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: February 2011

DOCUMENT REVISION. R6.2 v01

RELEASED WITH: R6.2.0

PART NO. A0-0230-10-0007

Table of Contents

Quick Reference to Commands v

Quick List of Examples vi

Preface viii

Intended Audience ix

Organization of This Guide ix

Document Conventions ix

Advisory Paragraphs x

Typographic Conventions x

Vyatta Publications xi

Chapter 1 NAT Overview 1

What is NAT? 2

Benefits of NAT 3

Types of NAT 4

Source NAT (SNAT) 4

Destination NAT (DNAT) 5

Bidirectional NAT 5

Interaction Between NAT, Routing, Firewall, and DNS 6

Interaction Between NAT and Routing 7

Interaction between NAT and Firewall 9

Interaction between NAT and DNS 12

NAT Rules 12

NAT Rule Type Configuration 13

Filters: Protocols, Source, and Destination 13

The “protocols” Filter 13

The “source” Filter 13

The “destination” Filter 14

Address Conversion: “Inside” vs. “Outside” Addresses 14
Inside-Address 15
Outside-Address 15
“Inbound” and “Outbound” Interfaces 16

Chapter 2 NAT Configuration Examples 17
Source NAT (One-to-One) 18
Source NAT (Many-to-One) 19
Source NAT (Many-to-Many) 21
Source NAT (One-to-Many) 22
Masquerade 24
Destination NAT (One-to-One) 26
Destination NAT (One-to-Many) 29
Bidirectional NAT 30
Mapping Address Ranges 32
Masquerade NAT and VPN 34
The “exclude” Option 37

Chapter 3 NAT Commands 39
clear nat counters 41
service nat 42
service nat rule <rule-num> 43
service nat rule <rule-num> destination 44
service nat rule <rule-num> disable 46
service nat rule <rule-num> exclude 47
service nat rule <rule-num> inbound-interface <interface> 48
service nat rule <rule-num> inside-address 50
service nat rule <rule-num> log <state> 52
service nat rule <rule-num> outbound-interface <interface> 54
service nat rule <rule-num> outside-address 56
service nat rule <rule-num> protocol <protocol> 58
service nat rule <rule-num> source 60
service nat rule <rule-num> type <type> 62
show nat rules 64
show nat statistics 66
show nat translations 67

Glossary of Acronyms 70

Quick Reference to Commands

Use this section to help you quickly locate a command.

clear nat counters 41
service nat 42
service nat rule <rule-num> 43
service nat rule <rule-num> destination 44
service nat rule <rule-num> disable 46
service nat rule <rule-num> exclude 47
service nat rule <rule-num> inbound-interface <interface> 48
service nat rule <rule-num> inside-address 50
service nat rule <rule-num> log <state> 52
service nat rule <rule-num> outbound-interface <interface> 54
service nat rule <rule-num> outside-address 56
service nat rule <rule-num> protocol <protocol> 58
service nat rule <rule-num> source 60
service nat rule <rule-num> type <type> 62
show nat rules 64
show nat statistics 66
show nat translations 67

Quick List of Examples

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

Example 1-1 Creating a NAT rule 14
Example 1-2 Creating a source NAT (SNAT) rule 14
Example 1-3 Filtering packets by protocol 15
Example 1-4 Filtering packets by source address 15
Example 1-5 Filtering packets by source network address and port 15
Example 1-6 Filtering packets by destination address 15
Example 1-7 Setting an inside IP address 16
Example 1-8 Setting a range of inside addresses 16
Example 1-9 Setting an outside address 17
Example 1-10 Setting a range of outside addresses 17
Example 1-11 Setting the inbound interface 17
Example 1-12 Setting the outbound interface 18
Example 2-1 Source NAT (one-to-one) 20
Example 2-2 Source NAT (many-to-one) 21
Example 2-3 Source NAT (many-to-many) 23
Example 2-4 Source NAT (one-to-many) 24
Example 2-5 Masquerade 26
Example 2-6 Destination NAT (one-to-one) 28
Example 2-7 Destination NAT (one-to-one): filtering port name 29
Example 2-8 Destination NAT(one-to-many) 31
Example 2-9 Bidirectional NAT 32
Example 2-10 Mapping address ranges 33
Example 2-11 Masquerade NAT configured to bypass a VPN tunnel 35
Example 2-12 Single NAT exclusion rule: correct behavior 36
Example 2-13 Multiple NAT exclusion rules: unexpected behavior 37

Example 2-14 Single NAT exclusion rule: correct behavior—using the “exclude” option 38
Example 2-15 Multiple NAT exclusion rules: expected behavior—using exclude 38
Example 3-1 Displaying NAT rule information 69
Example 3-2 Displaying NAT statistics information 70
Example 3-3 Displaying NAT translations 72
Example 3-4 Displaying NAT translation detail 72
Example 3-5 Displaying NAT translation for source address 15.0.0.16 72
Example 3-6 Monitoring source NAT translations 73
Example 3-7 Detailed monitoring of source NAT translations 73

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 Reference to Commands

  Use this list to help you quickly locate commands.

- Quick 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:

Chapter	Description	Page
Chapter 1: NAT Overview	This chapter explains how to set up network address translation (NAT) on the Vyatta System.	1
Chapter 2: NAT Configuration Examples	This chapter provides configuration examples for network address translation (NAT) on the Vyatta System.	19
Chapter 3: NAT Commands	This chapter describes network address translation (NAT) commands.	40
Glossary of Acronyms		74

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.

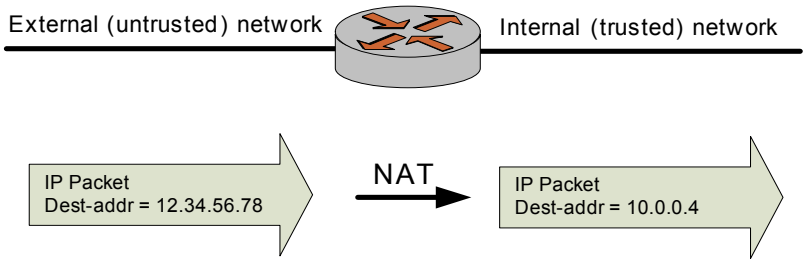
This chapter presents the following topics:

- What is NAT?
- Benefits of NAT
- Types of NAT
- Interaction Between NAT, Routing, Firewall, and DNS
- NAT Rules
- NAT Rule Type Configuration
- Filters: Protocols, Source, and Destination
- Address Conversion: “Inside” vs. “Outside” Addresses
- “Inbound” and “Outbound” Interfaces

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 cannot 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.

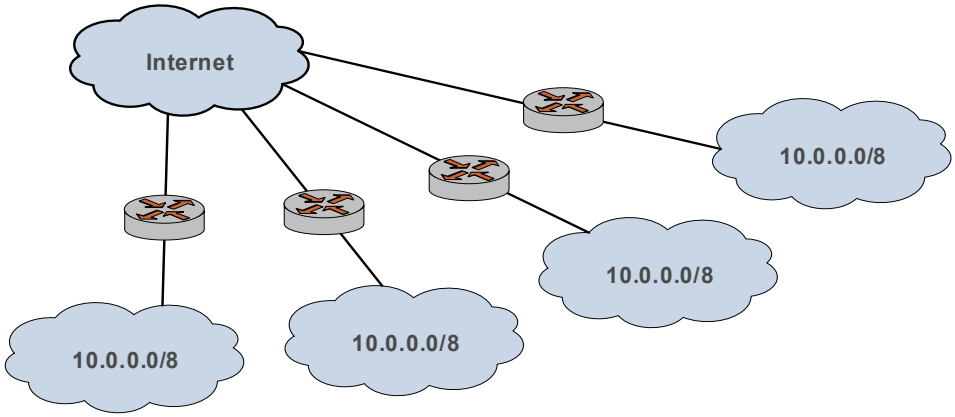
Benefits of NAT

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.

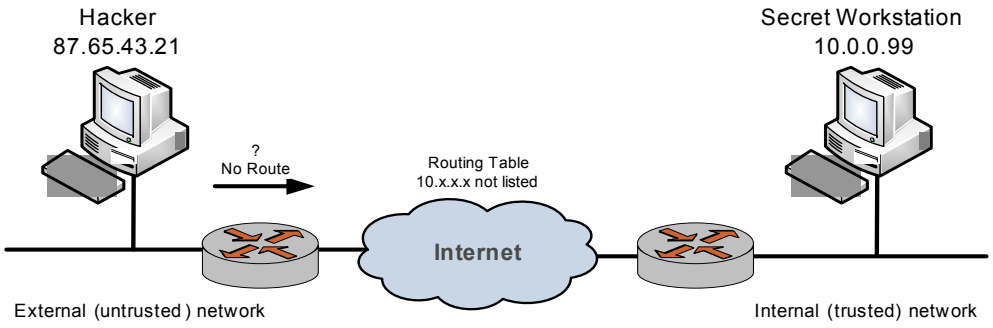
Figure 1-2 Reusing private address space



- 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.

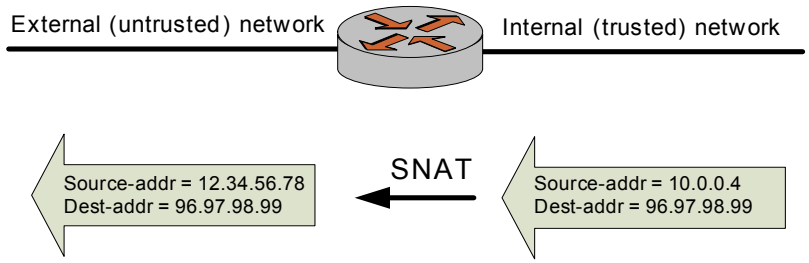
Source NAT (SNAT)

Tip: *SNAT is performed after routing.*

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 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)

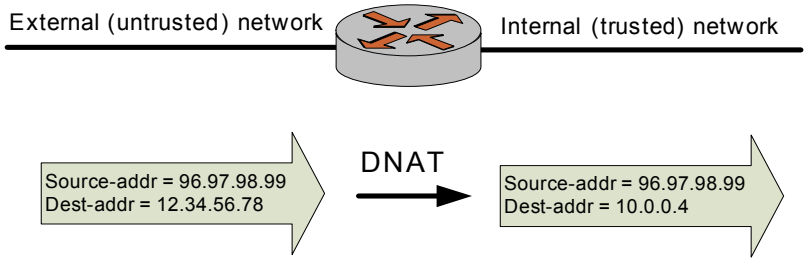


Destination NAT (DNAT)

Tip: *DNAT is performed before routing.*

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.

