CHAPTER 23

Network Address Translation

Network Address Translation (NAT) is a robust form of address translation that extends addressing capabilities by providing both static address translations and dynamic address translations. NAT allows a host that does not have a valid registered IP address to communicate with other hosts through the Internet. The hosts may be using private addresses or addresses assigned to another organization; in either case, NAT allows these addresses that are not Internet-ready to continue to be used but still allow communication with hosts across the Internet.

Network Address Translation Wizards

You can use a wizard to guide you in creating a Network Address Translation (NAT) rule. Choose one of the following wizards:

- Basic NAT

  Choose the Basic NAT wizard if you want to connect your network to the Internet (or the outside), and your network has hosts but no servers. Look at the sample diagram that appears to the right when you choose **Basic NAT**. If your network is made up only of PCs that require access to the Internet, choose **Basic NAT** and click the **Launch** button.

- Advanced NAT

  Choose the Advanced NAT wizard if you want to connect your network to the Internet (or the outside), and your network has hosts and servers, *and* the servers must be accessible to outside hosts (hosts on the Internet). Look at the sample diagram that appears to the right when you choose **Advanced NAT**.

If your network has e-mail servers, web servers, or other types of servers and you want them to accept connections from the Internet, choose **Advanced NAT** and click the **Launch** button.

Note If you do not want your servers to accept connections from the Internet, you can use the Basic NAT wizard.

Basic NAT Wizard: Welcome

The Basic NAT welcome window shows how the wizard will guide you through configuring NAT for connecting one or more LANs, but no servers, to the Internet.

Basic NAT Wizard: Connection

Choose an Interface

From the drop-down menu, choose the interface that connects to the Internet. This is the router WAN interface.

Choose Networks

The list of available networks shows the networks connected to your router. Choose which networks will share the WAN interface in the NAT configuration you set up. To choose a network, check its check box in the list of available networks.

Note Do not choose a network connected to the WAN interface set up in this NAT configuration. Remove that network from the NAT configuration by unchecking its check box.

The list shows the following information for each network:

- IP address range allocated to the network
- Network LAN interface
- Comments entered about the network

To remove a network from the NAT configuration, uncheck its check box.

Note If Cisco SDM detects a conflict between the NAT configuration and an existing VPN configuration for the WAN interface, it will inform you with a dialog box after you click **Next**.

Summary

This window shows you the NAT configuration you created, and allows you to save the configuration. The summary will appear similar to the following:

```
Interface that is connected to the Internet or to your Internet
service provider:
    FastEthernet0/0

IP address ranges that share the Internet connection:
    108.1.1.0 to 108.1.1.255
    87.1.1.0 to 87.1.1.255
    12.1.1.0 to 12.1.1.255
    10.20.20.0 to 10.20.20.255
```

If you used the Advanced NAT wizard, you may also see additional information similar to the following:

```
NAT rules for servers:
    Translate 10.10.10.19 TCP port 6080 to IP address of interface
FastEthernet0/0 TCP port 80
    Translate 10.10.10.20 TCP port 25 to 194.23.8.1 TCP port 25
```

Advanced NAT Wizard: Welcome

The Advanced NAT welcome window shows how the wizard will guide you through configuring NAT for connecting your LANs and servers to the Internet.

Advanced NAT Wizard: Connection

Choose an Interface

From the drop-down menu, choose the interface that connects to the Internet. This is the router WAN interface.

Additional Public IP Addresses

Click **Add** to enter public IP addresses that you own. You will be able to assign these IP address to servers on your network that you want to make available to the Internet.

To delete an IP address from the list, choose the IP address and click **Delete**.

Add IP Address

Enter a public IP address that you own. You will be able to assign this IP address to a server on your network that you want to make available to the Internet.

Advanced NAT Wizard: Networks

Choose Networks

The list of available networks shows the networks connected to your router. Choose which networks will share the WAN interface in the NAT configuration you set up. To choose a network, check its check box in the list of available networks.

Note Do not choose a network connected to the WAN interface set up in this NAT configuration. Remove that network from the NAT configuration by unchecking its check box.

