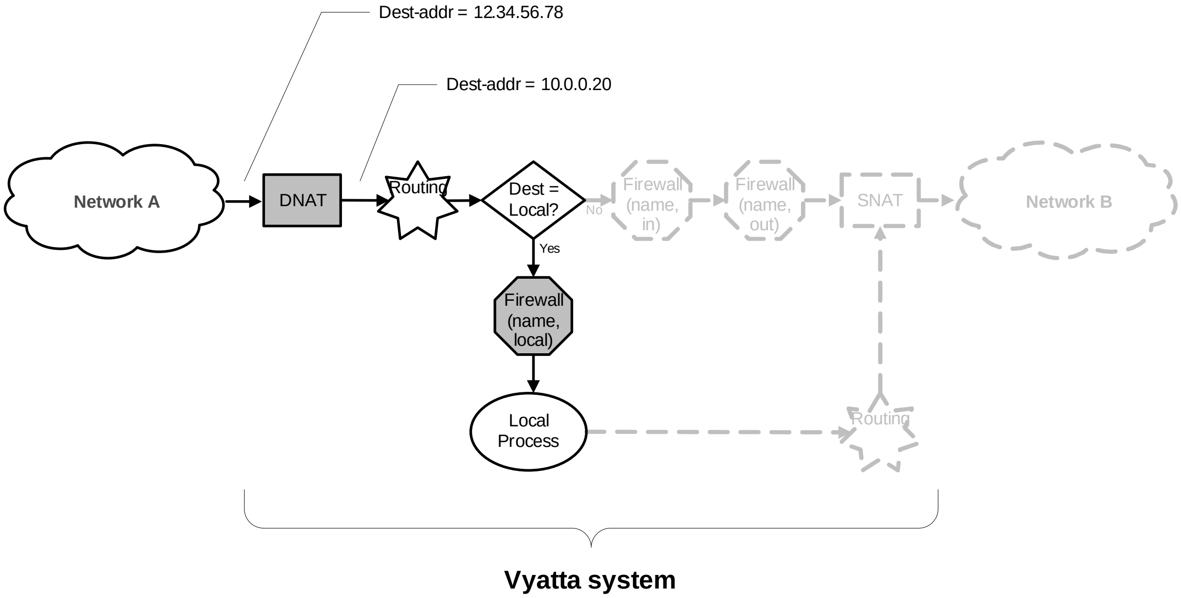
Figure 1-12 Pass-through DNAT firewall decisions



Scenario 1b: DNAT—Packets Destined for the Vyatta System

In this scenario, packets are destined for a process within the Vyatta system. When firewall rule sets are applied to locally bound packets on an interface, the firewall rules are applied *after* DNAT (that is, on the *translated* destination address); see Figure 1-13.

Figure 1-13 Vyatta system-destined DNAT firewall decisions

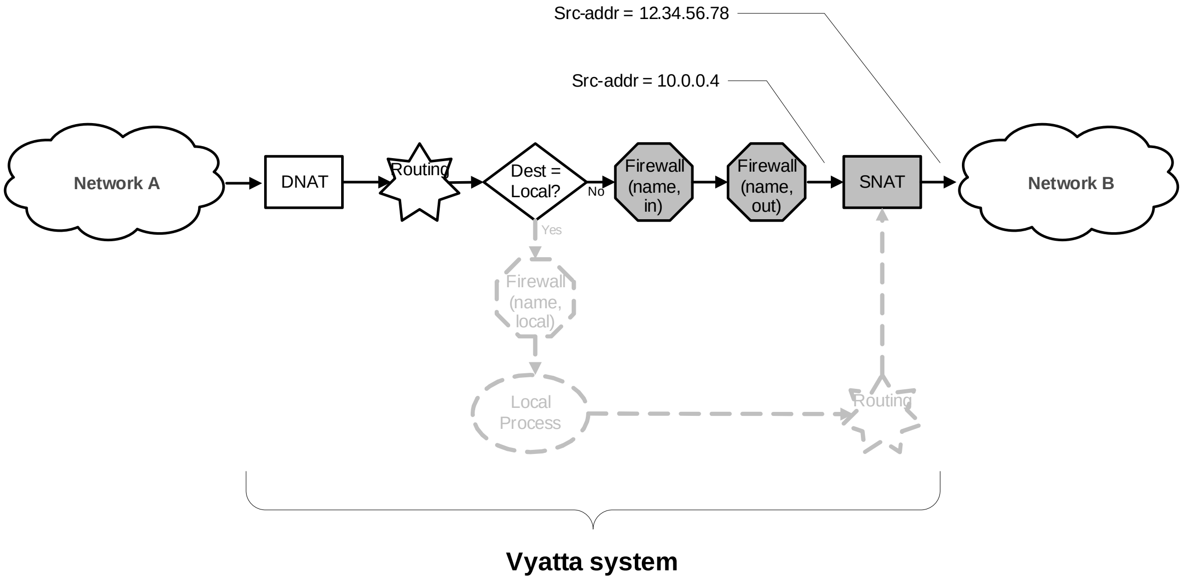


Scenario 2a: SNAT—Packets Passing Through the Vyatta System

***Tip:** SNAT firewall rules are applied on original source address.*

Firewall rules are applied *prior* to SNAT. This means that firewall decisions based on source address are made on the *original* source address—*not* the translated source address. This order of evaluation is true for both inbound and outbound packets; see Figure 1-14.

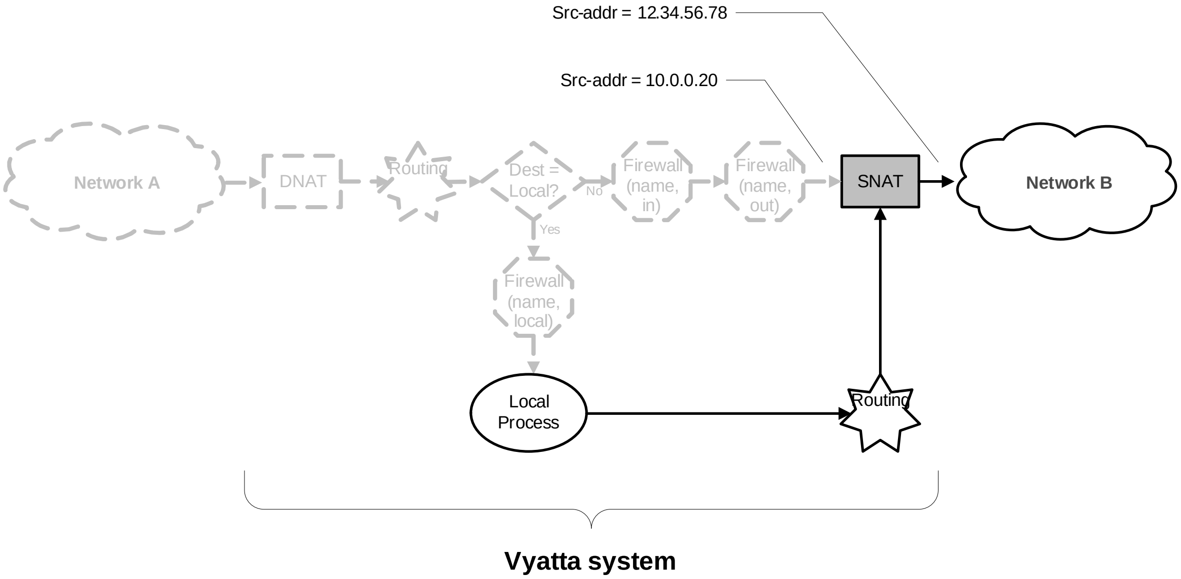
Figure 1-14 Pass-through SNAT firewall decisions



Scenario 2b: SNAT—Packets Originating From the Vyatta System

In this scenario, packets are originated by a process within the Vyatta system. Firewall rule sets are not involved.

Figure 1-15 Vyatta system-originated SNAT firewall decisions



Interaction Between NAT and DNS

NAT and DNS can be combined in various scenarios involving load balancing. These can include additional load-balancing switches that operate at higher protocol layers (Layers 4 through 7). For example, a large bank may have many web servers with transactions load-balanced across them.

In these cases the NAT configuration must be carefully considered to achieve the desired results. Discussion of DNS and load-balancing scenarios is beyond the scope of this chapter.

NAT Rules

NAT is configured as series of NAT “rules”. Each rule instructs NAT to perform a network address translation that you require. NAT rules are numbered, and are evaluated in numerical order. The NAT rule number can be changed using the **rename** and **copy** commands.

NOTE *Changes to NAT rules affect only connections established after the changes are made. Those connections that are already established at the time a change is made are not affected.*

Tip: *Leave a gap between NAT rule numbers.*

It is advisable to create your NAT rules leaving “space” between the numbers. For example, you might initially create your set of NAT rules numbered 10, 20, 30, and 40. This way, if you need to insert a new rule later on, and you want it to execute in a particular sequence, you can insert it between existing rules without having to change any other rules.

The Vyatta system allows you to configure **source** NAT (SNAT), or **destination** NAT rules. To implement bidirectional NAT, you define a NAT rule for SNAT and one for DNAT. Example 1-1 defines an SNAT rule 10.

Example 1-1 Creating a source NAT (SNAT) rule

```
vyatta@vyatta#set nat source rule 10
```

Traffic Filters

Filters control which packets will have the NAT rules applied to them. There are five different filters that can be applied within a NAT rule: **outbound-interface**, **inbound-interface**, **protocol**, **source**, and **destination**.

The “outbound-interface” Filter

The **outbound-interface** filter is applicable only to **source** NAT (SNAT) rules. It specifies the outbound traffic flow that the NAT translation is to be applied to. Example 1-2 sets SNAT rule 20 to apply a NAT translation to outbound traffic on interface eth1.

Example 1-2 Setting the outbound interface

```
vyatta@vyatta#set nat source rule 20 outbound-interface eth1
```

The “inbound-interface” Filter

The **inbound-interface** filter is applicable only to **destination** NAT (DNAT) rules. It specifies the inbound traffic flow that the NAT translation is to be applied to. Example 1-3 sets DNAT rule 20 to apply NAT rules to inbound traffic on interface eth0.

Example 1-3 Setting the inbound interface

```
vyatta@vyatta#set nat destination rule 20 inbound-interface eth0
```

The “protocol” Filter

The **protocol** filter specifies which protocol types the NAT translation will be applied to. Only packets of the specified protocol are NATted. The default is **all** protocols. The **protocol** filter can be used in SNAT and DNAT rules.

Example 1-4 sets SNAT rule 10 to apply to TCP protocol packets. Only TCP packets will have address translation performed.

Example 1-4 Filtering packets by protocol

```
vyatta@vyatta#set nat source rule 10 protocol tcp
```

The “source” Filter

The **source** filter specifies which packets the NAT translation will be applied to, based on their source address and/or port. Only packets with a source address and/or port matching that defined in the filter are NATted.