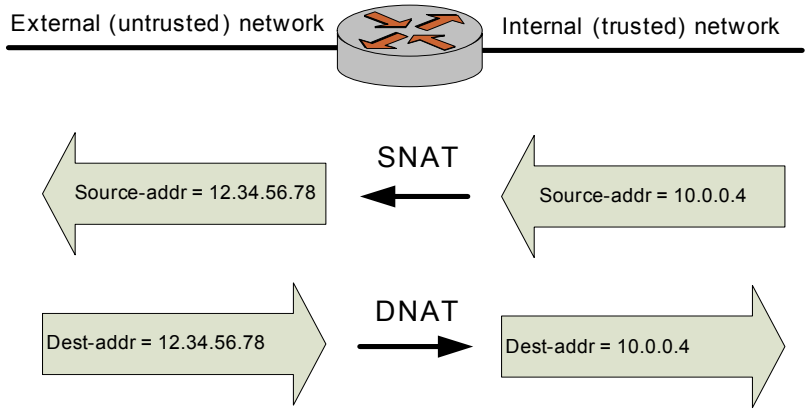
Figure 1-5 Destination NAT (DNAT)



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



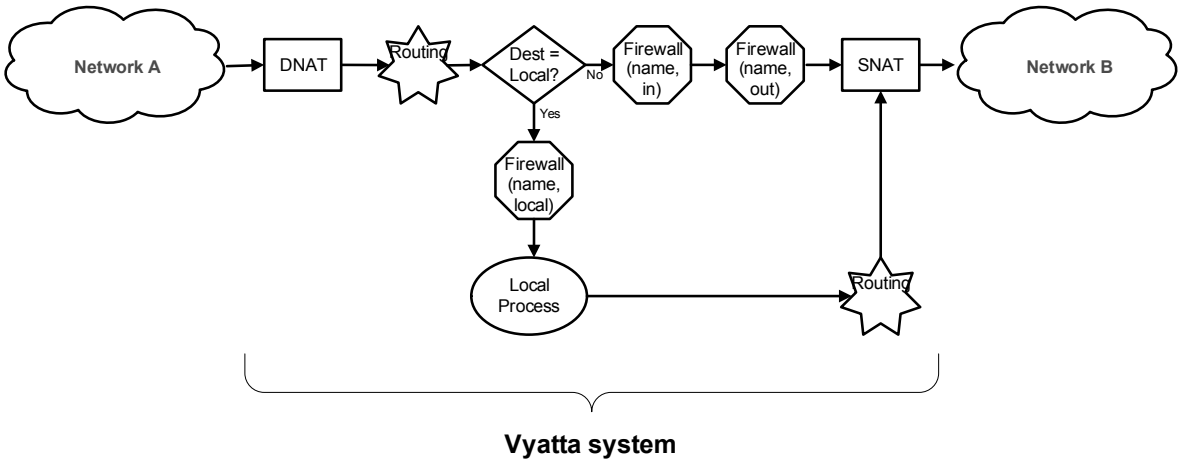
Interaction Between NAT, Routing, Firewall, and DNS

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.

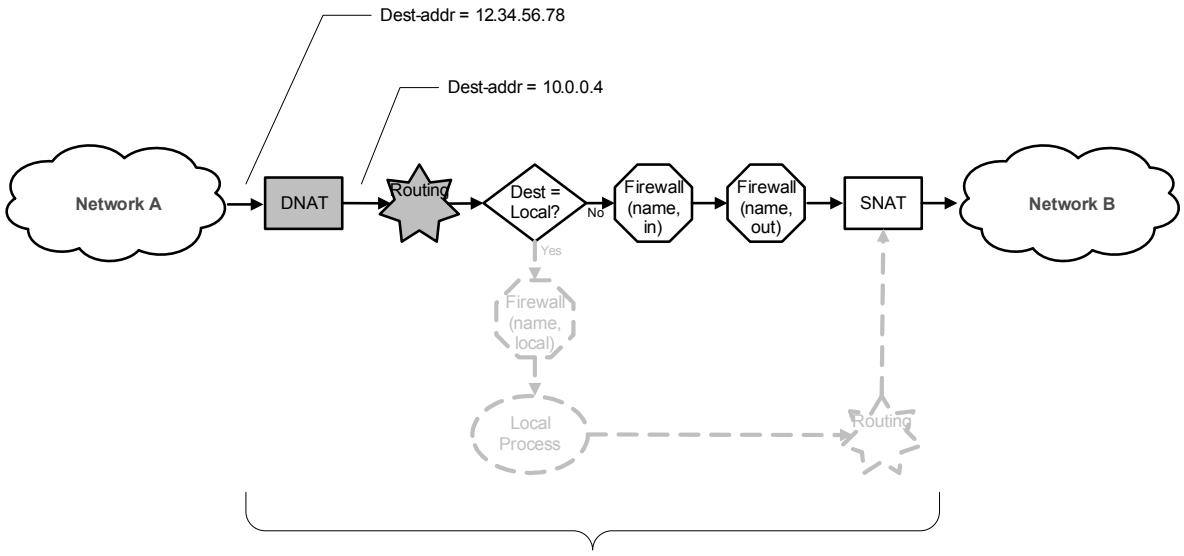
Scenario 1a: DNAT—Packets Passing Through the Vyatta System

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 converted 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 *converted* destination address—*not* the original destination address; see Figure 1-8.

Figure 1-8 Pass-through DNAT routing decisions

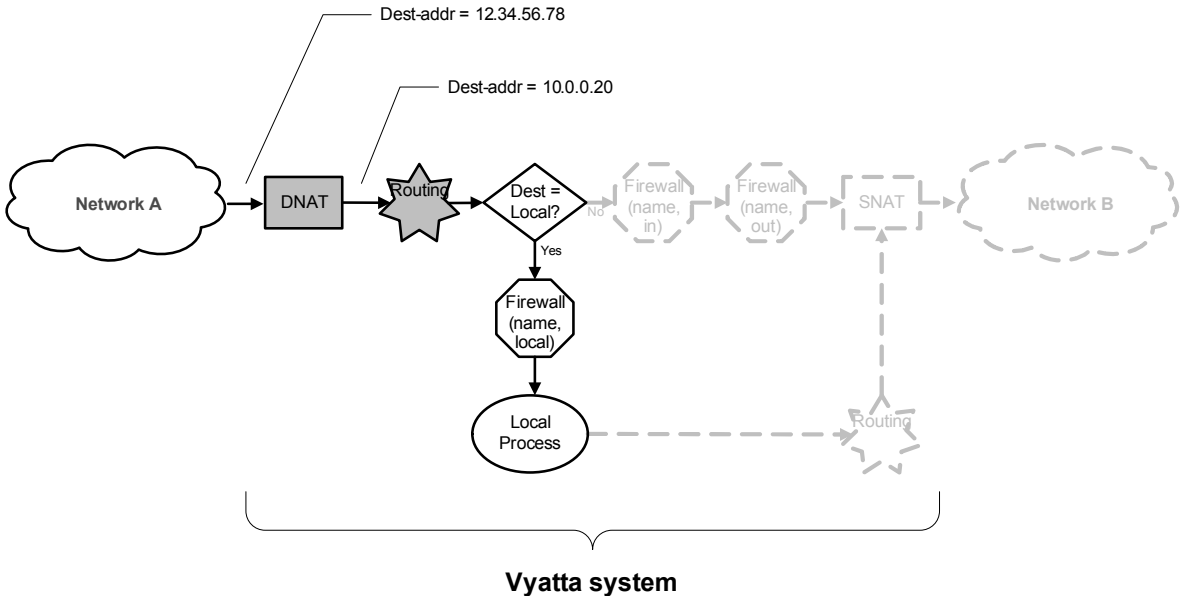


Scenario 1b: DNAT—Packets Destined for the Vyatta System

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 *converted* destination address—*not* the original destination address; see Figure 1-9.

Figure 1-9 Vyatta system-destined DNAT routing decisions

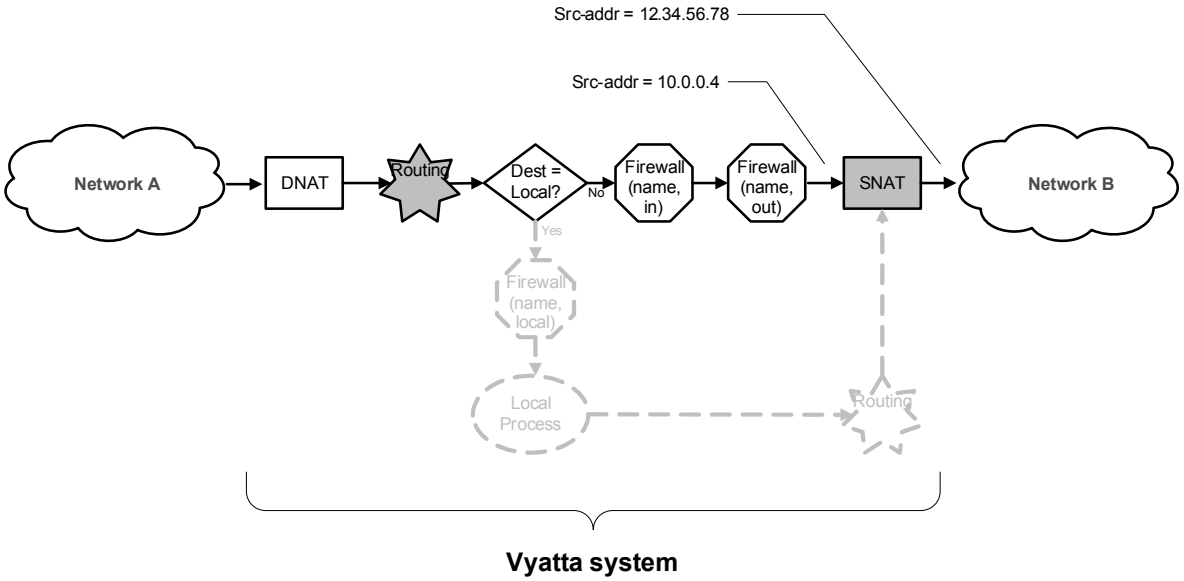


Scenario 2a: SNAT—Packets Passing Through the Vyatta System

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 converted source address; see Figure 1-10.

