Concepts & Examples
ScreenOS Reference Guide

Volume 8:
Address Translation

Release 5.4.0, Rev. A

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

Part Number: 530-015775-01, Revision A

FCC Statement

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. The equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: The equipment described in this manual generates and may radiate radio-frequency energy. If it is not installed in accordance with Juniper Networks' installation instructions, it may cause interference with radio and television reception. This equipment has been tested and found to comply with the limits for a Class B digital device in accordance with the specifications in part 15 of the FCC rules. These specifications are designed to provide reasonable protection against such interference in a residential installation. However, there is no guarantee that interference will not occur in a particular installation.

If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Consult the dealer or an experienced radio/TV technician for help.
- Connect the equipment to an outlet on a circuit different from that to which the receiver is connected.

Caution: Changes or modifications to this product could void the user's warranty and authority to operate this device.

Disclaimer

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR JUNIPER NETWORKS REPRESENTATIVE FOR A COPY.

Writers: ScreenOS Team

Editor: Lisa Eldridge

Table of Contents

About This Volume

Volume 8: Address Translation focuses on the various methods available in ScreenOS to perform address translation. This volume contains the following chapters, which describe how to configure the Juniper Networks security device to perform the following types of translation:

- Chapter 1, "Address Translation," gives an overview of the various translation options, which are covered in detail in subsequent chapters.
- Chapter 2, "Source Network Address Translation," describes NAT-src, the translation of the source IP address in a packet header, with and without Port Address Translation (PAT).
- Chapter 3, "Destination Network Address Translation," describes NAT-dst, the translation of the destination IP address in a packet header, with and without destination port address mapping. This section also includes information on the packet flow when doing NAT-src, routing considerations, and address shifting.
- Chapter 4, "Mapped and Virtual Addresses," describes the mapping of one destination IP address to another based on IP address alone (mapped IP) or based on destination IP address and destination port number (virtual IP).

NOTE: For coverage of interface-based Source Network Address Translation—referred to simply as *NAT*—see "NAT Mode" on page **2**-102.

Document Conventions

This document uses several types of conventions, which are introduced in the following sections:

CLI Conventions

The following conventions are used to present the syntax of CLI commands in examples and in text.

In examples:

- Anything inside square brackets [ ] is optional.
- Anything inside braces **{ }** is required.
- If there is more than one choice, each choice is separated by a pipe (|). For example:

  ```
  set interface { ethernet1 | ethernet2 | ethernet3 } manage
  ```

  means "set the management options for the ethernet1, the ethernet2, *or* the ethernet3 interface."

- Variables are in *italic* type:

  ```
  set admin user name1 password xyz
  ```

In text:

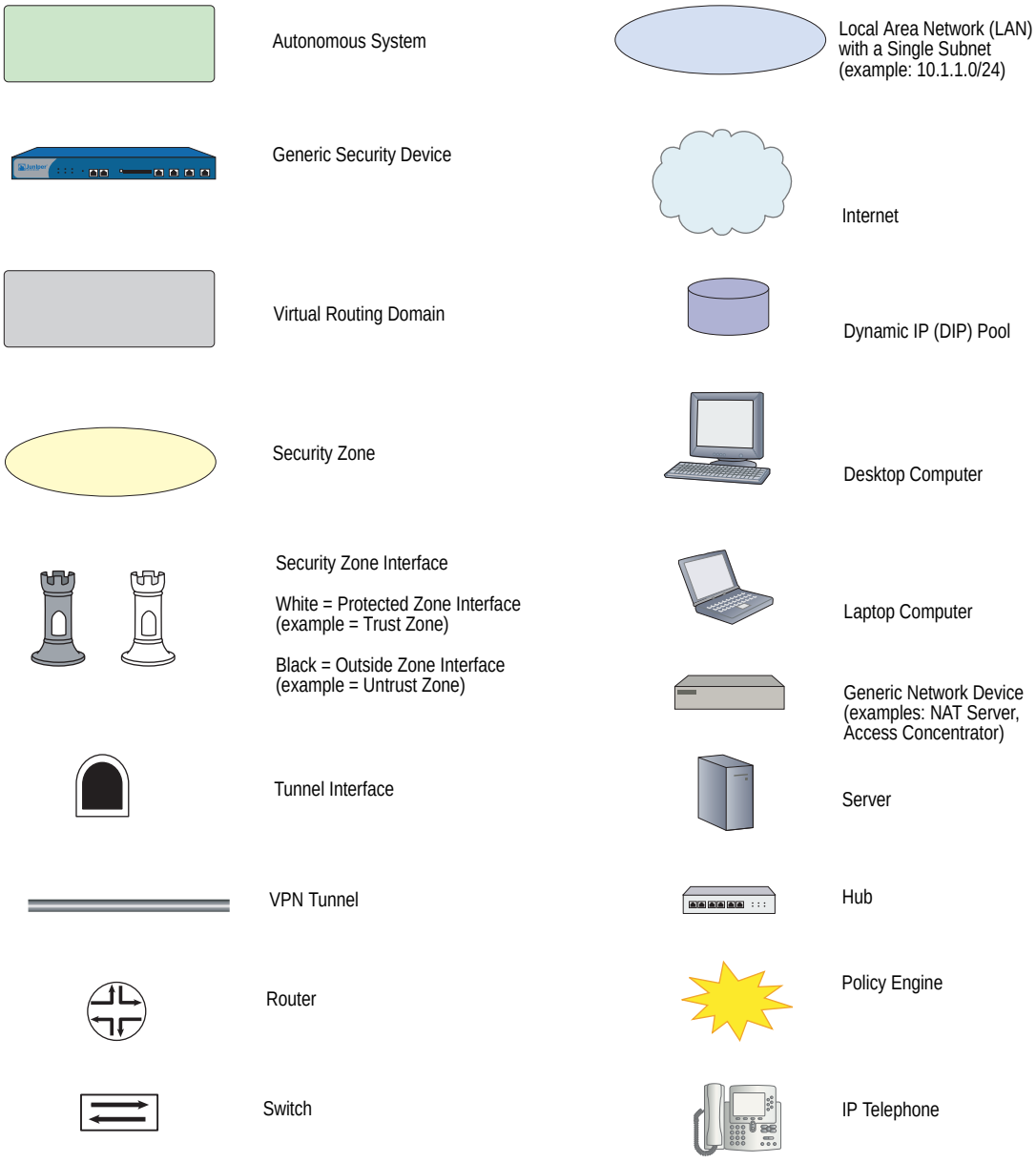
- Commands are in **boldface** type.
- Variables are in *italic* type.

NOTE: When entering a keyword, you only have to type enough letters to identify the word uniquely. For example, typing **set adm u kath j12fmt54** is enough to enter the command **set admin user kathleen j12fmt54**. Although you can use this shortcut when entering commands, all the commands documented here are presented in their entirety.

Illustration Conventions

The following figure shows the basic set of images used in illustrations throughout this manual.

Figure 1: Images in Manual Illustrations



Naming Conventions and Character Types

ScreenOS employs the following conventions regarding the names of objects—such as addresses, admin users, auth servers, IKE gateways, virtual systems, VPN tunnels, and zones—defined in ScreenOS configurations:

- If a name string includes one or more spaces, the entire string must be enclosed within double quotes; for example:

  set address trust “local LAN” 10.1.1.0/24

- Any leading spaces or trailing text within a set of double quotes are trimmed; for example, **“ local LAN ”** becomes **“local LAN”**.

- Multiple consecutive spaces are treated as a single space.

- Name strings are case-sensitive, although many CLI keywords are case-insensitive. For example, **“local LAN”** is different from **“local lan”**.

ScreenOS supports the following character types:

- Single-byte character sets (SBCS) and multiple-byte character sets (MBCS). Examples of SBCS are ASCII, European, and Hebrew. Examples of MBCS—also referred to as double-byte character sets (DBCS)—are Chinese, Korean, and Japanese.

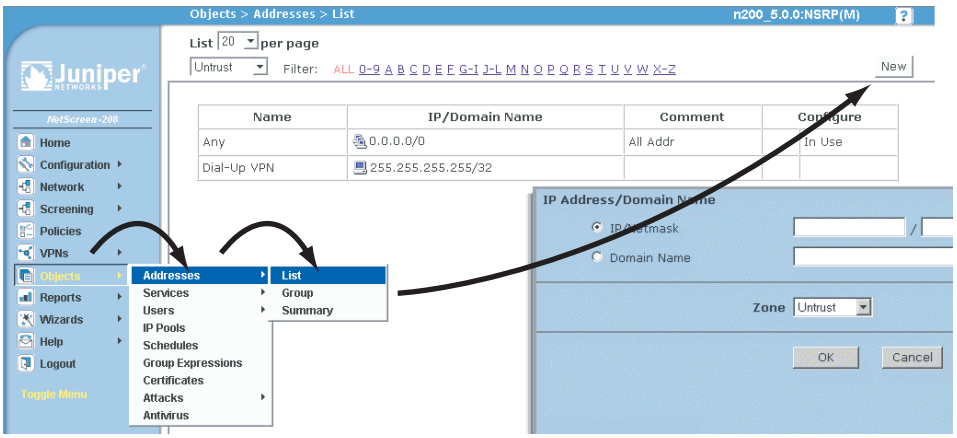
- ASCII characters from 32 (0x20 in hexadecimals) to 255 (0xff), except double quotes (“), which have special significance as an indicator of the beginning or end of a name string that includes spaces.

NOTE: A console connection only supports SBCS. The WebUI supports both SBCS and MBCS, depending on the character sets that your browser supports.

WebUI Conventions

A chevron (>) shows the navigational sequence through the WebUI, which you follow by clicking menu options and links. The following figure shows the following path to the address configuration dialog box—Objects > Addresses > List > New:

Figure 2: WebUI Navigation



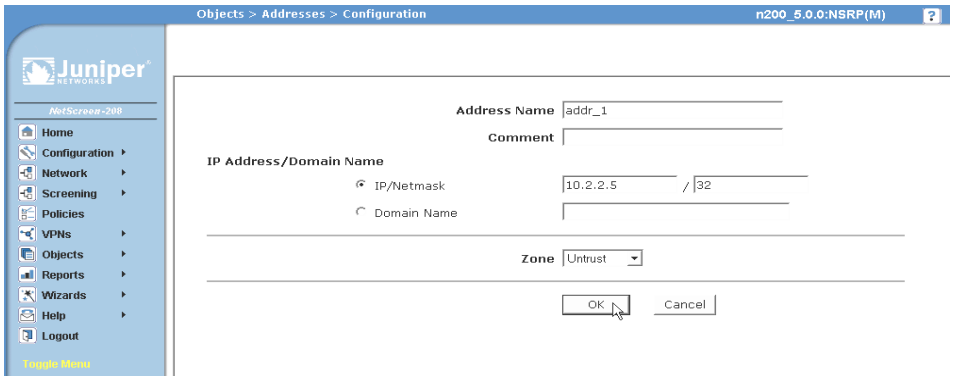
To perform a task with the WebUI, you first navigate to the appropriate dialog box, where you then define objects and set parameters. The set of instructions for each task is divided into navigational path and configuration settings:

The next figure lists the path to the address configuration dialog box with the following sample configuration settings:

Objects > Addresses > List > New: Enter the following, then click **OK**:

Address Name: addr_1
IP Address/Domain Name:
IP/Netmask: (select), 10.2.2.5/32
Zone: Untrust

Figure 3: Navigational Path and Configuration Settings



Juniper Networks Documentation

To obtain technical documentation for any Juniper Networks product, visit www.juniper.net/techpubs/.

For technical support, open a support case using the Case Manager link at http://www.juniper.net/support/ or call 1-888-314-JTAC (within the United States) or 1-408-745-9500 (outside the United States).

If you find any errors or omissions in this document, please contact us at the email address below:

techpubs-comments@juniper.net

Chapter 1
Address Translation

ScreenOS provides many methods for performing source and destination IP and port address translation. This chapter describes the various address translation methods available and contains the following sections:

Introduction to Address Translation

ScreenOS provides several mechanisms for applying Network Address Translation (NAT). NAT includes the translation of the Internet Protocol (IP) address in an IP packet header and, optionally, the translation of the port number in the Transmission Control Protocol (TCP) segment or User Datagram Protocol (UDP) datagram header. The translation can involve the source address (and, optionally, the source port number), the destination address (and, optionally, the destination port number), or a combination of translated elements.

Source Network Address Translation

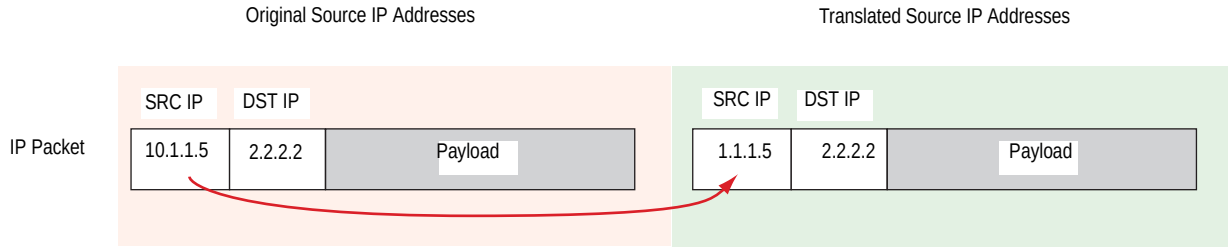
When performing Source Network Address Translation (NAT-src), the security device translates the original source IP address to a different address. The translated address can come from a Dynamic IP (DIP) pool or from the egress interface of the security device. If the security device draws the translated address from a DIP pool, it can do so either arbitrarily or deterministically; that is, it can draw any address from the DIP pool at random, or it can consistently draw a specific address in relation to the original source IP address.

NOTE: Deterministic address translation uses a technique called address shifting, which is explained later in this chapter. For information about address shifting that applies to NAT-src, see "NAT-Src from a DIP Pool with Address Shifting" on page 20. For information about address shifting that applies to NAT-dst, see "NAT-Src and NAT-Dst in the Same Policy" on page 50.

If the translated address comes from the egress interface, the security device translates the source IP address in all packets to the IP address of that interface. You can configure the security device to apply NAT-src at either the interface level or at the policy level. If you configure a policy to apply NAT-src and the ingress interface is in NAT mode, the policy-based NAT-src settings override the interface-based NAT. (This chapter focusses on policy-based NAT-src. For details on interface-based NAT-src—or NAT alone—see "NAT Mode" on page **2-**102. For more information about DIP pools, see "Dynamic IP Pools" on page **2-**152.)

NOTE: You can use policy-based NAT-src when the ingress interface is in Route or NAT mode. If it is in NAT mode, the policy-level NAT-src parameters supersede the interface-level NAT parameters.

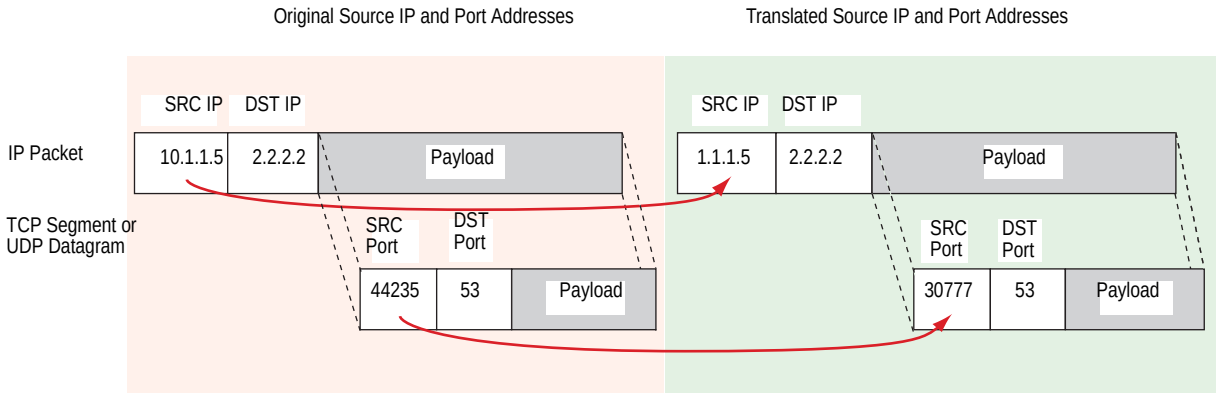
Figure 1: Source IP Address Translation



With policy-based NAT-src, you can optionally choose to have the security device perform Port Address Translation (PAT) on the original source port number. When PAT is enabled, the security device can translate up to ~64,500 different IP addresses to a single IP address with up to ~64,500 different port numbers. The security device uses the unique, translated port number to maintain session state information for traffic to and from the same, single IP address. For interface-based NAT-src—or just NAT—PAT is enabled automatically. Because the security device translates all original IP addresses to the same translated IP address (that of the egress interface), the security device uses the translated port number to identify each session to which a packet belongs. Similarly, if a DIP pool consists of only one IP address and you want the security device to apply NAT-src to multiple hosts using that address, then PAT is required for the same reason.

NOTE: With PAT enabled, the security device maintains a pool of free port numbers to assign along with addresses from the DIP pool. The figure of ~64,500 is derived by subtracting 1023, the numbers reserved for the well-known ports, from the maximum number of ports, which is 65,535. Thus, when the security device performs NAT-src with a DIP pool containing a single IP address and PAT is enabled, the security device can translate the original IP addresses of up to ~64,500 hosts to a single IP address and translate each original port number to a unique port number.

Figure 2: Source IP and Source Port Address Translation



For custom applications that require a specific source port number to operate properly, performing PAT causes such applications to fail. To provide for such cases, you can disable PAT.

NOTE: For more information about NAT-src, see “Source Network Address Translation” on page 13.

Destination Network Address Translation

Screen OS offers the following three mechanisms for performing Destination Network Address Translation (NAT-dst):

- **Policy-based NAT-dst**: see “Policy-Based NAT-Dst” on page 4
- **MIP**: see “Mapped IP” on page 6
- **VIP**: see “Virtual IP” on page 6

All three options translate the original destination IP address in an IP packet header to a different address. WIth policy-based NAT-dst and VIPs, you can optionally enable port mapping.

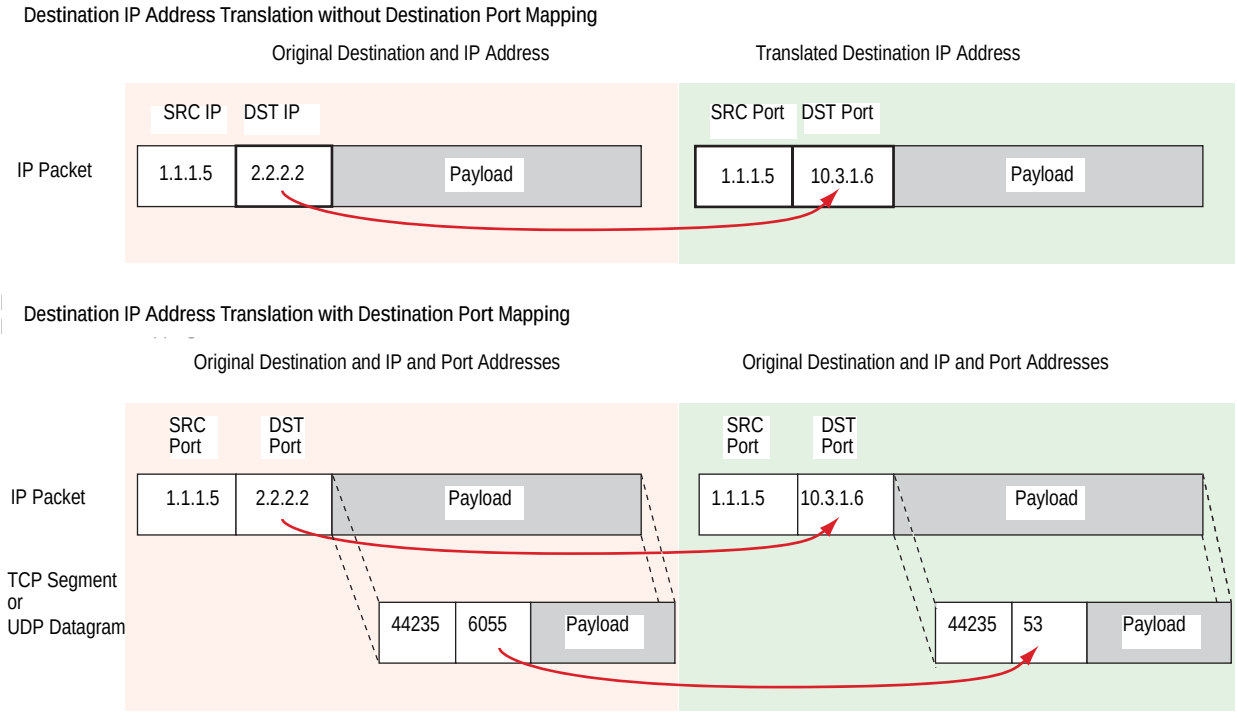
NOTE: For information about port mapping, see the “Policy-Based NAT-Dst” on page 4 and “Destination Network Address Translation” on page 27.

ScreenOS does not support the use of policy-based NAT-dst in combination with MIPs and VIPs. If you have configured a MIP or VIP, the security device applies the MIP or VIP to any traffic to which a policy-based NAT-dst configuration also applies. In other words, MIPs and VIPs disable policy-based NAT-dst if the security device is accidentally configured to apply both to the same traffic.

Policy-Based NAT-Dst

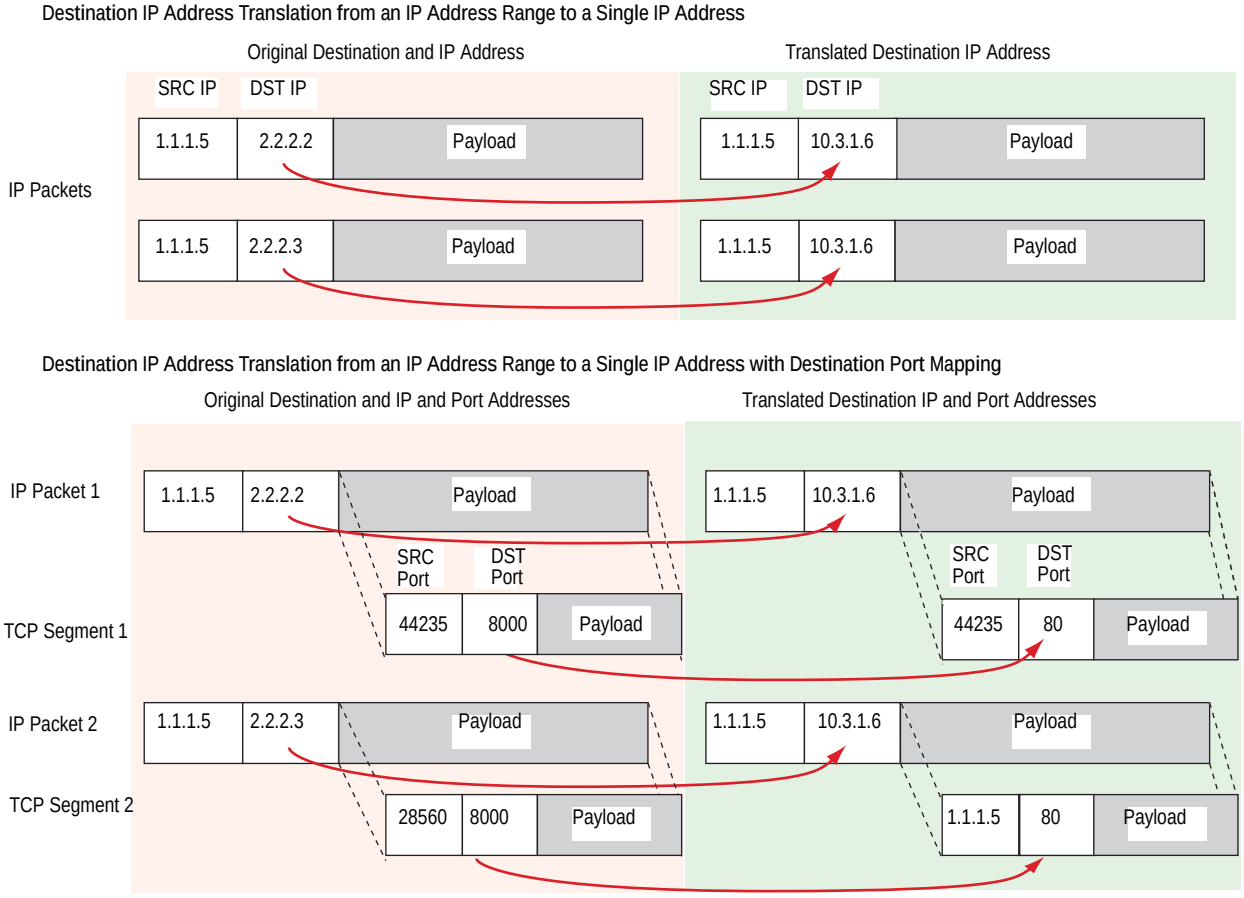
You can configure a policy to translate one destination IP address to another address, one IP address range to a single IP address, or one IP address range to another IP address range. When a single destination IP address translates to another IP address or an IP address range translates to a single IP address, ScreenOS can support NAT-dst with or without port mapping. Port mapping is the deterministic translation of one original destination port number to another specific number, unlike PAT, which translates any original source port number randomly assigned by the initiating host to another number randomly assigned by the security device.