If the **source** filter is not specified, then by default, the rule matches packets arriving from any source address and port. The **source** filter can be used in SNAT and DNAT rules.

Example 1-5 sets SNAT rule 10 to apply to packets with a source address of 10.0.0.4. Only packets with a source address of 10.0.0.4 will have address translation performed.

Example 1-5 Filtering packets by source address

```
vyatta@vyatta#set nat source rule 10 source address 10.0.0.4
```

Example 1-6 sets SNAT rule 20 to apply to packets with a source network of 10.0.0.0/24 and port 80. Only packets with a source address on the 10.0.0.0/24 subnet with a source port of 80 will have address translation performed.

Example 1-6 Filtering packets by source network address and port

```
vyatta@vyatta#set nat source rule 20 source address 10.0.0.0/24
vyatta@vyatta#set nat source rule 20 source port 80
```

The “destination” Filter

The **destination** filter specifies which packets the NAT translation will be applied to, based on their destination address and/or port. Only packets with a destination address and/or port matching that defined in the filter are NATted.

If the **destination** filter is not specified, then by default, the rule matches packets sent to any destination address and port. The **destination** filter can be used in SNAT and DNAT rules.

Example 1-7 sets SNAT rule 30 to apply to packets with a destination address of 12.34.56.78. Only packets with a destination address of 12.34.56.78 will have address translation performed.

Example 1-7 Filtering packets by destination address

```
vyatta@vyatta#set nat source rule 30 destination address 12.34.56.78
```

Address Conversion: “Translation” Addresses

The **translation** address defines the address conversion that takes place. It specifies the information that is substituted into the packet for the original address.

Source Address Translations

SNAT rules substitute the packet’s source address with the **translation** address. Port translation is also available and can be specified as part of the translation address.

Note that the **translation** address *must* either be set to one of the addresses defined on the outbound interface or set to **masquerade**, indicating that the primary IP address of the outbound interface is to be used as the translation address.

Example 1-8 sets rule 10 to substitute 12.34.56.78 as the source IP address of outbound packets matching its filter criteria.

Example 1-8 Setting a source IP address

```
vyatta@vyatta#set nat source rule 10 translation address 12.34.56.78
```

Example 1-9 sets rule 20 to substitute addresses 12.34.56.64 through 12.34.56.79 as the source IP addresses of outbound packets that match its filter criteria.

Example 1-9 Setting a range of source IP addresses

```
vyatta@vyatta#set nat source rule 20 translation address
12.34.56.64-12.34.56.79
```

Example 1-10 sets rule 30 to substitute the primary address of the outbound interface as the source IP address of outbound packets that match its filter criteria.

Example 1-10 Setting a source IP address to that of the outbound interface

```
vyatta@vyatta#set nat source rule 30 translation address masquerade
```

Destination Address Translations

DNAT rules substitute the packet’s destination address with the **translation** address. Port translation is also available and can be specified as part of the translation address.

Example 1-11 sets rule 40 to substitute 10.0.0.4 as the destination IP address of inbound packets matching its filter criteria.

Example 1-11 Setting a destination IP address

```
vyatta@vyatta#set nat destination rule 40 translation address 10.0.0.4
```

Example 1-12 sets rule 50 to substitute addresses 10.0.0.0 through 10.0.0.3 as the range of destination IP addresses for inbound packets that match its filter criteria.

Example 1-12 Setting a range of destination IP addresses

```
vyatta@vyatta#set nat destination rule 50 translation address
10.0.0.0-10.0.0.3
```

Chapter 2: NAT Configuration Examples

This chapter provides configuration examples for using network address translation (NAT) on the Vyatta system.

NOTE *Each NAT rule in these examples could be independently deployed on a system. These examples are not intended to be deployed together. For that reason, all rules in the examples are given the same rule number (Rule 10).*

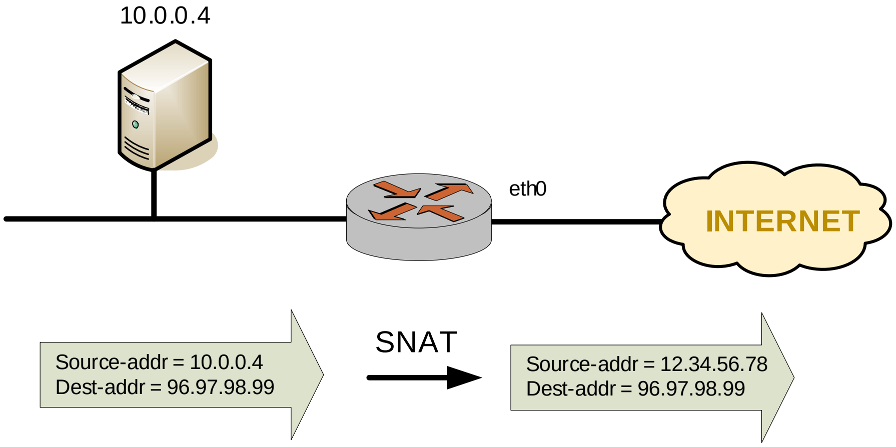
This chapter presents the following topics:

Source NAT (One-to-One)

Figure 2-1 shows an example of source NAT (SNAT) where a single “inside” source address is translated to a single “outside” source address. In this example:

- An internal news server (an NNTP device) needs to connect to an external news server.
- The external news server accepts connections only from known clients.
- The internal news server does not receive connections from outside the local network.

Figure 2-1 Source NAT (one-to-one)



To configure NAT in this way, perform the following steps in configuration mode.

Example 2-1 Source NAT (one-to-one)

Step	Command
Create Rule 10. Rule 10 is an SNAT rule.	`vyatta@vyatta# set nat source rule 10`

Apply this rule to packets coming from address 10.0.0.4 and egressing through interface eth0.	`vyatta@vyatta# set nat source rule 10 source address 10.0.0.4`
	`vyatta@vyatta# set nat source rule 10 outbound-interface eth0`

Example 2-1 Source NAT (one-to-one)

Use 12.34.56.78 as the source address in outgoing packets. Make sure that the translation address is one of the addresses defined on the outbound interface if it is part of the connected subnet on that interface. This ensures that the Vyatta system replies to ARP requests from remote devices for the translation address.

```
vyatta@vyatta# set nat source rule 10 translation address
12.34.56.78
```

Commit the change.

```
vyatta@vyatta# commit
```

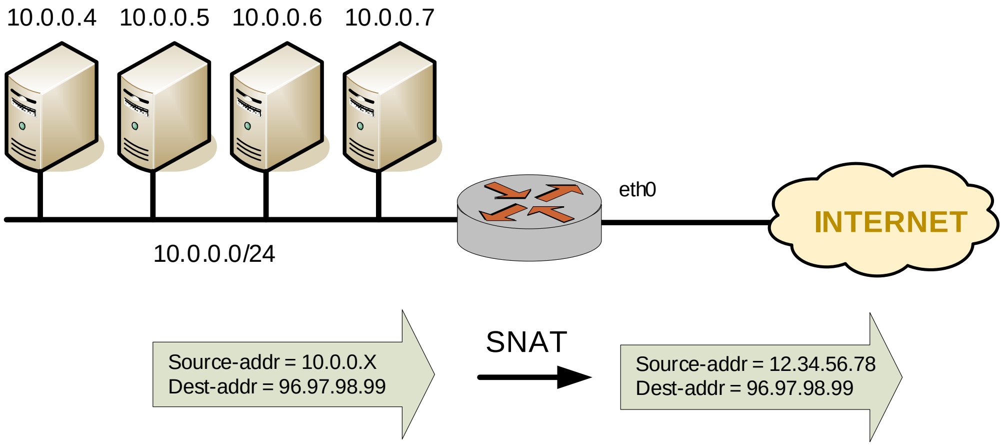
Show the configuration.

```
vyatta@vyatta# show nat source rule 10
   outbound-interface eth0
   source {
       address 10.0.0.4
   }
   translation {
       address 12.34.56.78
   }
```

Source NAT (Many-to-One)

Figure 2-2 shows an example of SNAT where many different “inside” addresses are dynamically translated to a single “outside” address. In this example, all hosts on the 10.0.0.0/24 subnet will show the same source address externally.

Figure 2-2 Source NAT (many-to-one)



To configure NAT in this way, perform the following steps in configuration mode.

Example 2-2 Source NAT (many-to-one)

Step	Command
Create Rule 10. Rule 10 is an SNAT rule.	`vyatta@vyatta# set nat source rule 10`

Apply this rule to packets coming from any host on network 10.0.0.0/24 and egressing through interface eth0.	`vyatta@vyatta# set nat source rule 10 source address 10.0.0.0/24`
	`vyatta@vyatta# set nat source rule 10 outbound-interface eth0`

Use 12.34.56.78 as the source address in outgoing packets. Make sure that the translation address is one of the addresses defined on the outbound interface if it is part of the connected subnet on that interface. This ensures that the Vyatta system replies to ARP requests from remote devices for the translation address.	`vyatta@vyatta# set nat source rule 10 translation address 12.34.56.78`
Commit the change.	`vyatta@vyatta# commit`

Example 2-2 Source NAT (many-to-one)

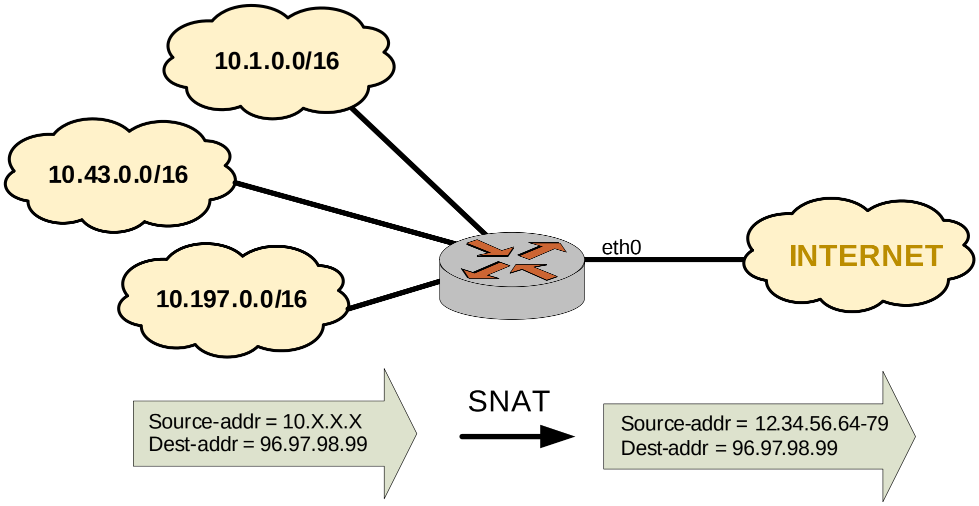
Show the configuration.

```
vyatta@vyatta# show nat source rule 10
    outbound-interface eth0
    source {
         address 10.0.0.0/24
    }
    translation {
         address 12.34.56.78
    }
```

Source NAT (Many-to-Many)

In many-to-many translations, a number of private addresses are mapped to a number of public addresses. This provides a way of reducing the possibility of port exhaustions that is possible in a many-to-one scenario. For this reason, it can provide more capacity for outbound translations. Figure 2-3 shows a large private address space (a /8 network prefix, here represented as three /16 subnets) mapped to a small range of external addresses.