Figure 1-10 Pass-through SNAT routing decisions

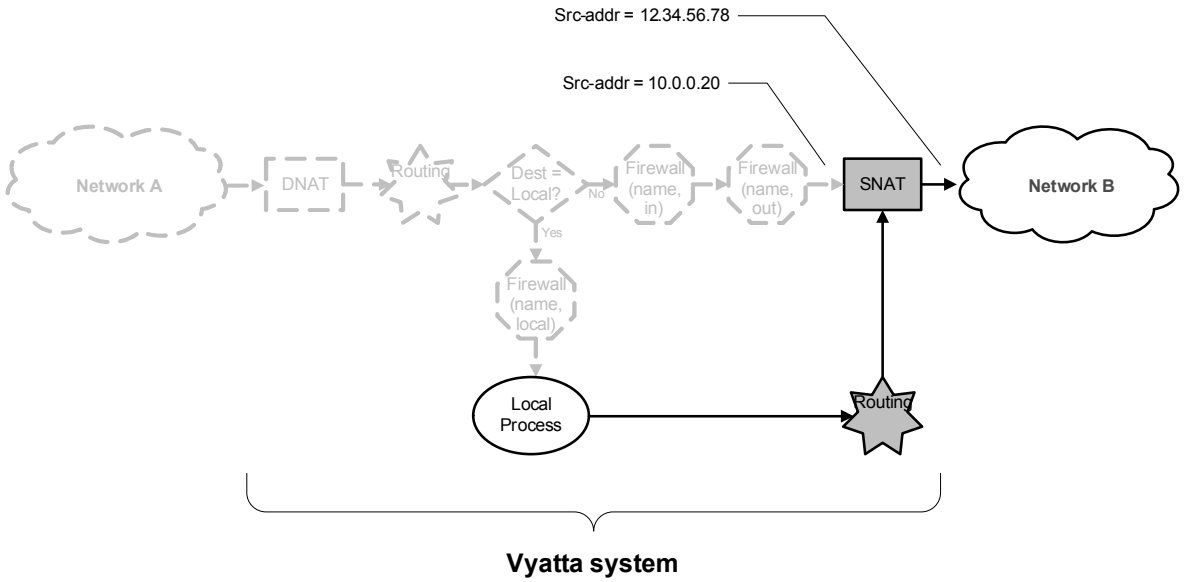


Scenario 2b: SNAT—Packets Originating From the Vyatta System

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

Again, because routing decisions are made prior to SNAT, routing decisions based on source address are made on the *original* source *address—not* the converted 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.

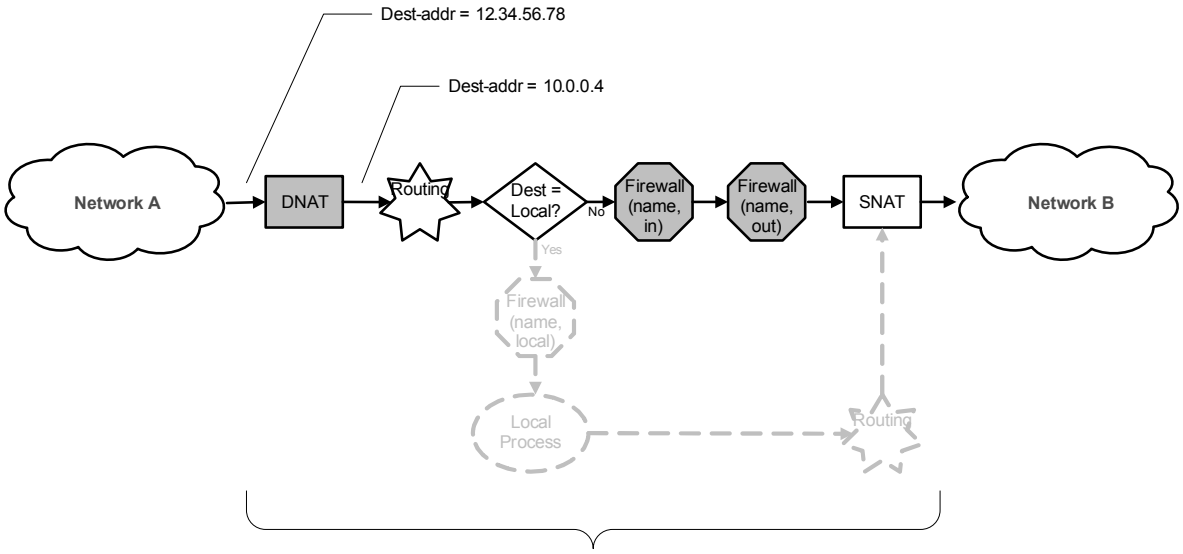
Scenario 1a: DNAT—Packets Passing Through the Vyatta System

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 *converted* destination address).

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

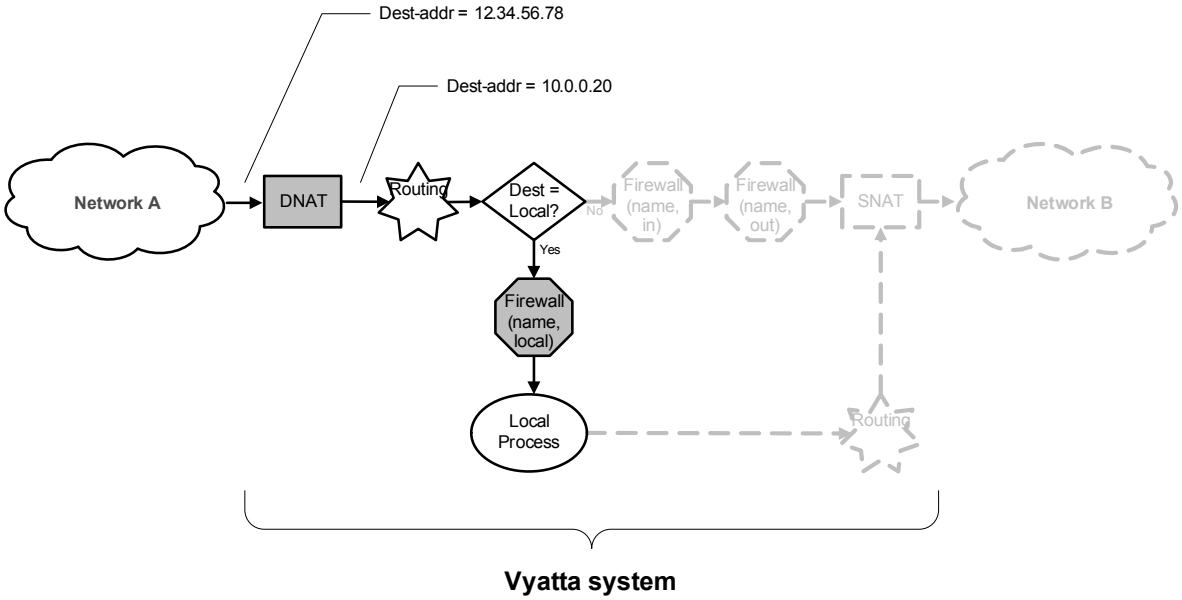
Figure 1-12 Pass-through DNAT firewall decisions



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 *converted* destination address); see Figure 1-13.

Figure 1-13 Vyatta system-destined DNAT firewall decisions

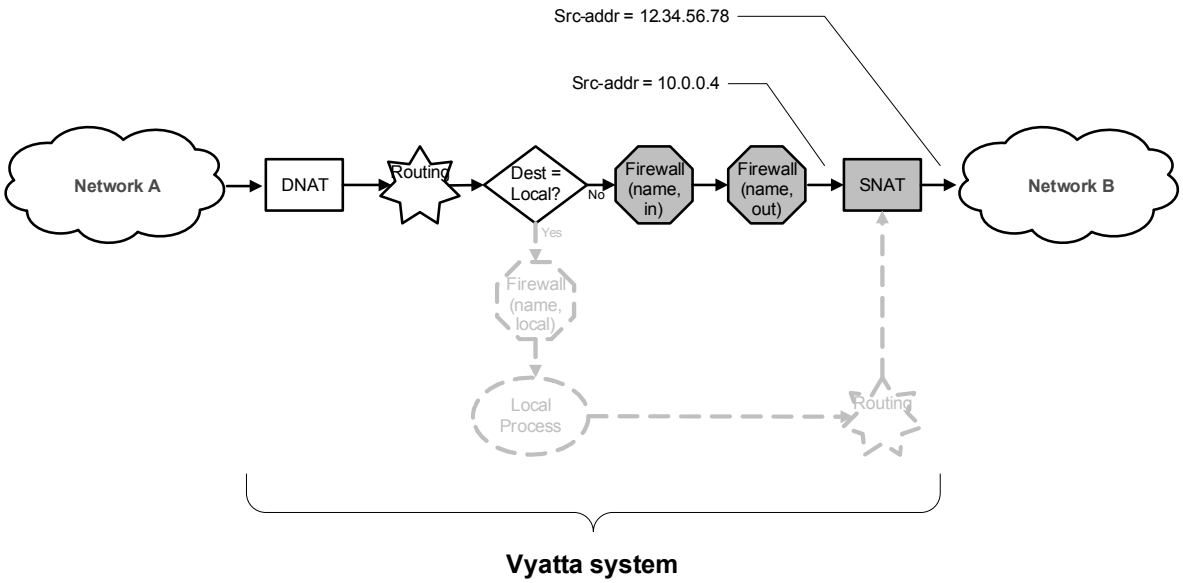


Scenario 2a: SNAT—Packets Passing Through the Vyatta System

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 converted source address. This order of evaluation is true for both inbound and outbound packets; see Figure 1-14.