Figure 3: Destination IP Address Translation



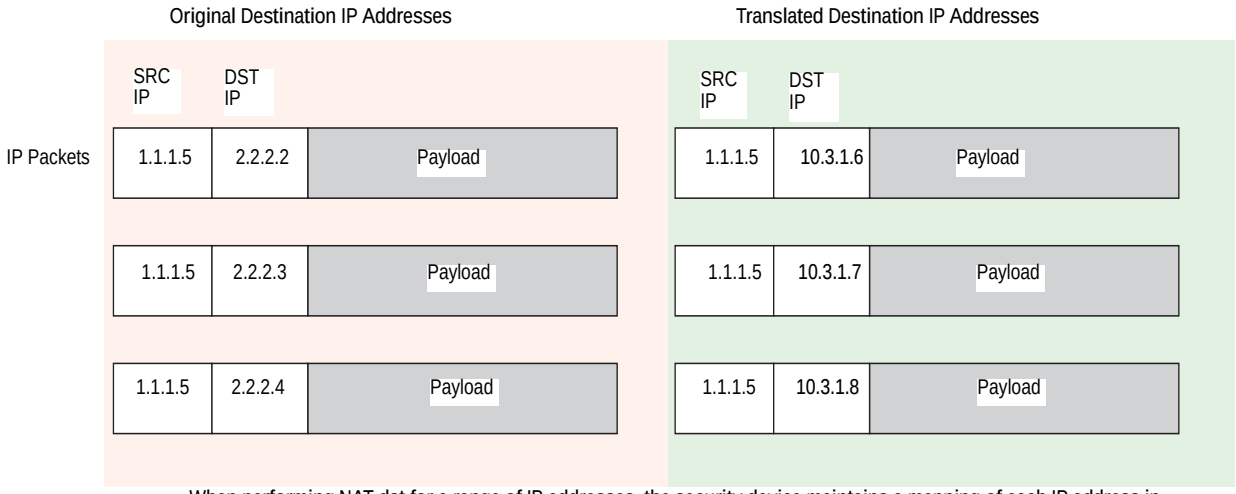
When you configure a policy to perform NAT-dst to translate an address range to a single address, the security device translates any destination IP address from within the user-defined range of original destination addresses to a single address. You can also enable port mapping.

Figure 4: NAT-Dst from an IP Address Range to a Single IP Address



When you configure a policy to perform NAT-dst for an address range, the security device uses address shifting to translate a destination IP address from within a range of original destination addresses to a known address in another range of addresses.

Figure 5: NAT-Dst with Address Shifting



When performing NAT-dst for a range of IP addresses, the security device maintains a mapping of each IP address in one address range to a corresponding IP address in another address range.

NOTE: You can combine NAT-src and NAT-dst within the same policy. Each translation mechanism operates independently and unidirectional. That is, if you enable NAT-dst on traffic from zone1 to zone2, the security device does not perform NAT-src on traffic originating from zone2 and destined to zone1 unless you specifically configure it to do so. For more information, see "Directional Nature of NAT-Src and NAT-Dst" on page 10. For more information about NAT-dst, see "Destination Network Address Translation" on page 27.

Mapped IP

A Mapped Internet Protocol (MIP) is a mapping of one IP address to another IP address. You define one address in the same subnet as an interface IP address. The other address belongs to the host to which you want to direct traffic. Address translation for a MIP behaves bidirectionally, so that the security device translates the destination IP address in all traffic coming to a MIP to the host IP address and source IP address in all traffic originating from the host IP address to the MIP address. MIPs do not support port mapping. For more information about MIPs, see "Mapped IP Addresses" on page 63.

Virtual IP

A Virtual Internet Protocol (VIP) is a mapping of one IP address to another IP address based on the destination port number. A single IP address defined in the same subnet as an interface can host mappings of several services—identified by various destination port numbers—to as many hosts. VIPs also support port mapping. Unlike MIPs, address translation for a VIP behaves unidirectional. The security device translates the destination IP address in all traffic coming to a VIP to a host IP address. (The security device only checks if the destination IP address is bound to a VIP on packets arriving at an interface bound to the Untrust zone.) The security device does not translate the original source IP address in outbound traffic from a VIP host to that of the VIP address. Instead, the security device applies interface-based or policy-based NAT-src if you have previously configured it. Otherwise, the security device does not perform any NAT-src on traffic originating from a VIP host. For more information about VIPs, see "Virtual IP Addresses" on page 80.

NOTE: On some Juniper Networks security devices, you can define a VIP to be the same as an interface IP address. This ability is convenient when the security device only has one assigned IP address, and when the IP address is assigned dynamically.

Whereas the address translation mechanisms for MIPs and VIPs are bidirectional, the capabilities provided by policy-based NAT-src and NAT-dst separate address translation for inbound and outbound traffic, providing better control and security. For example, if you use a MIP to a webserver, whenever that server initiates outbound traffic to get an update or patch, its activity is exposed, which might provide information for a vigilant attacker to exploit. The policy-based address translation methods allow you to define a different address mapping when the webserver receives traffic (using NAT-dst) than when it initiates traffic (using NAT-src). By thus keeping its activities hidden, you can better protect the server from anyone attempting to gather information in preparation for an attack. In this ScreenOS release, policy-based NAT-src and NAT-dst offer a single approach that can duplicate and surpass the functionality of interface-based MIPs and VIPs.

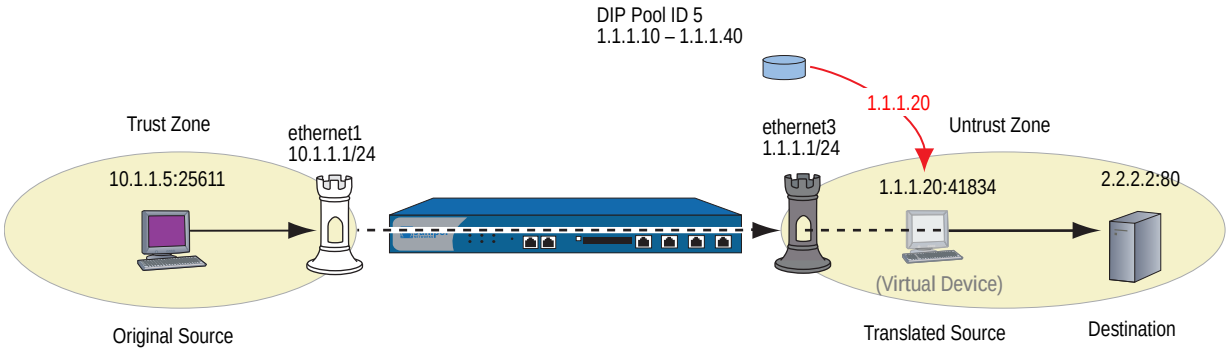
Policy-Based Translation Options

ScreenOS provides the following ways to apply Source Network Address Translation (NAT-src) and Destination Network Address Translation (NAT-dst). Note that you can always combine NAT-src with NAT-dst within the same policy.

Example: NAT-Src from a DIP Pool with PAT

The security device translates the original source IP address to an address drawn from a Dynamic IP (DIP) pool. The security device also applies source Port Address Translation (PAT). For more information, see “NAT-Src from a DIP Pool with PAT Enabled” on page 15.

Figure 6: NAT-Src with Port Address Translation

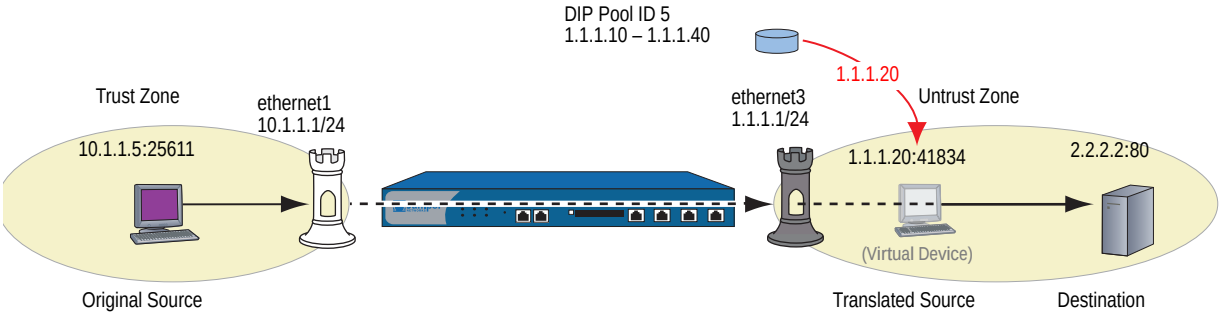


NOTE: In Figure 6 and in subsequent figures, a “virtual device” is used to indicate a translated source or destination address when that address does not belong to an actual device.

Example: NAT-Src From a DIP Pool Without PAT

The security device translates the original source IP address to an address drawn from a DIP pool. The security device does not apply source PAT. For more information, see “NAT-Src from a DIP Pool with PAT Disabled” on page 18.

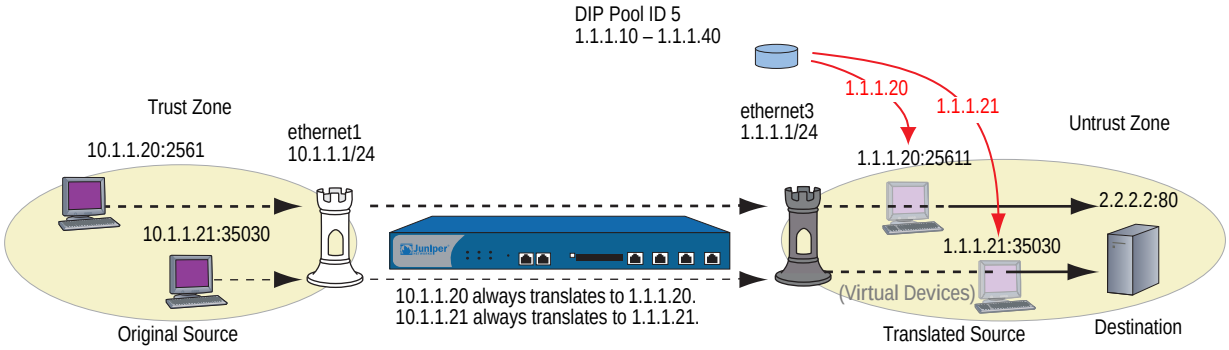
Figure 7: NAT-Src Without Port Address Translation



Example: NAT-Src from a DIP Pool with Address Shifting

The security device translates the original source IP address to an address drawn from a dynamic IP (DIP) pool, consistently mapping each original address to a particular translated address. The security device does not apply source Port Address Translation (PAT). For more information, see "NAT-Src from a DIP Pool with Address Shifting" on page 20.

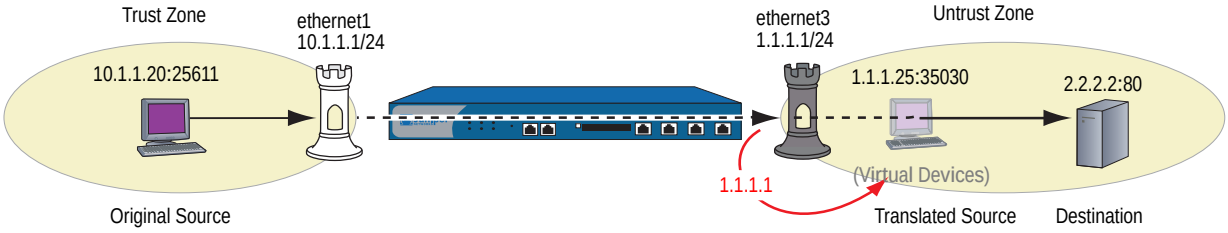
Figure 8: NAT-Src with Address Shifting



Example: NAT-Src from the Egress Interface IP Address

The security device translates the original source IP address to the address of the egress interface. The security device applies source PAT as well. For more information, see "NAT-Src from the Egress Interface IP Address" on page 24.

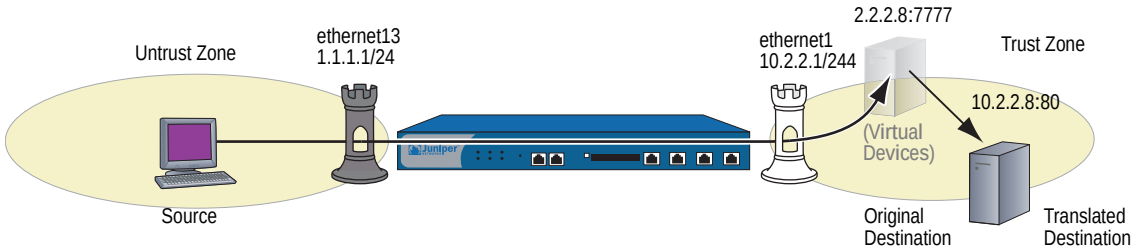
Figure 9: NAT-Src Using the Egress Interface IP Address



Example: NAT-Dst to a Single IP Address with Port Mapping

The security device performs Destination Network Address Translation (NAT-dst) and destination port mapping. For more information, see "NAT-Dst with Port Mapping" on page 47.

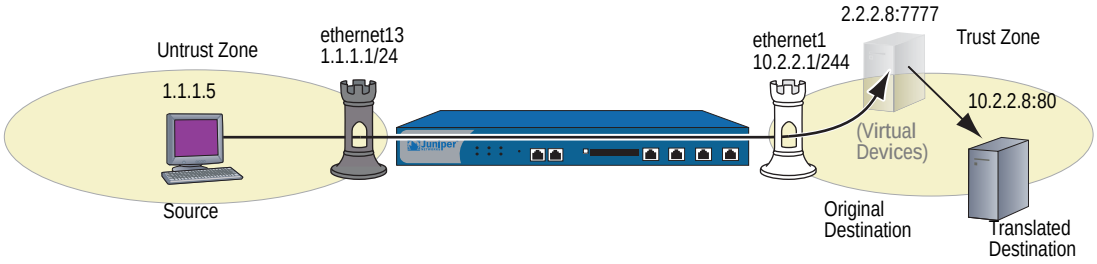
Figure 10: NAT-Dst with Port Mapping



Example: NAT-Dst to a Single IP Address Without Port Mapping

The security device performs NAT-dst but does not change the original destination port number. For more information, see “Destination Network Address Translation” on page 27.

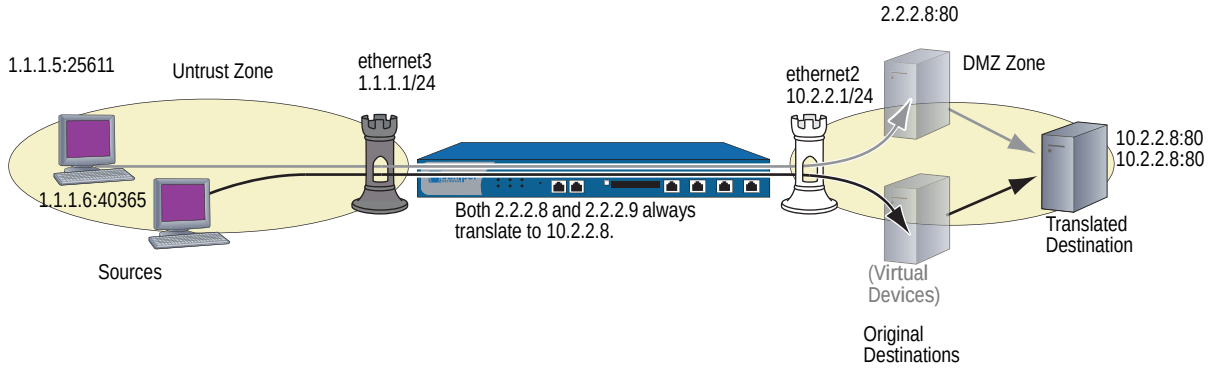
Figure 11: NAT-Dst Without Port Mapping



Example: NAT-Dst from an IP Address Range to a Single IP Address

The security device performs NAT-dst to translate a range of IP addresses to a single IP address. If you also enable port mapping, the security device translates the original destination port number to another number. For more information, see “NAT-Dst—Many-to-One Mapping” on page 41.

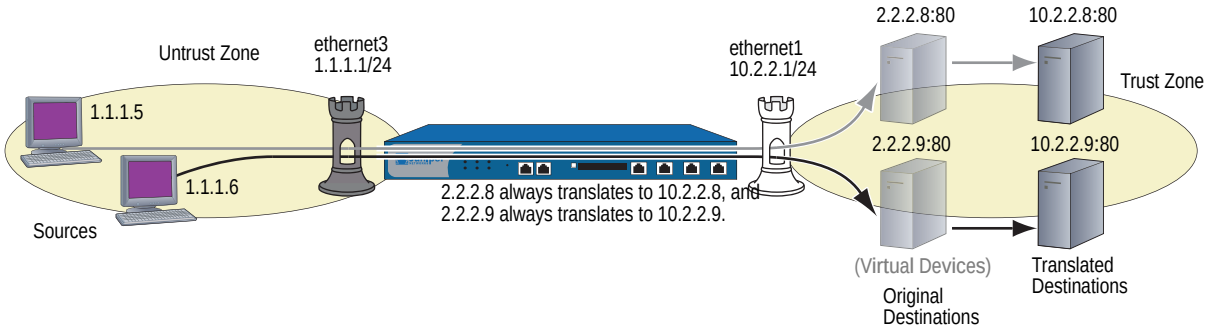
Figure 12: NAT-Dst from an Address Range to a Single IP Address



Example: NAT-Dst Between IP Address Ranges

When you apply NAT-dst for a range of IP addresses, the security device maintains a consistent mapping of an original destination address to a translated address within the specified range using a technique called address shifting. Note that address shifting does not support port mapping. For more information, see "NAT-Dst—Many-to-Many Mapping" on page 44.

Figure 13: NAT-Dst Between Address Ranges

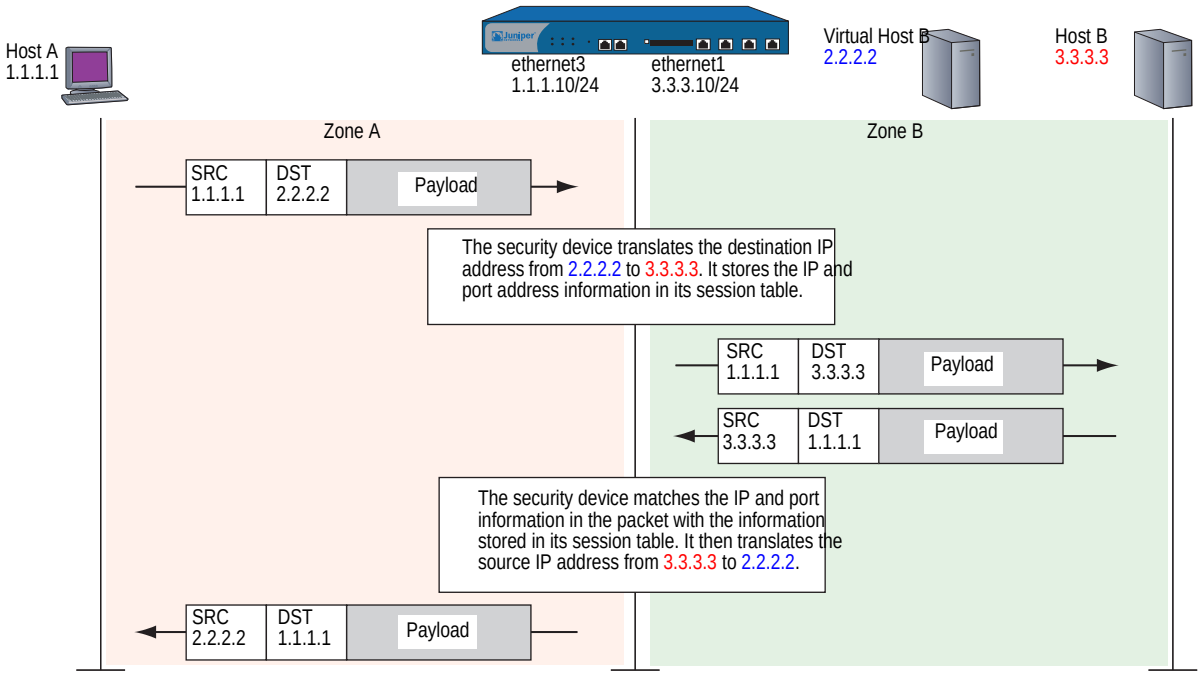


Directional Nature of NAT-Src and NAT-Dst

The application of NAT-src is separate from that of NAT-dst. You determine their applications on traffic by the direction indicated in a policy. For example, if the security device applies a policy requiring NAT-dst for traffic sent from host A to virtual host B, the security device translates the original destination IP address from 2.2.2.2 to 3.3.3.3. (It also translates the source IP address from 3.3.3.3 to 2.2.2.2 in responding traffic.)

Figure 14: Packet Flow for NAT-Dst

set policy from “zone A” to “zone B” “host A” “virtual host B” any nat dst ip 3.3.3.3 permit set vrouter trust-vr route 2.2.2.2/32 interface ethernet1.

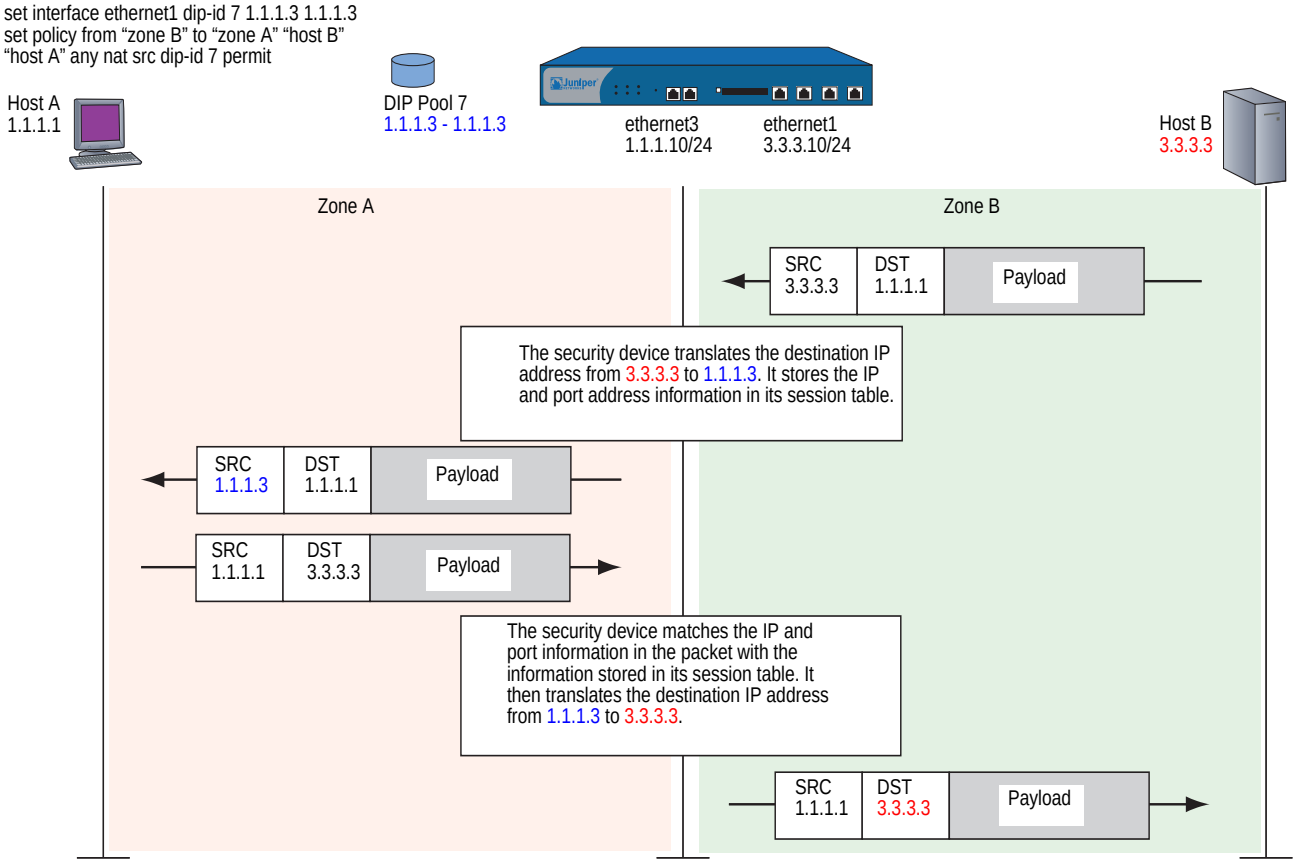


NOTE: You must set a route to 2.2.2.2/32 (virtual host B) so the security device can do a route lookup to determine the destination zone. For more about NAT-dst routing issues, see “Routing for NAT-Dst” on page 32.

However, if you only create the above policy specifying NAT-dst from host A to host B, the security device does not translate the original source IP address of host B if host B initiates traffic to host A, rather than responding to traffic from host A. For the security device to do translate the source IP address of host B when it initiates traffic to host A, you must configure a second policy from host B to host A specifying NAT-src. (This behavior differs from that of MIPs. See “Mapped IP Addresses” on page 63.)

NOTE: To retain focus on the IP address translation mechanisms, Port Address Translation (PAT) is not shown. If you specify fixed port numbers for a DIP pool consisting of a single IP address, then only one host can use that pool at a time. The policy above specifies only “host B” as the source address. If “host B” is the only host that uses DIP pool 7, then it is unnecessary to enable PAT.