The list shows the following information for each network:

- IP address range allocated to the network
- Network LAN interface

- Comments entered about the network

To remove a network from the NAT configuration, uncheck its check box.

To add a network not directly connected to your router to the list, click **Add Networks**.

Note If Cisco SDM does not allow you to place a check mark next to a network for which you want to configure a NAT rule, the interface associated with the network has already been designated as a NAT interface. This status will be indicated by the word *Designated* in the Comments column. If you want to configure a NAT rule for that interface, exit the wizard, click the **Edit NAT** tab, click **Designate NAT Interfaces**, and uncheck the interface. Then return to the wizard and configure the NAT rule.

Add Network

You can add a network to the list of networks made available in the Advanced NAT wizard. You must have the network IP address and network mask. For more information, see IP Addresses and Subnet Masks.

IP Address

Enter the network IP address.

Subnet Mask

Enter the network subnet mask in this field, or choose the number of subnet bits from the scrolling field on the right. The subnet mask tells the router which bits of the IP address designate the network address and which bits designate the host address.

Advanced NAT Wizard: Server Public IP Addresses

This window allows you to translate public IP addresses to the private IP addresses of internal servers that you want to make accessible from the Internet.

The list shows the private IP addresses and ports (if used) and the public IP addresses and ports (if used) to which they are translated.

To reorder the list based on the private IP addresses, click the column head **Private IP Address**. To reorder the list based on the public IP addresses, click the column head **Public IP Address**.

Add Button

To add a translation rule for a server, click **Add**.

Edit Button

To edit a translation rule for a server, choose it in the list and click **Edit**.

Delete Button

To delete a translation rule, choose it in the list and click **Delete**.

Add or Edit Address Translation Rule

In this window you can enter or edit the IP address translation information for a server.

Private IP Address

Enter the IP address that the server uses on your internal network. This is an IP address that cannot be used externally on the Internet.

Public IP Address

From the drop-down menu, choose the public IP address to which the server's private IP address will be translated. The IP addresses that appear in the drop-down menu include the IP address of the router WAN interface and any public IP addresses you own that were entered in the connections window (see Advanced NAT Wizard: Connection).

Type of Server

Choose one of the following server types from the drop-down menu:

- Web server

  An HTTP host serving HTML and other WWW-oriented pages.

- E-mail server

  An SMTP server for sending Internet mail.

- Other

  A server which is not a web or e-mail server, but which requires port translation to provide service. This choice activates the Translated Port field and the Protocol drop-down menu.

If you do not choose a server type, all traffic intended for the public IP address you choose for the server will be routed to that address, and no port translation will be done.

Original Port

Enter the port number used by the server to accept service requests from the internal network.

Translated Port

Enter the port number used by the server to accept service requests from the Internet.

Protocol

Choose **TCP** or **UDP** for the protocol used by the server with the original and translated ports.

Advanced NAT Wizard: ACL Conflict

If this window appears, Cisco SDM has detected a conflict between the NAT configuration and an existing ACL on the WAN interface. This ACL may be part of a firewall configuration, a VPN configuration, or the configuration of another feature.

Choose to modify the NAT configuration to remove the conflict, or choose to *not* modify the NAT configuration. If you choose to *not* modify the NAT configuration, the conflict may cause other features you have configured to stop working.

View Details

Click the **View Details** button to see the proposed modifications to the NAT configuration to resolve the conflict. This button is not displayed with all feature conflicts.

Details

This window lists the changes Cisco SDM will make to the NAT configuration to resolve conflicts between NAT and another feature configured on the same interface.

Network Address Translation Rules

The Network Address Translation Rules window lets you view NAT rules, view address pools, and set translation timeouts. From this window you can also designate interfaces as inside or outside interfaces.

For more information on NAT, follow the link More About NAT.

Designate NAT Interfaces

Click to designate interfaces as inside or outside. NAT uses the inside/outside designations as reference points when interpreting translation rules. Inside interfaces are those interfaces connected to the private networks that the router serves. Outside interfaces connect to the WAN or to the Internet. The designated inside and outside interfaces are listed above the NAT rule list.