Figure 2-3 Source NAT (many-to-many)



To configure NAT in this way, perform the following steps in configuration mode.

Example 2-3 Source NAT (many-to-many)

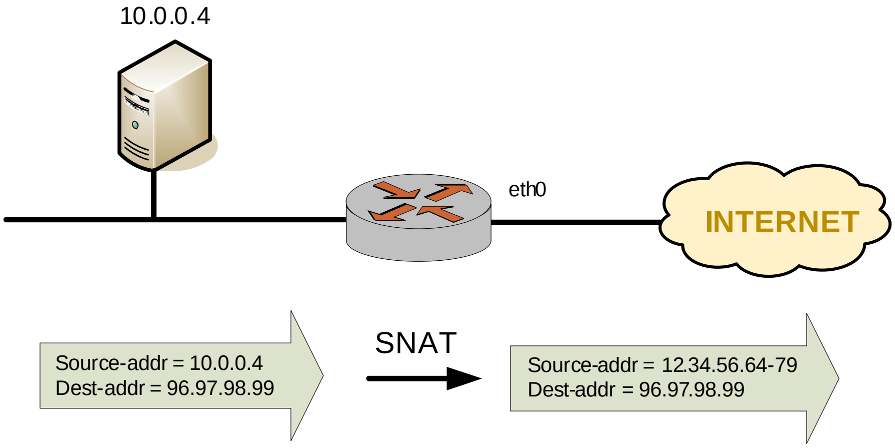
Step	Command
Create Rule 10. Rule 10 is an SNAT rule.	vyatta@vyatta# **set nat source rule 10**
Apply this rule to packets coming from any host on network 10.0.0.0/8 and egressing via interface eth0.	vyatta@vyatta# **set nat source rule 10 source address 10.0.0.0/8** vyatta@vyatta# **set nat source rule 10 outbound-interface eth0**
Choose an address in the range 12.34.56.64 through 12.34.56.79 as the source address in outgoing packets. Note that the translation address should be addresses defined on the outbound interface if it is part of the connected subnet on that interface. This is to ensure that the Vyatta system will reply to ARP requests from remote devices for one of the translation addresses.	vyatta@vyatta# **set nat source rule 10 translation address 12.34.56.64-12.34.56.79**
Commit the change.	vyatta@vyatta# commit

Show the configuration.	vyatta@vyatta# **show nat source rule 10**
	    outbound-interface eth0
	    source {
	        address 10.0.0.0/8
	    }
	    translation {
	        address 12.34.56.64-12.34.56.79
	    }

Source NAT (One-to-Many)

The scenario described in this section is less common. In this scenario, a single test source device behind the NAT device appears externally to be multiple devices, as shown in Figure 2-4. One application of this scenario might be to test an upstream load-balancing device.

Figure 2-4 Source NAT (one-to-many)



To configure NAT in this way, perform the following steps in configuration mode.

Example 2-4 Source NAT (one-to-many)

Step	Command
Create Rule 10. Rule 10 is an SNAT rule.	`vyatta@vyatta# **set nat source rule 10**`

Apply this rule to packets coming from address 10.0.0.4 and egressing via interface eth0.	`vyatta@vyatta# set nat source rule 10 source address 10.0.0.4`
	`vyatta@vyatta# set nat source rule 10 outbound-interface eth0`

Choose an address in the range 12.34.56.64 through 12.34.56.79 as the source address in outgoing packets. Note that the translation address should be addresses defined on the outbound interface if it is part of the connected subnet on that interface. This is to ensure that the Vyatta system will reply to ARP requests from remote devices for one of the translation addresses.	`vyatta@vyatta# set nat source rule 10 translation address 12.34.56.64-12.34.56.79`
Commit the change.	`vyatta@vyatta# commit`

Example 2-4 Source NAT (one-to-many)

Show the configuration.

```
vyatta@vyatta# show nat source rule 10
   outbound-interface eth0
   source {
      address 10.0.0.4
   }
   translation {
      address 12.34.56.64-12.34.56.79
   }
```

Masquerade

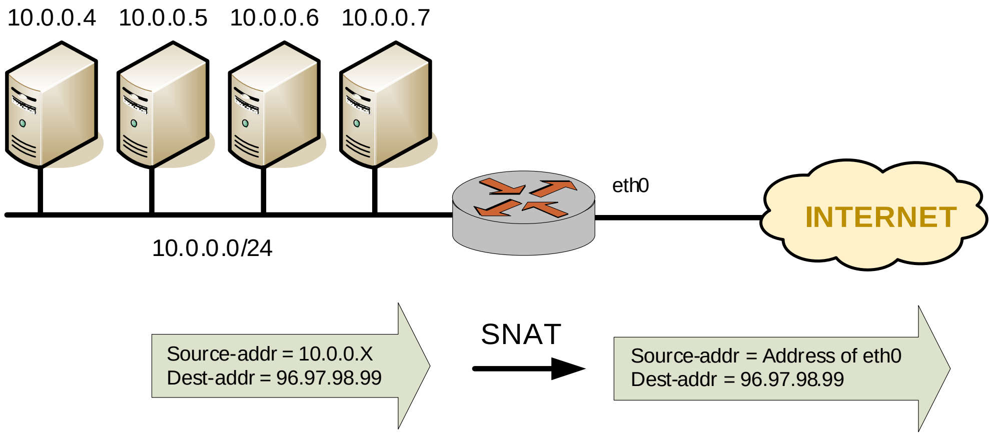
Masquerade NAT is a special case of source NAT. It is typically used in situations where the Internet-facing interface has a dynamic IP address provided by a mechanism such as DHCP. In these cases, configuring a static translation address is not appropriate as the address assigned to the interface can change. Specifying **masquerade** as the the translation address instructs the system to use the IP address currently assigned to the **outbound-interface** as the translation address.

Masquerade NAT rules typically consist of match conditions containing:

- The source network (usually the private IP network assigned to LAN devices)
- The outbound interface (the Internet-facing interface that is assigned the dynmic IP address)

Figure 2-5 shows an example of masquerade NAT.

Figure 2-5 Masquerade



To configure NAT in this way, perform the following steps in configuration mode.

Example 2-5 Masquerade

Step	Command
Create Rule 10. Rule 10 is an SNAT rule.	`vyatta@vyatta# set nat source rule 10`

Apply this rule to packets coming from any host on network 10.0.0.0/24 and egressing via interface eth0.	`vyatta@vyatta# set nat source rule 10 source address 10.0.0.0/24`
	`vyatta@vyatta# set nat source rule 10 outbound-interface eth0`

Use the IP address of the outbound interface as the outside address.	`vyatta@vyatta# set nat source rule 10 translation address masquerade`
Commit the change.	`vyatta@vyatta# commit`

Show the configuration.	`vyatta@vyatta# show nat source rule 10`
	`    outbound-interface eth0`
	`    source {`
	`         address 10.0.0.0/24`
	`    }`
	`    translation {`
	`        address masquerade`
	`    }`

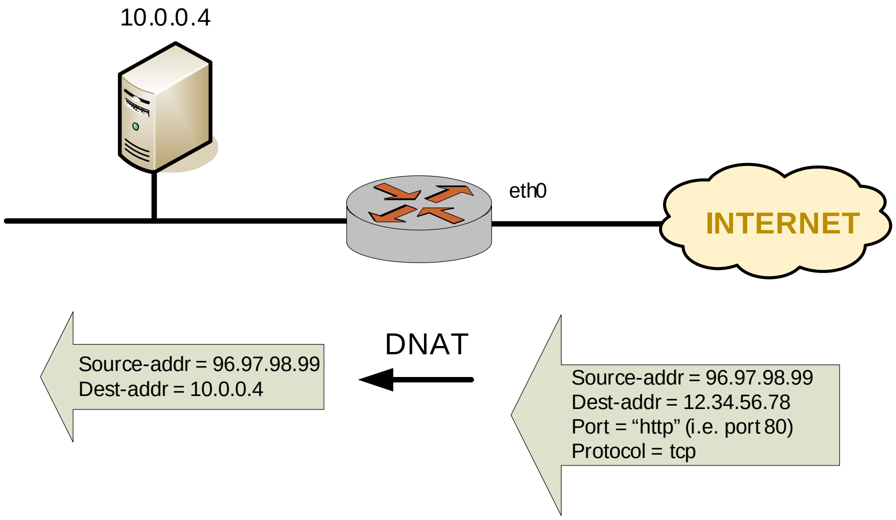
Destination NAT (One-to-One)

Destination NAT (DNAT) is used where only inbound traffic is expected.

Scenario 1: Packets destined for internal web server

For example, DNAT might be used in a scenario where a corporate web server needs to be reachable from external locations but never initiates outbound sessions, as shown in Figure 2-6.

Figure 2-6 Destination NAT (one-to-one)



To configure NAT in this way, perform the following steps in configuration mode.

Example 2-6 Destination NAT (one-to-one)

Step	Command
Create Rule 10. Rule 10 is a DNAT rule.	vyatta@vyatta# **set nat destination rule 10**
Apply this rule to all incoming TCP packets on eth0 bound for address 12.34.56.78 on the HTTP port.	vyatta@vyatta# **set nat destination rule 10 inbound-interface eth0** vyatta@vyatta# **set nat destination rule 10 destination address 12.34.56.78** vyatta@vyatta# **set nat destination rule 10 destination port http** vyatta@vyatta# **set nat destination rule 10 protocol tcp**

Example 2-6 Destination NAT (one-to-one)

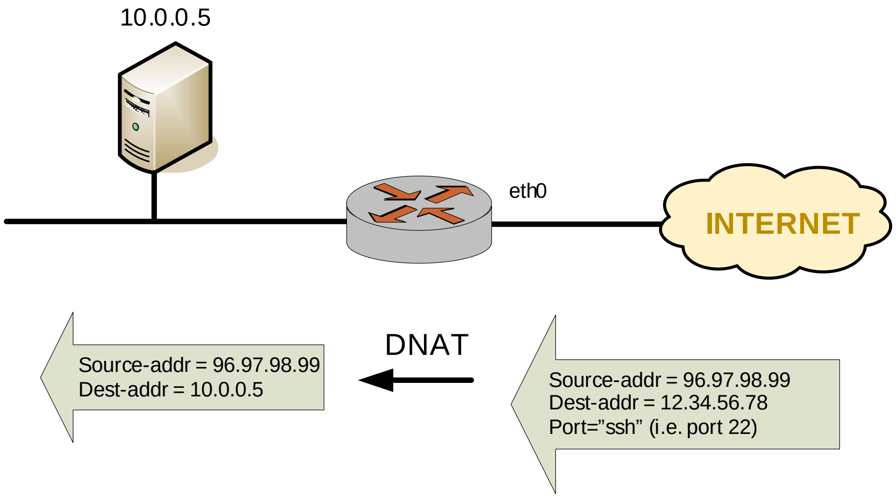
Forward traffic to address 10.0.0.4.	vyatta@vyatta# **set nat destination rule 10 translation address 10.0.0.4**
Commit the change.	vyatta@vyatta# commit

Show the configuration.	vyatta@vyatta# **show nat destination rule 10**
	    destination {
	        address 12.34.56.78
	        port http
	    }
	    inbound-interface eth0
	    protocols tcp
	    translation {
	        address 10.0.0.4
	    }

Scenario 2: Packets destined for an internal SSH server

In this scenario, all traffic destined for the SSH port is passed through to a host containing an SSH server, as shown in Figure 2-7.