Figure 15: Packet Flow for Source IP Address Translation



Chapter 2

Source Network Address Translation

ScreenOS provides many methods for performing Source Network Address Translation (NAT-src) and source Port Address Translation (PAT). This chapter describes the various address translation methods available and is organized into the following sections:

Introduction to NAT-Src

It is sometimes necessary for the security device to translate the original source IP address in an IP packet header to another address. For example, when hosts with private IP addresses initiate traffic to a public address space, the security device must translate the private source IP address to a public one. Also, when sending traffic from one private address space through a VPN to a site using the same addresses, the security devices at both ends of the tunnel must translate the source and destination IP addresses to mutually neutral addresses.

NOTE: For information about public and private IP addresses, see "Public IP Addresses" on page **2**-56 and "Private IP Addresses" on page **2**-56.

A dynamic IP (DIP) address pool provides the security device with a supply of addresses from which to draw when performing Source Network Address Translation (NAT-src). When a policy requires NAT-src and references a specific DIP pool, the security device draws addresses from that pool when performing the translation.

NOTE: The DIP pool must use addresses within the same subnet as the default interface in the destination zone referenced in the policy. If you want to use a DIP pool with addresses outside the subnet of the destination zone interface, you must define a DIP pool on an extended interface. For more information, see "Using DIP in a Different Subnet" on page 156.

The DIP pool can be as small as a single IP address, which, if you enable Port Address Translation (PAT), can support up to ~64,500 hosts concurrently. Although all packets receiving a new source IP address from that pool get the same address, they each get a different port number. By maintaining a session table entry that matches the original address and port number with the translated address and port number, the security device can track which packets belong to which session and which sessions belong to which hosts.

NOTE: When PAT is enabled, the security device also maintains a pool of free port numbers to assign along with addresses from the DIP pool. The figure of ~64,500 is derived by subtracting 1023, the numbers reserved for the well-known ports, from the maximum number of ports, which is 65,535.

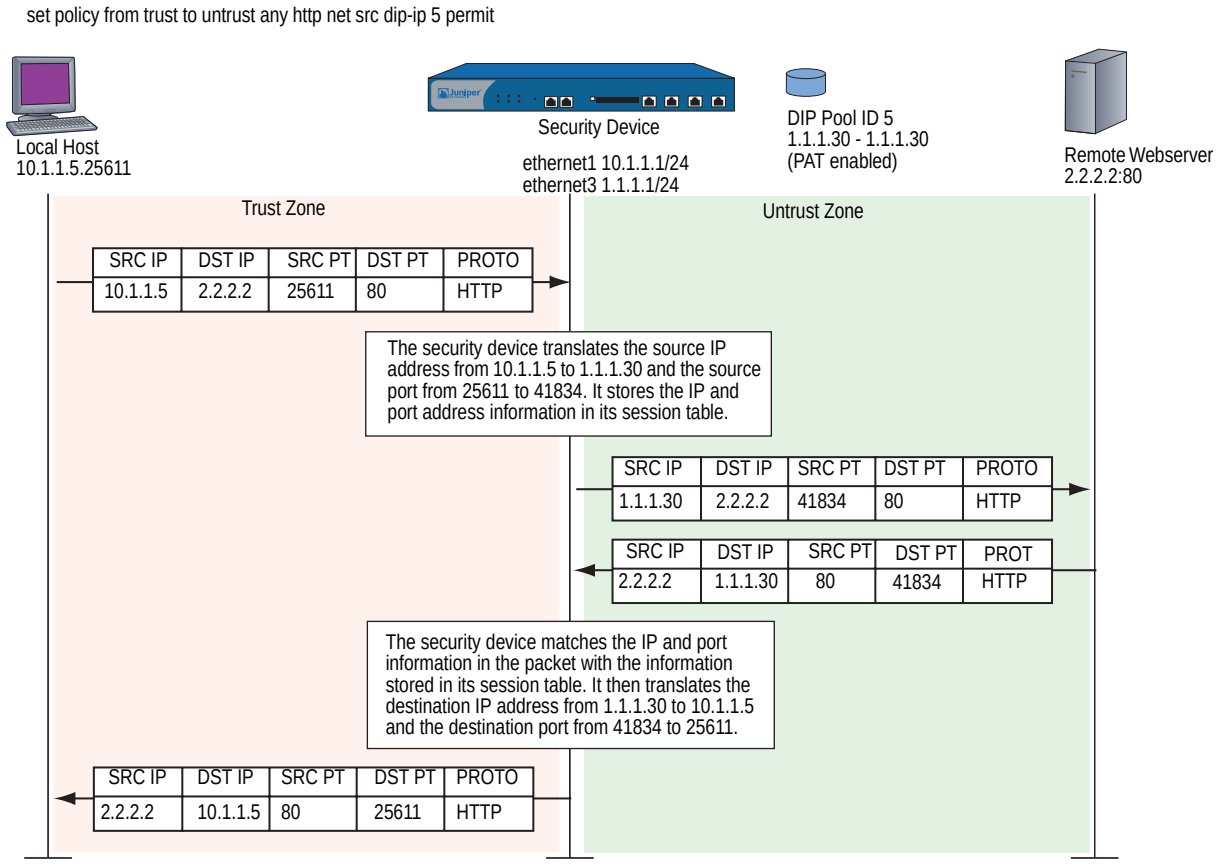
If you use NAT-src but do not specify a DIP pool in the policy, the security device translates the source address to that of the egress interface in the destination zone. In such cases, PAT is required and automatically enabled.

For applications requiring that a particular source port number remain fixed, you must disable PAT and define a DIP pool with a range of IP addresses large enough for each concurrently active host to receive a different translated address. For fixed-port DIP, the security device assigns one translated source address to the same host for all its concurrent sessions. In contrast, when the DIP pool has PAT enabled, the security device might assign a single host different addresses for different concurrent sessions—unless you define the DIP as sticky (see "Sticky DIP Addresses" on page 155).

NAT-Src from a DIP Pool with PAT Enabled

When applying Source Network Address Translation (NAT-src) with Port Address Translation (PAT), the security device translates IP addresses and port numbers, and performs stateful inspection as illustrated in Figure 16 (note that only the elements in the IP packet and TCP segment headers relevant to NAT-src are shown).

Figure 16: NAT-Src Using a DIP Pool with PAT Enabled



Example: NAT-Src with PAT Enabled

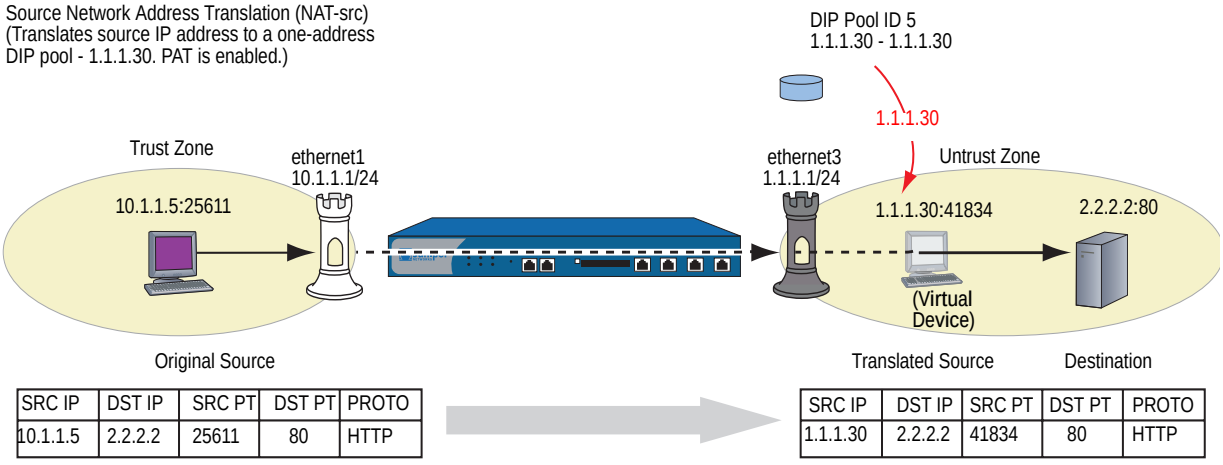
In this example, you define a DIP pool 5 on ethernet3, an interface bound to the Untrust zone. The DIP pool contains a single IP address—1.1.1.30—and has PAT enabled by default.

NOTE: When you define a DIP pool, the security device enables PAT by default. To disable PAT, you must add the key word fix-port to the end of the CLI command, or clear the Port Translation option on the DIP configuration page in the WebUI. For example, **set interface ethernet3 dip 5 1.1.1.30 1.1.1.30 fix-port**, or Network > Interfaces > Edit (for ethernet3) > DIP: ID: 5; Start: 1.1.1.30; End: 1.1.1.30; Port Translation: (clear).

You then set a policy that instructs the security device to perform the following tasks:

- Permit HTTP traffic from any address in the Trust zone to any address in the Untrust zone
- Translate the source IP address in the IP packet header to 1.1.1.30, which is the sole entry in DIP pool 5
- Translate the original source port number in the TCP segment header or UDP datagram header to a new, unique number
- Send HTTP traffic with the translated source IP address and port number out ethernet3 to the Untrust zone

Figure 17: NAT-Src with PAT Enabled



SRC IP	DST IP	SRC PT	DST PT	PROTO
10.1.1.5	2.2.2.2	25611	80	HTTP

SRC IP	DST IP	SRC PT	DST PT	PROTO
1.1.1.30	2.2.2.2	41834	80	HTTP

WebUI

1. **Interfaces**

   Network > Interfaces > Edit (for ethernet1): Enter the following, then click **Apply**:

   Zone Name: Trust
   Static IP: (select this option when present)
   IP Address/Netmask: 10.1.1.1/24

   Select the following, then click **OK**:

   Interface Mode: NAT

   Network > Interfaces > Edit (for ethernet3): Enter the following, then click **OK**:

   Zone Name: Untrust
   Static IP: (select this option when present)
   IP Address/Netmask: 1.1.1.1/24

2. DIP

Network > Interfaces > Edit (for ethernet3) > DIP > New: Enter the following, then click **OK**:

ID: 5
IP Address Range: (select), 1.1.1.30 ~ 1.1.1.30
Port Translation: (select)
In the same subnet as the interface IP or its secondary IPs: (select)

3. Policy

Policies > (From: Trust, To: Untrust) New: Enter the following, then click **OK**:

Source Address:
Address Book Entry: (select), Any
Destination Address:
Address Book Entry: (select), Any
Service: HTTP
Action: Permit

> Advanced: Enter the following, then click **Return** to set the advanced options and return to the basic configuration page:

NAT:
Source Translation: (select)
(DIP on): 5 (1.1.1.30 - 1.1.1.30)/X-late

CLI

1. Interfaces

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.1.1.1/24
set interface ethernet1 nat
set interface ethernet3 zone untrust
set interface ethernet3 ip 1.1.1.1/24
```

2. DIP

```
set interface ethernet3 dip 5 1.1.1.30 1.1.1.30
```

3. Policy

```
set policy from trust to untrust any any http nat src dip-id 5 permit
save
```

NAT-Src from a DIP Pool with PAT Disabled

Certain configurations or situations may require you to perform Source Network Address Translation (NAT-src) for the IP address without performing Port Address Translation (PAT) for the source port number. For example, a custom application might require a specific number for the source port address. In such a case, you can define a policy instructing the security device to perform NAT-src without performing PAT.

Example: NAT-Src with PAT Disabled

In this example, you define a DIP pool 6 on ethernet3, an interface bound to the Untrust zone. The DIP pool contains a range of IP addresses from 1.1.1.50 to 1.1.1.150. You disable PAT. You then set a policy that instructs the security device to perform the following tasks:

- Permit traffic for a user-defined service named “e-stock” from any address in the Trust zone to any address in the Untrust zone

NOTE: It is assumed that you have previously defined the user-defined service “e-stock.” This fictional service requires that all e-stock transactions originate from specific source port numbers. For this reason, you must disable PAT for DIP pool 6.

- Translate the source IP address in the IP packet header to any available address in DIP pool 6
- Retain the original source port number in the TCP segment header or UDP datagram header
- Send e-stock traffic with the translated source IP address and original port number out ethernet3 to the Untrust zone

WebUI

1. **Interfaces**

   Network > Interfaces > Edit (for ethernet1): Enter the following, then click **Apply**:

   Zone Name: Trust
   Static IP: (select this option when present)
   IP Address/Netmask: 10.1.1.1/24
   Select the following, then click **OK**:
   Interface Mode: NAT

   Network > Interfaces > Edit (for ethernet3): Enter the following, then click **OK**:

   Zone Name: Untrust
   Static IP: (select this option when present)
   IP Address/Netmask: 1.1.1.1/24

2. **DIP**

   Network > Interfaces > Edit (for ethernet3) > DIP > New: Enter the following, then click **OK**:

   ID: 6
   IP Address Range: (select), 1.1.1.50 ~ 1.1.1.150
   Port Translation: (clear)
   In the same subnet as the interface IP or its secondary IPs: (select)

3. **Policy**

   Policies > (From: Trust, To: Untrust) New: Enter the following, then click **OK**:

   Source Address:
   Address Book Entry: (select), Any
   Destination Address:
   Address Book Entry: (select), Any
   Service: e-stock
   Action: Permit

   > Advanced: Enter the following, then click **Return** to set the advanced options and return to the basic configuration page:

   NAT:
   Source Translation: (select)
   DIP on: (select), 6 (1.1.1.50 - 1.1.1.150)

CLI

1. **Interfaces**

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.1.1.1/24
set interface ethernet1 nat
set interface ethernet3 zone untrust
set interface ethernet3 ip 1.1.1.1/24
```

2. **DIP**

```
set interface ethernet3 dip 6 1.1.1.50 1.1.1.150 fix-port
```

3. **Policy**

```
set policy from trust to untrust any any e-stock nat src dip-id 6 permit
save
```

NAT-Src from a DIP Pool with Address Shifting

You can define a one-to-one mapping from an original source IP address to a translated source IP address for a range of IP addresses. Such a mapping ensures that the security device always translates a particular source IP address from within that range to the same translated address within a DIP pool. There can be any number of addresses in the range. You can even map one subnet to another subnet, with a consistent one-to-one mapping of each original address in one subnet to its translated counterpart in the other subnet.

One possible use for performing NAT-src with address shifting is to provide greater policy granularity on another security device that receives traffic from the first one. For example, the admin for Device-A at site A defines a policy that translates the source addresses of its hosts when communicating with Device-B at site B through a site-to-site VPN tunnel. If Device-A applies NAT-src using addresses from a DIP pool without address shifting, the Device-B admin can only configure generic policies regarding the traffic it can allow from site A. Unless the Device-B admin knows the specific translated IP addresses, he can only set inbound policies for the range of source addresses drawn from the Device-A DIP pool. On the other hand, if the Device-B admin knows what the translated source addresses are (because of address shifting), the Device-B admin can now be more selective and restrictive with the policies he sets for inbound traffic from site A.

Note that it is possible to use a DIP pool with address shifting enabled in a policy that applies to source addresses beyond the range specified in the pool. In such cases, the security device passes traffic from all source addresses permitted in the policy, applying NAT-src with address shifting to those addresses that fall within the DIP pool range but leaving those addresses that fall outside the DIP pool range unchanged. If you want the security device to apply NAT-src to all source addresses, make sure that the range of source addresses is smaller or the same size as the range of the DIP pool.

NOTE: The security device does not support source Port Address Translation (PAT) with address shifting.

Example: NAT-Src with Address Shifting

In this example, you define DIP pool 10 on ethernet3, an interface bound to the Untrust zone. You want to translate five addresses between 10.1.1.11 and 10.1.1.15 to five addresses between 1.1.1.101 and 1.1.1.105, and you want the relationship between each original and translated address to be consistent:

Table 1: NAT-Src with Address Shifting

Original Source IP Address	Translated Source IP Address
10.1.1.11	1.1.1.101
10.1.1.12	1.1.1.102
10.1.1.13	1.1.1.103
10.1.1.14	1.1.1.104
10.1.1.15	1.1.1.105

You define addresses for five hosts in the Trust zone and added them to an address group named "group1". The addresses for these hosts are 10.1.1.11, 10.1.1.12, 10.1.1.13, 10.1.1.14, and 10.1.1.15. You configure a policy from the Trust zone to the Untrust zone that references that address group in a policy to which you apply NAT-src with DIP pool 10. The policy instructs the security device to perform NAT-src whenever a member of goup1 initiates HTTP traffic to an address in the Untrust zone. Furthermore, the security device always performs NAT-src from a particular IP address—such as 10.1.1.13—to the same translated IP address—1.1.1.103.

You then set a policy that instructs the security device to perform the following tasks:

- Permit HTTP traffic from group1 in the Trust zone to any address in the Untrust zone
- Translate the source IP address in the IP packet header to its corresponding address in DIP pool 10
- Send HTTP traffic with the translated source IP address and port number out ethernet3 to the Untrust zone

WebUI

1. **Interfaces**
   Network > Interfaces > Edit (for ethernet1): Enter the following, then click **Apply**:

   Zone Name: Trust
   Static IP: (select this option when present)
   IP Address/Netmask: 10.1.1.1/24
   Select the following, then click **OK**:
   Interface Mode: NAT

Network > Interfaces > Edit (for ethernet3): Enter the following, then click **OK**:

Zone Name: Untrust
Static IP: (select this option when present)
IP Address/Netmask: 1.1.1.1/24

2. **DIP**

Network > Interfaces > Edit (for ethernet3) > DIP > New: Enter the following, then click **OK**:

ID: 10
IP Shift: (select)
From: 10.1.1.11
To: 1.1.1.101 ~ 1.1.1.105
In the same subnet as the interface IP or its secondary IPs: (select)

3. **Addresses**

Objects > Addresses > List > New: Enter the following information, then click **OK**:

Address Name: host1
IP Address/Domain Name:
IP/Netmask: (select), 10.1.1.11/32
Zone: Trust

Objects > Addresses > List > New: Enter the following information, then click **OK**:

Address Name: host2
IP Address/Domain Name:
IP/Netmask: (select), 10.1.1.12/32
Zone: Trust

Objects > Addresses > List > New: Enter the following information, then click **OK**:

Address Name: host3
IP Address/Domain Name:
IP/Netmask: (select), 10.1.1.13/32
Zone: Trust

Objects > Addresses > List > New: Enter the following information, then click **OK**:

Address Name: host4
IP Address/Domain Name:
IP/Netmask: (select), 10.1.1.14/32
Zone: Trust

Objects > Addresses > List > New: Enter the following information, then click **OK**:

Address Name: host5
IP Address/Domain Name:
IP/Netmask: (select), 10.1.1.15/32
Zone: Trust

Objects > Addresses > Group > (for Zone: Trust) New: Enter the following group name, move the following addresses, then click **OK**:

Group Name: group1

Select **host1** and use the < < button to move the address from the Available Members column to the Group Members column.

Select **host2** and use the < < button to move the address from the Available Members column to the Group Members column.

Select **host3** and use the < < button to move the address from the Available Members column to the Group Members column.

Select **host4** and use the < < button to move the address from the Available Members column to the Group Members column.

Select **host5** and use the < < button to move the address from the Available Members column to the Group Members column.

4. Policy

Policies > (From: Trust, To: Untrust) New: Enter the following, then click **OK**:

Source Address:
Address Book Entry: (select), group1
Destination Address:
Address Book Entry: (select), Any
Service: HTTP
Action: Permit

> Advanced: Enter the following, then click **Return** to set the advanced options and return to the basic configuration page:

NAT:
Source Translation: (select)
(DIP on): 10 (1.1.1.101 - 1.1.1.105)

CLI

1. Interfaces

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.1.1.1/24
set interface ethernet1 nat
set interface ethernet3 zone untrust
set interface ethernet3 ip 1.1.1.1/24
```

2. DIP

```
set interface ethernet3 dip 10 shift-from 10.1.1.11 to 1.1.1.101 1.1.1.105
```

3. **Addresses**

```
set address trust host1 10.1.1.11/32
set address trust host2 10.1.1.12/32
set address trust host3 10.1.1.13/32
set address trust host4 10.1.1.14/32
set address trust host5 10.1.1.15/32

set group address trust group1 add host1
set group address trust group1 add host2
set group address trust group1 add host3
set group address trust group1 add host4
set group address trust group1 add host5
```

4. **Policy**

```
set policy from trust to untrust group1 any http nat src dip-id 10 permit
save
```

NAT-Src from the Egress Interface IP Address

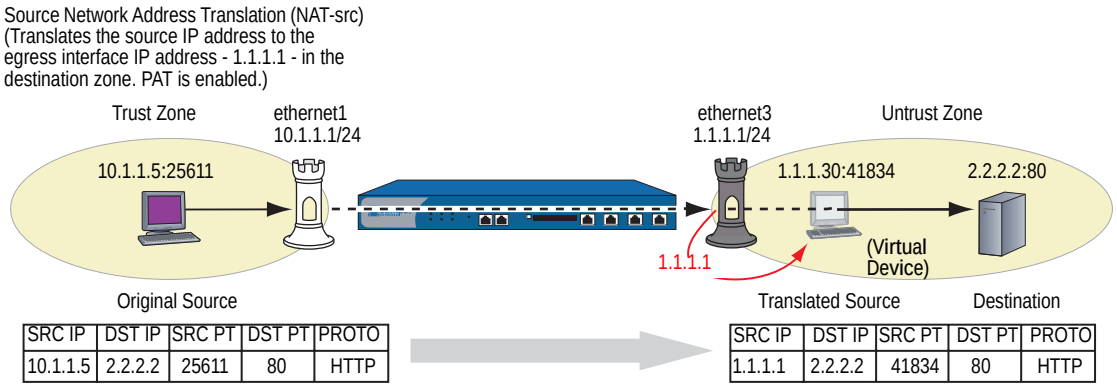
If you apply NAT-src to a policy but do not specify a DIP pool, then the security device translates the source IP address to the address of the egress interface. In such cases, the security device always applies PAT.

Example: NAT-Src Without DIP

In this example, you define a policy that instructs the security device to perform the following tasks:

- Permit HTTP traffic from any address in the Trust zone to any address in the Untrust zone
- Translate the source IP address in the IP packet header to 1.1.1.1, which is the IP address of ethernet3, the interface bound to the Untrust zone, and thus the egress interface for traffic sent to any address in the Untrust zone
- Translate the original source port number in the TCP segment header or UDP datagram header to a new, unique number
- Send traffic with the translated source IP address and port number out ethernet3 to the Untrust zone

Figure 18: NAT-Src Without DIP



WebUI

1. Interfaces

Network > Interfaces > Edit (for ethernet1): Enter the following, then click **Apply**:

Zone Name: Trust
Static IP: (select this option when present)
IP Address/Netmask: 10.1.1.1/24
Select the following, then click **OK**:
Interface Mode: NAT

Network > Interfaces > Edit (for ethernet3): Enter the following, then click **OK**:

Zone Name: Untrust
Static IP: (select this option when present)
IP Address/Netmask: 1.1.1.1/24

2. Policy

Policies > (From: Trust, To: Untrust) New: Enter the following, then click **OK**:

Source Address:
    Address Book Entry: (select), Any
Destination Address:
    Address Book Entry: (select), Any
Service: HTTP
Action: Permit

> Advanced: Enter the following, then click **Return** to set the advanced options and return to the basic configuration page:

NAT:
  Source Translation: (select)
  (DIP on): None (Use Egress Interface IP)

CLI

1. Interfaces

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.1.1.1/24
set interface ethernet1 nat
set interface ethernet3 zone untrust
set interface ethernet3 ip 1.1.1.1/24
```

2. Policy

```
set policy from trust to untrust any any http nat src permit
save
```

Chapter 3

Destination Network Address Translation

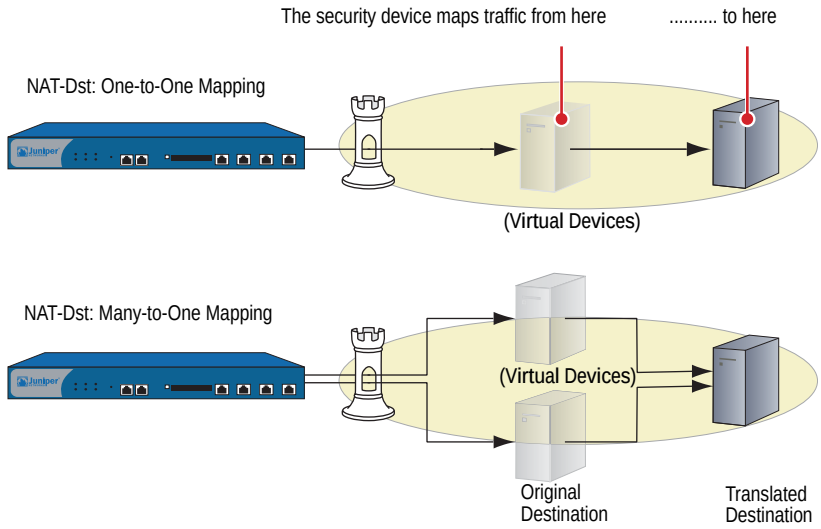
ScreenOS provides many methods for performing Destination Network Address Translation (NAT-dst) and destination port address mapping. This chapter describes the various address-translation methods available and contains the following sections:

NOTE: For information about destination address translation using a mapped IP (MIP) or virtual IP (VIP) address, see "Mapped and Virtual Addresses" on page 63.