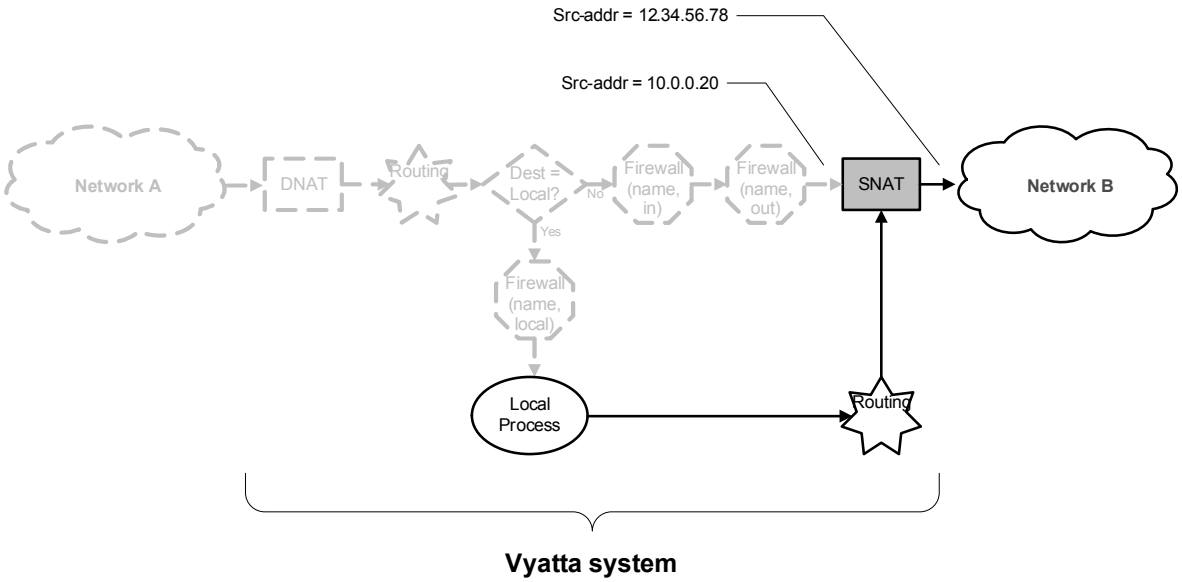
Figure 1-14 Pass-through SNAT firewall decisions



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 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.

Note that once configured, a NAT rule number is its permanent identifier. The number of the NAT rule cannot be changed in the same way that the rule’s attributes can be changed. To change the number of a NAT rule, you must delete the rule and re-create it using the new number.

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

For this reason, it makes sense to create your NAT rules leaving "space" between the numbers. For example, you might initial 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 delete and recreate any other rules.

To create or modify a NAT rule, you use the **set** command on the **service nat** configuration node, providing the number that will be the rule identifier; see Example 1-1:

Example 1-1 Creating a NAT rule

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

NAT Rule Type Configuration

The Vyatta system allows you to configure a NAT rule type of **source** (for SNAT), **destination** (for DNAT), or **masquerade** (for "masquerade" SNAT). To implement bidirectional NAT, you define a NAT rule for SNAT and one for DNAT. Example 1-2 defines an SNAT rule 10.

Example 1-2 Creating a source NAT (SNAT) rule

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

Filters: Protocols, Source, and Destination

Filters control which packets will have the NAT rules applied to them. There are three different filters that can be applied within a NAT rule: **protocols**, **source**, and **destination**.

The "protocols" Filter

The **protocols** option specifies which protocol types the NAT rule will be applied to. Only packets of the specified protocol are NATted. The default is **all** protocols.

Example 1-3 sets Rule 10 to apply to TCP protocol packets. Only TCP packets will have address substitution performed.

Example 1-3 Filtering packets by protocol

```
vyatta@vyatta#set service nat rule 10 protocols tcp
```

The “source” Filter

The **source** option filters packets based on their source address and/or port. Only packets with a source address and port matching that defined in the filter are NATted. (Port information is optional.)

If the source filter is not specified, then by default the rule matches packets arriving from any source address and port.

Example 1-4 sets Rule 10 to apply to packets with a source address of 10.0.0.4.

Example 1-4 Filtering packets by source address

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

Example 1-5 sets Rule 15 to apply to packets with a source network of 10.0.0.0/24 and port 80.

Example 1-5 Filtering packets by source network address and port

```
vyatta@vyatta#set service nat rule 15 source address 10.0.0.0/24
vyatta@vyatta#set service nat rule 15 source port 80
```

The “destination” Filter

The **destination** filter filters packets based on their destination address/port. Only packets with a destination address/port combination matching that defined within the filter are NATted. (Port information is optional.)

If the destination filter is not specified, by default the rule will match packets with any destination address or port.

Example 1-6 sets Rule 20 to apply to packets with a destination address of 12.34.56.78.

Example 1-6 Filtering packets by destination address

```
vyatta@vyatta#set service nat rule 20 destination address 12.34.56.78
```

In addition to “address” the other parameter associated with the “destination” filter is “port”.

Address Conversion: “Inside” vs. “Outside” Addresses

The **inside-address** and **outside-address** specify the address conversions that take place within the NAT rule. They define the information that is substituted into the packet for the original addresses.

Inside-Address

The **inside-address** is used with DNAT. The inside-address specifies the address that is substituted for the destination IP address of the incoming packet. Port translation is also available and can be specified as part of the inside-address.

Example 1-7 sets Rule 20 to substitute 10.0.0.4 as the destination IP address of inbound packets matching its criteria.

Example 1-7 Setting an inside IP address

```
vyatta@vyatta#set service nat rule 20 inside-address address 10.0.0.4
```

Example 1-8 sets Rule 25 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 criteria.

Example 1-8 Setting a range of inside addresses

```
vyatta@vyatta#set service nat rule 25 inside-address address
10.0.0.0-10.0.0.3
```

Outside-Address

The **outside-address** is used with SNAT. The outside-address specifies the address that is to be substituted for the source IP address of the outgoing packet. Port translation is also available and can be specified as part of the outside-address.

Note the following:

- Outside-address is *mandatory* for SNAT rules
- Outside-address *must* be one of the addresses defined on the outbound interface.
- Outside address *cannot be set* for rules of type **masquerade**. This is because masquerade always uses the primary IP address of the outbound interface. However, outside ports can be set for type **masquerade**.

Example 1-9 sets Rule 10 to substitute 12.34.56.78 as the source IP address of outbound packets matching its criteria.

Example 1-9 Setting an outside address

```
vyatta@vyatta#set service nat rule 10 outside-address address 12.34.56.78
```

Example 1-10 sets Rule 15 to substitute addresses 12.34.56.64 through 12.34.56.79 as the source IP addresses of outbound packets that match its criteria.

Example 1-10 Setting a range of outside addresses

```
vyatta@vyatta#set service nat rule 15 outside-address address
12.34.56.64-12.34.56.79
```

"Inbound" and "Outbound" Interfaces

For each NAT rule you may specify through which interface packets will enter or exit. Note the following:

- For **destination** (DNAT) rules, specify the inbound interface. This is the interface through which inbound traffic first enters the NAT device.
- For **source** (SNAT) rules, specify the outbound interface. This is the interface through which outbound traffic exits the NAT device.
- For **masquerade** (masquerade SNAT) rules, specify the outbound interface. This is the interface through which outbound traffic exits the NAT device.

Example 1-11 sets Rule 20 to listen on interface eth0 for inbound traffic.

Example 1-11 Setting the inbound interface

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

Example 1-12 sets Rule 10 to send outbound traffic out through interface eth1.

Example 1-12 Setting the outbound interface

```
vyatta@vyatta#set service nat rule 10 outbound-interface eth1
```

Chapter 2: NAT Configuration Examples

This chapter provides configuration examples for 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:

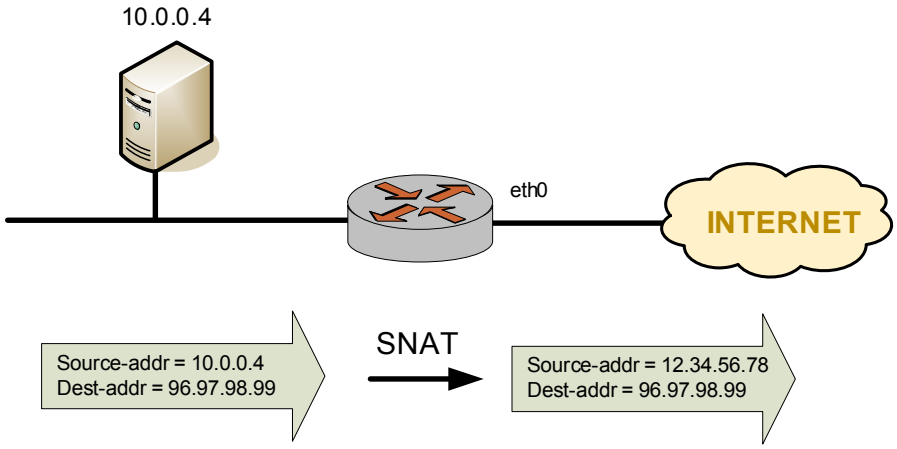
- Source NAT (One-to-One)
- Source NAT (Many-to-One)
- Source NAT (Many-to-Many)
- Source NAT (One-to-Many)
- Masquerade
- Destination NAT (One-to-One)
- Destination NAT (One-to-Many)
- Bidirectional NAT
- If connections are only initiated from the 10.0.0.0/24 network then only rule 10 is required. If connections are only initiated from the 11.22.33.0/24 network then only rule 20 is required.
- The “exclude” Option

Source NAT (One-to-One)

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

- An internal news server (NNTP) that 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 service nat rule 10 type source`
Apply this rule to packets coming from address 10.0.0.4.	`vyatta@vyatta# set service nat rule 10 source address 10.0.0.4`
Send traffic out through interface eth0. Use 12.34.56.78 as the source address in outgoing packets. Note that the outside-address should be one of the 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 the outside-address.	`vyatta@vyatta# set service nat rule 10 outbound-interface eth0` `vyatta@vyatta# set service nat rule 10 outside-address address 12.34.56.78`
Commit the change.	`vyatta@vyatta# commit`

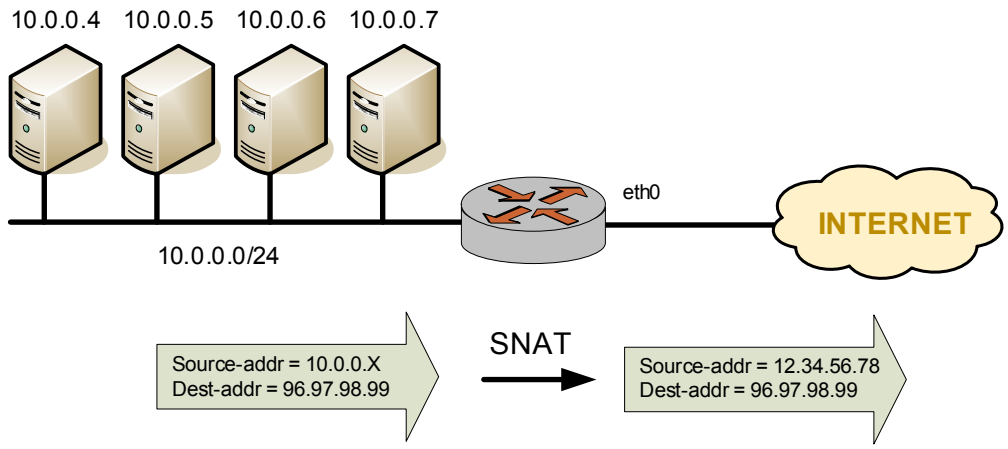
Example 2-1 Source NAT (one-to-one)