Address Pools

Click this button to configure or edit address pools. Address pools are used with dynamic address translation. The router can dynamically assign addresses from the pool as they are needed. When an address is no longer needed, it is returned to the pool.

Translation Timeouts

When dynamic NAT is configured, translation entries have a timeout period after which they expire and are purged from the translation table. Click this button to configure the timeout values for NAT translation entries and other values.

Network Address Translation Rules

This area shows the designated inside and outside interfaces and the NAT rules that have been configured.

Inside Interfaces

The inside interfaces are the interfaces that connect to the private networks the router serves. NAT uses the inside designation when interpreting a NAT translation rule. You can designate interfaces as inside by clicking **Designate NAT interfaces**.

Outside Interfaces

The outside interfaces are the router interfaces that connect to the WAN or the Internet. NAT uses the outside designation when interpreting a NAT translation rule. You can designate interfaces as outside by clicking **Designate NAT interfaces**.

Original Address

This is the private address or set of addresses that is used on the LAN.

Translated Address

This is the legal address or range of addresses that is used on the Internet or the external network.

Rule Type

Rules are either static address translation rules or dynamic address translation rules.

Static address translation allows hosts with private addresses to access the Internet and to be publicly accessible from the Internet. It statically maps one private IP address to one public or global address. If you wanted to provide static translation to ten private addresses, you would create a separate static rule for each address.

Dynamic address translation. There are two methods of dynamic addressing using NAT. One method maps multiple private addresses to a single public address and the port numbers of host sessions to determine which host to route returning traffic to. The second method uses named address pools. These address pools contain public addresses. When a host with a private address needs to establish communication outside the LAN, it is given a public address from this pool. When the host no longer needs it, the address is returned to the pool.

Clone selected entry on Add

If you want to use an existing rule as the basis for a new rule that you want to create, choose the rule and check this check box. When you click **Add**, the addresses in the rule you chose appear in the Add Address Translation Rule window. You can edit these addresses to obtain the ones you need for the new rule instead of entering the entire address into each field.

What Do You Want to Do?

If you want to:	Do this:
Designate the inside and outside interfaces. You must designate at least one inside interface and one outside interface in order for the router to perform NAT.	Click **Designate NAT interfaces**, and designate interfaces as inside or outside in the NAT Interface Setting window. Interfaces can also be designated as inside or outside interfaces in the Interfaces and Connections window.
Add, edit, or delete an address pool. Dynamic rules can use address pools to assign addresses to devices as they are needed.	Click **Address Pools**, and configure address pool information in the dialog box.
Set the translation timeout.	Click **Translation Timeouts**, and set the timeout in the Translation Timeouts window.
Add a NAT rule.	Click **Add**, and create the NAT rule in the Add Address Translation Rule window. If you want to use an existing NAT rule as a template for the new rule, choose the rule, click **Clone selected entry on Add**, and then click **Add**.

If you want to:	Do this:
Edit a NAT rule.	Choose the NAT rule that you want to edit, click **Edit**, and edit the rule in the Edit Address Translation Rule window.
Delete a NAT rule.	Choose the NAT rule that you want to delete, and click **Delete**. You must confirm deletion of the rule in the Warning box displayed.
View or edit route maps. If virtual private network (VPN) connections are configured on the router, the local IP addresses in the VPN must be protected from NAT translations. When both a VPN and NAT are configured, Cisco Router and Security Device Manager (Cisco SDM) creates route maps to protect IP addresses in a VPN from being translated. Additionally, route maps can be configured using the command-line interface (CLI). You can view configured route maps and edit the access rule they use.	Click **View Route MAP**.
Find out how to perform related configuration tasks.	See one of the following procedures: • How Do I Configure NAT Passthrough for a VPN? • How Do I Configure NAT on an Unsupported Interface? • How Do I Configure NAT Passthrough for a Firewall?