Figure 2-7 Destination NAT (one-to-one): filtering on port name


10.0.0.5
eth0
INTERNET
DNAT
Source-addr = 96.97.98.99
Dest-addr = 10.0.0.5
Source-addr = 96.97.98.99
Dest-addr = 12.34.56.78
Port="ssh" (i.e. port 22)

To configure NAT in this way, perform the following steps in configuration mode.

Example 2-7 Destination NAT (one-to-one): filtering port name

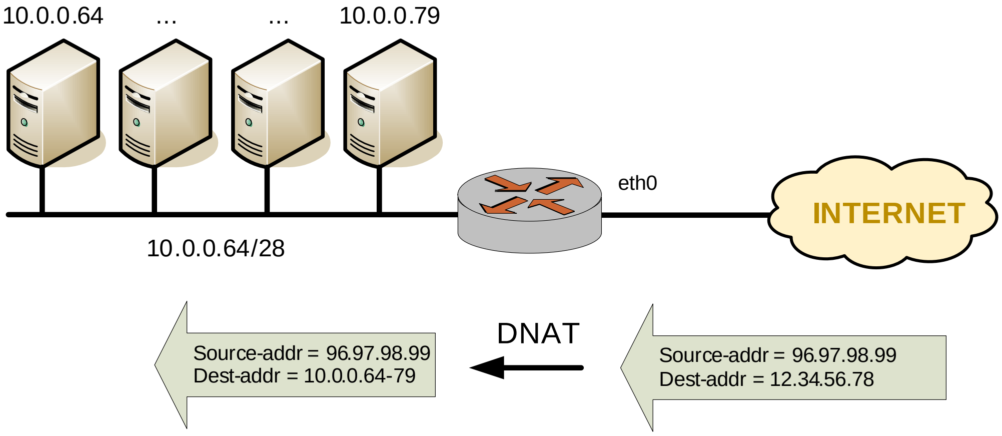
Step	Command
Create Rule 10. Rule 10 is a DNAT rule.	vyatta@vyatta# **set nat destination rule 10**
Apply this rule to all incoming packets on eth0 bound for the SSH port of address 12.34.56.78.	vyatta@vyatta# **set nat destination rule 10 inbound-interface eth0** vyatta@vyatta# **set nat destination rule 10 protocol tcp** vyatta@vyatta# **set nat destination rule 10 destination address 12.34.56.78** vyatta@vyatta# **set nat destination rule 10 destination port ssh**
Forward traffic to address 10.0.0.5.	vyatta@vyatta# **set nat destination rule 10 translation address 10.0.0.5**
Commit the change.	vyatta@vyatta# commit

Show the configuration.	vyatta@vyatta# **show nat destination rule 10**
	    destination {
	        address 12.34.56.78
	        port ssh
	    }
	    inbound-interface eth0
	    protocol tcp
	    translation {
	        address 10.0.0.5
	    }

Destination NAT (One-to-Many)

Another example where DNAT might be used in a scenario where a corporate web farm is accessed through a single IP address. In this case, a single IP address is translated to many IP addresses dynamically, as shown in Figure 2-8.

Figure 2-8 Destination NAT (one-to-many)



To configure NAT in this way, perform the following steps in configuration mode.

Example 2-8 Destination NAT(one-to-many)

Step	Command
Create Rule 10. Rule 10 is a DNAT rule.	`vyatta@vyatta#` **`set nat destination rule 10`**

Apply this rule to all incoming packets on eth0 bound for address 12.34.56.78.	`vyatta@vyatta#` **`set nat destination rule 10 inbound-interface eth0`**
	`vyatta@vyatta#` **`set nat destination rule 10 destination address 12.34.56.78`**

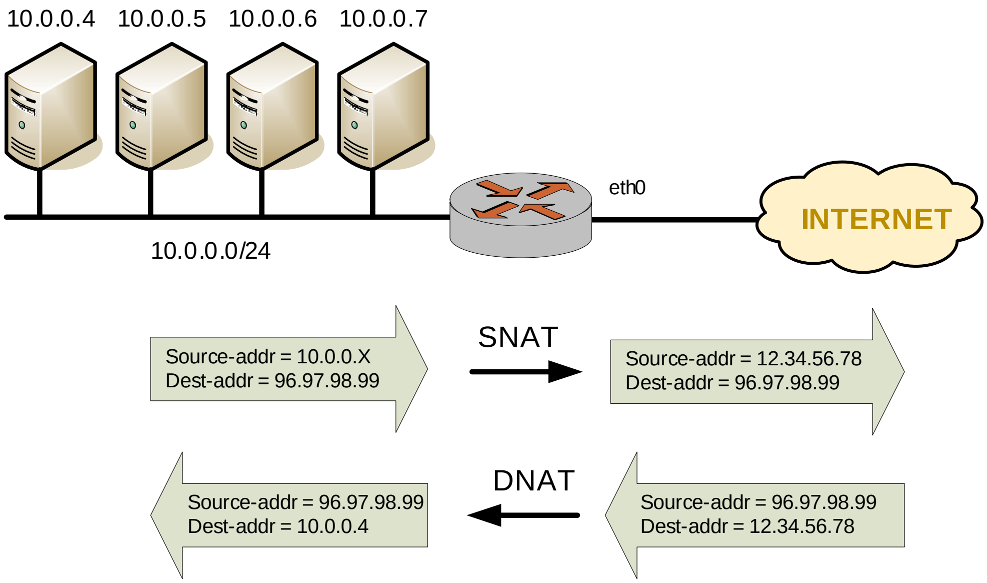
Forward traffic to addresses in the range 10.0.0.64 to 10.0.0.79.	`vyatta@vyatta#` **`set nat destination rule 10 translation address 10.0.0.64-10.0.0.79`**
Commit the change.	`vyatta@vyatta# commit`

Show the configuration.	`vyatta@vyatta#` **`show nat destination rule 10`**
	`destination {`
	`address 12.34.56.78`
	`}`
	`inbound-interface eth0`
	`translation {`
	`address 10.0.0.64-10.0.0.79`
	`}`

Bidirectional NAT

Bidirectional NAT is simply a combination of source and destination NAT. A typical scenario might use SNAT on the outbound traffic of an entire private network, and DNAT for specific internal services (for example, mail or web); see Figure 2-9.

Figure 2-9 Bidirectional NAT



To configure NAT in this way, perform the following steps in configuration mode. Note that source and destination rule numbers are independent. In this example, we highlight this by creating "source rule 10" and "destination rule 10".

Example 2-9 Bidirectional NAT

Step	Command
Create source (SNAT) rule 10.	`vyatta@vyatta# set nat source rule 10`

Apply this rule to packets coming from any host on network 10.0.0.0/24 and egressing via interface eth0.	`vyatta@vyatta# set nat source rule 10 source address 10.0.0.0/24`
	`vyatta@vyatta# set nat source rule 10 outbound-interface eth0`

Use 12.34.56.78 as the source address in outgoing packets.	`vyatta@vyatta# set nat source rule 10 translation address 12.34.56.78`

Example 2-9 Bidirectional NAT

Create destination (DNAT) rule 10.	`vyatta@vyatta# set nat destination rule 10`

Apply this rule to all incoming tcp packets on eth0 bound for address 12.34.56.78, port 80 (i.e. HTTP traffic).	`vyatta@vyatta# set nat rule destination 10 inbound-interface eth0`
	`vyatta@vyatta# set nat destination rule 10 destination address 12.34.56.78`
	`vyatta@vyatta# set nat destination rule 10 destination port 80`
	`vyatta@vyatta# set nat destination rule 10 protocol tcp`

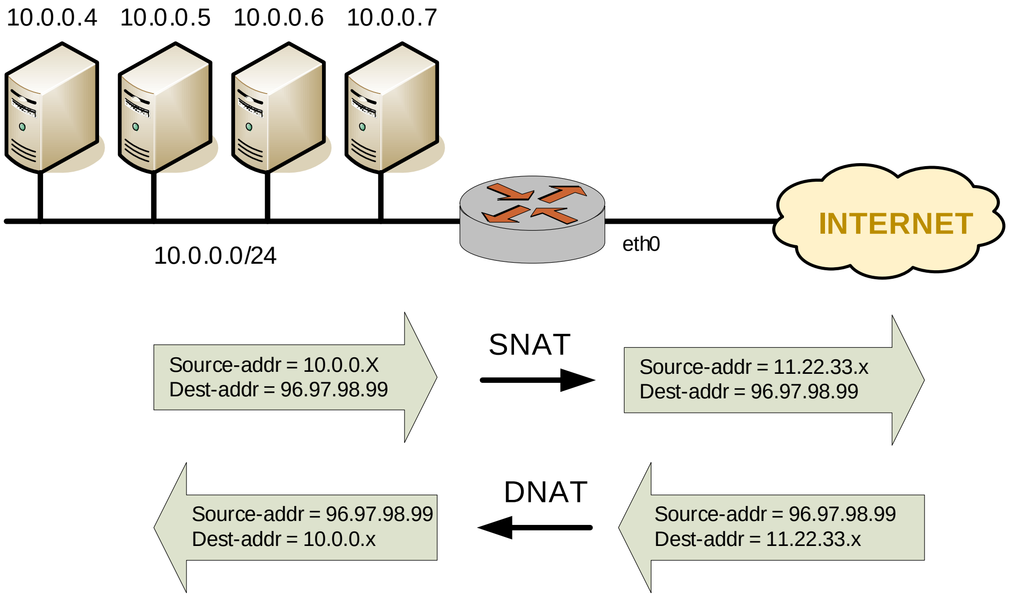
Forward traffic to address 10.0.0.4 (i.e the web server).	`vyatta@vyatta# set nat destination rule 10 translation address 10.0.0.4`
Commit the change.	`vyatta@vyatta# commit`

Show the configuration.	`vyatta@vyatta# show nat source rule 10`
	`    outbound-interface eth0`
	`    source {`
	`        address 10.0.0.0/24`
	`    }`
	`    translation {`
	`        address 12.34.56.78`
	`    }`
	`vyatta@vyatta# show nat destination rule 10`
	`    destination {`
	`        address 12.34.56.78`
	`        port 80`
	`    }`
	`    inbound-interface eth0`
	`    protocol tcp`
	`    translation {`
	`        address 10.0.0.4`
	`    }`

Mapping Address Ranges

The Vyatta system supports mapping an entire network of addresses to another network of addresses. This saves having to manually enter many NAT rules. For example, you can map the network 10.0.0.0/24 to 11.22.33.0/24. This would mean that 10.0.0.1 maps to 11.22.33.1, 10.0.0.2 maps to 11.22.33.2, and so on. The networks must be of the same size (that is, they must have the same network mask), as shown in Figure 2-10.