Show the configuration.	`vyatta@vyatta# show service nat rule 10`
	`  outbound-interface eth0`
	`  outside-address {`
	`  address 12.34.56.78`
	`  }`
	`  source {`
	`  address 10.0.0.4`
	`  }`
	`  type source`

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 service nat rule 10 type source`

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

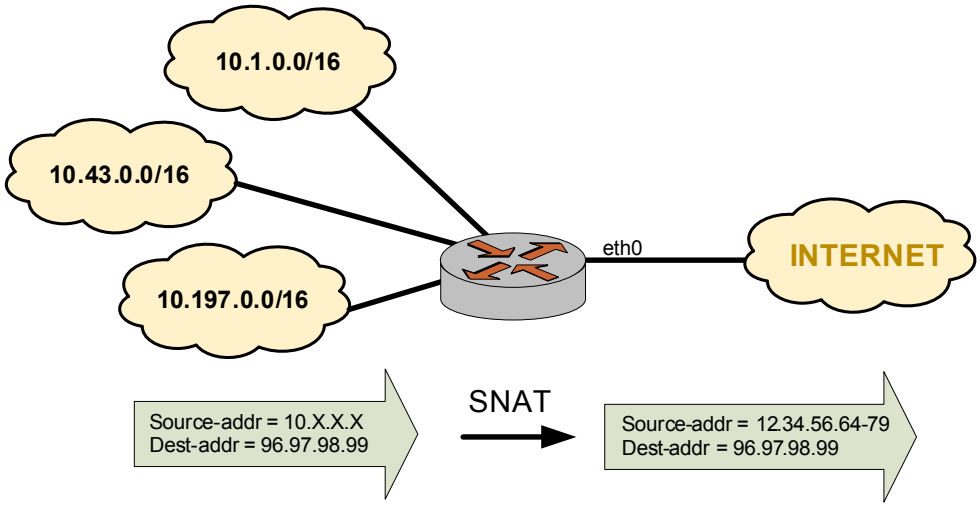
Apply this rule to packets coming from any host on network 10.0.0.0/24.	`vyatta@vyatta# set service nat rule 10 source address 10.0.0.0/24`
Send traffic out through interface eth0. Use 12.34.56.78 as the source address in outgoing packets. Note that the outside-address should be one of the addresses 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 the outside-address.	`vyatta@vyatta# set service nat rule 10 outbound-interface eth0` `vyatta@vyatta# set service nat rule 10 outside-address address 12.34.56.78`
Commit the change.	`vyatta@vyatta# commit`

Show the configuration.	`vyatta@vyatta# show service nat rule 10`
	`outbound-interface eth0`
	`outside-address {`
	`address 12.34.56.78`
	`}`
	`source {`
	`address 10.0.0.0/24`
	`}`
	`type source`

Source NAT (Many-to-Many)

In many-to-many translations, a number of private addresses are NATted to a number of public addresses. Figure 2-3 shows a large private address space (/8) NATted to a few external addresses (/28 or /30).

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 service nat rule 10 type source`
Apply this rule to packets coming from any host on network 10.0.0.0/8.	`vyatta@vyatta# set service nat rule 10 source address 10.0.0.0/8`
Send traffic out through 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 outside-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 outside-addresses.	`vyatta@vyatta# set service nat rule 10 outbound-interface eth0` `vyatta@vyatta# set service nat rule 10 outside-address address 12.34.56.64-12.34.56.79`
Commit the change.	`vyatta@vyatta# commit`

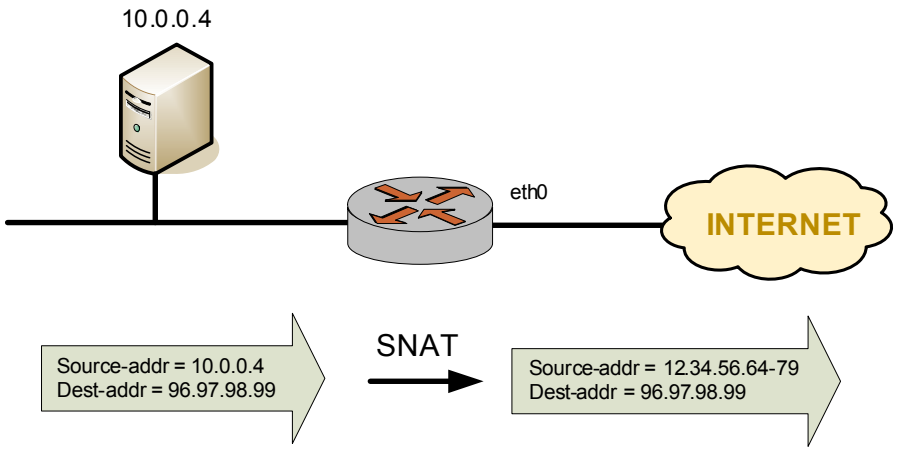
Example 2-3 Source NAT (many-to-many)

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

Source NAT (One-to-Many)

This scenario is less common. One application of this scenario might be to test an upstream load-balancing device. In this scenario, a single test source device behind the NAT device appears externally to be multiple devices; see Figure 2-4.

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 service nat rule 10 type source`

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

Apply this rule to packets coming from address 10.0.0.4.	`vyatta@vyatta# set service nat rule 10 source address 10.0.0.4`
Send traffic out through 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 outside-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 outside-addresses.	`vyatta@vyatta# set service nat rule 10 outbound-interface eth0` `vyatta@vyatta# set service nat rule 10 outside-address address 12.34.56.64-12.34.56.79`
Commit the change.	`vyatta@vyatta# commit`

Show the configuration.	`vyatta@vyatta# show service nat rule 10`
	`outbound-interface eth0`
	`outside-address {`
	`address 12.34.56.64-12.34.56.79`
	`}`
	`source {`
	`address 10.0.0.4`
	`}`
	`type source`

Masquerade

Masquerade NAT is used in situations where LAN devices are assigned private IPaddressess and reside behind the Vyatta router, which has an outside-facing (that is, Internet-facing) interface with only one public IP address. When masquerade NAT is used, all traffic leaving the private network "masquerades" such that packets appear to be sourced from the single public IP address. This mechanism works well for providing Internet connectivity to network devices and hosts that are assigned private (RFC 1918) IP addresses, since otherwise packets sourced from those IP addresses cannot traverse the Internet.

Masquerade NAT rules consist of a set of match conditions containing:

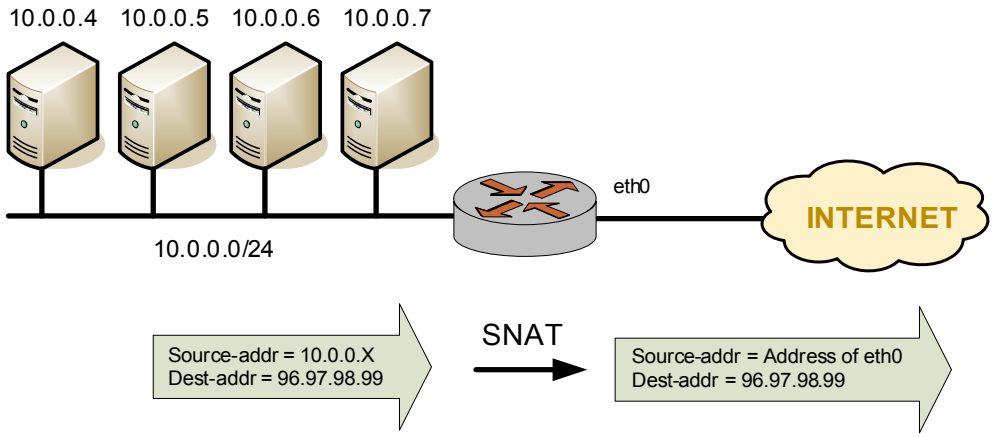
- The source network (usually the private IP network assigned to LAN devices)

- A destination network (usually 0.0.0.0/0, which is used to represent the Internet or “any” address)
- The outbound interface (the Internet-facing interface that is assigned the public IP).

When a packet is matched against the masquerade NAT rule, the source address of the packet is modified before it is forwarded to its destination.

In this scenario, a number of hosts need to initiate sessions to external resources, but only one external public IP address is available. This would be the case, for example, if connecting via a serial interface. 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 service nat rule 10 type masquerade`
Apply this rule to packets coming from any host on network 10.0.0.0/24.	`vyatta@vyatta# set service nat rule 10 source address 10.0.0.0/24`
Send traffic out through interface eth0. Use the IP address of the outbound interface as the outside address.	`vyatta@vyatta# set service nat rule 10 outbound-interface eth0`
Commit the change.	`vyatta@vyatta# commit`

Example 2-5 Masquerade

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

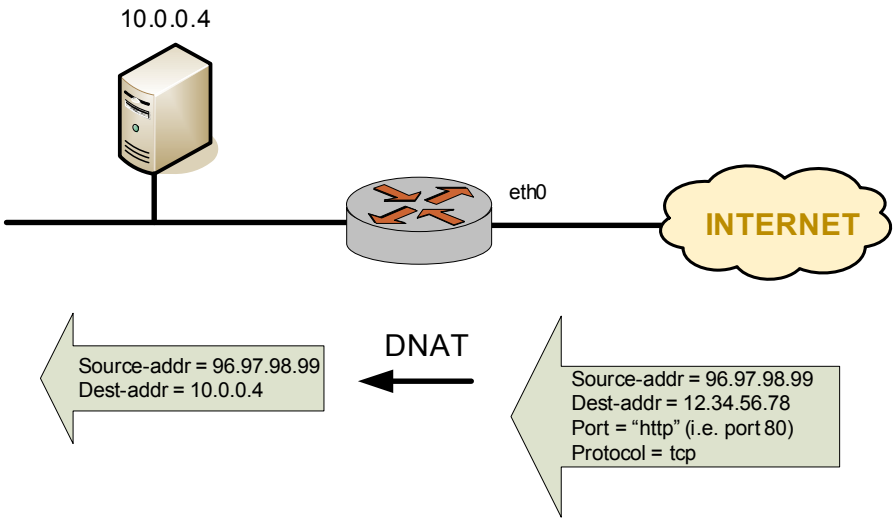
Destination NAT (One-to-One)

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 service nat rule 10 type destination`