Note Many conditions cause previously configured NAT rules to appear as read-only in the Network Address Translation Rules list. Read-only NAT rules are not editable. For more information, see the help topic Reasons that Cisco SDM Cannot Edit a NAT Rule.

Designate NAT Interfaces

Use this window to designate the inside and outside interfaces that you want to use in NAT translations. NAT uses the inside and outside designations when interpreting translation rules, because translations are performed from inside to outside, or from outside to inside.

Once designated, these interfaces are used in all NAT translation rules. The designated interfaces appear above the Translation Rules list in the main NAT window.

Interface

All router interfaces are listed in this column.

Inside (trusted)

Check to designate an interface as an inside interface. Inside interfaces typically connect to a LAN that the router serves.

Outside (untrusted)

Check to designate an interface as an outside interface. Outside interfaces typically connect to your organization's WAN or to the Internet.

Translation Timeout Settings

When you configure dynamic NAT translation rules, translation entries have a timeout period after which they expire and are purged from the translation table. Set the timeout values for various translations in this window.

DNS Timeout

Enter the number of seconds after which connections to DNS servers time out.

ICMP Timeout

Enter the number of seconds after which Internet Control Message Protocol (ICMP) flows time out. The default is 60 seconds.

PPTP Timeout

Enter the number of seconds after which NAT Point-to-Point Tunneling Protocol (PPTP) flows time out. The default is 86400 seconds (24 hours).

Dynamic NAT Timeout

Enter the maximum number of seconds that dynamic NAT translations should live.

Max Number of NAT Entries

Enter the maximum number of NAT entries in the translation table.

UDP flow timeouts

Enter the number of seconds that translations for User Datagram Protocol (UDP) flows should live. The default is 300 seconds (5 minutes).

TCP flow timeouts

Enter the number of seconds that translations for Transmission Control Protocol (TCP) flows should live. The default is 86400 seconds (24 hours).

Reset Button

Clicking this button resets translation and timeout parameters to their default values.

Edit Route Map

When VPNs and NAT are both configured on a router, packets that would normally meet the criteria for an IPSec rule will not do so if NAT translates their IP addresses. In this case, NAT translation will cause packets to be sent without being encrypted. Cisco SDM may create route maps to prevent NAT from translating IP addresses that you want to be preserved.

Although Cisco SDM only creates route maps to limit the action of NAT, route maps can be used for other purposes as well. If route maps have been created using the CLI, they will be visible in this window as well.

Name

The name of this route map.

Route map entries

This box lists the route map entries.

Name

The name of the route map entry.

Seq No.

The sequence number of the route map.

Action

Route maps created by Cisco SDM are configured with the **permit** keyword. If this field contains the value **deny**, the route map was created using the CLI.

Access Lists

The access lists that specify the traffic to which this route map applies.

To Edit a Route Map Entry

Choose the entry, click **Edit**, and edit the entry in the Edit Route Map Entry window.

Edit Route Map Entry

Use this window to edit the access list specified in a route map entry.

Name

A read-only field containing the name of the route map entry.

Seq No.

A read-only field containing the sequence number for the route map. When Cisco SDM creates a route map, it automatically assigns it a sequence number.

Action

Either **permit** or **deny**. Route maps created by Cisco SDM are configured with the **permit** keyword. If this field contains the value **deny**, the route map was created using the CLI.

Access Lists

This area shows the access lists associated with this entry. The route map uses these access lists to determine which traffic to protect from NAT translation.

To Edit an Access List in a Route Map Entry

Choose the access list, and click **Edit**. Then edit the access list in the windows displayed.

Address Pools

The Address Pools window shows the configured address pools that can be used in dynamic NAT translation.

Pool Name

This field contains the name of the address pool. Use this name to refer to the pool when configuring a dynamic NAT rule.

Address

This field contains the IP address range in the pool. Devices whose IP addresses match the access rule specified in the Add Address Translation Rule window will be given private IP addresses from this pool.

What Do You Want to Do?