Figure 2-10 Mapping address ranges



To configure NAT in this way, perform the following steps in configuration mode.

Example 2-10 Mapping address ranges

Step	Command
Create source (SNAT) rule 10.	`vyatta@vyatta# set nat source rule 10`

Apply this rule to packets coming from any host on network 10.0.0.0/24 and egressing via interface eth0.	`vyatta@vyatta# set nat source rule 10 source address 10.0.0.0/24`
	`vyatta@vyatta# set nat source rule 10 outbound-interface eth0`

Use 11.22.33.*x* as the source address in outgoing packets.	`vyatta@vyatta# set nat source rule 10 translation address 11.22.33.0/24`
Create destination (DNAT) rule 10.	`vyatta@vyatta# set nat destination rule 10`

Apply this rule to packets destined for any host on network 11.22.33.0/24 and ingressing via interface eth0.	`vyatta@vyatta# set nat destination rule 10 destination address 11.22.33.0/24`
	`vyatta@vyatta# set nat destination rule 10 inbound-interface eth0`

Use 10.0.0.*x* as the destination address in incoming packets.	`vyatta@vyatta# set nat destination rule 10 translation address 10.0.0.0/24`
Commit the change.	`vyatta@vyatta# commit`

Example 2-10 Mapping address ranges

Show the configuration.

```
vyatta@vyatta# show nat source rule 10
    outbound-interface eth0
    source {
        address 10.0.0.0/24
    }
    translation {
        address 11.22.33.0/24
    }
vyatta@vyatta# show nat destination rule 10
    destination {
        address 11.22.33.0/24
    }
    inbound-interface eth0
    translation {
        address 10.0.0.0/24
    }
```

The “exclude” Option

Sometimes it is desirable to exclude packets from NAT translation that match a certain criteria. This can be accomplished using the **exclude** option.

Example 2-11 uses **exclude** to exclude a subset of traffic (packets coming from 192.168.0.0/24 and destined for 172.16.50.0/24 through interface eth0) from translation. Note that rule 10 is used to exclude certain traffic from translation and rule 20 is used to perform a translation on the traffic that meets its filter criteria and is not excluded by rule 10.

Example 2-11 Source NAT exclusion rule using **exclude**

Step	Command
Create SNAT rule 10.	`vyatta@vyatta# set nat source rule 10`

Apply this rule to packets coming from any host on network 192.168.0.0/24, destined for 172.16.50.0/24, and egressing via interface eth0.	`vyatta@vyatta# set nat source rule 10 source address 192.168.0.0/24`
	`vyatta@vyatta# set nat source rule 10 destination address 172.16.50.0/24`
	`vyatta@vyatta# set nat source rule 10 outbound-interface eth0`

Exclude packets from NAT translation that match the filter criteria in this rule.	`vyatta@vyatta# set nat source rule 10 exclude`

Example 2-11 Source NAT exclusion rule using **exclude**

Create SNAT rule 20.	vyatta@vyatta# **set nat source rule 20**
Apply this rule to packets coming from any host on network 192.168.0.0/24 and egressing via interface eth0.	vyatta@vyatta# **set nat source rule 20 source address 192.168.0.0/24** vyatta@vyatta# **set nat source rule 20 outbound-interface eth0**
Use the primary IP address of the outbound interface as the translation address.	vyatta@vyatta# **set nat source rule 20 translation address masquerade**
Commit the change.	vyatta@vyatta# **commit**
Show the configuration.	vyatta@vyatta# **show nat source**

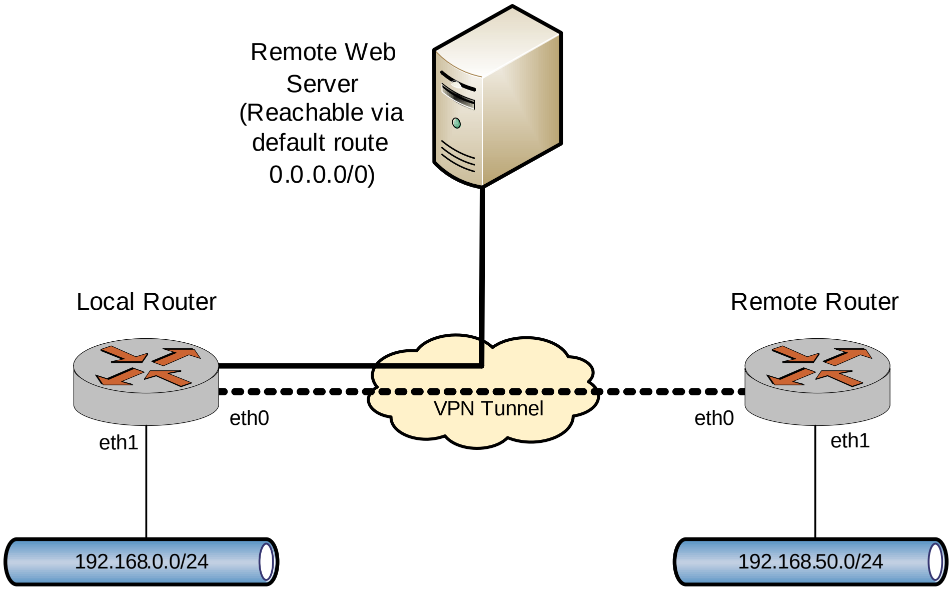
```
rule 10 {
    destination {
        address 172.16.50.0/24
    }
    exclude
    outbound-interface eth0
    source {
        address 192.168.0.0/24
    }
}
rule 20 {
    outbound-interface eth0
    source {
        address 192.168.0.0/24
    }
    translation {
        address masquerade
    }
}
```

Source NAT and VPN: Using the “exclude” Option

When a packet is matched against the source NAT (including masquerade NAT) filter criteria, the source address of the packet is modified before it is forwarded to its destination. This means that source NAT rules are applied before the VPN process compares the packets against the VPN configuration. If the source network configured for source NAT is also configured to use a site-to-site VPN connection using the same externally facing interface, the packets will not be recognized by the VPN process, since the source address has been changed. Consequently, they will not be placed into the VPN tunnel for transport.

To account for this behavior, packets destined for a VPN tunnel must be excluded from having NAT applied. You can do this by using an exclusion rule, as shown in Figure 2-11.

Figure 2-11 Source NAT and VPN



To configure NAT in this way, perform the following steps in configuration mode.

Example 2-12 Masquerade NAT configured to bypass a VPN tunnel

Step	Command
Create SNAT rule 10.	vyatta@vyatta# **set nat source rule 10**
Apply this rule to packets coming from any host on network 192.168.0.0/24, going to 192.168.50.0/24, and egressing via interface eth0.	vyatta@vyatta# **set nat source rule 10 source address 192.168.0.0/24** vyatta@vyatta# **set nat source rule 10 destination address 192.168.50.0/24** vyatta@vyatta# **set nat source rule 10 outbound-interface eth0**
Exclude packets from NAT translation that match the filter criteria in this rule.	vyatta@vyatta# **set nat source rule 10 exclude**
Create SNAT rule 20.	vyatta@vyatta# **set nat source rule 20**

Example 2-12 Masquerade NAT configured to bypass a VPN tunnel

Apply this rule to packets coming from any host on network 192.168.0.0/24 and egressing via interface eth0.	vyatta@vyatta# **set nat source rule 20 source address 192.168.0.0/24** vyatta@vyatta# **set nat source rule 20 outbound-interface eth0**
Use the primary IP address of the outbound interface as the translation address.	vyatta@vyatta# **set nat source rule 20 translation address masquerade**
Commit the change.	vyatta@vyatta# **commit**
Show the configuration.	vyatta@vyatta# **show nat source**

```
rule 10 {
    destination {
        address 192.168.50.0/24
    }
    exclude
    outbound-interface eth0
    source {
        address 192.168.0.0/24
    }
}
rule 20 {
    outbound-interface eth0
    source {
        address 192.168.0.0/24
    }
    translation {
        address masquerade
    }
}
```

The Negation Operator

Another way to exclude a subset of traffic from being translated is by using the negation operator: “!”. Example 2-13 provides the same functionality as in the previous example, but uses the negation operator instead of the **exclude** option.

Example 2-13 Masquerade NAT configured to exclude a subset of traffic by using the negation operator

Step	Command
Create SNAT rule 10.	vyatta@vyatta# **set nat source rule 10**
Apply this rule to packets coming from any host on network 192.168.0.0/24, not going to 192.168.50.0/24, and egressing via interface eth0.	vyatta@vyatta# **set nat source rule 10 source address 192.168.0.0/24** vyatta@vyatta# **set nat source rule 10 destination address !192.168.50.0/24** vyatta@vyatta# **set nat source rule 10 outbound-interface eth0**
Use the primary IP address of the outbound interface as the translation address.	vyatta@vyatta# **set nat source rule 10 translation address masquerade**
Commit the change.	vyatta@vyatta# **commit**

Show the configuration.	vyatta@vyatta# **show nat source**
	rule 10 {
	    destination {
	        address !192.168.50.0/24
	    }
	    outbound-interface eth0
	    source {
	        address 192.168.0.0/24
	    }
	    translation {
	        address masquerade
	    }
	}

Note that you should take extreme care using more than one negation operator rule in combination. NAT rules are evaluated sequentially, and a sequence of rules that use the negation operator may result in unexpected behavior.

Consider the set of two NAT rules shown in Example 2-14.

Example 2-14 Multiple source NAT rules using the negation operator: unexpected behavior

```
rule 10 {
    destination {
        address !192.168.50.0/24
    }
    outbound-interface eth0
    source {
        address 192.168.0.0/24
    }
    translation {
        address masquerade
    }
}
rule 20 {
    destination {
        address !172.16.50.0/24
    }
    outbound-interface eth0
    source {
        address 192.168.0.0/24
    }
    translation {
        address masquerade
    }
}
```

This combination rules will NOT result in the exclusion of networks 192.168.50.0/24 and 172.16.50.0/24. As explained above, these NAT rules are evaluated sequentially: when a packet arrives, it is tested against the first rule and if it does not match, it is tested against the second rule, and so on until it matches a rule.