Introduction to NAT-Dst

You can define policies to translate the destination address from one IP address to another. Perhaps you need the security device to translate one or more public IP addresses to one or more private addresses. The relationship of the original destination address to the translated destination address can be a one-to-one relationship, a many-to-one relationship, or a many-to-many relationship. Figure 19 depicts the concepts of one-to-one and many-to-one NAT-dst relationships.

Figure 19: NAT-Dst—One-to-One and Many-to-One

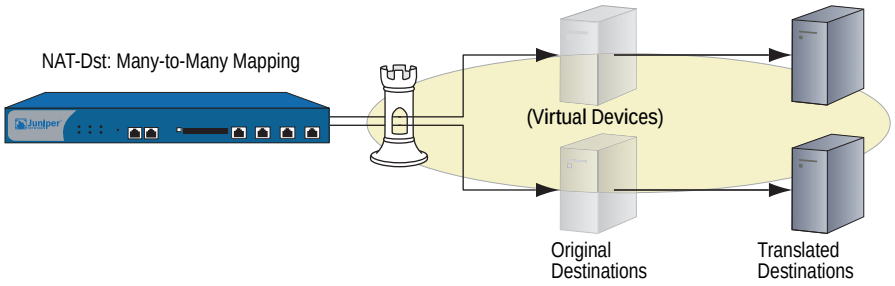


Note: The original and the translated destination IP addresses must be in the same security zone.

Both of the configurations shown in Figure 19 support destination port mapping. Port mapping is the deterministic translation of one original destination port number to another specific number. The relationship of the original-to-translated number in port mapping differs from Port Address Translation (PAT). With port mapping, the security device translates a predetermined original port number to another predetermined port number. With PAT, the security device translates a randomly assigned original source port number to another randomly assigned number.

You can translate a range of destination addresses to another range—such as one subnet to another—with address shifting, so that the security device consistently maps each original destination address to a specific translated destination address. Note that security does not support port mapping with address shifting. Figure 20 depicts the concept of a many-to-many relationship for NAT-dst.

Figure 20: NAT-Dst—Many-to-Many



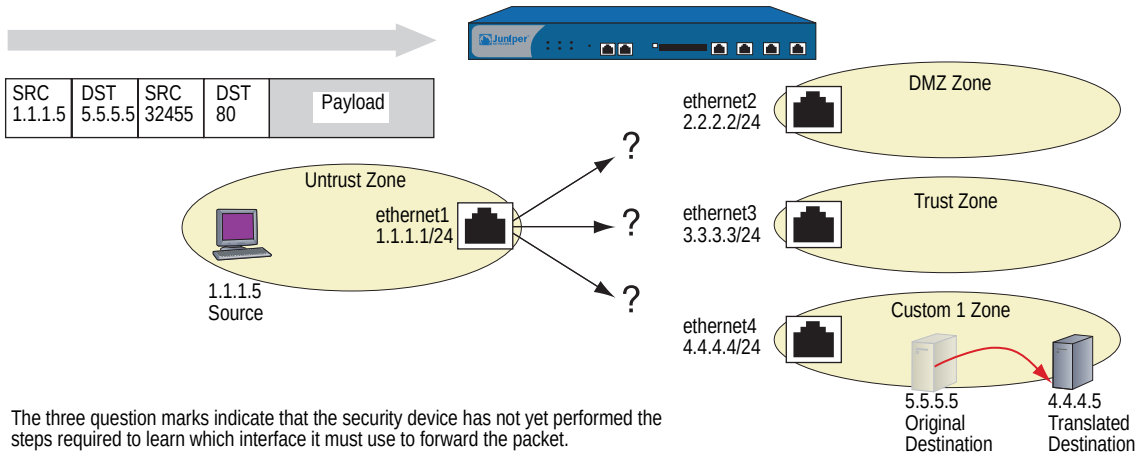
There must be entries in the route table for both the original destination IP address and the translated destination IP address. The security device performs a route lookup using the original destination IP address to determine the destination zone for a subsequent policy lookup. It then performs a second route lookup using the translated address to determine where to send the packet. To ensure that the routing decision is in accord with the policy, both the original destination IP address and the translated IP address must be in the same security zone. (For more information about the relationship of the destination IP address, route lookup, and policy lookup, see "Packet Flow for NAT-Dst" on this page.)

Packet Flow for NAT-Dst

The following steps describe the path of a packet through a security device and the various operations that it performs when applying NAT-dst:

1. An HTTP packet with source IP address:port number 1.1.1.5:32455 and destination IP address:port number 5.5.5.5:80 arrives at ethernet1, which is bound to the Untrust zone.

Figure 21: NAT-Dst Packet Flow—Packet Arrival



The three question marks indicate that the security device has not yet performed the steps required to learn which interface it must use to forward the packet.

2. If you have enabled SCREEN options for the Untrust zone, the security device activates the SCREEN module at this point. SCREEN checking can produce one of the following three results:

   - If a SCREEN mechanism detects anomalous behavior for which it is configured to block the packet, the security device drops the packet and makes an entry in the event log.
   - If a SCREEN mechanism detects anomalous behavior for which it is configured to record the event but not block the packet, the security device records the event in the SCREEN counters list for the ingress interface and proceeds to the next step.
   - If the SCREEN mechanisms detect no anomalous behavior, the security device proceeds to the next step.

   If you have not enabled any SCREEN options for the Untrust zone, the security device immediately proceeds to the next step.

3. The session module performs a session lookup, attempting to match the packet with an existing session.

   If the packet does not match an existing session, the security device performs First Packet Processing, a procedure involving the remaining steps.

   If the packet matches an existing session, the security device performs Fast Processing, using the information available from the existing session entry to process the packet. Fast Processing bypasses all but the last step because the information generated by the bypassed steps has already been obtained during the processing of the first packet in the session.

4. The address-mapping module checks if a Mapped IP (MIP) or Virtual IP (VIP) configuration uses the destination IP address 5.5.5.5.

NOTE: The security device checks if the destination IP address is used in a VIP configuration only if the packet arrives at an interface bound to the Untrust zone.

   If there is such a configuration, the security device resolves the MIP or VIP to the translated destination IP address and bases its route lookup on that. It then does a policy lookup between the Untrust and Global zones. If it finds a policy match that permits the traffic, the security device forwards the packet out the egress interface determined in the route lookup.

   If 5.5.5.5 is not used in a MIP or VIP configuration, the security device proceeds to the next step.

5. To determine the destination zone, the route module does a route lookup of the original destination IP address; that is, it uses the destination IP address that appears in the header of the packet that arrives at ethernet1. (The route module uses the ingress interface to determine which virtual router to use for the route lookup.) It discovers that 5.5.5.5/32 is accessed through ethernet4, which is bound to the Custom1 zone.

trust-vr Route Table			
To Reach:	**Use Interface:**	**In Zone:**	**Use Gateway:**
0.0.0.0/0	ethernet1	Untrust	1.1.1.250
1.1.1.0/24	ethernet1	Untrust	0.0.0.0
2.2.2.0/24	ethernet2	DMZ	0.0.0.0
3.3.3.0/24	ethernet3	Trust	0.0.0.0
4.4.4.0/24	ethernet4	Custom1	0.0.0.0
5.5.5.5/32	**ethernet4**	Custom1	**0.0.0.0**

6. The policy engine does a policy lookup between the Untrust and Custom1 zones (as determined by the corresponding ingress and egress interfaces). The source and destination IP addresses and the service match a policy redirecting HTTP traffic from 5.5.5.5 to 4.4.4.5.

   set policy from untrust to custom1 any v-server1 http nat dst ip 4.4.4.5 permit

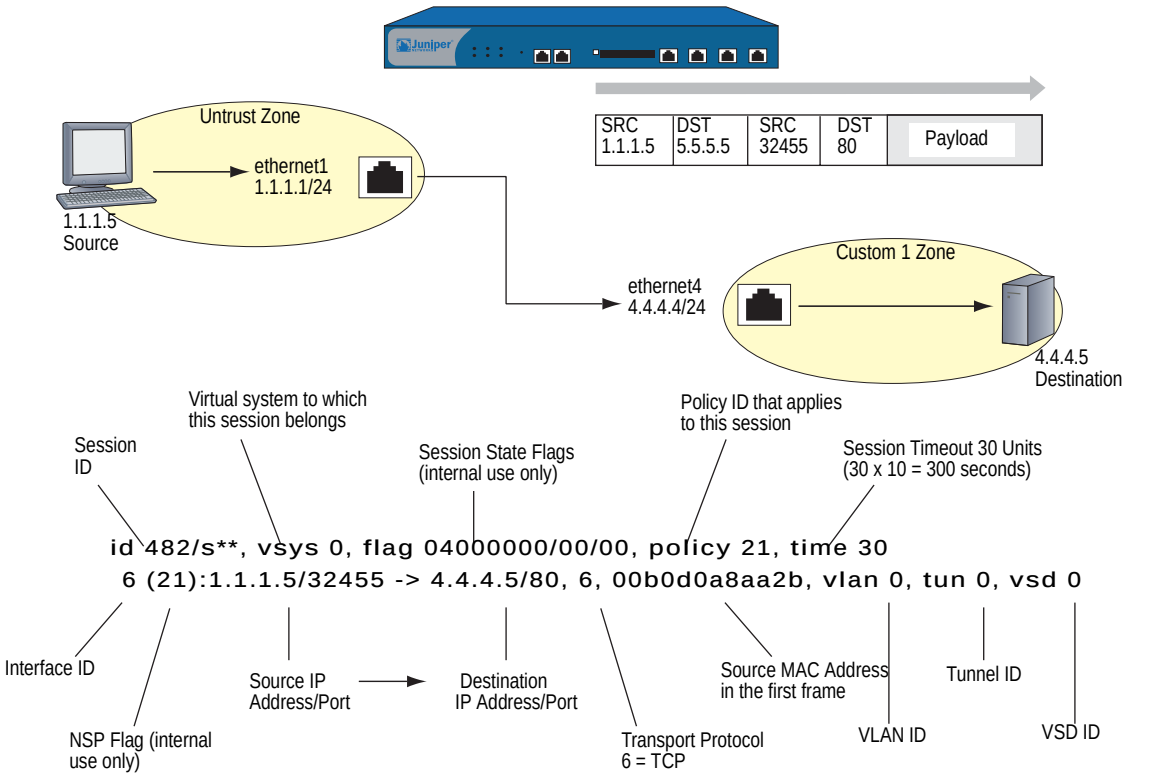
   (You have previously defined the address "v-server1" with IP address 5.5.5.5/32. It is in the Custom1 zone.)

   The security device translates the destination IP address from 5.5.5.5 to 4.4.4.5. The policy indicates that neither NAT-Src nor PAT-dst is required.

7. The security device does a second route lookup using the translated IP address and discovers that 4.4.4.5/32 is accessed through ethernet4.

8. The address-mapping module translates the destination IP address in the packet header to 4.4.4.5. The security device then forwards the packet out ethernet4 and makes an entry in its session table (unless this packet is part of an existing session and an entry already exists).

Figure 22: NAT-Dst Packet Flow—Packet Forwarding



Note: Because this session does not involve a virtual system, VLAN, VPN tunnel, or virtual security device (VSD), the setting for all these ID numbers is z

Routing for NAT-Dst

When you configure addresses for NAT-dst, the security device must have routes in its routing table to both the original destination address that appears in the packet header and the translated destination address (that is, the address to which the security device redirects the packet). As explained in “Packet Flow for NAT-Dst” on page 29, the security device uses the original destination address to do a route lookup, and thereby determine the egress interface. The egress interface in turn provides the destination zone—the zone to which the interface is bound—so that the security device can do a policy lookup. When the security device finds a policy match, the policy defines the mapping of the original destination address to the translated destination address. The security device then performs a second route lookup to determine the interface through which it must forward the packet to reach the new destination address. In summary, the route to the original destination address provides a means to perform the policy lookup, and the route to the translated destination address specifies the egress interface through which the security device is to forward the packet.

In the following three scenarios, the need to enter static routes differs according to the network topology surrounding the destination addresses referenced in this policy:

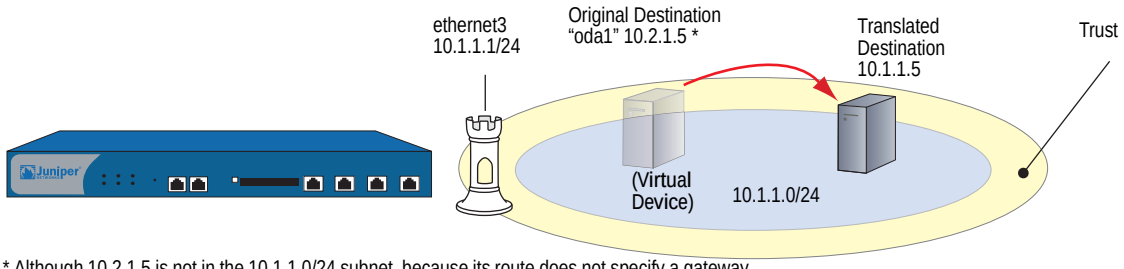
set policy from untrust to trust any oda1 http nat dst ip 10.1.1.5 permit

in which "oda1" is the original destination address 10.2.1.5, and the translated destination address is 10.1.1.5.

Example: Addresses Connected to One Interface

In this scenario, the routes to both the original and translated destination addresses direct traffic through the same interface, ethernet3. The security device automatically adds a route to 10.1.1.0/24 through ethernet3 when you configure the IP address of the ethernet3 interface as 10.1.1.1/24. To complete the routing requirements, you must add an additional route to 10.2.1.5/32 through ethernet3.

Figure 23: Original and Translated Addresses Using the Same Egress Interface



* Although 10.2.1.5 is not in the 10.1.1.0/24 subnet, because its route does not specify a gateway, it is illustrated as if it is in the same connected subnet as the 10.1.1.0/24 address space.

WebUI

Network > Routing > Routing Entries > (trust-vr) New: Enter the following, then click **OK**:

Network Address / Netmask: 10.2.1.5/32
Gateway: (select)
Interface: ethernet3
Gateway IP Address: 0.0.0.0

CLI

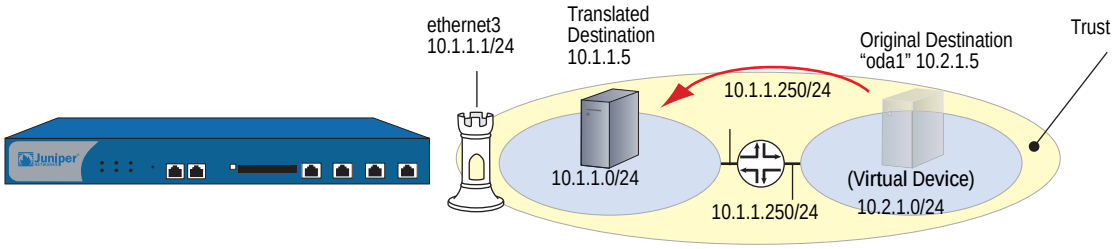
```
set vrouter trust-vr route 10.2.1.5/32 interface ethernet3
save
```

Example: Addresses Connected to One Interface But Separated by a Router

In this scenario, the routes to both the original and translated destination addresses direct traffic through ethernet3. The security device automatically adds a route to 10.1.1.0/24 through ethernet3 when you configure the IP address of the ethernet3 interface as 10.1.1.1/24. To complete the routing requirements, you must add a route to 10.2.1.0/24 through ethernet3 and the gateway connecting the 10.1.1.0/24 and the 10.2.1.0/24 subnets.

NOTE: Because this route is required to reach any address in the 10.2.1.0/24 subnet, you have probably already configured it. If so, no extra route needs to be added just for the policy to apply NAT-dst to 10.2.1.5.

Figure 24: Original and Translated Addresses Separated by a Router



WebUI

Network > Routing > Routing Entries > (trust-vr) New: Enter the following, then click **OK**:

Network Address / Netmask: 10.2.1.0/24
Gateway: (select)
Interface: ethernet3
Gateway IP Address: 10.1.1.250

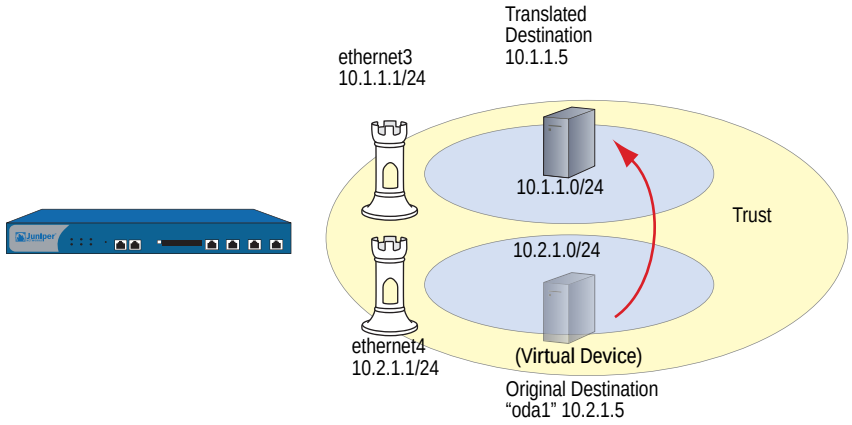
CLI

```
set vrouter trust-vr route 10.2.1.0/24 interface ethernet3 gateway 10.1.1.250
save
```

Example: Addresses Separated by an Interface

In this scenario, two interfaces are bound to the Trust zone: ethernet3 with IP address 10.1.1.1/24 and ethernet4 with IP address 10.2.1.1/24. The security device automatically adds a route to 10.1.1.0/24 through ethernet3 and 10.2.1.0/24 through ethernet4 when you configure the IP addresses of these interfaces. By putting the original destination address in the 10.2.1.0/24 subnet and the translated destination address in the 10.1.1.0/24 subnet, you do not have to add any other routes for the security device to apply NAT-dst from 10.1.1.5 to 10.2.1.5.

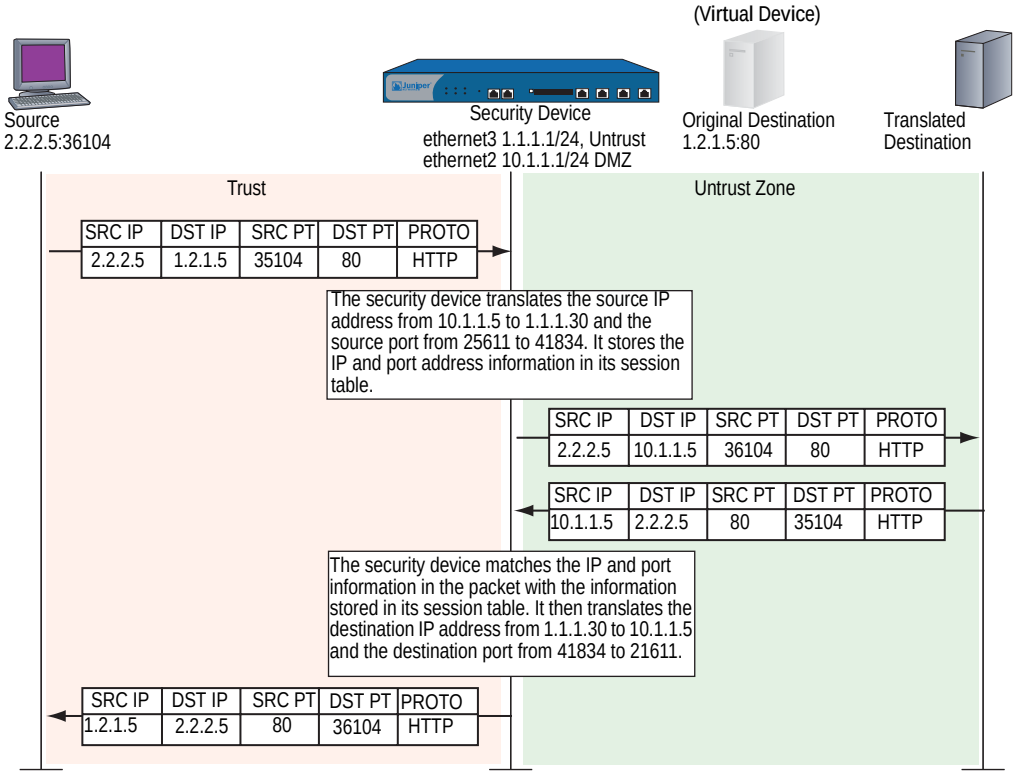
Figure 25: Original and Translated Addresses Using Different Egress Interfaces



NAT-Dst—One-to-One Mapping

When applying Destination Network Address Translation (NAT-dst) without PAT, the security device translates the destination IP address and performs stateful inspection as illustrated in Figure 26 (note that only the elements in the IP packet and TCP segment headers relevant to NAT-dst are shown).

Figure 26: One-to-One NAT-Dst



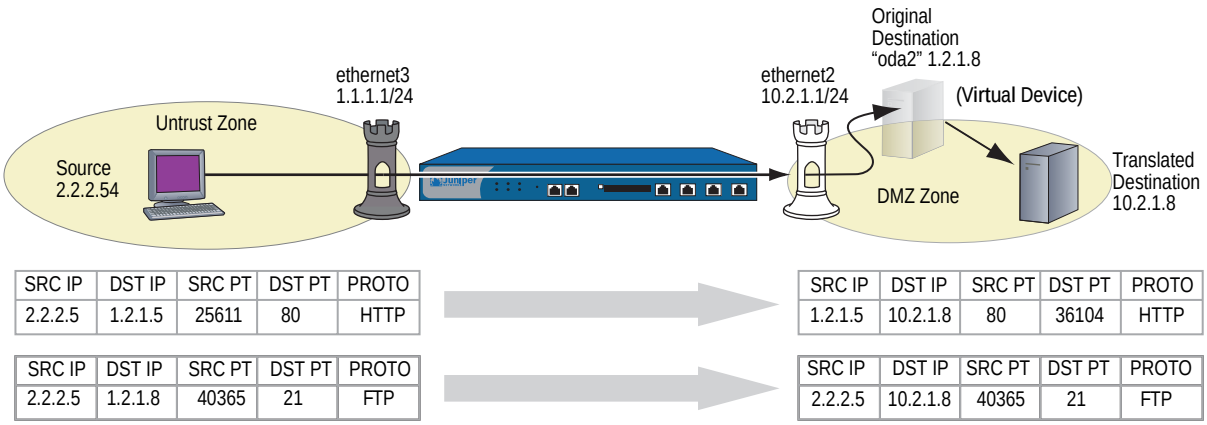
Example: One-to-One Destination Translation

In this example, you set a policy to provide one-to-one Destination Network Address Translation (NAT-dst) without changing the destination port addresses. The policy instructs the security device to perform the following tasks:

- Permit both FTP and HTTP traffic (defined as the service group “http-ftp”) from any address in the Untrust zone to a the original destination address named “oda2” with address 1.2.1.8 in the DMZ zone
- Translate the destination IP address in the IP packet header from 1.2.1.8 to 10.2.1.8
- Leave the original destination port number in the TCP segment header as is (80 for HTTP and 21 for FTP)
- Forward HTTP and FTP traffic to 10.2.1.8 in the DMZ zone

You bind ethernet3 to the Untrust zone and assign it IP address 1.1.1.1/24. You bind ethernet2 to the DMZ and assign it IP address 10.2.1.1/24. You also define a route to the original destination address 1.2.1.8 through ethernet2. Both the Untrust and DMZ zones are in the trust-vr routing domain.

Figure 27: NAT-Dst—One-to-One



SRC IP	DST IP	SRC PT	DST PT	PROTO
2.2.2.5	1.2.1.5	25611	80	HTTP

SRC IP	DST IP	SRC PT	DST PT	PROTO
1.2.1.5	10.2.1.8	80	36104	HTTP

SRC IP	DST IP	SRC PT	DST PT	PROTO
2.2.2.5	1.2.1.8	40365	21	FTP

SRC IP	DST IP	SRC PT	DST PT	PROTO
2.2.2.5	10.2.1.8	40365	21	FTP

WebUI

1. **Interfaces**

   Network > Interfaces > Edit (for ethernet3): Enter the following, then click **OK**:

   Zone Name: Untrust
   Static IP: (select this option when present)
   IP Address/Netmask: 1.1.1.1/24

   Network > Interfaces > Edit (for ethernet2): Enter the following, then click **OK**:

   Zone Name: DMZ
   Static IP: (select this option when present)
   IP Address/Netmask: 10.2.1.1/24

2. **Address**

   Objects > Addresses > List > New: Enter the following information, then click **OK**:

   Address Name: oda2
   IP Address/Domain Name:
   IP/Netmask: (select), 1.2.1.8/32
   Zone: DMZ

3. **Service Group**

   Objects > Services > Group: Enter the following group name, move the following services, then click **OK**:

   Group Name: HTTP-FTP

   Select **HTTP** and use the < < button to move the service from the Available Members column to the Group Members column.

   Select **FTP** and use the < < button to move the service from the Available Members column to the Group Members column.