If you want to:	Do this:
Add an address pool to the router configuration.	Click **Add**, and configure the pool in the Add Address Pool window. If you want to use an existing pool as a template for the new pool, choose the existing pool, check **Clone selected entry on Add**, and click **Add**.
Edit an existing address pool.	Choose the pool entry, click **Edit**, and edit the pool configuration in the Edit Address Pool window.
Delete an address pool.	Choose the pool entry, click **Delete**, and confirm deletion in the Warning box displayed.

Note If Cisco SDM detects a previously configured NAT address pool that uses the "type" keyword, that address pool will be read-only and cannot be edited.

Add or Edit Address Pool

Use this window to specify an address pool for dynamic address translation, an address for Port Address Translation (PAT), or a TCP load-balancing rotary pool.

Pool Name

Enter the name of the address pool.

Port Address Translation (PAT)

There may be times when most of the addresses in the pool have been assigned, and the IP address pool is nearly depleted. When this occurs, PAT can be used with a single IP address to satisfy additional requests for IP addresses. Check this check box if you want the router to use PAT when the address pool is close to depletion.

IP Address

Enter the lowest-numbered IP address in the range in the left field; enter the highest-numbered IP address in the range in the right field. For more information, see Available Interface Configurations.

Network Mask

Enter the subnet mask or the number of network bits that specify how many bits in the IP addresses are network bits.

Add or Edit Static Address Translation Rule: Inside to Outside

Use this help topic when you have chosen From Inside to Outside in the Add or the Edit Static Address Translation Rule window.

Use this window to add or edit a static address translation rule. If you are editing a rule, the rule type (static or dynamic) and the direction are disabled. If you need to change these settings, delete the rule, and re-create it using the settings you want.

Two types of static address translations use NAT: simple static and extended static.

Note If you create a NAT rule that would translate addresses of devices that are part of a VPN, Cisco SDM will prompt you to allow it to create a route map that protects those addresses from being translated by NAT. If NAT is allowed to translate addresses of devices on a VPN, their translated addresses will not match the IPSec rule used in the IPSec policy, and traffic will be sent unencrypted. You can view route maps created by Cisco SDM or created using the CLI by clicking the **View Route Maps** button in the NAT window.

Direction

This help topic describes how to use the Add Address Translation Rule fields when **From inside to outside** is chosen.

From inside to outside

Choose this option if you want to translate private addresses on the LAN to legal addresses on the Internet or on your organization's intranet. You may want to choose this option if you use private addresses on your LAN that are not globally unique on the Internet.

Translate from Interface

This area shows the interfaces from which packets needing address translation come in to the router. It provides fields for you to specify the IP address of a single host, or a network address and subnet mask that represent the hosts on a network.

Inside Interface(s)

If you chose **From inside to outside** for Direction, this area lists the designated inside interfaces.

Note If this area contains no interface names, close the Add Address Translation Rule window, click **Designate NAT interfaces** in the NAT window, and designate the router interfaces as inside or outside. Then return to this window and configure the NAT rule.

IP Address

Do one of the following:

- If you want to create a one-to-one static mapping between the address of a single host and a translated address, known as the *inside global address*, enter the IP address for that host. Do not enter a subnet mask in the Network Mask field.
- If you want to create *n*-to-*n* mappings between the private addresses in a subnet to corresponding inside global addresses, enter any valid address from the subnet whose addresses you want translated, and enter a network mask in the next field.

Network Mask

If you want Cisco SDM to translate the addresses of a subnet, enter the mask for that subnet. Cisco SDM determines the network and subnet number and the set of addresses needing translation from the IP address and mask that you supply.

Translate to Interface

This area shows the interfaces from which packets with translated addresses exit the router. It also provides fields for specifying the translated address and other information.

Outside Interface(s)

If you chose **From inside to outside** for Direction, this area contains the designated outside interfaces.

Type

- Choose **IP Address** if you want the address to be translated to the address defined in the IP Address field.
- Choose **Interface** if you want the *Translate from* address to use the address of an interface on the router. The *Translate from* address will be translated to the IP address assigned to the interface that you specify in the Interface field.

Interface

This field is enabled if Interface is chosen in the Type field. This field lists the interfaces on the router. Choose the interface whose IP address you want the local inside address translated to.