In the example, a packet with a destination in 192.168.50.0/24 does NOT meet the match criteria in rule 10 (which matches all packets with destination NOT in 192.168.50.0/24). As a result, the packet “falls through” to rule 20. A packet with a destination in 192.168.50.0/24 DOES match rule 20 (because it is not in 172.16.50.0/24), and therefore the packet has NAT applied, which is not the desired result.

Similarly, a packet with a destination in 172.16.50.0/24 will be matched and NATted by rule 10.

Chapter 3: NAT Commands

This chapter describes network address translation (NAT) commands.

This chapter contains the following commands.

Configuration Commands	
nat	Enables NAT on the system.
nat <rule-type> rule <rule-num>	Defines a NAT rule.
nat <rule-type> rule <rule-num> description <desc>	Specifies a brief description for a NAT rule.
nat <rule-type> rule <rule-num> destination	Specifies the destination address and port to match in a NAT rule.
nat <rule-type> rule <rule-num> disable	Disables a NAT rule.
nat <rule-type> rule <rule-num> exclude	Creates an exclusion rule, excluding the specified packets from being translated.
nat <rule-type> rule <rule-num> inbound-interface <interface>	Specifies the interface on which to match inbound traffic to apply destination NAT rules to.
nat <rule-type> rule <rule-num> log <state>	Specifies whether or not matched NAT rules are logged.
nat <rule-type> rule <rule-num> outbound-interface <interface>	Specifies the interface to match outbound traffic to apply source NAT rules to.
nat <rule-type> rule <rule-num> protocol <protocol>	Specifies which protocols are to have NAT performed on them.
nat <rule-type> rule <rule-num> source	Specifies the source address and port to match in a NAT rule.
nat <rule-type> rule <rule-num> translation	Specifies the translated address and/or port in a NAT rule.
Operational Commands	
clear nat <rule-type> counters	Clears statistics counters for active NAT rules.
monitor nat <rule-type> background	Monitors NAT in the background.
monitor nat <rule-type> rule <rule-num>	Monitors a NAT rule.
monitor nat <rule-type> translations	Monitors active NAT translation events.
show nat <rule-type> rules	Lists configured NAT rules.
show nat <rule-type> statistics	Displays statistics for NAT.
show nat <rule-type> translations	Displays active NAT translations.

clear nat <rule-type> counters

Clears statistics counters for active NAT rules.

Syntax

clear nat *rule-type* **counters** [**rule** *rule-num*]

Command Mode

Operational mode.

Parameters

rule-type	Mandatory. An identifier for the type of rule. Supported values are as follows: **source:** Defines a source NAT (SNAT) rule. **destination:** Defines a destination NAT (DNAT) rule.
rule-num	A numeric identifier for the rule. The range is 1–9999.

Default

Statistics counters for all NAT translation rules of the specified type are cleared.

Usage Guidelines

Use this command to clear counters for NAT translation rules. Counters are cleared for all rules of the specified type by default. If a rule number is specified, only counters for that rule are cleared.

monitor nat <rule-type> background

Monitors NAT in the background.

Syntax

monitor nat *rule-type* **background [start | stop]**

Command Mode

Operational mode.

Parameters

rule-type	Mandatory. An identifier for the type of rule. Supported values are as follows: **source:** Defines a source NAT (SNAT) rule. **destination:** Defines a destination NAT (DNAT) rule.
start	Start background NAT monitoring.
stop	Stop background NAT monitoring.

Usage Guidelines

Use this command to monitor NAT in the background.

monitor nat <rule-type> rule <rule-num>

Monitors a NAT rule.

Syntax

monitor nat *rule-type* **rule** *rule-num* [**background** [**start** | **stop**]]

Command Mode

Operational mode.

Parameters

rule-type	Mandatory. An identifier for the type of rule. Supported values are as follows: **source:** Defines a source NAT (SNAT) rule. **destination:** Defines a destination NAT (DNAT) rule.
rule-num	Mandatory. Multi-node. A numeric identifier for the rule. The range is 1–9999.
start	Start background NAT monitoring.
stop	Stop background NAT monitoring.

Usage Guidelines

Use this command to monitor a NAT rule.

monitor nat <rule-type> translations

Monitors active NAT translation events.

Syntax

monitor nat *rule-type* **translations** [**detail**]

Command Mode

Operational mode.

Parameters

rule-type	Mandatory. An identifier for the type of rule. Supported values are as follows: **source:** Defines a source NAT (SNAT) rule. **destination:** Defines a destination NAT (DNAT) rule.
detail	Provides detailed NAT translation event information.

Usage Guidelines

Use this command to monitor NAT translation information.

Examples

Example 3-1 shows sample output for the **monitor nat source translations** command.

Example 3-1 Displaying NAT source translations

```
vyatta@vyatta:~$ monitor nat source translations
Type control-c to quit
Pre-NAT                 Post-NAT                Prot  Timeout
15.0.0.16               172.16.117.100          tcp   106
15.0.0.20               172.16.117.101          tcp   431959
15.0.0.16               172.16.117.100          tcp   58
vyatta@vyatta:~$
```

Example 3-2 shows sample output for the **monitor nat source translations detail** command.

Example 3-2 Displaying NAT source translation detail

```
vyatta@vyatta:~$ monitor nat source translations detail
Type control-c to quit
Pre-NAT src          Pre-NAT dst        Post-NAT src         Post-NAT dst
15.0.0.16:41920      172.16.117.17:22   172.16.117.100:41920 172.16.117.17:22
  tcp: 15.0.0.16 ==> 172.16.117.100  timeout: 103 use: 1
15.0.0.20:55853      172.16.117.17:23   172.16.117.101:55853 172.16.117.17:23
  tcp: 15.0.0.20 ==> 172.16.117.101  timeout: 431956 use: 1
15.0.0.16:46585      172.16.117.17:23   172.16.117.100:46585 172.16.117.17:23
  tcp: 15.0.0.16 ==> 172.16.117.100  timeout: 54 use: 1
```

nat

Enables NAT on the system.

Syntax

set nat

delete nat

show nat

Command Mode

Configuration mode.

Configuration Statement

```
nat {
}
```

Parameters

None.

Default

None.

Usage Guidelines

Use this command to enable Network Address Translation (NAT) on the Vyatta system.

Use the **set** form of this command to create and modify NAT configuration.

Use the **delete** form of this command to remove NAT configuration and disable NAT on the system.

Use the **show** form of this command to view NAT configuration.

nat <rule-type> rule <rule-num>

Defines a NAT rule.

Syntax

set nat *rule-type* **rule** *rule-num*

delete nat *rule-type* **rule** [*rule-num*]

show nat *rule-type* **rule** [*rule-num*]

Command Mode

Configuration mode.

Configuration Statement

```
nat {
    rule-type {
        rule rule-num {
        }
    }
}
```

Parameters

rule-type	Mandatory. An identifier for the type of rule. Supported values are as follows: **source:** Defines a source NAT (SNAT) rule. **destination:** Defines a destination NAT (DNAT) rule.
rule-num	Mandatory. Multi-node. A numeric identifier for the rule. The range is 1–9999.

Default

None.

Usage Guidelines

Use this command to specify a NAT rule configuration.

The *rule-type* defines the rule as either a **source** NAT rule or a **destination** NAT rule. Source NAT rules translate the source IP address. Destination NAT rules translate the destination IP address.

Source rules typically egress from the trusted to the untrusted network. For source NAT rules, the translation address typically defines the IP address that faces the untrusted network. This is the address that is substituted in for the original source IP address in egressing packets.

Destination rules typically ingress from the untrusted to the trusted network. For destination NAT rules, the translation address typically defines an IP address inside the trusted network. This is the address that is substituted in for the original destinatiuon IP address in ingressing packets.

NAT rules are executed in numeric order. To allow insertion of more rules in the future, choose rule numbers with space between; for example, number your initial rule set 10, 20, 30, 40, and so on.

Use the **set** form of this command to create or modify a NAT rule.

Use the **delete** form of this command to remove a NAT rule.

Use the **show** form of this command to view NAT rule configuration.

nat <rule-type> rule <rule-num> description <desc>

Specifies a brief description for a NAT rule.

Syntax

set nat *rule-type* **rule** *rule-num* **description** *desc*

delete nat *rule-type* **rule** *rule-num* **description**

show nat *rule-type* **rule** *rule-num* **description**

Command Mode

Configuration mode.

Configuration Statement

```
nat {
    rule-type {
        rule rule-num {
            description desc
        }
    }
}
```

Parameters

rule-type	Mandatory. An identifier for the type of rule. Supported values are as follows: **source:** Defines a source NAT (SNAT) rule. **destination:** Defines a destination NAT (DNAT) rule.
rule-num	A numeric identifier for the rule. The range is 1–9999.
desc	A description for the rule. If the description contains spaces, it must be enclosed in double quotes.

Default

None.

Usage Guidelines

Use this command to specify a description for a NAT rule.

Use the **set** form of this command to add or modify the description.

Use the **delete** form of this command to remove the description.

Use the **show** form of this command to view description configuration.

nat <rule-type> rule <rule-num> destination

Specifies the destination address and port to match in a NAT rule.

Syntax

set nat *rule-type* **rule** *rule-num* **destination** [**address** *address* | **port** *port*]

delete nat *rule-type* **rule** *rule-num* **destination** [**address** | **port**]

show nat *rule-type* **rule** *rule-num* **destination** [**address** | **port**]

Command Mode

Configuration mode.

Configuration Statement

```
nat {
    rule-type {
        rule rule-num {
            destination {
                address address
                port port
            }
        }
    }
}
```

Parameters

rule-type	Mandatory. An identifier for the type of rule. Supported values are as follows: **source:** Defines a source NAT (SNAT) rule. **destination:** Defines a destination NAT (DNAT) rule.
rule-num	Mandatory. Multi-node. A numeric identifier for the rule. The range is 1–9999.

address	The destination address to match. The following formats are valid: *ip-address*: An IPv4 address. *ip-address/prefix*: An IPv4 network address, where 0.0.0.0/0 matches any network. *ip-address–ip-address*: A range of contiguous IPv4 addresses; for example, 192.168.1.1–192.168.1.150. **!***ip-address*: Every IPv4 address EXCEPT the one specified. **!***ip-address/prefix*: Every IPv4 network address EXCEPT the one specified. **!***ip-address–ip-address*: All IP addresses EXCEPT those in the specified range.
port	The destination port to match. *port* is only valid for TCP and UDP protocols. The following formats are valid: *port-name*: The name of an IP service; for example, **http**. You can specify any service name in the file **etc/services**. *port-num*: A port number. The range is 1 to 65535. *start–end*: A range of ports; for example, 1001–1005. You can use a combination of these formats in a comma-separated list. You can also negate the entire list by prepending it with an exclamation mark (“!”); for example, **!22,telnet,http,123,1001-1005**.

Default

None.

Usage Guidelines

Use this command to specify the destination to match in a NAT rule.