Apply this rule to all incoming tcp packets on eth0 bound for address 12.34.56.78 on the HTTP port.	`vyatta@vyatta# set service nat rule 10 inbound-interface eth0`
	`vyatta@vyatta# set service nat rule 10 destination address 12.34.56.78`
	`vyatta@vyatta# set service nat rule 10 protocols tcp`
	`vyatta@vyatta# set service nat rule 10 destination port http`

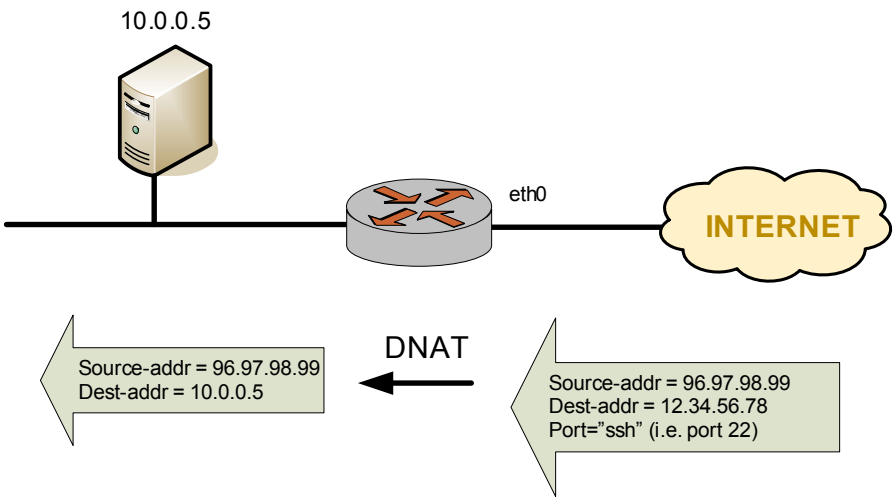
Forward traffic to address 10.0.0.4.	`vyatta@vyatta# set service nat rule 10 inside-address address 10.0.0.4`
Commit the change.	`vyatta@vyatta# commit`

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

Scenario 2: Packets destined for 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



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 service nat rule 10 type destination`

Apply this rule to all incoming packets on eth0 bound for the SSH port of address 12.34.56.78.	`vyatta@vyatta# set service nat rule 10 inbound-interface eth0`
	`vyatta@vyatta# set service nat rule 10 protocol tcp`
	`vyatta@vyatta# set service nat rule 10 destination port ssh`
	`vyatta@vyatta# set service nat rule 10 destination address 12.34.56.78`

Forward traffic to address 10.0.0.5.	`vyatta@vyatta# set service nat rule 10 inside-address address 10.0.0.5`
Commit the change.	`vyatta@vyatta# commit`

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

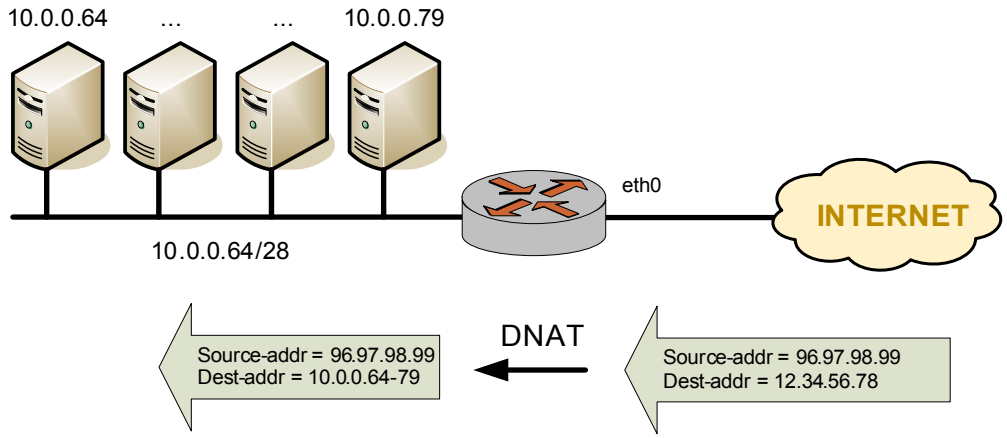
Show the configuration.

```
vyatta@vyatta# show service nat rule 10
      destination {
        address 12.34.56.78
        port ssh
      }
      inbound-interface eth0
      inside-address {
        address 10.0.0.5
      }
      protocols tcp
      type destination
```

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 (i.e. a single IP address 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)

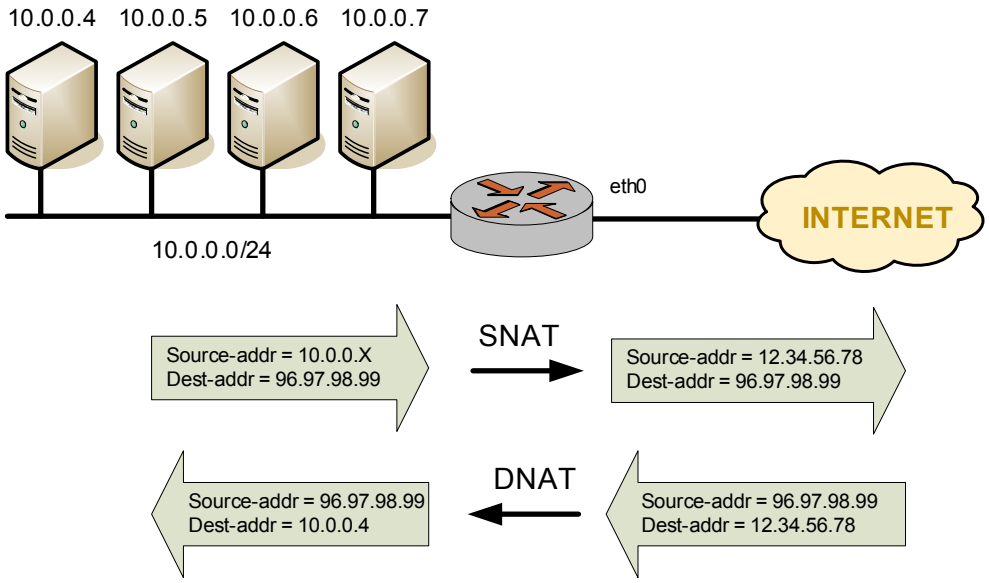
Step	Command
Create Rule 10. Rule 10 is a DNAT rule.	`vyatta@vyatta# set service nat rule 10 type destination`
Apply this rule to all incoming packets on eth0 bound for address 12.34.56.78.	`vyatta@vyatta# set service nat rule 10 inbound-interface eth0` `vyatta@vyatta# set service nat rule 10 destination address 12.34.56.78`
Forward traffic to addresses in the range 10.0.0.64 to 10.0.0.79.	`vyatta@vyatta# set service nat rule 10 inside-address address 10.0.0.64-10.0.0.79`
Commit the change.	`vyatta@vyatta# commit`

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

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.

Example 2-9 Bidirectional NAT

Step	Command
Create Rule 10. Rule 10 is an SNAT rule.	`vyatta@vyatta# set service nat rule 10 type source`
Apply this rule to packets coming from any host in the 10.0.0.0/24 network.	`vyatta@vyatta# set service nat rule 10 source address 10.0.0.0/24`
Send traffic through interface eth0. Use 12.34.56.78 as the source address in outgoing packets.	`vyatta@vyatta# set service nat rule 10 outbound-interface eth0` `vyatta@vyatta# set service nat rule 10 outside-address address 12.34.56.78`
Create Rule 20. Rule 20 is a DNAT rule.	`vyatta@vyatta# set service nat rule 20 type destination`
Apply this rule to all incoming packets on eth0 bound for address 12.34.56.78.	`vyatta@vyatta# set service nat rule 20 inbound-interface eth0` `vyatta@vyatta# set service nat rule 20 destination address 12.34.56.78`
Forward traffic to address 10.0.0.4.	`vyatta@vyatta# set service nat rule 20 inside-address address 10.0.0.4`

Example 2-9 Bidirectional NAT

Commit the change.	`vyatta@vyatta# commit`

Show the configuration.	`vyatta@vyatta# show service nat rule 10`
	`  outbound-interface eth0`
	`  outside-address {`
	`  address 12.34.56.78`
	`  }`
	`  source {`
	`  address 10.0.0.0/24`
	`  }`
	`  type source`
	`vyatta@vyatta# show service nat rule 20`
	`  destination {`
	`  address 12.34.56.78`
	`  }`
	`  inbound-interface eth0`
	`  inside-address {`
	`  address 10.0.0.4`
	`  }`
	`  type destination`

Mapping Address Ranges

The Vyatta system supports mapping an entire network of addresses to another network of addresses. For example, you can map the network 10.0.0.0/24 to 11.22.33.0/24 would mean 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.

Assuming that connections are expected to be initiated from either network, perform the following steps in configuration mode.

Example 2-10 Mapping address ranges

Step	Command
Create Rule 10. Rule 10 is an SNAT rule.	`vyatta@vyatta# set service nat rule 10 type source`
Apply this rule to packets coming from any host in the 10.0.0.0/24 network.	`vyatta@vyatta# set service nat rule 10 source address 10.0.0.0/24`

Example 2-10 Mapping address ranges

Send traffic through interface eth0. Use 11.22.33.*x* as the source address in outgoing packets.	`vyatta@vyatta# set service nat rule 10 outbound-interface eth0` `vyatta@vyatta# set service nat rule 10 outside-address address 11.22.33.0/24`
Create Rule 20. Rule 20 is a SNAT rule.	`vyatta@vyatta# set service nat rule 20 type source`
Apply this rule to packets coming from any host in the 11.22.33.0/24 network.	`vyatta@vyatta# set service nat rule 20 source address 11.22.33.0/24`
Send traffic through interface eth1. Use 10.0.0.*x* as the source address in outgoing packets.	`vyatta@vyatta# set service nat rule 20 outbound-interface eth1` `vyatta@vyatta# set service nat rule 20 outside-address address 10.0.0.0/24`
Commit the change.	`vyatta@vyatta# commit`

Show the configuration.	`vyatta@vyatta# show service nat rule 10`
	`  outbound-interface eth0`
	`  outside-address {`
	`  address 11.22.33.0/24`
	`  }`
	`  source {`
	`  address 10.0.0.0/24`
	`  }`
	`  type source`
	`vyatta@vyatta# show service nat rule 20`
	`  outbound-interface eth1`
	`  outside-address {`
	`  address 10.0.0.0/24`
	`  }`
	`  source {`
	`  address 11.22.33.0/24`
	`  }`
	`  type source`

If connections are only initiated from the 10.0.0.0/24 network then only rule 10 is required. If connections are only initiated from the 11.22.33.0/24 network then only rule 20 is required.