Note If **Interface** is chosen in the Type field, only translations that redirect TCP/IP ports are supported. The Redirect Port check box is automatically checked and cannot be unchecked.

IP Address

This field is enabled if you chose **IP Address** in the Type field. Do one of the following:

- If you are creating a one-to-one mapping between a single inside local address and a single inside global address, enter the inside global address in this field.
- If you are mapping the inside local addresses of a subnet to the corresponding inside global addresses, enter any IP address that you want to use in the translation in this field. The network mask entered in the *Translate from* Interface area will be used to calculate the remaining inside global addresses.

Note If you do not enter a network mask in the Translate from Interface area, Cisco SDM will perform only one translation.

Redirect Port

Check this check box if you want to include port information for the inside device in the translation. This enables you to use the same public IP address for multiple devices, as long as the port specified for each device is different. You must create an entry for each port mapping for this "Translated to" address.

Click **TCP** if this is a TCP port number; click **UDP** if it is a UDP port number.

In the Original Port field, enter the port number on the inside device.

In the Translated Port field, enter the port number that the router is to use for this translation.

Configuration Scenarios

Click Static Address Translation Scenarios for examples that illustrate how the fields in this window are used.

Add or Edit Static Address Translation Rule: Outside to Inside

Use this help topic when you have chosen From Outside to Inside in the Add or the Edit Static Address Translation Rule window.

Use this window to add or edit a static address translation rule. If you are editing a rule, then the rule type (static or dynamic) and the direction are disabled. If you need to change these settings, delete the rule, and re-create it using the settings you want.

Two types of static address translations use NAT: simple static and extended static.

Note If you create a NAT rule that would translate addresses of devices that are part of a VPN, Cisco SDM will prompt you to allow it to create a route map that protects those addresses from being translated by NAT. If NAT is allowed to translate

addresses of devices on a VPN, their translated addresses will not match the IPSec rule used in the IPSec policy, and traffic will be sent unencrypted. You can view route maps created by Cisco SDM or created using the CLI by clicking the **View Route Maps** button in the NAT window.

Direction

Choose the traffic direction for this rule.

From outside to inside

Choose this option if you want to translate incoming addresses to addresses that will be valid on your LAN. You may want to do this when you are merging networks and must make one set of incoming addresses compatible with an existing set on the LAN served by the router.

This help topic describes how the remaining fields are used when From outside to inside is chosen.

Translate from Interface

This area shows the interfaces from which packets needing address translation come in to the router. It provides fields for you to specify the IP address of a single host, or a network address and subnet mask that represent the hosts on a network.

Outside Interfaces

If you choose **From outside to inside**, this area contains the designated outside interfaces.

Note If this area contains no interface names, close the Add Address Translation Rule window, click **Designate NAT interfaces** in the NAT window, and designate the router interfaces as inside or outside. Then return to this window and configure the NAT rule.

IP Address

Do one of the following:

- If you want to create a one-to-one static mapping between the outside global address of a single remote host and a translated address, known as the *outside local address*, enter the IP address for the remote host.

- If you want to create *n*-to-*n* mappings between the addresses in a remote subnet to corresponding outside local addresses, enter any valid address from the subnet whose addresses you want translated, and enter a network mask in the next field.

Network Mask

If you want Cisco SDM to translate the addresses in a remote subnet, enter the mask for that subnet. Cisco SDM determines the network and subnet number and the set of addresses needing translation from the IP address and mask that you supply.

Translate to Interface

This area shows the interfaces from which packets with translated addresses exit the router. It also provides fields for specifying the translated address and other information.

Inside Interface(s)

If you choose **From outside to inside**, this area contains the designated inside interfaces.

IP Address

Do one of the following:

- If you are creating a one-to-one mapping between a single outside global address and a single outside local address, enter the outside local address in this field.
- If you are mapping the outside global addresses of a remote subnet to the corresponding outside local addresses, enter any IP address that you want to use in the translation in this field. The network mask entered in the Translate from Interface area will be used to calculate the remaining outside local addresses.