4. **Route**

   Network > Routing > Routing Entries > trust-vr New: Enter the following, then click **OK**:

   Network Address / Netmask: 1.2.1.8/32
   Gateway: (select)
   Interface: ethernet2
   Gateway IP Address: 0.0.0.0

5. **Policy**

   Policies > (From: Untrust, To: DMZ) New: Enter the following, then click **OK**:

   Source Address:
   Address Book Entry: (select), Any
   Destination Address:
   Address Book Entry: (select), oda2
   Service: HTTP-FTP
   Action: Permit

   > Advanced: Enter the following, then click **Return** to set the advanced options and return to the basic configuration page:

   NAT:
   Destination Translation: (select)
   Translate to IP: (select), 10.2.1.8
   Map to Port: (clear)

CLI

1. **Interfaces**
   set interface ethernet3 zone untrust
   set interface ethernet3 ip 1.1.1.1/24
   set interface ethernet2 zone dmz
   set interface ethernet2 ip 10.2.1.1/24
2. **Address**
   set address dmz oda2 1.2.1.8/32
3. **Service Group**
   set group service http-ftp
   set group service http-ftp add http
   set group service http-ftp add ftp
4. **Route**
   set vrouter trust-vr route 1.2.1.8/32 interface ethernet2
5. **Policy**
   set policy from untrust to dmz any oda2 http-ftp nat dst ip 10.2.1.8 permit
   save

Translating from One Address to Multiple Addresses

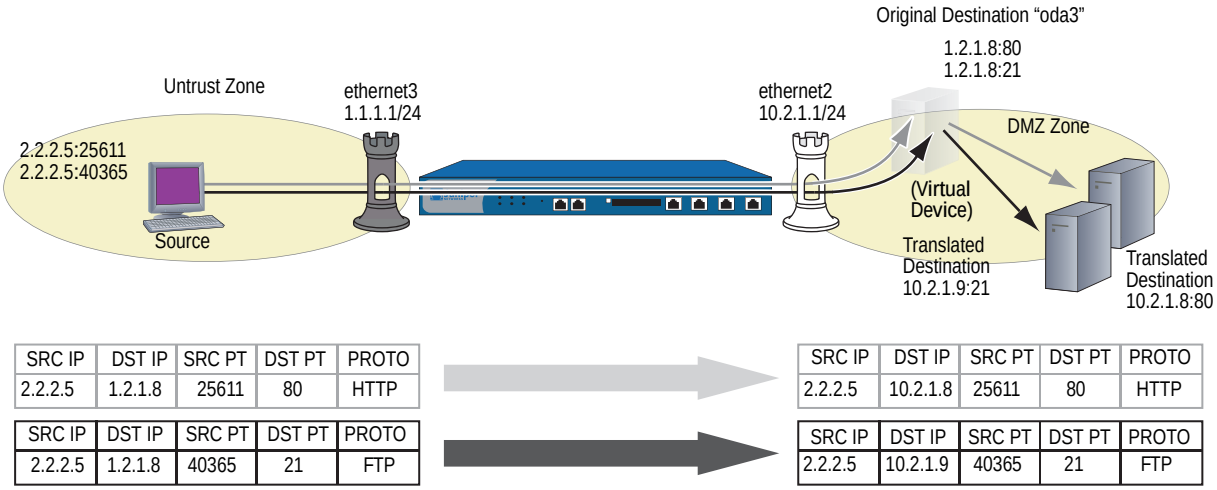
The security device can translate the same original destination address to different translated destination addresses specified in different policies, depending on the type of service or the source address specified in each policy. You might want the security device to redirect HTTP traffic from 1.2.1.8 to 10.2.1.8, and FTP traffic from 1.2.1.8 to 10.2.1.9 (see the following example). Perhaps you want the security device to redirect HTTP traffic sent from host1 to 1.2.1.8 over to 10.2.1.8, but HTTP traffic sent from host2 to 1.2.1.8 over to 10.2.1.37. In both cases, the security device redirects traffic sent to the same original destination address to different translated addresses.

Example: One-to-Many Destination Translation

In this example, you create two policies that use the same original destination address (1.2.1.8), but that direct traffic sent to that address to two different translated destination addresses based on the service type. These policies instruct the security device to perform the following tasks:

- Permit both FTP and HTTP traffic from any address in the Untrust zone to a user-defined address named “oda3” in the DMZ zone
- For HTTP traffic, translate the destination IP address in the IP packet header from 1.2.1.8 to 10.2.1.8
- For FTP traffic, translate the destination IP address from 1.2.1.8 to 10.2.1.9
- Leave the original destination port number in the TCP segment header as is (80 for HTTP, 21 for FTP)
- Forward HTTP traffic to 10.2.1.8 and FTP traffic to 10.2.1.9 in the DMZ zone

Figure 28: NAT-Dst—One-to-Many



SRC IP	DST IP	SRC PT	DST PT	PROTO
2.2.2.5	1.2.1.8	25611	80	HTTP

SRC IP	DST IP	SRC PT	DST PT	PROTO
2.2.2.5	10.2.1.8	25611	80	HTTP

SRC IP	DST IP	SRC PT	DST PT	PROTO
2.2.2.5	1.2.1.8	40365	21	FTP

SRC IP	DST IP	SRC PT	DST PT	PROTO
2.2.2.5	10.2.1.9	40365	21	FTP

You bind ethernet3 to the Untrust zone and assign it IP address 1.1.1.1/24. You bind ethernet2 to the DMZ, and assign it IP address 10.2.1.1/24. You also define a route to the original destination address 1.2.1.8 through ethernet2. Both the Untrust zone and the DMZ zone are in the trust-vr routing domain.

WebUI

1. **Interfaces**

   Network > Interfaces > Edit (for ethernet3): Enter the following, then click **OK**:

   Zone Name: Untrust
   Static IP: (select this option when present)
   IP Address/Netmask: 1.1.1.1/24

   Network > Interfaces > Edit (for ethernet2): Enter the following, then click **OK**:

   Zone Name: DMZ
   Static IP: (select this option when present)
   IP Address/Netmask: 10.2.1.1/24

2. **Address**

   Objects > Addresses > List > New: Enter the following information, then click **OK**:

   Address Name: oda3
   IP Address/Domain Name:
   IP/Netmask: (select), 1.2.1.8/32
   Zone: DMZ

3. **Route**

   Network > Routing > Routing Entries > trust-vr New: Enter the following, then click **OK**:

   Network Address / Netmask: 1.2.1.8/32
   Gateway: (select)
   Interface: ethernet2
   Gateway IP Address: 0.0.0.0

4. **Policies**

   Policies > (From: Untrust, To: DMZ) New: Enter the following, then click **OK**:

   Source Address:
   Address Book Entry: (select), Any
   Destination Address:
   Address Book Entry: (select), oda3
   Service: HTTP
   Action: Permit

   > Advanced: Enter the following, then click **Return** to set the advanced options and return to the basic configuration page:

   NAT:
   Destination Translation: (select)
   Translate to IP: (select), 10.2.1.8
   Map to Port: (clear)

   Policies > (From: Untrust, To: DMZ) New: Enter the following, then click **OK**:

   Source Address:
   Address Book Entry: (select), Any
   Destination Address:
   Address Book Entry: (select), oda3
   Service: FTP
   Action: Permit

   > Advanced: Enter the following, then click **Return** to set the advanced options and return to the basic configuration page:

   NAT:
   Destination Translation: (select)
   Translate to IP: (select), 10.2.1.9
   Map to Port: (clear)

CLI

1. **Interfaces**

   ```
   set interface ethernet3 zone untrust
   set interface ethernet3 ip 1.1.1.1/24
   set interface ethernet2 zone dmz
   set interface ethernet2 ip 10.2.1.1/24
   ```

2. **Address**

   ```
   set address dmz oda3 1.2.1.8/32
   ```

3. **Route**

   ```
   set vrouter trust-vr route 1.2.1.8/32 interface ethernet2
   ```

4. **Policies**

   ```
   set policy from untrust to dmz any oda3 http nat dst ip 10.2.1.8 permit
   set policy from untrust to dmz any oda3 ftp nat dst ip 10.2.1.9 permit
   save
   ```

NAT-Dst—Many-to-One Mapping

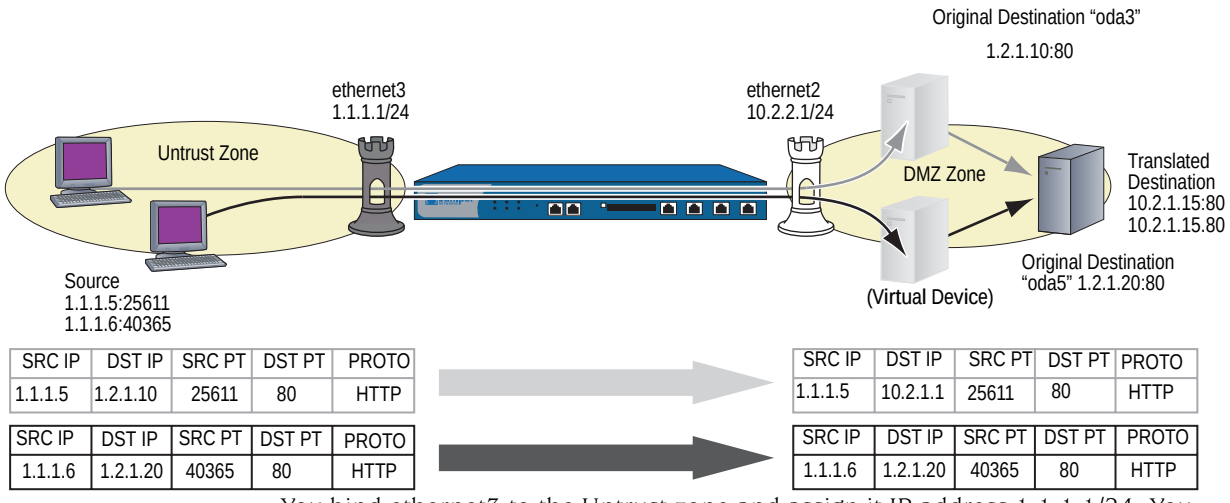
The relationship of the original destination address to the translated destination address can also be a many-to-one relationship. In this case, the security device forwards traffic sent to several original destination addresses to a single translated destination address. Optionally, you can also specify destination port mapping.

Example: Many-to-One Destination Translation

In this example, you create a policy that redirects traffic sent to different original destination addresses (1.2.1.10 and 1.2.1.20) to the same translated destination address. This policy instructs the security device to perform the following tasks:

- Permit HTTP traffic from any address in the Untrust zone to a user-defined address group named “oda45” with addresses “oda4” (1.2.1.10) and “oda5” (1.2.1.20) in the DMZ zone
- Translate the destination IP addresses in the IP packet header from 1.2.1.10 and 1.2.1.20 to 10.2.1.15
- Leave the original destination port number in the TCP segment header as is (80 for HTTP)
- Forward the HTTP traffic to 10.2.1.15 in the DMZ zone

Figure 29: NAT-Dst—Many-to-One



You bind ethernet3 to the Untrust zone and assign it IP address 1.1.1.1/24. You bind ethernet2 to the DMZ and assign it IP address 10.2.1.1/24. You also define a route to the original destination addresses 1.2.1.10 and 1.2.1.20 through ethernet2. Both the Untrust zone and the DMZ zone are in the trust-vr routing domain.

WebUI

1. **Interfaces**
   Network > Interfaces > Edit (for ethernet3): Enter the following, then click **OK**:

   Zone Name: Untrust
   Static IP: (select this option when present)
   IP Address/Netmask: 1.1.1.1/24

   Network > Interfaces > Edit (for ethernet2): Enter the following, then click **OK**:

   Zone Name: DMZ
   Static IP: (select this option when present)
   IP Address/Netmask: 10.2.1.1/24

2. **Addresses**
   Objects > Addresses > List > New: Enter the following information, then click **OK**:

   Address Name: oda4
   IP Address/Domain Name:
   IP/Netmask: (select), 1.2.1.10/32
   Zone: DMZ

   Objects > Addresses > List > New: Enter the following information, then click **OK**:

   Address Name: oda5
   IP Address/Domain Name:
   IP/Netmask: (select), 1.2.1.20/32
   Zone: DMZ

   Objects > Addresses > Group > (for Zone: DMZ) New: Enter the following group name, move the following addresses, then click **OK**:

   Group Name: oda45

   Select **oda4** and use the < < button to move the address from the Available Members column to the Group Members column.

   Select **oda5** and use the < < button to move the address from the Available Members column to the Group Members column.

3. **Routes**

   Network > Routing > Routing Entries > trust-vr New: Enter the following, then click **OK**:

   Network Address / Netmask: 1.2.1.10/32
   Gateway: (select)
   Interface: ethernet2
   Gateway IP Address: 0.0.0.0

   Network > Routing > Routing Entries > trust-vr New: Enter the following, then click **OK**:

   Network Address / Netmask: 1.2.1.20/32
   Gateway: (select)
   Interface: ethernet2
   Gateway IP Address: 0.0.0.0

4. **Policy**

   Policies > (From: Untrust, To: DMZ) New: Enter the following, then click **OK**:

   Source Address:
   Address Book Entry: (select), Any
   Destination Address:
   Address Book Entry: (select), oda45
   Service: HTTP
   Action: Permit

   > Advanced: Enter the following, then click **Return** to set the advanced options and return to the basic configuration page:

   NAT:
   Destination Translation: (select)
   Translate to IP: (select), 10.2.1.15
   Map to Port: (clear)

CLI

1. **Interfaces**

   set interface ethernet3 zone untrust
   set interface ethernet3 ip 1.1.1.1/24
   set interface ethernet2 zone dmz
   set interface ethernet2 ip 10.2.1.1/24

2. **Addresses**

   set address dmz oda4 1.2.1.10/32
   set address dmz oda5 1.2.1.20/32
   set group address dmz oda45 add oda4
   set group address dmz oda45 add oda5

3. **Routes**

   set vrouter trust-vr route 1.2.1.10/32 interface ethernet2
   set vrouter trust-vr route 1.2.1.20/32 interface ethernet2

4. **Policy**

   set policy from untrust to dmz any oda45 http nat dst ip 10.2.1.15 permit
   save

NAT-Dst—Many-to-Many Mapping

You can use Destination Network Address Translation (NAT-dst) to translate one range of IP addresses to another range. The range of addresses can be a subnet or a smaller set of addresses within a subnet. ScreenOS employs an address shifting mechanism to maintain the relationships among the original range of destination addresses after translating them to the new range of addresses. For example, if the range of original addresses is 10.1.1.1 – 10.1.1.50 and the starting address for the translated address range is 10.100.3.101, then the security device translates the addresses as follows:

- 10.1.1.1 – 10.100.3.101
- 10.1.1.2 – 10.100.3.102
- 10.1.1.3 – 10.100.3.103

  …

- 10.1.1.48 – 10.100.3.148
- 10.1.1.49 – 10.100.3.149
- 10.1.1.50 – 10.100.3.150

If, for example, you want to create a policy that applies the above translations to HTTP traffic from any address in zone A to an address group named “addr1-50”, which contains all the addresses from 10.1.1.1 to 10.1.1.50, in zone B, you can enter the following CLI command:

```
set policy id 1 from zoneA to zoneB any addr1-50 http nat dst ip 10.100.3.101
    10.100.3.150 permit
```

If any host in zone A initiates HTTP traffic to an address within the defined range in zone B, such as 10.1.1.37, then the security device applies this policy and translates the destination address to 10.100.3.137.

The security device only performs NAT-dst if the source and destination zones, the source and destination addresses, and the service specified in the policy all match these components in the packet. For example, you might create another policy that permits traffic from any host in zone A to any host in zone B and position it after policy 1 in the policy list:

```
set policy id 1 from zoneA to zoneB any addr1-50 http nat dst ip 10.100.3.101
    10.100.3.150 permit
set policy id 2 from zoneA to zoneB any any any permit
```

If you have these two policies configured, the following kinds of traffic sent from a host in zone A to a host in zone B bypass the NAT-dst mechanism:

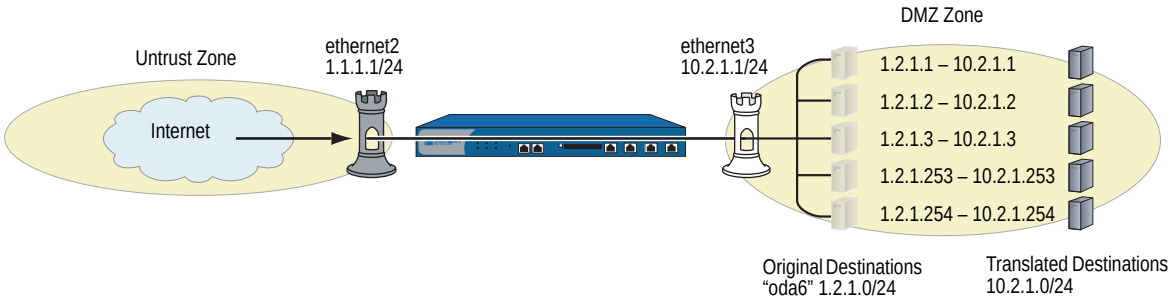
- A zone A host initiates non-HTTP traffic to 10.1.1.37 in zone B. The security device applies policy 2 because the service is not HTTP and passes the traffic without translating the destination address.
- A zone A host initiates HTTP traffic to 10.1.1.51 in zone B. The security device also applies policy 2 because the destination address is not in the addr1-50 address group, and passes the traffic without translating the destination address.

Example: Many-to-Many Destination Translation

In this example, you configure a policy that applies NAT-dst when any kind of traffic is sent to any host in a subnet, instructing the security device to perform the following tasks:

- Permit all traffic types from any address in the Untrust zone to any address in the DMZ zone
- Translate the original destination address named "oda6" from the 1.2.1.0/24 subnet to a corresponding address in the 10.2.1.0/24 subnet
- Leave the original destination port number in the TCP segment header as is
- Forward HTTP traffic to the translated address in the DMZ

Figure 30: NAT-Dst—Many-to-Many



You bind ethernet3 to the Untrust zone and assign it IP address 1.1.1.1/24. You bind ethernet2 to the DMZ and assign it IP address 10.2.1.1/24. You also define a route to the original destination address subnet (1.2.1.0/24) through ethernet2. Both the Untrust zone and the DMZ zone are in the trust-vr routing domain.

WebUI

1. **Interfaces**
   Network > Interfaces > Edit (for ethernet3): Enter the following, then click **OK**:

   Zone Name: Untrust
   Static IP: (select this option when present)
   IP Address/Netmask: 1.1.1.1/24

Network > Interfaces > Edit (for ethernet2): Enter the following, then click **OK**:

Zone Name: DMZ
Static IP: (select this option when present)
IP Address/Netmask: 10.2.1.1/24

2. **Address**
   Objects > Addresses > List > New: Enter the following information, then click **OK**:

   Address Name: oda6
   IP Address/Domain Name:
   IP/Netmask: (select), 1.2.1.0/24
   Zone: DMZ

3. **Route**
   Network > Routing > Routing Entries > trust-vr New: Enter the following, then click **OK**:

   Network Address / Netmask: 1.2.1.0/24
   Gateway: (select)
   Interface: ethernet2
   Gateway IP Address: 0.0.0.0

4. **Policy**
   Policies > (From: Untrust, To: DMZ) New: Enter the following, then click **OK**:

   Source Address:
   Address Book Entry: (select), Any
   Destination Address:
   Address Book Entry: (select), oda6
   Service: Any
   Action: Permit

   > Advanced: Enter the following, then click **Return** to set the advanced options and return to the basic configuration page:

   NAT:
   Destination Translation: (select)
   Translate to IP Range: (select), 10.2.1.0 – 10.2.1.254

CLI

1. **Interfaces**
   set interface ethernet3 zone untrust
   set interface ethernet3 ip 1.1.1.1/24
   set interface ethernet2 zone dmz
   set interface ethernet2 ip 10.2.1.1/24

2. **Address**
   set address dmz oda6 1.2.1.0/24

3. **Route**
   set vrouter trust-vr route 1.2.1.0/24 interface ethernet2

4. **Policy**
   set policy from untrust to dmz any oda6 any nat dst ip 10.2.1.1 10.2.1.254 permit
   save

NAT-Dst with Port Mapping

When you configure the security device to perform Destination Network Address Translation (NAT-dst), you can optionally enable port mapping. One reason to enable port mapping is to support multiple server processes for a single service on a single host. For example, one host can run two webservers—one at port 80 and another at port 8081. For HTTP service 1, the security device performs NAT-dst without port mapping (dst port 80 -> 80).

For HTTP service 2, the security device performs NAT-dst to the same destination IP address with port mapping (dst port 80 -> 8081). The host can sort HTTP traffic to the two webservers by the two distinct destination port numbers.

NOTE: ScreenOS does not support port mapping for NAT-dst with address shifting. See "NAT-Dst—Many-to-Many Mapping" on page 44.

Example: NAT-Dst with Port Mapping

In this example, you create two policies that perform NAT-dst and port mapping on Telnet traffic from the Trust and Untrust zones to a Telnet server in the DMZ zone. These policies instruct the security device to perform the following tasks:

- Permit Telnet from any address in the Untrust and Trust zones to 1.2.1.15 in the DMZ zone
- Translate the original destination IP address named "oda7" from 1.2.1.15 to 10.2.1.15
- Translate the original destination port number in the TCP segment header from 23 to 2200
- Forward Telnet traffic to the translated address in the DMZ zone

You configure the following interface-to-zone bindings and address assignments:

- ethernet1: Trust zone, 10.1.1.1/24
- ethernet2: DMZ zone, 10.2.1.1/24.
- ethernet3: Untrust zone, 1.1.1.1/24.

You define an address entry "oda7" with IP address 1.2.1.15/32 in the DMZ zone. You also define a route to the original destination address 1.2.1.15 through ethernet2. The Trust, Untrust, and DMZ zones are all in the trust-vr routing domain.

WebUI

1. **Interfaces**
   Network > Interfaces > Edit (for ethernet1): Enter the following, then click **Apply**:

   Zone Name: Trust
   Static IP: (select this option when present)
   IP Address/Netmask: 10.1.1.1/24
   Select the following, then click **OK**:
   Interface Mode: NAT

   Network > Interfaces > Edit (for ethernet2): Enter the following, then click **OK**:

   Zone Name: DMZ
   Static IP: (select this option when present)
   IP Address/Netmask: 10.2.1.1/24

   Network > Interfaces > Edit (for ethernet3): Enter the following, then click **OK**:

   Zone Name: Untrust
   Static IP: (select this option when present)
   IP Address/Netmask: 1.1.1.1/24

2. **Address**
   Objects > Addresses > List > New: Enter the following information, then click **OK**:

   Address Name: oda7
   IP Address/Domain Name:
   IP/Netmask: (select), 1.2.1.15/32
   Zone: DMZ

3. **Route**
   Network > Routing > Routing Entries > trust-vr New: Enter the following, then click **OK**:

   Network Address / Netmask: 1.2.1.15/32
   Gateway: (select)
   Interface: ethernet2
   Gateway IP Address: 0.0.0.0

4. **Policies**
   Policies > (From: Trust, To: DMZ) New: Enter the following, then click **OK**:

   Source Address:
   Address Book Entry: (select), Any
   Destination Address:
   Address Book Entry: (select), oda7
   Service: Telnet
   Action: Permit

> Advanced: Enter the following, then click **Return** to set the advanced options and return to the basic configuration page:

NAT:
Destination Translation: (select)
Translate to IP: (select), 10.2.1.15
Map to Port: (select), 2200

Policies > (From: Untrust, To: DMZ) New: Enter the following, then click **OK**:

Source Address:
Address Book Entry: (select), Any
Destination Address:
Address Book Entry: (select), oda7
Service: Telnet
Action: Permit

> Advanced: Enter the following, then click **Return** to set the advanced options and return to the basic configuration page:

NAT:
Destination Translation: (select)
Translate to IP: (select), 10.2.1.15
Map to Port: (select), 2200

CLI

1. **Interfaces**

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.1.1.1/24
set interface ethernet1 nat
set interface ethernet2 zone dmz
set interface ethernet2 ip 10.2.1.1/24
set interface ethernet3 zone untrust
set interface ethernet3 ip 1.1.1.1/24
```

2. **Address**

```
set address dmz oda7 1.2.1.15/32
```

3. **Route**

```
set vrouter trust-vr route 1.2.1.15/32 interface ethernet2
```

4. **Policies**