Note that you should take care in using more than one “exclusion” rule (that is, a rule using the negation operation (“!”) in combination. NAT rules are evaluated sequentially, and a sequence of exclusion rules could result in unexpected behavior.

Use the **set** form of this command to create a NAT destination filter.

Use the **delete** form of this command to remove a NAT destination filter configuration.

Use the **show** form of this command to view NAT destination filter configuration.

nat <rule-type> rule <rule-num> disable

Disables a NAT rule.

Syntax

set nat *rule-type* **rule** *rule-num* **disable**

delete nat *rule-type* **rule** *rule-num* **disable**

show nat *rule-type* **rule** *rule-num*

Command Mode

Configuration mode.

Configuration Statement

```
nat {
    rule-type {
        rule rule-num {
            disable
        }
    }
}
```

Parameters

rule-type	Mandatory. An identifier for the type of rule. Supported values are as follows: **source:** Defines a source NAT (SNAT) rule. **destination:** Defines a destination NAT (DNAT) rule.
rule-num	Mandatory. Multi-node. A numeric identifier for the rule. The range is 1–9999.

Default

The rule is enabled.

Usage Guidelines

Use this command to disable a NAT rule.

Use the **set** form of this command to disable a NAT rule.

Use the **delete** form of this command to return a rule to its enabled state.

Use the **show** form of this command to view the configuration.

nat <rule-type> rule <rule-num> exclude

Creates an exclusion rule, excluding the specified packets from being translated.

Syntax

set nat *rule-type* **rule** *rule-num* **exclude**

delete nat *rule-type* **rule** *rule-num* **exclude**

show nat *rule-type* **rule** *rule-num*

Command Mode

Configuration mode.

Configuration Statement

```
nat {
    rule-type {
        rule rule-num {
            exclude
        }
    }
}
```

Parameters

rule-type	Mandatory. An identifier for the type of rule. Supported values are as follows: **source:** Defines a source NAT (SNAT) rule. **destination:** Defines a destination NAT (DNAT) rule.
rule-num	Mandatory. Multi-node. A numeric identifier for the rule. The range is 1–9999.

Default

None.

Usage Guidelines

Use this command to specify that packets matching this rule are to be excluded from address translation. Exclusion can be used in scenarios where certain types of traffic (for example VPN traffic) should not be translated.

Use the **set** form of this command to specify that packets matching this rule will be excluded from NAT.

Use the **delete** form of this command to remove the configuration

Use the **show** form of this command to view the configuration.

nat <rule-type> rule <rule-num> inbound-interface <interface>

Specifies the interface on which to match inbound traffic to apply destination NAT rules to.

Syntax

set nat *rule-type* **rule** *rule-num* **inbound-interface** *interface*

delete nat *rule-type* **rule** *rule-num* **inbound-interface**

show nat *rule-type* **rule** *rule-num* **inbound-interface**

Command Mode

Configuration mode.

Configuration Statement

```
nat {
    rule-type {
        rule rule-num {
            inbound-interface interface
        }
    }
}
```

Parameters

rule-type	Mandatory. An identifier for the type of rule. Supported values are as follows: **destination:** Defines a destination NAT (DNAT) rule.
rule-num	Mandatory. Multi-node. A numeric identifier for the rule. The range is 1–9999.

interface	The inbound Ethernet or serial interface to match. Destination NAT (DNAT) will be performed on traffic received on this interface. You can specify an individual vif, rather than an entire interface. To do this, refer to the vif using *int.vif* notation. For example to refer to vif 40 on interface eth0, use **eth0.40**. You can also specify **eth+** to indicate all ethernet interfaces and **any** to indicate any interface.

Default

None.

Usage Guidelines

Use this command to specify the Ethernet or serial interface on which inbound traffic will have destination NAT (DNAT) rules applied.

NOTE *This command can only be used for destination NAT rules (that is, NAT rules with a rule-type of* ***destination****). It is not applicable to rules with a rule-type of* ***source****.*

Use the **set** form of this command to specify inbound interface configuration

Use the **delete** form of this command to remove inbound interface configuration.

Use the **show** form of this command to view inbound interface configuration.

nat <rule-type> rule <rule-num> log <state>

Specifies whether or not matched NAT rules are logged.

Syntax

set nat *rule-type* **rule** *rule-num* **log** *state*

delete nat *rule-type* **rule** *rule-num* **log**

show nat *rule-type* **rule** *rule-num* **log**

Command Mode

Configuration mode.

Configuration Statement

```
nat {
    rule-type {
        rule rule-num {
            log state
        }
    }
}
```

Parameters

rule-type	Mandatory. An identifier for the type of rule. Supported values are as follows: **source:** Defines a source NAT (SNAT) rule. **destination:** Defines a destination NAT (DNAT) rule.
rule-num	Mandatory. Multi-node. A numeric identifier for the rule. The range is 1–9999.
state	Specifies whether or not to create log entries for matched NAT rules. Supported values are as follows: **disable:** Log entries are not generated for matched rules. **enable:** Log entries are generated for matched rules.

Default

Log entries are not generated for matched rules.

Usage Guidelines

Use this command to specify whether or not log entries are created when a NAT rule is matched.

Take care when enabling this feature as it can create very large log files and quickly fill a disk.

Use the **set** form of this command to set the state of NAT logging.

Use the **delete** form of this command to restore the default NAT logging configuration.

Use the **show** form of this command to view NAT logging configuration.

nat <rule-type> rule <rule-num> outbound-interface <interface>

Specifies the interface to match outbound traffic to apply source NAT rules to.

Syntax

set nat *rule-type* **rule** *rule-num* **outbound-interface** *interface*

delete nat *rule-type* **rule** *rule-num* **outbound-interface**

show nat *rule-type* **rule** *rule-num* **outbound-interface**

Command Mode

Configuration mode.

Configuration Statement

```
nat {
    rule-type {
        rule rule-num {
            outbound-interface interface
        }
    }
}
```

Parameters

rule-type	Mandatory. An identifier for the type of rule. Supported values are as follows: **source:** Defines a source NAT (SNAT) rule.
rule-num	Mandatory. Multi-node. A numeric identifier for the rule. The range is 1–9999.

interface Mandatory for **source** rules. Not configurable for **destination** rules. The outbound Ethernet or serial interface. Source NAT (SNAT) or masquerade NAT will be performed on traffic transmitted from this interface.

You can specify an individual vif, rather than an entire interface. To do this, refer to the vif using *int.vif* notation. For example to refer to vif 40 on interface eth0, use **eth0.40**.

You can also specify **eth+** to indicate all ethernet interfaces and **any** to indicate any interface.

Default

None.

Usage Guidelines

Use this command to specify the Ethernet or serial interface on which outbound traffic will have source NAT (SNAT) rules applied.

NOTE *This command can only be used on source NAT rules (that is, NAT rules with a rule-type of **source**). It is not applicable to rules with a rule-type of **destination**.*

Use the **set** form of this command to specify the outbound interface.

Use the **delete** form of this command to remove outbound interface configuration.

Use the **show** form of this command to view outbound interface configuration.

nat <rule-type> rule <rule-num> protocol <protocol>

Specifies which protocols are to have NAT performed on them.

Syntax

set nat *rule-type* **rule** *rule-num* **protocol** *protocol*

delete nat *rule-type* **rule** *rule-num* **protocol**

show nat *rule-type* **rule** *rule-num* **protocol**

Command Mode

Configuration mode.

Configuration Statement

```
nat {
    rule-type {
        rule rule-num {
            protocol protocol
        }
    }
}
```

Parameters

rule-type	Mandatory. An identifier for the type of rule. Supported values are as follows: **source:** Defines a source NAT (SNAT) rule. **destination:** Defines a destination NAT (DNAT) rule.
rule-num	Mandatory. Multi-node. A numeric identifier for the rule. The range is 1–9999.
protocol	The protocol(s) on which to perform NAT. Any protocol literals or numbers listed in **/etc/protocols** can be used. The keywords **all** (for all protocols) and **tcp_udp** (for both TCP and UDP protocols) are also supported. Prefixing the protocol name with the exclamation mark character (“!”) matches every protocol except the specified protocol. For example, **!tcp** matches all protocols except TCP.

Default

None.

Usage Guidelines

Use this command to specify the protocol(s) on which to perform NAT.

Note that you should take care in using more than one “exclusion” rule (that is, a rule using the negation operation (“!”) in combination. NAT rules are evaluated sequentially, and a sequence of exclusion rules could result in unexpected behavior.

Use the **set** form of this command to specify the protocol(s) on which to perform NAT.

Use the **delete** form of this command to remove the configuration

Use the **show** form of this command to view the configuration.

nat <rule-type> rule <rule-num> source

Specifies the source address and port to match in a NAT rule.

Syntax

set nat *rule-type* **rule** *rule-num* **source** [**address** *address* | **port** *port*]

delete nat *rule-type* **rule** *rule-num* **source** [**address** | **port**]

show nat *rule-type* **rule** *rule-num* **source** [**address** | **port**]

Command Mode

Configuration mode.

Configuration Statement

```
nat {
    rule-type {
        rule rule-num {
            source {
                address address
                port port
            }
        }
    }
}
```

Parameters

rule-type	Mandatory. An identifier for the type of rule. Supported values are as follows: **source:** Defines a source NAT (SNAT) rule. **destination:** Defines a destination NAT (DNAT) rule.
rule-num	Mandatory. Multi-node. A numeric identifier for the rule. The range is 1–9999.

address	The source address to match. The following formats are valid: *ip-address*: Matches the specified IP address. *ip-address/prefix*: A network address, where 0.0.0.0/0 matches any network. *ip-address–ip-address*: Matches a range of contiguous IP addresses; for example, 192.168.1.1–192.168.1.150. **!***ip-address*: Matches all IP addresses except the one specified. **!***ip-address/prefix*: Matches all network addresses except the one specified. **!***ip-address–ip-address*: Matches all IP addresses except those in the specified range.
port	The source port to match. *port* is only valid for TCP and UDP protocols. The following formats are valid: *port-name*: Matches the name of an IP service; for example, **http**. You can specify any service name in the file **etc/services**. *port-num*: Matches a port number. The range is 1 to 65535. *start–end*: Matches the specified range of ports; for example, 1001–1005. You can use a combination of these formats in a comma-separated list. You can also negate the entire list by prepending it with an exclamation mark (“!”); for example, **!22,telnet,http,123,1001-1005**.

Default

None.

Usage Guidelines

Use this command to specify the source to match in a NAT rule.

Note that you should take care in using more than one “exclusion” rule (that is, a rule using the negation operation (“!”) in combination. NAT rules are evaluated sequentially, and a sequence of exclusion rules could result in unexpected behavior.

Use the **set** form of this command to create a NAT source filter.

Use the **delete** form of this command to remove a NAT source filter configuration.

Use the **show** form of this command to view NAT source filter configuration.

nat <rule-type> rule <rule-num> translation

Specifies the translated address and/or port in a NAT rule.