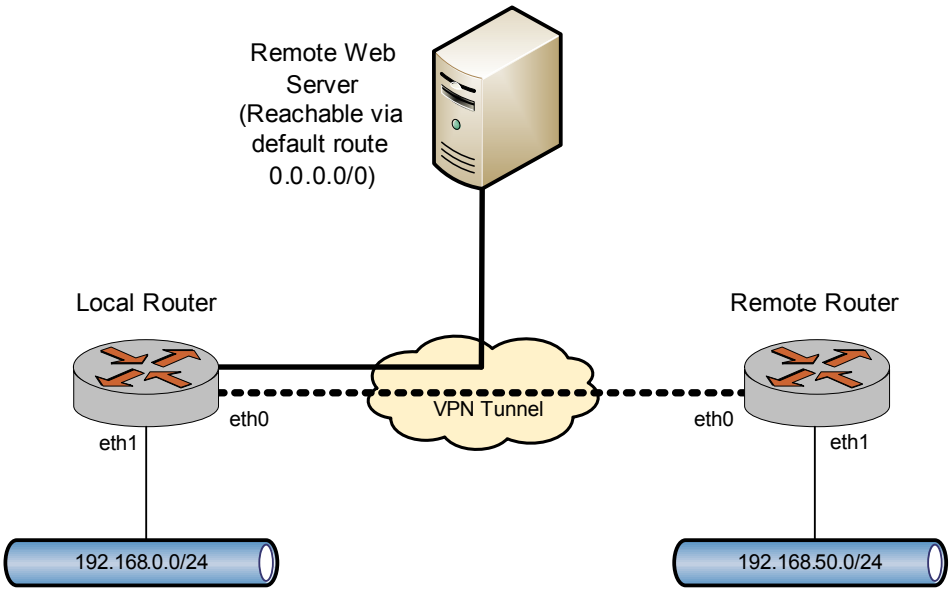
Network mapping works in a similar way with DNAT.

Masquerade NAT and VPN

When a packet is matched against the masquerade NAT rule, the source address of the packet is modified before it is forwarded to its destination. This means that masquerade NAT rules are applied before the VPN process compares the packets against the VPN configuration. If the source network configured for masquerade 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) and 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 being masqueraded by using an "exclusion" rule (that is, a rule using the negation operator ["!"]). This is shown in Figure 2-10.

Figure 2-10 Masquerade NAT and VPN



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

Example 2-11 Masquerade NAT configured to bypass a VPN tunnel

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

Example 2-11 Masquerade NAT configured to bypass a VPN tunnel

Apply this rule to packets coming from any host on network 192.168.0.0/24.	`vyatta@vyatta# set service nat rule 10 source address 192.168.0.0/24`
Apply this rule to all packets except those destined for network 192.168.50.0/24.	`vyatta@vyatta# set service nat rule 10 destination address !192.168.50.0/24`
Send traffic out through interface eth0. Use the IP address of the outbound interface as the outside address.	`vyatta@vyatta# set service nat rule 10 outbound-interface eth0`
Commit the change.	`vyatta@vyatta# commit`

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

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

Consider the NAT rule shown in Example 2-12.

Example 2-12 Single NAT exclusion rule: correct behavior

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

This NAT will exclude the 192.168.50.0/24 network, as expected.

On the other hand, consider the set of two NAT rules shown in Example 2-13.

Example 2-13 Multiple NAT exclusion rules: unexpected behavior

```
rule 10 {
    destination {
        address !192.168.50.0/24
    }
    outbound-interface eth0
    source {
        address 192.168.0.0/24
    }
    type masquerade
}
rule 20 {
    destination {
        address !172.16.50.0/24
    }
    outbound-interface eth0
    source {
        address 192.168.0.0/24
    }
    type 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 is NATted, which is not the desired result.

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

The “exclude” Option

Another way to exclude packets from NAT is to use the **exclude** option, which excludes packets that match a given rule from NAT. Example 2-14 uses **exclude** to provide the same functionality as that demonstrated in Example 2-12.

Example 2-14 Single NAT exclusion rule: correct behavior—using the “**exclude**” option

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

Note that an additional rule (rule 20) is required to handle packets that are not excluded.

Example 2-15 uses **exclude** to provide the behavior that was expected, but not achieved, in Example 2-13. In this example, rule 30 handles packets that are not excluded.

Example 2-15 Multiple NAT exclusion rules: expected behavior—using **exclude**

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

```
    }
    type masquerade
}
rule 20 {
    destination {
        address 172.16.50.0/24
    }
    exclude
    outbound-interface eth0
    source {
        address 192.168.0.0/24
    }
    type masquerade
}
rule 30 {
    outbound-interface eth0
    source {
        address 192.168.0.0/24
    }
    type masquerade
}
```

Chapter 3: NAT Commands

This chapter describes network address translation (NAT) commands.

This chapter contains the following commands.

Configuration Commands	
service nat	Enables NAT on the system.
service nat rule <rule-num>	Defines a NAT rule.
service nat rule <rule-num> description <desc>	Specifies a brief description for a NAT rule.
service nat rule <rule-num> destination	Specifies the destination address and port to match in a NAT rule.
service nat rule <rule-num> disable	Disables a NAT rule.
service nat rule <rule-num> exclude	Creates an exclusion rule, excluding the specified packets from being translated.
service nat rule <rule-num> inbound-interface <interface>	Specifies the interface on which to receive inbound traffic for a destination NAT rule.
service nat rule <rule-num> inside-address	Defines the inside address for a destination NAT rule.
service nat rule <rule-num> log <state>	Specifies whether or not matched NAT rules are logged.
service nat rule <rule-num> outbound-interface <interface>	Specifies the interface on which to transmit outbound traffic for source and masquerade NAT rules.
service nat rule <rule-num> outside-address	Defines an outside address configuration for a Source NAT (SNAT) rule.
service nat rule <rule-num> protocol <protocol>	Specifies which protocols are to have NAT performed on them.
service nat rule <rule-num> source	Specifies the source address and port to match in a NAT rule.
service nat rule <rule-num> type <type>	Sets the type of translation for a NAT rule.
Operational Commands	
clear nat counters	Clears statistics counters for active NAT rules.
show nat rules	Lists configured NAT rules.
show nat statistics	Displays statistics for NAT.
show nat translations	Displays active NAT translations.

clear nat counters

Clears statistics counters for active NAT rules.

Syntax

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

Command Mode

Operational mode.

Parameters

rule-num	A numeric identifier for the rule. The range is 1–9999.

Default

Statistics counters for all NAT translation rules are cleared.

Usage Guidelines

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

service nat

Enables NAT on the system.

Syntax

set service nat

delete service nat

show service nat

Command Mode

Configuration mode.

Configuration Statement

```
service {
    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.

service nat rule <rule-num>

Defines a NAT rule.

Syntax

set service nat rule *rule-num*

delete service nat rule [*rule-num*]

show service nat rule [*rule-num*]

Command Mode

Configuration mode.

Configuration Statement

```
service {
    nat {
        rule rule-num {
        }
    }
}
```

Parameters

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.

NAT rules are executed in numeric order. Note that the identifier of a NAT rule (its number) cannot be changed after configuration. 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.

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

Specifies a brief description for a NAT rule.

Syntax

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

delete service nat rule *rule-num* **description**

show service nat rule *rule-num* **description**

Command Mode

Configuration mode.

Configuration Statement

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

Parameters

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.

service nat rule <rule-num> destination

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

Syntax

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

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

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

Command Mode

Configuration mode.

Configuration Statement

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

Parameters

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. 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.

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

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

service nat rule <rule-num> disable

Disables a NAT rule.

Syntax

set service nat rule *rule-num* **disable**

delete service nat rule *rule-num* **disable**

show service nat rule *rule-num*

Command Mode

Configuration mode.

Configuration Statement

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

Parameters

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.

service nat rule <rule-num> exclude

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

Syntax

set service nat rule *rule-num* **exclude**

delete service nat rule *rule-num* **exclude**

show service nat rule *rule-num*

Command Mode

Configuration mode.

Configuration Statement

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

Parameters

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.

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

Specifies the interface on which to receive inbound traffic for a destination NAT rule.

Syntax

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

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

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

Command Mode

Configuration mode.

Configuration Statement

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

Parameters

rule-num	Mandatory. Multi-node. A numeric identifier for the rule. The range is 1–9999.
interface	The inbound Ethernet or serial interface. 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 inbound Ethernet or serial interface at which destination NAT (DNAT) traffic will be received. inbound Ethernet or serial interface. Destination NAT will be performed on traffic received on this interface.

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

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.

service nat rule <rule-num> inside-address

Defines the inside address for a destination NAT rule.

Syntax

set service nat rule *rule-num* **inside-address** [**address** *address* | **port** *port*]

delete service nat rule *rule-num* **inside-address** [**address** *address* | **port** *port*]

show service nat rule *rule-num* **inside-address** [**address** *address* | **port** *port*]

Command Mode

Configuration mode.

Configuration Statement

```
service {
    nat {
        rule rule-num {
            inside-address {
                address address
                port port
            }
        }
    }
}
```

Parameters

rule-num	Mandatory. Multi-node. A numeric identifier for the rule. The range is 1–9999.
address	The address, range of addresses, or network address to be used to translate the inside address. The following formats are valid: *ipv4-address*: Translates to the specified IP address. *ipv4-address–ipv4-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. *ipv4net*: Translates to the specified network. This is typically used in bidirectional NAT to translate one network of addresses to another.

port	The IP port to be used to translate the inside address. The following formats are valid: *port-num*: Translates to the specified port. 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 defines the "inside" IP address for a destination NAT (DNAT) rule.

Defining an inside address is mandatory for **destination** rules. Inside address is not used with **source** or **masquerade** rules.

Destination rules ingress from the untrusted to the trusted network. The inside address defines the IP address of the host on the trusted network. This is the address that will be substituted for the original destination IP address on packets sent to the system.

Use the **set** form of this command to create an inside address configuration for a Destination NAT (DNAT) rule.

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

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

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

Specifies whether or not matched NAT rules are logged.

Syntax

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

delete service nat rule *rule-num* **log**

show service nat rule *rule-num* **log**

Command Mode

Configuration mode.

Configuration Statement

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

Parameters

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.