```
set policy from trust to dmz any oda7 telnet nat dst ip 10.2.1.15 port 2200 permit
set policy from untrust to dmz any oda7 telnet nat dst ip 10.2.1.15 port 2200
    permit
save
```

NAT-Src and NAT-Dst in the Same Policy

You can combine Source Network Address Translation (NAT-Src) and Destination Network Address Translation (NAT-dst) in the same policy. This combination provides you with a method of changing both the source and the destination IP addresses at a single point in the data path.

Example: NAT-Src and NAT-Dst Combined

In the example shown in Figure 31, you configure a security device (Device-1) that is between a service provider's customers and server farms. The customers connect to Device-1 through ethernet1, which has IP address 10.1.1.1/24 and is bound to the Trust zone. Device-1 then forwards their traffic through one of two route-based VPN tunnels to reach the servers they want to target. The tunnel interfaces that are bound to these tunnels are in the Untrust zone. Both the Trust and Untrust zones are in the trust-vr routing domain.

NOTE: Policy-based VPNs do not support NAT-dst. You must use a route-based VPN configuration with NAT-dst.

Because the customers might have the same addresses as those of the servers to which they want to connect, Device-1 must perform both Source and Destination Network Address Translation (NAT-Src and NAT-dst). To retain addressing independence and flexibility, the security devices protecting the server farms—Device-A and Device-B—perform NAT-dst. The service provider instructs the customers and the server farm admins to reserve addresses 10.173.10.1–10.173.10.7, 10.173.20.0/24, 10.173.30.0/24, 10.173.40.0/24, and 10.173.50.0/24 for this purpose. These addresses are used as follows:

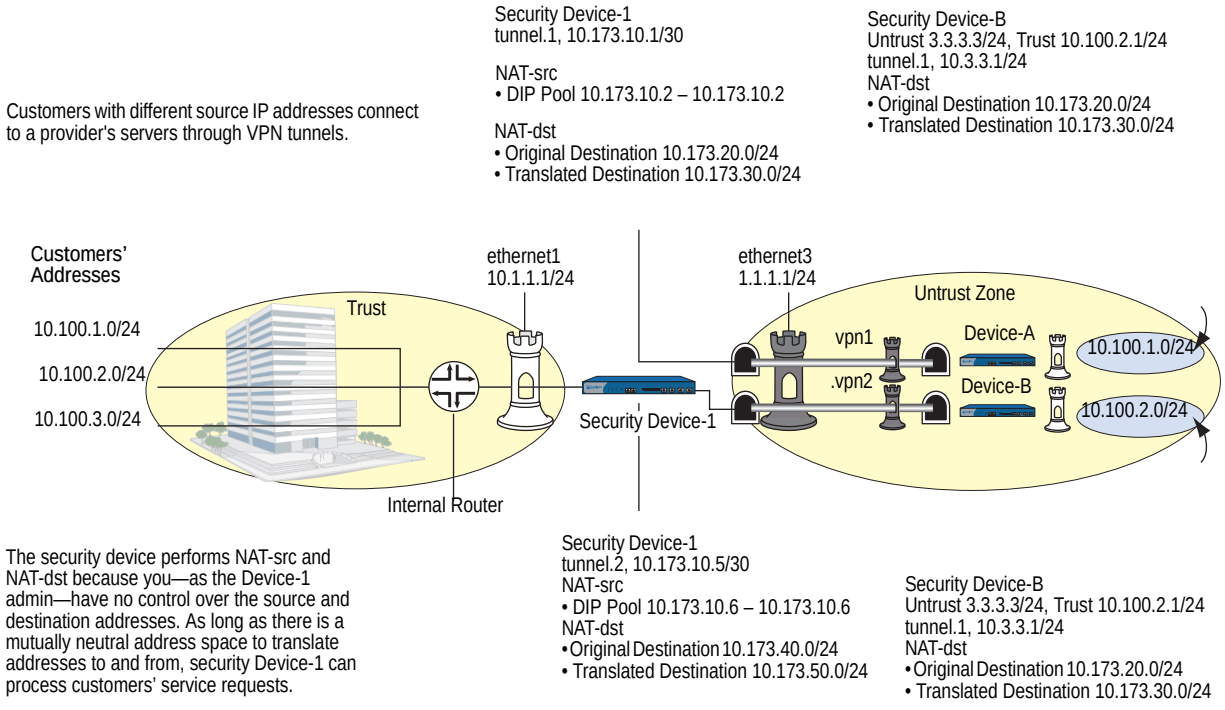
- The two tunnel interfaces have the following address assignments:
  - tunnel.1, 10.173.10.1/30
  - tunnel.2, 10.173.10.5/30
- Each tunnel interface supports the following DIP pools with PAT enabled:
  - tunnel.1, DIP ID 5: 10.173.10.2–10.173.10.2
  - tunnel.2, DIP ID 6: 10.173.10.6–10.173.10.6
- When Device-1 performs NAT-dst, it translates original destination addresses with address shifting as follows:
  - 10.173.20.0/24 to 10.173.30.0/24
  - 10.173.40.0/24 to 10.173.50.0/24

NOTE: For information about address shifting when performing NAT-dst, see "NAT-Dst—Many-to-Many Mapping" on page 44.

The configurations for both tunnels—vpn1 and vpn2—use the following parameters: AutoKey IKE, preshared key ("device1" for vpn1, and "device2" for vpn2), and the security level predefined as "Compatible" for both Phase 1 and Phase 2 proposals. (For details about these proposals, see "Tunnel Negotiation" on page 5-8.) The proxy ID for both vpn1 and vpn2 is 0.0.0.0/0 - 0.0.0.0/0 - any.

NOTE: The configuration for Device-1 is provided first. The VPN configurations for Device-A and Device-B follow and are included for completeness.

Figure 31: NAT-Src and NAT-Dst Combined



WebUI (Security Device-1)

1. Interfaces

Network > Interfaces > Edit (for ethernet1): Enter the following, then click **Apply**:

Zone Name: Trust
Static IP: (select this option when present)
IP Address/Netmask: 10.1.1.1/24
Select the following, then click **OK**:
Interface Mode: NAT

Network > Interfaces > Edit (for ethernet3): Enter the following, then click **OK**:

Zone Name: Untrust
Static IP: (select this option when present)
IP Address/Netmask: 1.1.1.1/24

Network > Interfaces > New Tunnel IF: Enter the following, then click **OK**:

Tunnel Interface Name: tunnel.1
Zone (VR): Untrust (trust-vr)
Fixed IP: (select)
IP Address / Netmask: 10.173.10.1/30

Network > Interfaces > New Tunnel IF: Enter the following, then click **OK**:

Tunnel Interface Name: tunnel.1
Zone (VR): Untrust (trust-vr)
Fixed IP: (select)
IP Address / Netmask: 10.173.10.5/30

2. DIP Pools

Network > Interfaces > Edit (for tunnel.1) > DIP > New: Enter the following, then click **OK**:

ID: 5
IP Address Range: (select), 10.173.10.2 ~ 10.173.10.2
Port Translation: (select)
In the same subnet as the interface IP or its secondary IPs: (select)

Network > Interfaces > Edit (for tunnel.2) > DIP > New: Enter the following, then click **OK**:

ID: 6
IP Address Range: (select), 10.173.10.6 ~ 10.173.10.6
Port Translation: (select)
In the same subnet as the interface IP or its secondary IPs: (select)

3. Addresses

Objects > Addresses > List > New: Enter the following, then click **OK**:

Address Name: serverfarm-A
IP Address/Domain Name:
IP/Netmask: (select), 10.173.20.0/24
Zone: Untrust

Objects > Addresses > List > New: Enter the following, then click **OK**:

Address Name: serverfarm-B
IP Address/Domain Name:
IP/Netmask: (select), 10.173.40.0/24
Zone: Untrust

4. **VPNs**

   VPNs > AutoKey IKE > New: Enter the following, then click **OK**:

   VPN Name: vpn1
   Security Level: Compatible
   Remote Gateway: Create a Simple Gateway: (select)
   Gateway Name: gw-A
   Type: Static IP: (select), Address/Hostname: 2.2.2.2
   Preshared Key: device1
   Security Level: Compatible
   Outgoing Interface: ethernet3

NOTE: The outgoing interface does not have to be in the same zone to which the tunnel interface is bound, although in this case they are in the same zone.

   > Advanced: Enter the following advanced settings, then click **Return** to return to the basic AutoKey IKE configuration page:

   Bind to Tunnel Interface: (select), tunnel.1
   Proxy-ID: (select)
   Local IP / Netmask: 0.0.0.0/0
   Remote IP / Netmask: 0.0.0.0/0
   Service: ANY

   VPNs > AutoKey IKE > New: Enter the following, then click **OK**:

   VPN Name: vpn2
   Security Level: Compatible
   Remote Gateway: Create a Simple Gateway: (select)
   Gateway Name: gw-B
   Type: Static IP: (select), Address/Hostname: 3.3.3.3
   Preshared Key: device2
   Security Level: Compatible
   Outgoing Interface: ethernet3

   > Advanced: Enter the following advanced settings, then click **Return** to return to the basic AutoKey IKE configuration page:

   Bind to Tunnel Interface: (select), tunnel.2
   Proxy-ID: (select)
   Local IP / Netmask: 0.0.0.0/0
   Remote IP / Netmask: 0.0.0.0/0
   Service: ANY

5. **Routes**

   Network > Routing > Routing Entries > trust-vr New: Enter the following, then click **OK**:

   Network Address / Netmask: 0.0.0.0/0
   Gateway: (select)
   Interface: ethernet3
   Gateway IP Address: 1.1.1.250

Network > Routing > Routing Entries > trust-vr New: Enter the following, then click **OK**:

Network Address / Netmask: 10.173.20.0/24
Gateway: (select)
Interface: tunnel.1
Gateway IP Address: 0.0.0.0

Network > Routing > Routing Entries > trust-vr New: Enter the following, then click **OK**:

Network Address / Netmask: 10.173.30.0/24
Gateway: (select)
Interface: tunnel.1
Gateway IP Address: 0.0.0.0

Network > Routing > Routing Entries > trust-vr New: Enter the following, then click **OK**:

Network Address / Netmask: 10.173.40.0/24
Gateway: (select)
Interface: tunnel.2
Gateway IP Address: 0.0.0.0

Network > Routing > Routing Entries > trust-vr New: Enter the following, then click **OK**:

Network Address / Netmask: 10.173.50.0/24
Gateway: (select)
Interface: tunnel.2
Gateway IP Address: 0.0.0.0

6. **Policies**

Policies > (From: Trust, To: Untrust) New: Enter the following, then click **OK**:

Source Address:
Address Book Entry: (select), Any
Destination Address:
Address Book Entry: (select), serverfarm-A
Service: ANY
Action: Permit
Position at Top: (select)

> Advanced: Enter the following advanced settings, then click **Return** to return to the basic Policy configuration page:

NAT:
Source Translation: (select)
(DIP on): 5 (10.173.10.2–10.173.10.2)/X-late
Destination Translation: (select)
Translate to IP Range: (select), 10.173.30.0 – 10.173.30.255

Policies > (From: Trust, To: Untrust) New: Enter the following, then click **OK**:

Source Address:
Address Book Entry: (select), Any
Destination Address:
Address Book Entry: (select), serverfarm-B
Service: ANY
Action: Permit
Position at Top: (select)

> Advanced: Enter the following advanced settings, then click **Return** to return to the basic Policy configuration page:

NAT:
Source Translation: (select)
(DIP on): 6 (10.173.10.6–10.173.10.6)/X-late
Destination Translation: (select)
Translate to IP Range: (select), 10.173.50.0 – 10.173.50.255

CLI (Security Device-1)

1. **Interfaces**

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.1.1.1/24
set interface ethernet1 nat
set interface ethernet3 zone untrust
set interface ethernet3 ip 1.1.1.1/24
set interface tunnel.1 zone untrust
set interface tunnel.1 ip 10.173.10.1/30
set interface tunnel.2 zone untrust
set interface tunnel.2 ip 10.173.10.5/30
```

2. **DIP Pools**

```
set interface tunnel.1 dip-id 5 10.173.10.2 10.173.10.2
set interface tunnel.2 dip-id 6 10.173.10.6 10.173.10.6
```

3. **Addresses**

```
set address untrust serverfarm-A 10.173.20.0/24
set address untrust serverfarm-B 10.173.40.0/24
```

4. **VPNs**

```
set ike gateway gw-A ip 2.2.2.2 main outgoing-interface ethernet3 preshare
    device1 sec-level compatible
set vpn vpn1 gateway gw-A sec-level compatible
set vpn vpn1 bind interface tunnel.1
set vpn vpn1 proxy-id local-ip 0.0.0.0/0 remote-ip 0.0.0.0/0 any
set ike gateway gw-B ip 3.3.3.3 main outgoing-interface ethernet3 preshare
    device2 sec-level compatible
set vpn vpn2 gateway gw-B sec-level compatible
set vpn vpn2 bind interface tunnel.2
set vpn vpn2 proxy-id local-ip 0.0.0.0/0 remote-ip 0.0.0.0/0 any
```

5. **Routes**

```
set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 1.1.1.250
set vrouter trust-vr route 10.173.20.0/24 interface tunnel.1
set vrouter trust-vr route 10.173.30.0/24 interface tunnel.1
set vrouter trust-vr route 10.173.40.0/24 interface tunnel.2
set vrouter trust-vr route 10.173.50.0/24 interface tunnel.2
```

6. Policies

set policy top from trust to untrust any serverfarm-A any nat src dip-id 5 dst ip 10.173.30.0 10.173.30.255 permit
set policy top from trust to untrust any serverfarm-B any nat src dip-id 6 dst ip 10.173.50.0 10.173.50.255 permit
save

WebUI (Security Device-A)

1. Interfaces

Network > Interfaces > Edit (for ethernet1): Enter the following, then click **Apply**:

Zone Name: Trust
Static IP: (select this option when present)
IP Address/Netmask: 10.100.1.1/24

Select the following, then click **OK**:

Interface Mode: NAT

Network > Interfaces > Edit (for ethernet3): Enter the following, then click **OK**:

Zone Name: Untrust
Static IP: (select this option when present)
IP Address/Netmask: 2.2.2.2/24

Network > Interfaces > New Tunnel IF: Enter the following, then click **OK**:

Tunnel Interface Name: tunnel.1
Zone (VR): Untrust (trust-vr)
Fixed IP: (select)
IP Address / Netmask: 10.2.2.1/24

2. Addresses

Objects > Addresses > List > New: Enter the following, then click **OK**:

Address Name: serverfarm-A
IP Address/Domain Name:
IP/Netmask: (select), 10.173.30.0/24
Zone: Trust

Objects > Addresses > List > New: Enter the following, then click **OK**:

Address Name: customer1
IP Address/Domain Name:
IP/Netmask: (select), 10.173.10.2/32
Zone: Untrust

3. **VPN**

VPNs > AutoKey IKE > New: Enter the following, then click **OK**:

VPN Name: vpn1
Security Level: Compatible
Remote Gateway: Create a Simple Gateway: (select)
Gateway Name: gw-1
Type: Static IP: (select), Address/Hostname: 1.1.1.1
Preshared Key: device1
Security Level: Compatible
Outgoing Interface: ethernet3

> Advanced: Enter the following advanced settings, then click **Return** to return to the basic AutoKey IKE configuration page:

Bind to Tunnel Interface: (select), tunnel.1
Proxy-ID: (select)
Local IP / Netmask: 0.0.0.0/0
Remote IP / Netmask: 0.0.0.0/0
Service: ANY

4. **Routes**

Network > Routing > Routing Entries > trust-vr New: Enter the following, then click **OK**:

Network Address / Netmask: 0.0.0.0/0
Gateway: (select)
Interface: ethernet3
Gateway IP Address: 2.2.2.250

Network > Routing > Routing Entries > trust-vr New: Enter the following, then click **OK**:

Network Address / Netmask: 10.173.10.2/32
Gateway: (select)
Interface: tunnel.1
Gateway IP Address: 0.0.0.0

Network > Routing > Routing Entries > trust-vr New: Enter the following, then click **OK**:

Network Address / Netmask: 10.173.30.0/24
Gateway: (select)
Interface: ethernet1
Gateway IP Address: 0.0.0.0

5. **Policy**

Policies > (From: Untrust, To: Trust) New: Enter the following, then click **OK**:

Source Address:
Address Book Entry: (select), customer1
Destination Address:
Address Book Entry: (select), serverfarm-A
Service: ANY
Action: Permit
Position at Top: (select)

> Advanced: Enter the following advanced settings, then click **Return** to return to the basic Policy configuration page:

NAT:
Destination Translation: (select)
Translate to IP Range: (select), 10.100.1.0 – 10.100.1.255

CLI (Security Device-A)

1. **Interfaces**

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.100.1.1/24
set interface ethernet1 nat
set interface ethernet3 zone untrust
set interface ethernet3 ip 2.2.2.2/24
set interface tunnel.1 zone untrust
set interface tunnel.1 ip 10.2.2.1/24
```

2. **Addresses**

```
set address trust serverfarm-A 10.173.30.0/24
set address untrust customer1 10.173.10.2/32
```

3. **VPN**

```
set ike gateway gw-1 ip 1.1.1.1 main outgoing-interface ethernet3 preshare
    device1 sec-level compatible
set vpn vpn1 gateway gw-1 sec-level compatible
set vpn vpn1 bind interface tunnel.1
set vpn vpn1 proxy-id local-ip 0.0.0.0/0 remote-ip 0.0.0.0/0 any
```

4. **Routes**

```
set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 2.2.2.250
set vrouter trust-vr route 10.173.10.2/32 interface tunnel.1
set vrouter trust-vr route 10.173.30.0/24 interface ethernet1
```

5. **Policy**

```
set policy top from untrust to trust customer1 serverfarm-A any nat dst ip
    10.100.1.0 10.100.1.255 permit
save
```

WebUI (Security Device-B)

1. **Interfaces**

Network > Interfaces > Edit (for ethernet1): Enter the following, then click **Apply**:

Zone Name: Trust
Static IP: (select this option when present)
IP Address/Netmask: 10.100.2.1/24
Select the following, then click **OK**:
Interface Mode: NAT

Network > Interfaces > Edit (for ethernet3): Enter the following, then click **OK**:

Zone Name: Untrust
Static IP: (select this option when present)
IP Address/Netmask: 3.3.3.3/24

Network > Interfaces > New Tunnel IF: Enter the following, then click **OK**:

Tunnel Interface Name: tunnel.1
Zone (VR): Untrust (trust-vr)
Fixed IP: (select)
IP Address / Netmask: 10.3.3.1/24

2. Addresses

Objects > Addresses > List > New: Enter the following, then click **OK**:

Address Name: serverfarm-B
IP Address/Domain Name:
IP/Netmask: (select), 10.173.50.0/24
Zone: Trust

Objects > Addresses > List > New: Enter the following, then click **OK**:

Address Name: customer1
IP Address/Domain Name:
IP/Netmask: (select), 10.173.10.6/32
Zone: Untrust

3. VPN

VPNs > AutoKey IKE > New: Enter the following, then click **OK**:

VPN Name: vpn1
Security Level: Compatible
Remote Gateway: Create a Simple Gateway: (select)
Gateway Name: gw-1
Type: Static IP: (select), Address/Hostname: 1.1.1.1
Preshared Key: device2
Security Level: Compatible
Outgoing Interface: ethernet3

> Advanced: Enter the following advanced settings, then click **Return** to return to the basic AutoKey IKE configuration page:

Bind to Tunnel Interface: (select), tunnel.1
Proxy-ID: (select)
Local IP / Netmask: 0.0.0.0/0
Remote IP / Netmask: 0.0.0.0/0
Service: ANY

4. Routes

Network > Routing > Routing Entries > trust-vr New: Enter the following, then click **OK**:

Network Address / Netmask: 0.0.0.0/0
Gateway: (select)
Interface: ethernet3
Gateway IP Address: 3.3.3.250

Network > Routing > Routing Entries > trust-vr New: Enter the following, then click **OK**:

Network Address / Netmask: 10.173.10.6/32
Gateway: (select)
Interface: tunnel.1
Gateway IP Address: 0.0.0.0

Network > Routing > Routing Entries > trust-vr New: Enter the following, then click **OK**:

Network Address / Netmask: 10.173.50.0/24
Gateway: (select)
Interface: ethernet1
Gateway IP Address: 0.0.0.0

5. Policy

Policies > (From: Untrust, To: Trust) New: Enter the following, then click **OK**:

Source Address:
Address Book Entry: (select), customer1
Destination Address:
Address Book Entry: (select), serverfarm-B
Service: ANY
Action: Permit
Position at Top: (select)

> Advanced: Enter the following advanced settings, then click **Return** to return to the basic Policy configuration page:

NAT:
Destination Translation: (select)
Translate to IP Range: (select), 10.100.2.0 – 10.100.2.255

CLI (Security Device-B)

1. Interfaces

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.100.2.1/24
set interface ethernet1 nat
set interface ethernet3 zone untrust
set interface ethernet3 ip 3.3.3.3/24
set interface tunnel.1 zone untrust
set interface tunnel.1 ip 10.3.3.1/24
```

2. Addresses

```
set address trust serverfarm-B 10.173.50.0/24
set address untrust customer1 10.173.10.6/32
```

3. VPN

```
set ike gateway gw-1 ip 1.1.1.1 main outgoing-interface ethernet3 preshare
    device2 sec-level compatible
set vpn vpn2 gateway gw-1 sec-level compatible
set vpn vpn2 bind interface tunnel.1
set vpn vpn2 proxy-id local-ip 0.0.0.0/0 remote-ip 0.0.0.0/0 any
```

4. **Routes**

   ```
   set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 3.3.3.250
   set vrouter trust-vr route 10.173.10.6/32 interface tunnel.1
   set vrouter trust-vr route 10.173.50.0/24 interface ethernet1
   ```

5. **Policy**

   ```
   set policy top from untrust to trust customer1 serverfarm-B any nat dst ip
       10.100.2.0 10.100.2.255 permit
   save
   ```

Chapter 4

Mapped and Virtual Addresses

ScreenOS provides many methods for performing destination IP address and destination Port Address Translation (PAT). This chapter describes how to use Mapped IP (MIP) and Virtual IP (VIP) addresses and is organized into the following sections:

Mapped IP Addresses

Mapped IP (MIP) is a direct one-to-one mapping of one IP address to another. The security device forwards incoming traffic destined for a MIP to the host with the address to which the MIP points. Essentially, a MIP is static destination address translation, mapping the destination IP address in an IP packet header to another static IP address. When a MIP host initiates outbound traffic, the security device translates the source IP address of the host to that of the MIP address. This bidirectional translation symmetry differs from the behavior of source and destination address translation (see "Directional Nature of NAT-Src and NAT-Dst" on page 10).

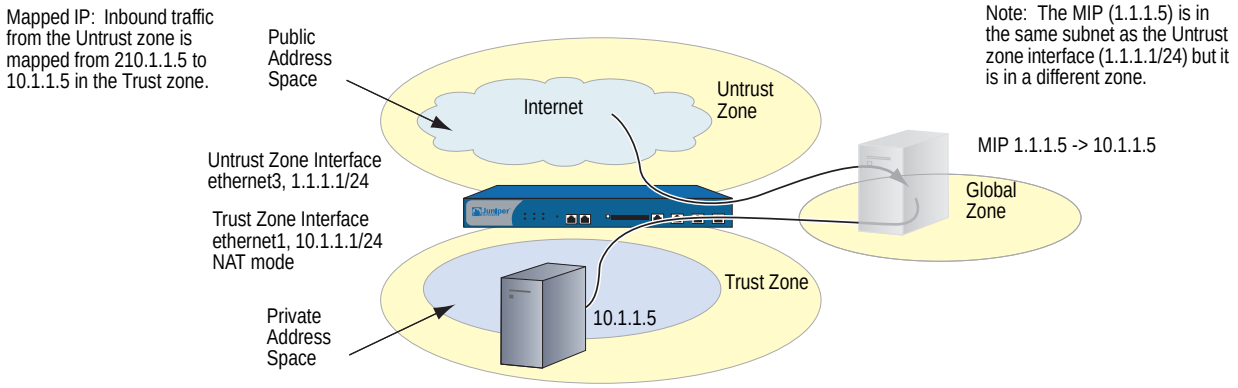
MIPs allow inbound traffic to reach private addresses in a zone whose interface is in NAT mode. MIPs also provide part of the solution to the problem of overlapping address spaces at two sites connected by a VPN tunnel. (For the complete solution to this problem, see "VPN Sites with Overlapping Addresses" on page **5-**139.)

NOTE: An overlapping address space is when the IP address range in two networks is partially or completely the same.

You can create a MIP in the same subnet as a tunnel interface with an IP address/netmask, or in the same subnet as the IP address/netmask of an interface bound to a Layer 3 (L3) security zone. Although you configure MIPs for interfaces bound to tunnel zones and security zones, the MIP that you define is stored in the Global zone.

NOTE: An exception is a MIP defined for an interface in the Untrust zone. That MIP can be in a different subnet from an Untrust zone interface IP address. However, if that is the case, you must add a route on the external router pointing to an Untrust zone interface so that incoming traffic can reach the MIP. Also, you must define a static route on the security device associating the MIP with the interface that hosts it.

Figure 32: Mapped IP Address



NOTE: On some security devices, a MIP can use the same address as an interface, but a MIP address cannot be in a DIP pool.

You can map an address-to-address or subnet-to-subnet relationship. When a subnet-to-subnet mapped IP configuration is defined, the netmask is applied to both the mapped IP subnet and the original IP subnet.