Syntax

set nat *rule-type* **rule** *rule-num* **translation** [**address** *address* | **port** *port*]

delete nat *rule-type* **rule** *rule-num* **translation** [**address** | **port**]

show nat *rule-type* **rule** *rule-num* **translation** [**address** | **port**]

Command Mode

Configuration mode.

Configuration Statement

```
nat {
    rule-type {
        rule rule-num {
            translation {
                address address
                port port
            }
        }
    }
}
```

Parameters

rule-type	Mandatory. An identifier for the type of rule. Supported values are as follows: **source:** Defines a source NAT (SNAT) rule. **destination:** Defines a destination NAT (DNAT) rule.
rule-num	Mandatory. Multi-node. A numeric identifier for the rule. The range is 1–9999.

address

The IP address or range of addresses to substitue for the original addresses. If *rule-type* is **source**, the address or addresses chosen must be present on the outbound interface.

The following formats are valid:

ip-address: Translates to the specified IP address.

ip-address/prefix: Translates to the specified network. This is typically used in bidirectional NAT to translate one network of addresses to another.

ip-address–ip-address: Translates to one of the IP addresses in the specified pool of contiguous IP addresses; for example, 192.168.1.1–192.168.1.150.

masquerade: This is only available when *rule-type* is set to **source**. It specifies that the source IP address is to be set to to the primary IP address on the oubound interface.

port

The IP port to substitute for the original port. *port* is only valid for TCP and UDP protocols. *port* can not be used if the **source address** (or **destination address**) and the **translation address** are IPv4 subnets.

The following formats are valid:

port-num: Translates to the specified port number. The range is 1 to 65535.

start–end: Translates to one of the ports in the specified pool of contiguous ports; for example, 1001–1005.

Default

None.

Usage Guidelines

Use this command to specify the address and/or port translation in a NAT rule.

A translation address or a port must be specified for each rule.

Use the **set** form of this command to specify a NAT translation.

Use the **delete** form of this command to remove a NAT translation.

Use the **show** form of this command to view NAT translation.

show nat <rule-type> rules

Lists configured NAT rules.

Syntax

show nat *rule-type* **rules**

Command Mode

Operational mode.

Parameters

rule-type	Mandatory. An identifier for the type of rule. Supported values are as follows: **source:** Defines a source NAT (SNAT) rule. **destination:** Defines a destination NAT (DNAT) rule.

Usage Guidelines

Use this command to display the NAT rules you have configured. You can use this command for troubleshooting, to confirm whether traffic is matching the NAT rules as expected.

Example

Example 3-3 shows sample output for the **show nat** *rule-type* **rules** command.

In the output for this example, the following abbreviations occur:

- **saddr** represents the source address
- **sport** represents the source port
- **daddr** represents the destination address
- **dport** represents the destination port
- **proto** represents the protocol
- **intf** represents the interface.

Note also the following about this example:

- There is only one interface column (**intf**). For a source NAT rule, this interface refers to the outgoing interface; for a destination NAT rule, this interface is the incoming interface.
- In the **translation** column, first two rows report translation information and the third row (if it occurs) reports the conditions required for translation to be performed. In the example, rule 10, which is an SNAT rule, translates source address 192.168.74.0/24 to 172.16.139.0/24, leaves the source port at its original value, and translates when (and only when) the destination port is 80 for any destination address.
- An “X” at the front of a rule (as for rule 20 in the example) means that the rule has been excluded.
- An “M” signifies a masquerade rule.

Example 3-3 Displaying source NAT rule information

```
vyatta@vyatta:~$ show nat source rules
Disabled rules are not shown
Codes: X - exclude rule, M - masquerade rule

rule   intf     translation
----   ----     -----------
10     eth2     saddr 192.168.74.0/24 to 172.16.139.0/24
    proto-tcp   sport ANY
                when daddr ANY, dport 80

X20    eth0     saddr ANY to 172.16.117.200
    proto-tcp   sport ANY to 80
                when daddr ANY, dport 8080
```

show nat <rule-type> statistics

Displays statistics for NAT.

Syntax

show nat *rule-type* **statistics**

Command Mode

Operational mode.

Parameters

rule-type Mandatory. An identifier for the type of rule. Supported values are as follows:

source: Defines a source NAT (SNAT) rule.

destination: Defines a destination NAT (DNAT) rule.

Usage Guidelines

Use this command to display current statistics for NAT.

Examples

Example 3-4 shows sample output for the **show nat source statistics** command.

Example 3-4 Displaying source NAT statistics information

```
vyatta@vyatta:~$ show nat source statistics
rule  pkts    bytes    interface
----  ----    -----    ---------
10      16      224    eth2
20       7      148    eth3
```

show nat <rule-type> translations

Displays active NAT translations.

Syntax

show nat *rule-type* **translations** [**address** *addr* | **detail**]

Command Mode

Operational mode.

Parameters

rule-type	Mandatory. An identifier for the type of rule. Supported values are as follows: **source:** Defines a source NAT (SNAT) rule. **destination:** Defines a destination NAT (DNAT) rule.
address *addr*	Provides output of NAT translations for address *addr*.
detail	Provides detailed output of NAT translations.

Usage Guidelines

Use this command to display NAT translation information.

Examples

Example 3-5 shows sample output for the **show nat source translations** command.

Example 3-5 Displaying NAT source translations

```
vyatta@vyatta:~$ show nat source translations
Pre-NAT              Post-NAT             Prot  Timeout
15.0.0.16            172.16.117.100       tcp   106
15.0.0.20            172.16.117.101       tcp   431959
15.0.0.16            172.16.117.100       tcp   58
vyatta@vyatta:~$
```

Example 3-6 shows sample output for the **show nat source translations detail** command.

Example 3-6 Displaying NAT source translation detail

```
vyatta@vyatta:~$ show nat source translations detail
Pre-NAT src          Pre-NAT dst        Post-NAT src         Post-NAT dst
15.0.0.16:41920      172.16.117.17:22   172.16.117.100:41920 172.16.117.17:22
  tcp: 15.0.0.16 ==> 172.16.117.100  timeout: 103 use: 1
15.0.0.20:55853      172.16.117.17:23   172.16.117.101:55853 172.16.117.17:23
  tcp: 15.0.0.20 ==> 172.16.117.101  timeout: 431956 use: 1
15.0.0.16:46585      172.16.117.17:23   172.16.117.100:46585 172.16.117.17:23
  tcp: 15.0.0.16 ==> 172.16.117.100  timeout: 54 use: 1
vyatta@vyatta:~$
```

Example 3-7 shows sample output for the **show nat source translations address 15.0.0.16** command.

Example 3-7 Displaying NAT source translation for address 15.0.0.16

```
vyatta@vyatta:~$ show nat source translations address 15.0.0.16
Pre-NAT src          Pre-NAT dst        Post-NAT src         Post-NAT dst
15.0.0.16:57634      172.16.117.17:22   172.16.117.100:57634 172.16.117.17:22
  tcp: 15.0.0.16 ==> 172.16.117.100  timeout: 106 use: 1
15.0.0.16:46884      172.16.117.17:23   172.16.117.100:46884 172.16.117.17:23
  tcp: 15.0.0.16 ==> 172.16.117.100  timeout: 115 use: 1
vyatta@vyatta:~$
```

Glossary of Acronyms

ACL	access control list
ADSL	Asymmetric Digital Subscriber Line
AMI	Amazon Machine Image
API	Application Programming Interface
AS	autonomous system
ARP	Address Resolution Protocol
AWS	Amazon Web Services
BGP	Border Gateway Protocol
BIOS	Basic Input Output System
BPDU	Bridge Protocol Data Unit
CA	certificate authority
CCMP	AES in counter mode with CBC-MAC
CHAP	Challenge Handshake Authentication Protocol
CLI	command-line interface
DDNS	dynamic DNS
DHCP	Dynamic Host Configuration Protocol
DHCPv6	Dynamic Host Configuration Protocol version 6

DLCI	data-link connection identifier
DMI	desktop management interface
DMZ	demilitarized zone
DN	distinguished name
DNS	Domain Name System
DSCP	Differentiated Services Code Point
DSL	Digital Subscriber Line
eBGP	external BGP
EBS	Amazon Elastic Block Storage
EC2	Amazon Elastic Compute Cloud
EGP	Exterior Gateway Protocol
ECMP	equal-cost multipath
ESP	Encapsulating Security Payload
FIB	Forwarding Information Base
FTP	File Transfer Protocol
GRE	Generic Routing Encapsulation
HDLC	High-Level Data Link Control
I/O	Input/Ouput
ICMP	Internet Control Message Protocol
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
IGP	Interior Gateway Protocol
IPS	Intrusion Protection System
IKE	Internet Key Exchange
IP	Internet Protocol
IPOA	IP over ATM

IPsec	IP security
IPv4	IP Version 4
IPv6	IP Version 6
ISP	Internet Service Provider
KVM	Kernel-Based Virtual Machine
L2TP	Layer 2 Tunneling Protocol
LACP	Link Aggregation Control Protocol
LAN	local area network
LDAP	Lightweight Directory Access Protocol
LLDP	Link Layer Discovery Protocol
MAC	medium access control
MIB	Management Information Base
MLPPP	multilink PPP
MRRU	maximum received reconstructed unit
MTU	maximum transmission unit
NAT	Network Address Translation
ND	Neighbor Discovery
NIC	network interface card
NTP	Network Time Protocol
OSPF	Open Shortest Path First
OSPFv2	OSPF Version 2
OSPFv3	OSPF Version 3
P2P	peer-to-peer
PAM	Pluggable Authentication Module
PAP	Password Authentication Protocol
PAT	Port Address Translation

PCI	peripheral component interconnect
PKI	Public Key Infrastructure
PPP	Point-to-Point Protocol
PPPoA	PPP over ATM
PPPoE	PPP over Ethernet
PPTP	Point-to-Point Tunneling Protocol
PVC	permanent virtual circuit
QoS	quality of service
RADIUS	Remote Authentication Dial-In User Service
RHEL	Red Hat Enterprise Linux
RIB	Routing Information Base
RIP	Routing Information Protocol
RIPng	RIP next generation
Rx	receive
S3	Amazon Simple Storage Service
SLAAC	Stateless Address Auto-Configuration
SNMP	Simple Network Management Protocol
SMTP	Simple Mail Transfer Protocol
SONET	Synchronous Optical Network
SSH	Secure Shell
SSID	Service Set Identifier
STP	Spanning Tree Protocol
TACACS+	Terminal Access Controller Access Control System Plus
TCP	Transmission Control Protocol
TKIP	Temporal Key Integrity Protocol
ToS	Type of Service

Tx	transmit
UDP	User Datagram Protocol
vif	virtual interface
VLAN	virtual LAN
VPC	Amazon virtual private cloud
VPN	Virtual Private Network
VRRP	Virtual Router Redundancy Protocol
WAN	wide area network
WAP	wireless access point
WPA	Wired Protected Access