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

Specifies the interface on which to transmit outbound traffic for source and masquerade NAT rules.

Syntax

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

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

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

Command Mode

Configuration mode.

Configuration Statement

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

Parameters

rule-num	Mandatory. Multi-node. A numeric identifier for the rule. The range is 1–9999.
interface	Optional for **source** rules; mandatory for **masquerade** rules. Not configurable for **destination** rules. The outbound Ethernet or serial interface. Source NAT (SNAT) or masquerade 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 outbound serial or Ethernet interface from which Source NAT (SNAT) or masquerade traffic is to be transmitted. Source NAT (SNAT) or masquerade will be performed on traffic transmitted from this interface.

Configuring an outbound interface is optional for **source** rules and mandatory for **masquerade** rules. Outbound address cannot be configured for **destination** rules.

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.

service nat rule <rule-num> outside-address

Defines an outside address configuration for a Source NAT (SNAT) rule.

Syntax

set service nat rule *rule-num* **outside-address** [**address** *address* | **port** *port*]

delete service nat rule *rule-num* **outside-address** [**address** | **port**]

show service nat rule *rule-num* **outside-address** [**address** | **port**]

Command Mode

Configuration mode.

Configuration Statement

```
service {
    nat {
        rule rule-num {
            outside-address {
                address address
                port port
            }
        }
    }
}
```

Parameters

rule-num	Mandatory. Multi-node. A numeric identifier for the rule. The range is 1–9999.

address	The address or range of addresses to be used to translate the outside address. 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–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. *ipv4net*: Translates to the specified network. This is typically used in bidirectional NAT to translate one network of addresses to another.
port	The IP port to be used to translate the outside address. The following formats are valid: *port-num*: Translates to the specified port. 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 set the "outside" IP address for a source NAT (SNAT) rule.

Setting the outside address is mandatory for **source** NAT rules. Setting the outside address is not allowed with **destination** NAT rules or **masquerade** rules; for **masquerade** rules, the primary address of the interface is always used.

NOTE *The outside-address should be one of the 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 the outside-address.*

Use the **set** form of this command to create an outside address configuration for a Source NAT (SNAT) rule.

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

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

service nat rule <rule-num> protocol <protocol>

Specifies which protocols are to have NAT performed on them.

Syntax

set service nat rule *rule-num* **protocol** *protocol*

delete service nat rule *rule-num* **protocol**

show service nat rule *rule-num* **protocol**

Command Mode

Configuration mode.

Configuration Statement

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

Parameters

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.

service nat rule <rule-num> source

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

Syntax

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

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

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

Command Mode

Configuration mode.

Configuration Statement

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

Parameters

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. 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.

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

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

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

Sets the type of translation for a NAT rule.

Syntax

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

delete service nat rule *rule-num* **type**

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

Command Mode

Configuration mode.

Configuration Statement

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

Parameters

rule-num	Mandatory. Multi-node. A numeric identifier for the rule. The range is 1–9999.
type	Indicates whether this rule is translating the source IP or the destination IP. Note that this is dependent on the direction of the interface. The supported values are as follows: **source:** This rule translates the source network address. Typically "source" rules are applied to outbound packets. **destination:** This rule translates the destination network address. Typically "destination" rules are applied to inbound packets. **masquerade:** This rule is a type of source NAT. It translates the source network address using the outbound router interface IP address as the translated address.

Default

None.

Usage Guidelines

Use this command to specify whether the rule is translating the source or destination IP address.

You must create explicit NAT rules for each direction of traffic. For example, if you configure a one-to-one source NAT rule and you want inbound traffic to match the NAT rule, you must explicitly create a matching destination NAT rule.

Source rules typically egress from the trusted to the untrusted network. For source NAT rules, the outside 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.

Use the **set** form of this command to specify whether the rule is translating the source or destination IP address.

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

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

show nat rules

Lists configured NAT rules.

Syntax

show nat rules

Command Mode

Operational mode.

Parameters

None.

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 3-1 shows sample output for the **show nat 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 or masquerade 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 30 in the example) means that the rule has been excluded.

Example 3-1 Displaying NAT rule information

```
vyatta@vyatta:~$ show nat rules

Type Codes:  SRC - source, DST - destination, MASQ - masquerade
              X at the front of rule implies rule is excluded

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

20     DST   eth2     daddr 172.16.139.0/24 to 192.168.74.0/24
    proto-all         dport ANY

X30    MASQ  eth0     saddr ANY to 172.16.117.200
    proto-tcp         sport ANY to 80
                      when daddr ANY, dport 8080
```

show nat statistics

Displays statistics for NAT.

Syntax

show nat statistics

Command Mode

Operational mode.

Parameters

None.

Usage Guidelines

Use this command to display current statistics for NAT.

Examples

Example 3-2 shows sample output for the **show nat statistics** command.

Example 3-2 Displaying NAT statistics information

```
vyatta@vyatta:~$ show nat statistics

Type Codes:  SRC - source, DST - destination, MASQ - masquerade

rule  count     type     IN         OUT
----  -------   ----  ---------  ---------
1     6         MASQ      -      eth2
2     6         MASQ      -      eth3
```

show nat translations

Displays active NAT translations.

Syntax

show nat translations [**destination** [**address** *addr* | **detail** | **monitor** [**detail**]] | **detail** | **monitor** | **source** [**address** *addr* | **detail** | **monitor** [**detail**]]]

Command Mode

Operational mode.

Parameters

destination	Provides output of destination NAT translations.
destination address *addr*	Provides output of detination NAT translations for destination address *addr*.
destination detail	Provides detailed output of destination NAT translations.
destination monitor	Provides real-time monitoring of destination NAT translations. Type Ctrl-C to quit.
destination monitor detail	Provides detailed real-time monitoring of destination NAT translations. Type Ctrl-C to quit.
detail	Provides detailed output of all NAT translations.
monitor	Provides real-time monitoring of all NAT translations. Type Ctrl-C to quit.
source	Provides output of source NAT translations.
source address *addr*	Provides output of source NAT translations for source address *addr*.
source detail	Provides detailed output of source NAT translations.
source monitor	Provides real-time monitoring of source NAT translations. Type Ctrl-C to quit.

source monitor detail	Provides detailed real-time monitoring of source NAT translations. Type Ctrl-C to quit.

Usage Guidelines

Use this command to display NAT translation information.

Examples

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

Example 3-3 Displaying NAT translations

```
vyatta@vyatta:~$ show nat translations
Pre-NAT             Post-NAT            Type  Prot  Timeout
15.0.0.16           172.16.117.100      snat  tcp   106
15.0.0.20           172.16.117.101      snat  tcp   431959
15.0.0.16           172.16.117.100      snat  tcp   58
20.0.0.16:23        15.0.0.16:5000      dnat  tcp   431996
vyatta@vyatta:~$
```

Example 3-4 shows sample output for the **show nat translations detail** command.

Example 3-4 Displaying NAT translation detail

```
vyatta@vyatta:~$ show nat translations detail
Inside src          Inside dst         Outside src          Outside dst
15.0.0.16:41920     172.16.117.17:22   172.16.117.100:41920 172.16.117.17:22
  tcp: snat: 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: snat: 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: snat: 15.0.0.16 ==> 172.16.117.100  timeout: 54 use: 1
172.16.117.17:51391  20.0.0.16:23      172.16.117.17:51391  15.0.0.16:5000
  tcp: dnat: 20.0.0.16:23 ==> 15.0.0.16:5000  timeout: 431993 use: 1
vyatta@vyatta:~$
```

Example 3-5 shows sample output for the **show nat translations source address 15.0.0.16** command.

Example 3-5 Displaying NAT translation for source address 15.0.0.16

```
vyatta@vyatta:~$ show nat translations source address 15.0.0.16
Inside src          Inside dst         Outside src          Outside dst
15.0.0.16:57634     172.16.117.17:22   172.16.117.100:57634 172.16.117.17:22
  tcp: snat: 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: snat: 15.0.0.16 ==> 172.16.117.100  timeout: 115 use: 1
vyatta@vyatta:~$
```

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

Example 3-6 Monitoring source NAT translations

```
vyatta@vyatta:~$ show nat translations source monitor
Type control-C to quit
Pre-NAT              Post-NAT             Type  Prot  Timeout  Type
15.0.0.16            172.16.117.100       snat  icmp  30       new
15.0.0.16            172.16.117.100       snat  icmp  29       update
15.0.0.16            172.16.117.100       snat  icmp           destroy
15.0.0.16            172.16.117.100       snat  icmp  30       new
15.0.0.16            172.16.117.100       snat  icmp  30       update
15.0.0.16            172.16.117.100       snat  icmp           destroy
15.0.0.20            172.16.117.101       snat  tcp            destroy
vyatta@vyatta:~$
```

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

Example 3-7 Detailed monitoring of source NAT translations

```
vyatta@vyatta:~$ show nat translations source monitor detail
Type control-C to quit
Pre-NAT              Post-NAT             Type  Prot  Timeout  Type
15.0.0.16            172.16.117.17      172.16.117.100       172.16.117.17
  icmp: snat: 15.0.0.16 ==> 172.16.117.100  timeout: 30 type: new
15.0.0.16            172.16.117.17      172.16.117.100       172.16.117.17
  icmp: snat: 15.0.0.16 ==> 172.16.117.100  timeout: 30 type: update
15.0.0.16            172.16.117.17      172.16.117.100       172.16.117.17
  icmp: snat: 15.0.0.16 ==> 172.16.117.100 type: destroy
15.0.0.16            172.16.117.17      172.16.117.100       172.16.117.17
  icmp: snat: 15.0.0.16 ==> 172.16.117.100  timeout: 30 type: new
15.0.0.16            172.16.117.17      172.16.117.100       172.16.117.17
  icmp: snat: 15.0.0.16 ==> 172.16.117.100  timeout: 30 type: update
15.0.0.16            172.16.117.17      172.16.117.100       172.16.117.17
  icmp: snat: 15.0.0.16 ==> 172.16.117.100 type: destroy
vyatta@vyatta:~$
```

Glossary of Acronyms

ACL	access control list
ADSL	Asymmetric Digital Subscriber Line
API	Application Programming Interface
AS	autonomous system
ARP	Address Resolution Protocol
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
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
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
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

RIB	Routing Information Base
RIP	Routing Information Protocol
RIPng	RIP next generation
Rx	receive
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
VPN	Virtual Private Network
VRRP	Virtual Router Redundancy Protocol
WAN	wide area network
WAP	wireless access point
WPA	Wired Protected Access