MIP and the Global Zone

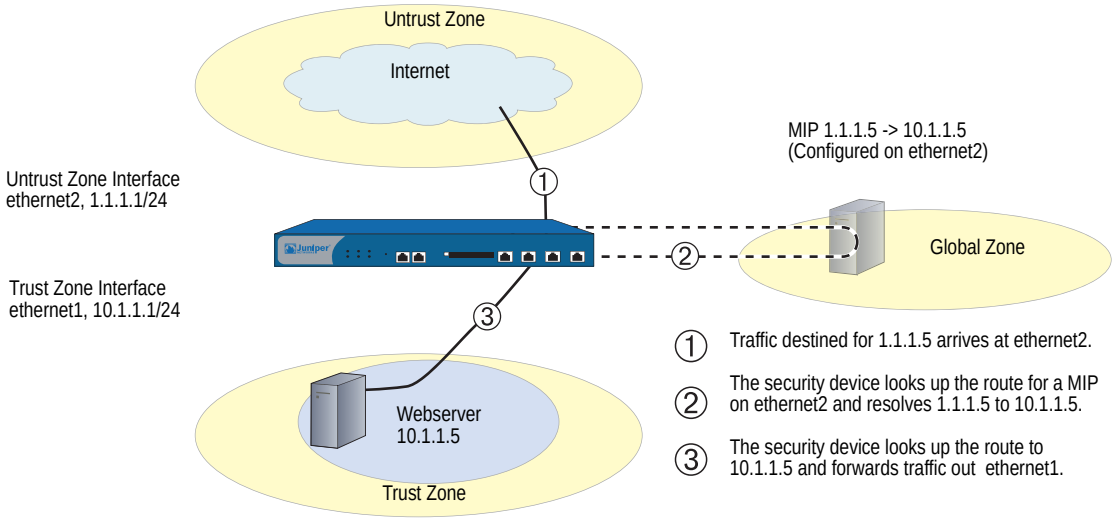
Setting a MIP for an interface in any zone generates an entry for the MIP in the Global zone address book. The Global zone address book stores all MIPs, regardless of the zone to which their interfaces belong. You can use these MIP addresses as the destination addresses in policies between any two zones, and as the destination addresses when defining a Global policy. (For information about Global policies, see “Global Policies” on page **2-**174.) Although the security device stores MIPs in the Global zone, you can use either the Global zone or the zone with the address to which the MIP points as the destination zone in a policy referencing a MIP.

Example: MIP on an Untrust Zone Interface

In this example, you bind ethernet1 to the Trust zone and assign it IP address 10.1.1.1/24. You bind ethernet2 to the Untrust zone and assign it IP address 1.1.1.1/24. Then you configure a MIP to direct incoming HTTP traffic destined for 1.1.1.5 in the Untrust zone to a webserver at 10.1.1.5 in the Trust zone. Finally, you create a policy permitting HTTP traffic from the any address in the Untrust zone to the MIP—and consequently to the host with the address to which the MIP points—in the Trust zone. All security zones are in the trust-vr routing domain.

NOTE: No address book entry is required for a MIP or for the host to which it points.

Figure 33: MIP on Untrust Zone Interface



WebUI

1. **Interfaces**

   Network > Interfaces > Edit (for ethernet1): Enter the following, then click **Apply**:

   Zone Name: Trust
   Static IP: (select this option when present)
   IP Address/Netmask: 10.1.1.1/24
   Select the following, then click **OK**:
   Interface Mode: NAT

   Network > Interfaces > Edit (for ethernet2): Enter the following, then click **OK**:

   Zone Name: Untrust
   Static IP: (select this option when present)
   IP Address/Netmask: 1.1.1.1/24

2. **MIP**

   Network > Interfaces > Edit (for ethernet2) > MIP > New: Enter the following, then click **OK**:

   Mapped IP: 1.1.1.5
   Netmask: 255.255.255.255
   Host IP Address: 10.1.1.5
   Host Virtual Router Name: trust-vr

3. **Policy**

   Policies > (From: Untrust, To: Trust) New: Enter the following, then click **OK**:

   Source Address:
   Address Book Entry: (select), Any
   Destination Address:
   Address Book Entry: (select), MIP(1.1.1.5)
   Service: HTTP
   Action: Permit

CLI

1. **Interfaces**

   set interface ethernet1 zone trust
   set interface ethernet1 ip 10.1.1.1/24
   set interface ethernet1 nat
   set interface ethernet2 zone untrust
   set interface ethernet2 ip 1.1.1.1/24

2. **MIP**

   set interface ethernet2 mip 1.1.1.5 host 10.1.1.5 netmask 255.255.255.255 vrouter trust-vr

---

NOTE: By default, the netmask for a MIP is 32 bits (255.255.255.255), mapping the address to a single host. You can also define a MIP for a range of addresses. For example, to define 1.1.1.5 as a MIP for the addresses 10.1.10.129–10.1.10.254 within a class C subnet through the CLI, use the following syntax: **set interface** *interface* **mip 1.1.1.5 host 10.1.10.128 netmask 255.255.255.128**. Be careful not to use a range of addresses that includes the interface or router addresses.

The default virtual router is the trust-vr. You do not have to specify that the virtual router is the trust-vr or that the MIP has a 32-bit netmask . These arguments are included in this command to provide symmetry with the WebUI configuration.

---

3. **Policy**

   set policy from untrust to trust any mip(1.1.1.5) http permit
   save

Example: Reaching a MIP from Different Zones

Traffic from different zones can still reach a MIP through other interfaces than the one on which you configured the MIP. To accomplish this, you must set a route on the routers in each of the other zones that points inbound traffic to the IP address of their respective interfaces to reach the MIP.

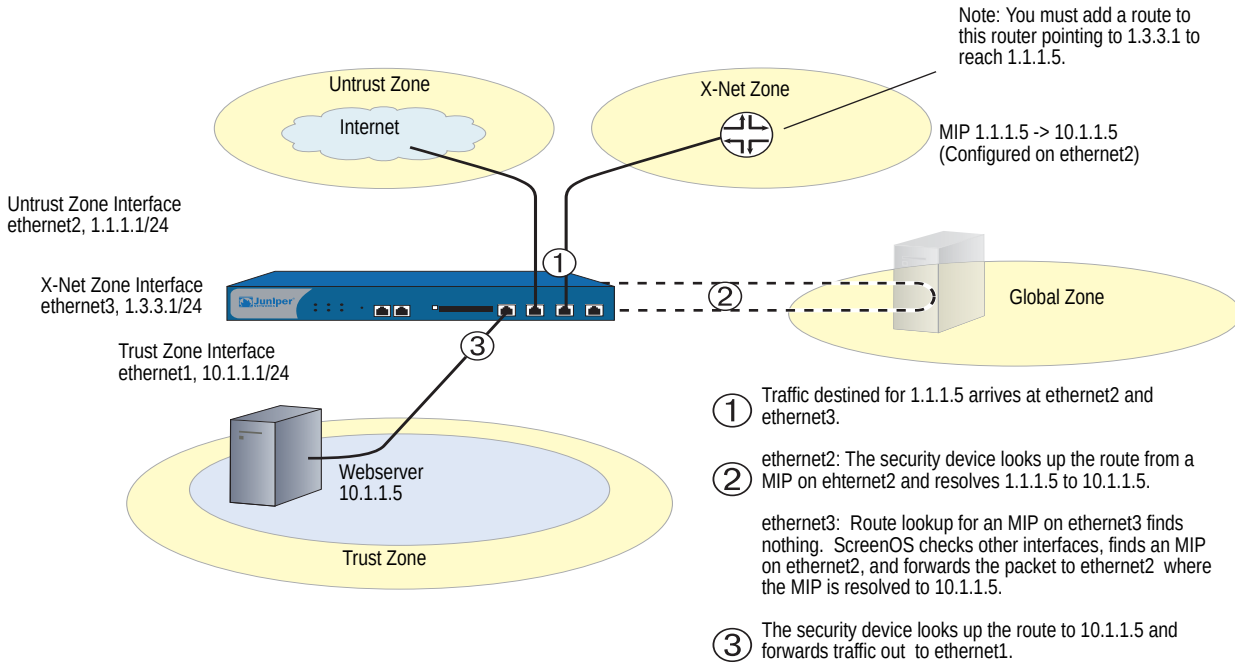
NOTE: If the MIP is in the same subnet as the interface on which you configured it, you do not have to add a route to the security device for traffic to reach the MIP via a different interface. However, if the MIP is in a different subnet than the IP address of its interface (which is possible only for a MIP on an interface in the Untrust zone), you must add a static route to the security device routing table. Use the **set vrouter** *name_str* **route** *ip_addr* **interface** *interface* command (or its equivalent in the WebUI), where *name_str* is the virtual router to which the specified interface belongs, and *interface* is interface on which you configured the MIP.

In this example, you configure a MIP (1.1.1.5) on the interface in the Untrust zone (ethernet2, 1.1.1.1/24) to map to a webserver in the Trust zone (10.1.1.5). The interface bound to the Trust zone is ethernet1 with IP address 10.1.1.1/24.

You create a security zone named X-Net, bind ethernet3 to it, and assign the interface the IP address 1.3.3.1/24. You define an address for 1.1.1.5 for use in a policy to allow HTTP traffic from any address in the X-Net zone to the MIP in the Untrust zone. You also configure a policy to allow the HTTP traffic to pass from the Untrust zone to the Trust zone. All security zones are in the trust-vr routing domain.

NOTE: You must enter a route on the router in the X-Net zone directing traffic destined for 1.1.1.5 (MIP) to 1.3.3.1 (IP address of ethernet3).

Figure 34: Reaching a MIP from Different Zones



WebUI

1. **Interfaces and Zones**
   Network > Interfaces > Edit (for ethernet1): Enter the following, then click **OK**:

   Zone Name: Trust
   Static IP: (select this option when present)
   IP Address/Netmask: 10.1.1.1/24
   Select the following, then click **OK**:
   Interface Mode: NAT

   Network > Interfaces > Edit (for ethernet2): Enter the following, then click **OK**:

   Zone Name: Untrust
   Static IP: (select this option when present)
   IP Address/Netmask: 1.1.1.1/24

   Network > Zones > New: Enter the following, then click **OK**:

   Zone Name: X-Net
   Virtual Router Name: untrust-vr
   Zone Type: Layer 3

   Network > Interfaces > Edit (for ethernet3): Enter the following, then click **OK**:

   Zone Name: X-Net
   IP Address/Netmask: 1.3.3.1/24

2. **Address**
   Objects > Addresses > List > New: Enter the following, then click **OK**:

   Address Name: 1.1.1.5
   IP Address/Domain Name:
   IP/Netmask: (select), 1.1.1.5/32
   Zone: Untrust

3. **MIP**
   Network > Interfaces > Edit (for ethernet2) > MIP > New: Enter the following, then click **OK**:

   Mapped IP: 1.1.1.5
   Netmask: 255.255.255.255
   Host IP Address: 10.1.1.5
   Host Virtual Router Name: trust-vr

4. Policies

Policies > (From: X-Net, To: Untrust) New: Enter the following, then click **OK**:

Source Address:
    Address Book Entry: (select), Any
Destination Address:
    Address Book Entry: (select), 1.1.1.5
Service: HTTP
Action: Permit

Policies > (From: Untrust, To: Trust) New: Enter the following, then click **OK**:

Source Address:
    Address Book Entry: (select), Any
Destination Address:
    Address Book Entry: (select), MIP(1.1.1.5)
Service: HTTP
Action: Permit

CLI

1. Interfaces and Zones

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.1.1.1/24
set interface ethernet1 nat
set interface ethernet2 zone untrust
set interface ethernet2 ip 1.1.1.1/24
set zone name X-Net
set interface ethernet3 zone X-Net
set interface ethernet3 ip 1.3.3.1/24
```

2. Address

```
set address untrust "1.1.1.5" 1.1.1.5/32
```

3. MIP

```
set interface ethernet2 mip 1.1.1.5 host 10.1.1.5 netmask 255.255.255.255
    vrouter trust-vr
```

NOTE: By default, the netmask for a MIP is 32 bits (255.255.255.255) and the default virtual router is the trust-vr. You do not have to specify them in the command. These arguments are included here to provide symmetry with the WebUI configuration.

---

4. Policies

```
set policy from X-Net to untrust any "1.1.1.5" http permit
set policy from untrust to trust any mip(1.1.1.5) http permit
save
```

Example: Adding a MIP to a Tunnel Interface

In this example, the IP address space for the network in the Trust zone is 10.1.1.0/24 and the IP address for the tunnel interface "tunnel.8" is 10.20.3.1. The physical IP address for a server on the network in the Trust zone is 10.1.1.25. To allow a remote site whose network in the Trust zone uses an overlapping address space to access the local server through a VPN tunnel, you create a MIP in the same subnet as the tunnel.8 interface. The MIP address is 10.20.3.25/32. (For a more complete example of a MIP with a tunnel interface, see "VPN Sites with Overlapping Addresses" on page **5-**139.)

WebUI

Network > Interfaces > Edit (for tunnel.8) > MIP > New: Enter the following, then click **OK**:

Mapped IP: 10.20.3.25
Netmask: 255.255.255.255
Host IP Address: 10.1.1.25
Host Virtual Router Name: trust-vr

CLI

```
set interface tunnel.8 mip 10.20.3.25 host 10.1.1.25 netmask 255.255.255.255
    vrouter trust-vr
save
```

NOTE: By default, the netmask for a MIP is 32 bits (255.255.255.255) and the default virtual router is the trust-vr. You do not have to specify them in the command. These arguments are included here to provide symmetry with the WebUI configuration.

When the remote administrator adds the address for the server to his Untrust zone address book, he must enter the MIP (10.20.3.25), not the physical IP address (10.1.1.25) of the server.

The remote administrator also needs to apply policy-based NAT-src (using DIP) on the outgoing packets bound for the server through the VPN so that the local administrator can add an Untrust zone address that does not conflict with the local Trust zone addresses. Otherwise, the source address in the incoming policy would seem to be in the Trust zone.

MIP-Same-as-Untrust

As IPv4 addresses become increasingly scarce, ISPs are becoming increasingly reluctant to give their customers more than one or two IP addresses. If you only have one IP address for the interface bound to the Untrust zone—the interface bound to the Trust zone is in Network Address Translation (NAT) mode—you can use the Untrust zone interface IP address as a mapped IP (MIP) to provide inbound access to an internal server or host, or to a VPN or L2TP tunnel endpoint.

A MIP maps traffic arriving at the one address to another address; so by using the Untrust zone interface IP address as a MIP, the security device maps all inbound traffic using the Untrust zone interface to a specified internal address. If the MIP on the Untrust interface maps to a VPN or L2TP tunnel endpoint, the device automatically forwards the IKE or L2TP packets that it receives to the tunnel endpoint, as long as there is no VPN or L2TP tunnel configured on the Untrust interface.

If you create a policy in which the destination address is a MIP using the Untrust zone interface IP address and you specify HTTP as the service in the policy, you lose Web management of the security device via that interface (because all inbound HTTP traffic to that address is mapped to an internal server or host). You can still manage the device via the Untrust zone interface using the WebUI by changing the port number for Web management. To change the Web management port number, do the following:

1. Admin > Web: Enter a registered port number (from 1024 to 65,535) in the HTTP Port field. Then click **Apply**.

2. When you next connect to the Untrust zone interface to manage the device, append the port number to the IP address—for example, http://209.157.66.170:5000.

Example: MIP on the Untrust Interface

In this example, you select the IP address of the Untrust zone interface (ethernet3, 1.1.1.1/24) as the MIP for a webserver whose actual IP address is 10.1.1.5 in the Trust zone. Because you want to retain Web management access to the ethernet3 interface, you change the web management port number to 8080. You then create a policy permitting HTTP service (on the HTTP default port number—80) from the Untrust zone to the MIP—and consequently to the host with the address to which the MIP points—in the Trust zone.

WebUI

1. Interfaces

Network > Interfaces > Edit (for ethernet1): Enter the following, then click **Apply**:

Zone Name: Trust
Static IP: (select this option when present)
IP Address/Netmask: 10.1.1.1/24

Enter the following, then click **OK**:

NAT: (select)

NOTE: By default, any interface that you bind to the Trust zone is in NAT mode. Consequently, this option is already enabled for interfaces bound to the Trust zone.

Network > Interfaces > Edit (for ethernet3): Enter the following, then click **OK**:

Zone Name: Untrust
Static IP: (select this option when present)
IP Address/Netmask: 1.1.1.1/24

2. **HTTP Port**
   Configuration > Admin > Management: Type **8080** in the HTTP Port field, then click **Apply**.

   (The HTTP connection is lost.)

3. **Reconnection**
   Reconnect to the security device, appending 8080 to the IP address in the URL address field in your browser. (If you are currently managing the device via the untrust interface, enter **http://1.1.1.1:8080**.)

4. **MIP**
   Network > Interface > Edit (for ethernet3) > MIP > New: Enter the following, then click **OK**:

   Mapped IP: 1.1.1.1
   Netmask: 255.255.255.255
   Host IP Address: 10.1.1.5
   Host Virtual Router Name: trust-vr

NOTE: The netmask for a MIP using an Untrust zone interface IP address must be 32 bits.

5. **Route**
   Network > Routing > Routing Entries > trust-vr New: Enter the following, then click **OK**:

   Network Address / Netmask: 0.0.0.0/0
   Gateway: (select)
   Interface: ethernet3
   Gateway IP Address: 1.1.1.250

6. **Policy**
   Policies > (From: Untrust, To: Trust) New: Enter the following, then click **OK**:

   Source Address:
   Address Book Entry: (select), Any
   Destination Address:
   Address Book Entry: (select), MIP(1.1.1.1)
   Service: HTTP
   Action: Permit

CLI

1. **Interfaces**
   set interface ethernet1 zone trust
   set interface ethernet1 ip 10.1.1.1/24
   set interface ethernet1 nat
   set interface ethernet3 zone untrust
   set interface ethernet3 ip 1.1.1.1/24

2. **HTTP Port**
   set admin port 8080

3. **MIP**
   set interface ethernet3 mip 1.1.1.1 host 10.1.1.5 netmask 255.255.255.255
   vrouter trust-vr

NOTE: By default, the netmask for a MIP is 32 bits (255.255.255.255) and the default virtual router is the trust-vr. You do not have to specify them in the command. These arguments are included here to provide symmetry with the WebUI configuration.

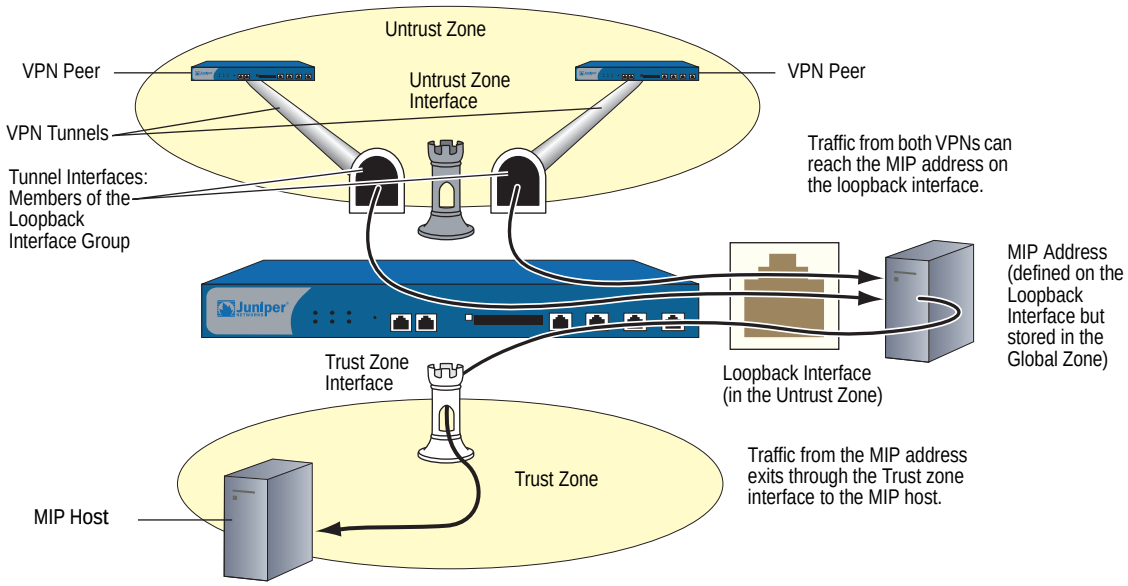
4. **Route**
   set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 1.1.1.250

5. **Policy**
   set policy from untrust to trust any mip(1.1.1.1) http permit
   save

MIP and the Loopback Interface

Defining a MIP on the loopback interface allows a MIP to be accessed by a group of interfaces. The primary application for this is to allow access to a host through one of several VPN tunnels using a single MIP address. The MIP host can also initiate traffic to a remote site through the appropriate tunnel.

Figure 35: MIP on the Loopback Interface



You can think of the loopback interface as a resource holder that contains a MIP address. You configure a loopback interface with the name loopback.*id_num* (where *id_num* is an index number that uniquely identifies the interface in the device) and assign an IP address to the interface (see “Loopback Interfaces” on page 2-66). To allow other interfaces to use a MIP on the loopback interface, you then add the interfaces as members of the loopback group.

The loopback interface and its member interfaces must be in different IP subnets in the same zone. Any type of interface can be a member of a loopback group as long as the interface has an IP address. If you configure a MIP on both a loopback interface and one of its member interfaces, the loopback interface configuration takes precedence. A loopback interface cannot be a member of another loopback group.

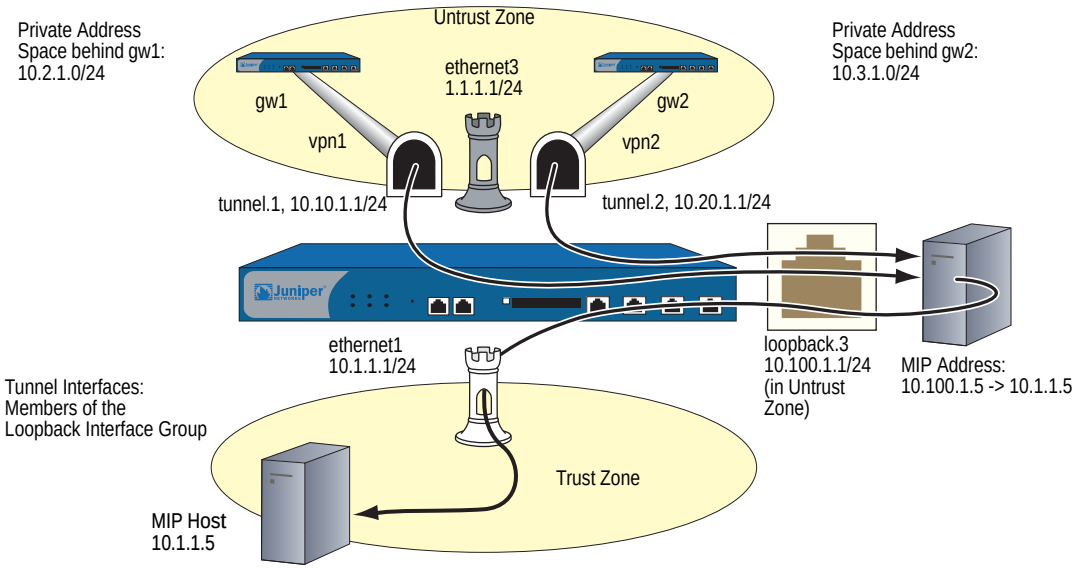
Example: MIP for Two Tunnel Interfaces

In this example, you configure the following interfaces:

- ethernet1, Trust zone, 10.1.1.1/24
- ethernet3, Untrust zone, 1.1.1.1/24
- tunnel.1, Untrust zone, 10.10.1.1/24, bound to vpn1
- tunnel.2, Untrust zone, 10.20.1.1/24, bound to vpn2
- loopback.3, Untrust zone, 10.100.1.1/24

The tunnel interfaces are members of the loopback.3 interface group. The loopback.3 interface contains MIP address 10.100.1.5, which maps to a host at 10.1.1.5 in the Trust zone.

Figure 36: MIP for Two Tunnel Interfaces



When a packet destined for 10.100.1.5 arrives at through a VPN tunnel to tunnel.1, the security device searches for the MIP on the loopback interface loopback.3. When it finds a match on loopback.3, the security device translates the original destination IP (10.100.1.5) to the host IP address (10.1.1.5) and forwards the packet through ethernet1 to the MIP host. Traffic destined for 10.100.1.5 can also arrive through a VPN tunnel bound to tunnel.2. Again, the security device finds a match on loopback.3 and translates the original destination IP 10.100.1.5 to 10.1.1.5 and forwards the packet to the MIP host.

You also define addresses, VPN tunnels, routes, and policies as needed to complete the configuration. All security zones are in the trust-vr routing domain.

WebUI

1. **Interfaces**
   Network > Interfaces > Edit (for ethernet1): Enter the following, then click **Apply**:

   Zone Name: Trust
   Static IP: (select this option when present)
   IP Address/Netmask: 10.1.1.1/24

   Enter the following, then click **OK**:

   NAT: (select)

NOTE: By default, any interface that you bind to the Trust zone is in NAT mode. Consequently, this option is already enabled for interfaces bound to the Trust zone.

   Network > Interfaces > Edit (for ethernet3): Enter the following, then click **OK**:

   Zone Name: Untrust
   Static IP: (select this option when present)
   IP Address/Netmask: 1.1.1.1/24

   Network > Interfaces > New Loopback IF: Enter the following, then click **OK**:

   Interface Name: loopback.3
   Zone: Untrust (trust-vr)
   IP Address / Netmask: 10.100.1.1/24

   Network > Interfaces > New Tunnel IF: Enter the following, then click **Apply**:

   Tunnel Interface Name: tunnel.1
   Zone (VR): Untrust (trust-vr)
   Fixed IP: (select)
   IP Address / Netmask: 10.10.1.1/24

   Select **loopback.3** in the Member of Loopback Group drop-down list, then click **OK**.

Network > Interfaces > New Tunnel IF: Enter the following, then click **Apply**:

Tunnel Interface Name: tunnel.2
Zone (VR): Untrust (trust-vr)
Fixed IP: (select)
IP Address / Netmask: 10.20.1.1/24

Select **loopback.3** in the Member of Loopback Group drop-down list, then click **OK**.

2. MIP

Network > Interfaces > Edit (for loopback.3) > MIP > New: Enter the following, then click **OK**:

Mapped IP: 10.100.1.5
Netmask: 255.255.255.255
Host IP Address: 10.1.1.5
Host Virtual Router Name: trust-vr

3. Addresses

Objects > Addresses > List > New: Enter the following, then click **OK**:

Address Name: local_lan
IP Address/Domain Name:
IP/Netmask: (select), 10.1.1.0/24
Zone: Trust

Objects > Addresses > List > New: Enter the following, then click **OK**:

Address Name: peer-1
IP Address/Domain Name:
IP/Netmask: (select), 10.2.1.0/24
Zone: Untrust

Objects > Addresses > List > New: Enter the following, then click **OK**:

Address Name: peer-2
IP Address/Domain Name:
IP/Netmask: (select), 10.3.1.0/24
Zone: Untrust

4. VPNs

VPNs > AutoKey IKE > New: Enter the following, then click **OK**:

VPN Name: vpn1
Security Level: Compatible
Remote Gateway: Create a Simple Gateway: (select)
Gateway Name: gw1
Type: Static IP: (select), Address/Hostname: 2.2.2.2
Preshared Key: device1
Security Level: Compatible
Outgoing Interface: ethernet3

> Advanced: Enter the following advanced settings, then click **Return** to return to the basic AutoKey IKE configuration page:

Bind to Tunnel Interface: (select), tunnel.1
Proxy-ID: (select)
Local IP / Netmask: 0.0.0.0/0
Remote IP / Netmask: 0.0.0.0/0
Service: ANY

VPNs > AutoKey IKE > New: Enter the following, then click **OK**:

VPN Name: vpn2
Security Level: Compatible
Remote Gateway: Create a Simple Gateway: (select)
Gateway Name: gw2
Type: Static IP: (select), Address/Hostname: 3.3.3.3
Preshared Key: device2
Security Level: Compatible
Outgoing Interface: ethernet3

> Advanced: Enter the following advanced settings, then click **Return** to return to the basic AutoKey IKE configuration page:

Bind to Tunnel Interface: (select), tunnel.2
Proxy-ID: (select)
Local IP / Netmask: 0.0.0.0/0
Remote IP / Netmask: 0.0.0.0/0
Service: ANY

5. Routes

Network > Routing > Routing Entries > trust-vr New: Enter the following, then click **OK**:

Network Address / Netmask: 10.2.1.0/24
Gateway: (select)
Interface: tunnel.1
Gateway IP Address: 0.0.0.0

Network > Routing > Routing Entries > trust-vr New: Enter the following, then click **OK**:

Network Address / Netmask: 10.3.1.0/24
Gateway: (select)
Interface: tunnel.2
Gateway IP Address: 0.0.0.0

Network > Routing > Routing Entries > trust-vr New: Enter the following, then click **OK**:

Network Address / Netmask: 0.0.0.0/0
Gateway: (select)
Interface: ethernet3
Gateway IP Address: 1.1.1.250

6. **Policies**

   Policies > (From: Untrust, To: Trust) New: Enter the following, then click **OK**:

   Source Address:
   Address Book Entry: (select), peer-1
   Destination Address:
   Address Book Entry: (select), MIP(10.100.1.5)
   Service: ANY
   Action: Permit

   Policies > (From: Untrust, To: Trust) New: Enter the following, then click **OK**:

   Source Address:
   Address Book Entry: (select), peer-2
   Destination Address:
   Address Book Entry: (select), MIP(10.100.1.5)
   Service: ANY
   Action: Permit

   Policies > (From: Trust, To: Untrust) New: Enter the following, then click **OK**:

   Source Address:
   Address Book Entry: (select), local_lan
   Destination Address:
   Address Book Entry: (select), Any
   Service: ANY
   Action: Permit

CLI

1. **Interfaces**

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.1.1.1/24
set interface ethernet1 nat
set interface ethernet3 zone untrust
set interface ethernet3 ip 1.1.1.1/24
set interface loopback.3 zone trust
set interface loopback.3 ip 10.100.1.1/24
set interface tunnel.1 zone untrust
set interface tunnel.1 ip 10.10.1.1/24
set interface tunnel.1 loopback-group loopback.3
set interface tunnel.2 zone untrust
set interface tunnel.2 ip 10.20.1.1/24
set interface tunnel.2 loopback-group loopback.3
```