Note If you do not enter a network mask in the Translate from Interface area, Cisco SDM will perform only one translation.

Redirect Port

Check this check box if you want to include port information for the outside device in the translation. This enables you to use extended static translation and to use the same public IP address for multiple devices, as long as the port specified for each device is different.

Click **TCP** if this is a TCP port number; click **UDP** if it is a UDP port number.

In the Original Port field, enter the port number on the outside device.

In the Translated Port field, enter the port number that the router is to use for this translation.

Configuration Scenarios

Click Static Address Translation Scenarios for examples that illustrate how the fields in this window are used.

Add or Edit Dynamic Address Translation Rule: Inside to Outside

Use this help topic when you have chosen From Inside to Outside in the Add or the Edit Dynamic Address Translation Rule window.

Add or edit an address translation rule in this window. If you are editing a rule, the rule type (static or dynamic) and the direction are disabled. If you need to change these settings, delete the rule, and re-create it using the settings you want.

A dynamic address translation rule dynamically maps hosts to addresses, using addresses included in a pool of addresses that are globally unique in the destination network. The pool is defined by specifying a range of addresses and giving the range a unique name. The configured router uses the available addresses in the pool (those not used for static translations or for its own WAN IP address) for connections to the Internet or other outside network. When an address is no longer in use, it is returned to the address pool to be dynamically assigned to another device later.

Note If you create a NAT rule that would translate addresses of devices that are part of a VPN, Cisco SDM will prompt you to allow it to create a route map that protects those addresses from being translated by NAT. If NAT is allowed to translate addresses of devices on a VPN, their translated addresses will not match the IPSec rule used in the IPSec policy, and traffic will be sent unencrypted.

Direction

Choose the traffic direction for this rule.

From inside to outside

Choose this option if you want to translate private addresses on the LAN to legal (globally unique) addresses on the Internet or on your organization's intranet.

This help topic describes how the remaining fields are used when From inside to outside is chosen.

Translate from Interface

This area shows the interfaces from which packets needing address translation come in to the router. It provides fields for specifying the IP address of a single host, or a network address and subnet mask that represent the hosts on a network.

Inside Interface(s)

If you chose **From inside to outside** for Direction, this area contains the designated inside interfaces.

Note If this area contains no interface names, close the Add Address Translation Rule window, click **Designate NAT interfaces** in the NAT window, and designate the router interfaces as inside or outside. Then return to this window and configure the NAT rule.

Access Rule

Dynamic NAT translation rules use access rules to specify the addresses that need translation. If you choose **From inside to outside**, these are the inside local addresses. Enter the name or number of the access rule that defines the addresses

you want to translate. If you do not know the name or number, you can click the **...** button and choose an existing access rule, or you can create a new access rule to use.

Translate to Interface

This area shows the interfaces from which packets with translated addresses exit the router. It also provides fields for specifying the translated address.

Outside Interface(s)

If you chose **From inside to outside** for Direction, this area contains the designated outside interfaces.

Type

Choose **Interface** if you want the *Translate from* addresses to use the address of an interface on the router. They will be translated to the address that you specify in the Interface field, and PAT will be used to distinguish each host on the network. Choose **Address Pool** if you want the addresses to be translated to addresses defined in a configured address pool.

Interface

If you choose **Interface** in the Type field, this field lists the interfaces on the router. Choose the interface whose IP address you want the local inside addresses translated to. PAT will be used to distinguish each host on the network.

Address Pool

If you choose **Address Pool** in the Type field, you can enter the name of a configured address pool in this field, or you can click **Address Pool** to choose or create an address pool.

Configuration Scenarios

Click Dynamic Address Translation Scenarios for examples that illustrate how the fields in this window are used.

Add or Edit Dynamic Address Translation Rule: Outside to Inside

Use this help topic when you have chosen From Outside to Inside in the Add or the Edit Dynamic Address Translation Rule window.

Add or edit an address translation rule in this window. If you are editing a rule, the rule type (static or dynamic) and the direction are disabled. If you need to change these settings, delete the rule, and re-create it using the settings you want.