2. **MIP**

```
set interface loopback.3 mip 10.100.1.5 host 10.1.1.5 netmask
    255.255.255.255 vrouter trust-vr
```

NOTE: By default, the netmask for a MIP is 32 bits (255.255.255.255) and the default virtual router is the trust-vr. You do not have to specify them in the command. These arguments are included here to provide symmetry with the WebUI configuration.

3. **Addresses**

   set address trust local_lan 10.1.1.0/24
   set address untrust peer-1 10.2.1.0/24
   set address untrust peer-2 10.3.1.0/24

4. **VPNs**

   set ike gateway gw1 address 2.2.2.2 outgoing-interface ethernet3 preshare device1 sec-level compatible
   set vpn vpn1 gateway gw1 sec-level compatible
   set vpn vpn1 bind interface tunnel.1
   set vpn vpn1 proxy-id local-ip 0.0.0.0/0 remote-ip 0.0.0.0/0 any
   set ike gateway gw2 address 3.3.3.3 outgoing-interface ethernet3 preshare device2 sec-level compatible
   set vpn vpn2 gateway gw2 sec-level compatible
   set vpn vpn2 bind interface tunnel.2
   set vpn vpn2 proxy-id local-ip 0.0.0.0/0 remote-ip 0.0.0.0/0 any

5. **Routes**

   set vrouter trust-vr route 10.2.1.0/24 interface tunnel.1
   set vrouter trust-vr route 10.3.1.0/24 interface tunnel.2
   set vrouter untrust-vr route 0.0.0.0/0 interface ethernet3 gateway 1.1.1.250

6. **Policies**

   set policy top from untrust to trust peer-1 mip(10.100.1.5) any permit
   set policy top from untrust to trust peer-2 mip(10.100.1.5) any permit
   set policy from trust to untrust local_lan any any permit
   save

MIP Grouping

Assigning a MIP to an interface sets aside a range of IP addresses to use as destination addresses for packets that pass through the interface. You can then use the MIP in a policy, which makes the address recognizable to interfaces receiving incoming packets or usable for interfaces transmitting outgoing packets.

However, there may be situations when it is necessary to invoke multiple MIPs in a single policy. For example, a single address range may not provide enough addresses when there are many destination hosts or gateways in a particular network topology. Such a solution requires *MIP grouping*, which allows you to design *multi-cell policies*. Such policies invoke multiple address ranges as possible source addresses.

Example: MIP Grouping with Multi-Cell Policy

In the following example, you create a policy that uses two different MIP address definitions (1.1.1.3 and 1.1.1.4).

NOTE: For this example, assume that the policy ID for the generated policy is 104.

WebUI

Network > Interface > Edit > MIP (List)

Policies > New

CLI

```
set interface ethernet1/2 mip 1.1.1.3 host 2.2.2.2
set interface ethernet1/2 mip 1.1.1.4 host 3.3.3.3
set policy from untrust to trust any mip(1.1.1.3) any permit
set policy id 104
(policy:104)-> set dst-address mip(1.1.1.4)
(policy:104)-> exit
get policy id 104
```

NOTE: After executing the last CLI command in this example, look for the following output for confirmation:

```
2 destinations: “MIP(1.1.1.3)”, “MIP(1.1.1.4)”
```

Virtual IP Addresses

A virtual IP (VIP) address maps traffic received at one IP address to another address based on the destination port number in the TCP or UDP segment header. For example,

- An HTTP packet destined for 1.1.1.3:80 (that is, IP address 1.1.1.3 and port 80) might get mapped to a webserver at 10.1.1.10.
- An FTP packet destined for 1.1.1.3:21 might get mapped to an FTP server at 10.1.1.20.
- An SMTP packet destined for 1.1.1.3:25 might get mapped to a mail server at 10.1.1.30.

The destination IP addresses are the same. The destination port numbers determine the host to which the security device forwards traffic.

Figure 37: Virtual IP Address

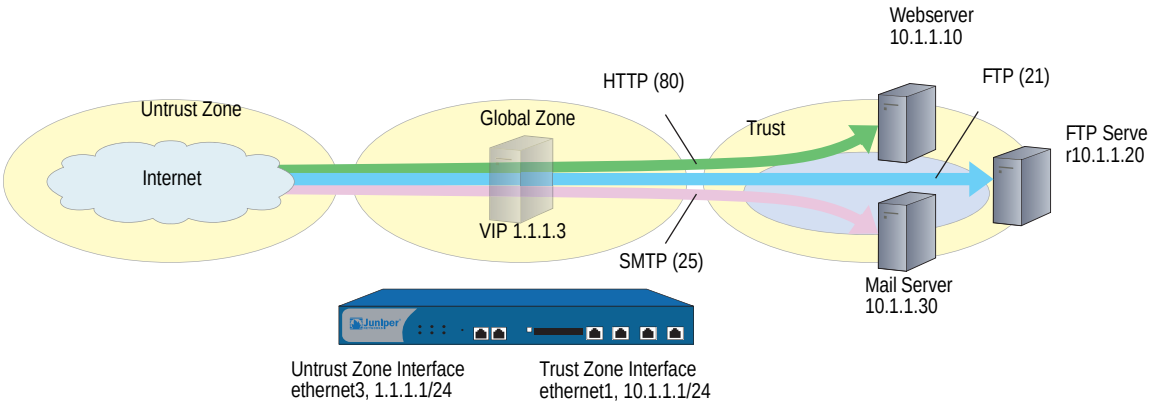


Table 2: Virtual IP Forwarding Table

Interface IP in Untrust Zone	VIP in Global Zone	Port	Forward to	Host IP in Trust Zone
1.1.1.1/24	1.1.1.3	80 (HTTP)		10.1.1.10
1.1.1.1/24	1.1.1.3	21 (FTP)		10.1.1.20
1.1.1.1/24	1.1.1.3	25 (SMTP)		10.1.1.30

The security device forwards incoming traffic destined for a VIP to the host with the address to which the VIP points. However, when a VIP host initiates outbound traffic, the security device only translates the original source IP address to another address if you have previously configured NAT on the ingress interface or NAT-src in a policy that applies to traffic originating from that host. Otherwise, the security device does not translate the source IP address on traffic originating from a VIP host.

You need the following information to define a Virtual IP:

- The IP address for the VIP must be in the same subnet as an interface in the Untrust zone or—on some security devices—can even be the same address as that interface

  On some security devices, an interface in the Untrust zone can receive its IP address dynamically via DHCP or PPPoE. If you want to use a VIP in such a situation, do either of the following using the WebUI (Network > Interfaces > Edit (for an interface in the Untrust zone) > VIP:

  - If you configure a VIP to use the same IP address as an Untrust zone interface on a device that supports multiple VIPs, the other "regular" VIPs become unusable.

  - If a regular VIP is configured, you cannot create a VIP using an Untrust zone interface until you delete the regular VIP first.

- The IP addresses for the servers that process the requests

- The type of service you want the security device to forward from the VIP to the IP address of the host

NOTE: You can only set a VIP on an interface in the Untrust zone.

Some notes about VIPs:

- You can use virtual port numbers for well-known services when running multiple server processes on a single machine. For example, if you have two FTP servers on the same machine, you can run one server on port 21 and the other on port 2121. Only those who know the virtual port number in advance and append it to the IP address in the packet header can gain access to the second FTP server.

- You can map predefined services and user-defined services.

- A single VIP can distinguish custom services with the same source and destination port numbers but different transports.

- Custom services can use any destination port number or number range from 1 to 65,535, not just from 1024 to 65,535.
- A single VIP can support custom services with multiple port entries by creating multiple service entries under that VIP—one service entry in the VIP for each port entry in the service. By default, you can use single-port services in a VIP. To be able to use multiple-port services in a VIP, you must first issue the CLI command **set vip multi-port**, and then reset the security device. (See "Example: VIP with Custom and Multiple-Port Services" on page 85.)
- The host to which the security device maps VIP traffic must be reachable from the trust-vr. If the host is in a routing domain other than that of the trust-vr, you must define a route to reach it.

VIP and the Global Zone

Setting a VIP for an interface in the Untrust zone generates an entry in the Global zone address book. The Global zone address book keeps all the VIPs of all interfaces, regardless of the zone to which the interface belongs. You can use these VIP addresses as the destination address in policies between any two zones, and as the destination address in Global policies.

Example: Configuring Virtual IP Servers

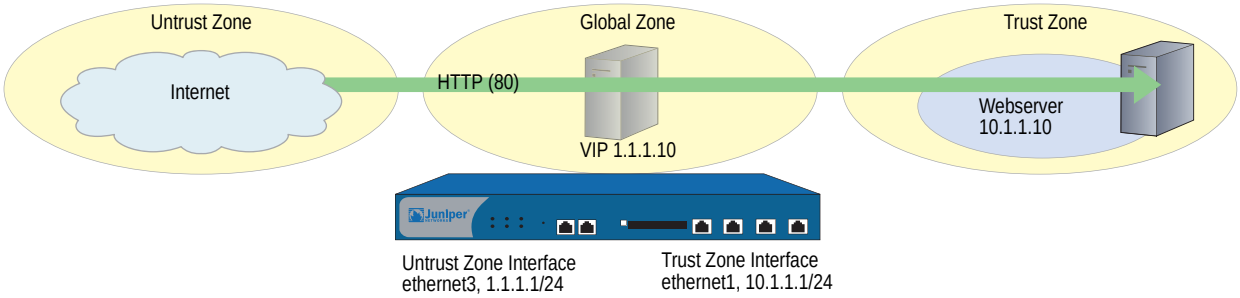
In this example, you bind interface ethernet1 to the Trust zone and assign it IP address 10.1.1.1/24. You bind interface ethernet3 to the Untrust zone and assign it IP address 1.1.1.1/24.

Then, you configure a VIP at 1.1.1.10 to forward inbound HTTP traffic to a webserver at 10.1.1.10, and you create a policy permitting traffic from the Untrust zone to reach the VIP—and consequently to the host with the address to which the VIP points—in the Trust zone.

Because the VIP is in the same subnet as the Untrust zone interface (1.1.1.0/24), you do not need to define a route for traffic from the Untrust zone to reach it. Also, no address book entry is required for the host to which a VIP forwards traffic. All security zones are in the trust-vr routing domain.

NOTE: If you want HTTP traffic from a security zone other than the Untrust zone to reach the VIP, you must set a route for 1.1.1.10 on the router in the other zone to point to an interface bound to that zone. For example, imagine that ethernet2 is bound to a user-defined zone, and you have configured a router in that zone to send traffic destined for 1.1.1.10 to ethernet2. After the router sends traffic to ethernet2, the forwarding mechanism in the security device locates the VIP on ethernet3, which maps it to 10.1.1.10, and sends it out ethernet1 to the Trust zone. This process is similar to that described in "Example: Reaching a MIP from Different Zones" on page 67. You must also set a policy permitting HTTP traffic from the source zone to the VIP in the Trust zone.

Figure 38: Virtual IP Server



WebUI

1. **Interfaces**

   Network > Interfaces > Edit (for ethernet1): Enter the following, then click **Apply**:

   Zone Name: Trust
   Static IP: (select this option when present)
   IP Address/Netmask: 10.1.1.1/24
   Select the following, then click **OK**:
   Interface Mode: NAT

   Network > Interfaces > Edit (for ethernet3): Enter the following, then click **OK**:

   Zone Name: Untrust
   Static IP: (select this option when present)
   IP Address/Netmask: 1.1.1.1/24

2. **VIP**

   Network > Interfaces > Edit (for ethernet3) > VIP: Enter the following address, then click **Add**:

   Virtual IP Address: 1.1.1.10

   Network > Interfaces > Edit (for ethernet3) > VIP > New VIP Service: Enter the following, then click **OK**:

   Virtual IP: 1.1.1.10
   Virtual Port: 80
   Map to Service: HTTP (80)
   Map to IP: 10.1.1.10

3. **Policy**

   Policies > (From: Untrust, To: Trust) New: Enter the following, then click **OK**:

   Source Address:
   Address Book Entry: (select), ANY
   Destination Address:
   Address Book Entry: (select), VIP(1.1.1.10)
   Service: HTTP
   Action: Permit

CLI

1. **Interfaces**
   set interface ethernet1 zone trust
   set interface ethernet1 ip 10.1.1.1/24
   set interface ethernet1 nat
   set interface ethernet3 zone untrust
   set interface ethernet2 ip 1.1.1.1/24
2. **VIP**
   set interface ethernet3 vip 1.1.1.10 80 http 10.1.1.10
3. **Policy**
   set policy from untrust to trust any vip(1.1.1.10) http permit
   save

Example: Editing a VIP Configuration

In this example, you modify the Virtual IP server configuration you created in the previous example. To restrict access to the webserver, you change the virtual port number for HTTP traffic from 80 (the default) to 2211. Now, only those that know to use port number 2211 when connecting to the webserver can access it.

WebUI

Network > Interfaces > Edit (for ethernet3) > VIP > Edit (in the VIP Services Configure section for 1.1.1.10): Enter the following, then click **OK**:

Virtual Port: 2211

CLI

unset interface ethernet3 vip 1.1.1.10 port 80
set interface ethernet3 vip 1.1.1.10 2211 http 10.1.1.10
save

Example: Removing a VIP Configuration

In this example, you delete the VIP configuration that you previously created and modified. Before you can remove a VIP, you must first remove any existing policies associated with it. The ID number for the policy that you created in “Example: Configuring Virtual IP Servers” on page 82 is 5.

WebUI

Policies > (From: Untrust, To: Trust) > Go: Click **Remove** for policy ID 5.

Network > Interfaces > Edit (for ethernet3) > VIP: Click **Remove** in the VIP Configure section for 1.1.1.10.

CLI

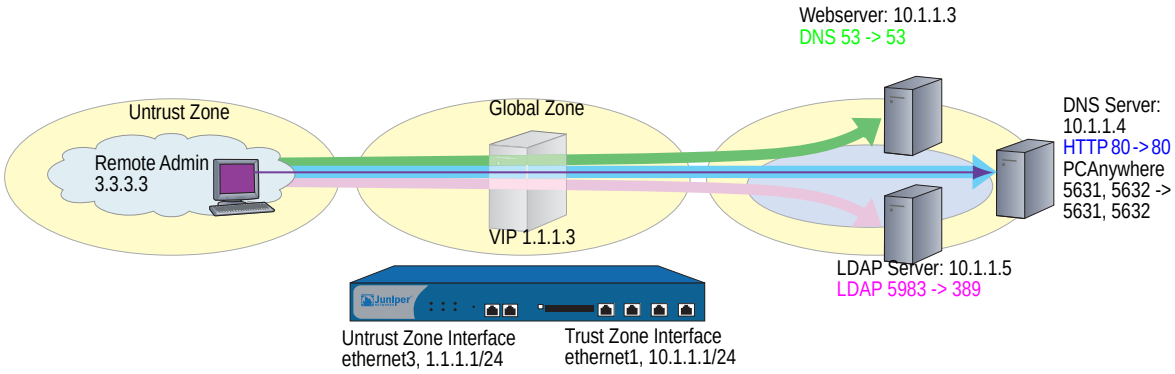
unset policy id 5
unset interface ethernet3 vip 1.1.1.10
save

Example: VIP with Custom and Multiple-Port Services

In the following example, you configure a VIP at 1.1.1.3 to route the following services to the following internal addresses:

Service	Transport	Virtual Port Number	Actual Port Number	Host IP Address
DNS	TCP, UDP	53	53	10.1.1.3
HTTP	TCP	80	80	10.1.1.4
PCAnywhere	TCP, UDP	5631, 5632	5631, 5632	10.1.1.4
LDAP	TCP, UDP	5983	389	10.1.1.5

Figure 39: VIP with Custom and Multiple-Port Services



The VIP routes DNS lookups to the DNS server at 10.1.1.3, HTTP traffic to the webserver at 10.1.1.4, and authentication checks to the database on the LDAP server at 10.1.1.5. For HTTP, DNS, and PCAnywhere, the virtual port numbers remain the same as the actual port numbers. For LDAP, a virtual port number (5983) is used to add an extra level of security to the LDAP authentication traffic.

For managing the HTTP server remotely, you define a custom service and name it PCAnywhere. PCAnywhere is a multiple-port service that sends and listens for data on TCP port 5631 and status checks on UDP port 5632.

You also enter the address of the Remote Admin at 3.3.3.3 in the Untrust zone address book, and configure policies from the Untrust zone to the Trust zone for all the traffic that you want to use the VIPs. All security zones are in the trust-vr routing domain.

WebUI

1. **Interfaces**
   Network > Interfaces > Edit (for ethernet1): Enter the following, then click **Apply**:

   Zone Name: Trust
   Static IP: (select this option when present)
   IP Address/Netmask: 10.1.1.1/24

   Select the following, then click **OK**:

   Interface Mode: NAT

   Network > Interfaces > Edit (for ethernet3): Enter the following, then click **OK**:

   Zone Name: Untrust
   Static IP: (select this option when present)
   IP Address/Netmask: 1.1.1.1/24

2. **Address**
   Objects > Addresses > List > New: Enter the following, then click **OK**:

   Address Name: Remote Admin
   IP Address/Domain Name:
   IP/Netmask: (select), 3.3.3.3/32
   Zone: Untrust

3. **Custom Service**
   Object > Services > Custom > New: Enter the following, then click **OK**:

   Service Name: PCAnywhere
   No 1:
   Transport protocol: TCP
   Source Port Low: 0
   Source Port High: 65535
   Destination Port Low: 5631
   Destination Port High: 5631
   No 2:
   Transport protocol: UDP
   Source Port Low: 0
   Source Port High: 65535
   Destination Port Low: 5632
   Destination Port High: 5632

4. **VIP Address and Services**

NOTE: To enable the VIP to support multiple-port services, you must use enter the CLI command **set vip multi-port**, save the configuration, and then reboot the device.

Network > Interfaces > Edit (for ethernet3) > VIP: click here to configure: Type **1.1.1.3** in the Virtual IP Address field, then click **Add**.

> New VIP Service: Enter the following, then click **OK**:

Virtual IP: 1.1.1.3
Virtual Port: 53
Map to Service: DNS
Map to IP: 10.1.1.3

> New VIP Service: Enter the following, then click **OK**:

Virtual IP: 1.1.1.3
Virtual Port: 80
Map to Service: HTTP
Map to IP: 10.1.1.4

> New VIP Service: Enter the following, then click **OK**:

Virtual IP: 1.1.1.3
Virtual Port: 5631
Map to Service: PCAnywhere
Map to IP: 10.1.1.4

NOTE: For multiple-port services, enter the lowest port number of the service as the virtual port number.

> New VIP Service: Enter the following, then click **OK**:

Virtual IP: 1.1.1.3
Virtual Port: 5983
Map to Service: LDAP
Map to IP: 10.1.1.5

NOTE: Using nonstandard port numbers adds another layer of security, preventing common attacks that check for services at standard port numbers.

---

5. Policies

Policies > (From: Untrust, To: Trust) New: Enter the following, then click **OK**:

Source Address:
    Address Book Entry: (select), Any
Destination Address:
    Address Book Entry: (select), VIP(1.1.1.3)
Service: DNS
Action: Permit

Policies > (From: Untrust, To: Trust) New: Enter the following, then click **OK**:

Source Address:
    Address Book Entry: (select), Any
Destination Address:
    Address Book Entry: (select), VIP(1.1.1.3)
Service: HTTP
Action: Permit

Policies > (From: Untrust, To: Trust) New: Enter the following, then click **OK**:

Source Address:
Address Book Entry: (select), Any
Destination Address:
Address Book Entry: (select), VIP(1.1.1.3)
Service: LDAP
Action: Permit

Policies > (From: Untrust, To: Trust) New: Enter the following, then click **OK**:

Source Address:
Address Book Entry: (select), Remote Admin
Destination Address:
Address Book Entry: (select), VIP(1.1.1.3)
Service: PCAnywhere
Action: Permit

CLI

1. **Interfaces**
   set interface ethernet1 zone trust
   set interface ethernet1 ip 10.1.1.1/24
   set interface ethernet1 nat
   set interface ethernet3 zone untrust
   set interface ethernet3 ip 1.1.1.1/24

2. **Address**
   set address untrust "Remote Admin" 3.3.3.3/32

3. **Custom Service**
   set service pcanywhere protocol udp src-port 0-65535 dst-port 5631-5631
   set service pcanywhere + tcp src-port 0-65535 dst-port 5632-5632

4. **VIP Address and Services**
   set vip multi-port
   save
   reset
   System reset, are you sure? y/[n] y
   set interface ethernet3 vip 1.1.1.3 53 dns 10.1.1.3
   set interface ethernet3 vip 1.1.1.3 + 80 http 10.1.1.4
   set interface ethernet3 vip 1.1.1.3 + 5631 pcanywhere 10.1.1.4
   set interface ethernet3 vip 1.1.1.3 + 5983 ldap 10.1.1.5

NOTE: For multiple-port services, enter the lowest port number of the service as the virtual port number.

---

5. **Policies**
   set policy from untrust to trust any vip(1.1.1.3) dns permit
   set policy from untrust to trust any vip(1.1.1.3) http permit
   set policy from untrust to trust any vip(1.1.1.3) ldap permit
   set policy from untrust to trust "Remote Admin" vip(1.1.1.3) pcanywhere permit
   save

Index

P

V

Z