A dynamic address translation rule dynamically maps hosts to addresses, using addresses included in a pool of addresses that are globally unique in the destination network. The pool is defined by specifying a range of addresses and giving the range a unique name. The configured router uses the available addresses in the pool (those not used for static translations or for its own WAN IP address) for connections to the Internet or other outside network. When an address is no longer in use, it is returned to the address pool to be dynamically assigned to another device later.

Note If you create a NAT rule that would translate addresses of devices that are part of a VPN, Cisco SDM will prompt you to allow it to create a route map that protects those addresses from being translated by NAT. If NAT is allowed to translate addresses of devices on a VPN, their translated addresses will not match the IPSec rule used in the IPSec policy, and traffic will be sent unencrypted.

Direction

Choose the traffic direction for this rule.

From outside to inside

Choose this option if you want to translate incoming addresses to addresses that will be valid on your LAN. You may want to do this when you are merging networks and must make one set of incoming addresses compatible with an existing set on the LAN served by the router.

This help topic describes how the remaining fields are used when From outside to inside is chosen.

Translate from Interface

This area shows the interfaces from which packets needing address translation come in to the router. It provides fields for specifying the IP address of a single host, or a network address and subnet mask that represent the hosts on a network.

Outside Interfaces

If you chose **From outside to inside**, this area contains the designated outside interfaces.

Note If this area contains no interface names, close the Add Address Translation Rule window, click **Designate NAT interfaces** in the NAT window, and designate the router interfaces as inside or outside. Then return to this window and configure the NAT rule.

Access Rule

Dynamic NAT translation rules use access rules to specify the addresses that need translation. If you choose **From outside to inside**, these are the outside global addresses. Enter the name or number of the access rule that defines the addresses you want to translate. If you do not know the name or number, you can click the **...** button and choose an existing access rule, or you can create a new access rule to use.

Translate to Interface

This area shows the interfaces from which packets with translated addresses exit the router. It also provides fields for specifying the translated address.

Inside Interface(s)

If you choose **From outside to inside**, this area contains the designated inside interfaces.

Type

Choose **Interface** if you want the *Translate from* addresses to use the address of an interface on the router. They will be translated to the address that you specify in the Interface field, and PAT will be used to distinguish each host on the network. Choose **Address Pool** if you want the addresses to be translated to addresses defined in a configured address pool.

Interface

If you choose **Interface** in the Type field, this field lists the interfaces on the router. Choose the interface whose IP address you want the local inside addresses translated to. PAT will be used to distinguish each host on the network.

Address Pool

If you choose Address Pool in the Type field, you can enter the name of a configured address pool in this field, or you can click **Address Pool** to choose or create an address pool.

Configuration Scenarios

Click Dynamic Address Translation Scenarios for examples that illustrate how the fields in this window are used.

How Do I . . .

This section contains procedures for tasks that the wizard does not help you complete.

How do I Configure Address Translation for Outside to Inside

The NAT wizard allows you to configure a Network Address Translation (NAT) rule to translate addresses from inside to outside. To configure a NAT rule to translate addresses from outside to inside, follow the directions in one of the following sections:

- Add or Edit Dynamic Address Translation Rule: Outside to Inside
- Add or Edit Static Address Translation Rule: Outside to Inside

How Do I Configure NAT With One LAN and Multiple WANs?

The NAT wizard allows you to configure a Network Address Translation (NAT) rule between one LAN interface on your router and one WAN interface. If you want to configure NAT between one LAN interface on your router and multiple WAN interfaces, first use the NAT wizard to configure an address translation rule between the LAN interface on your router and one WAN interface. Then follow the directions in one of the following sections:

- Add or Edit Static Address Translation Rule: Inside to Outside
- Add or Edit Dynamic Address Translation Rule: Inside to Outside

Each time you add a new address translation rule using the directions in one of these sections, choose the same LAN interface and a new WAN interface. Repeat this procedure for all WAN interfaces that you want to configure with address translation rules.