Configuring NAT on the Cisco ISA500 Security Appliance

This application note provides information on how to configure various NAT (Network Address Translation) methods on the ISA500 security appliance. It includes the following topics:

Supported NAT Methods

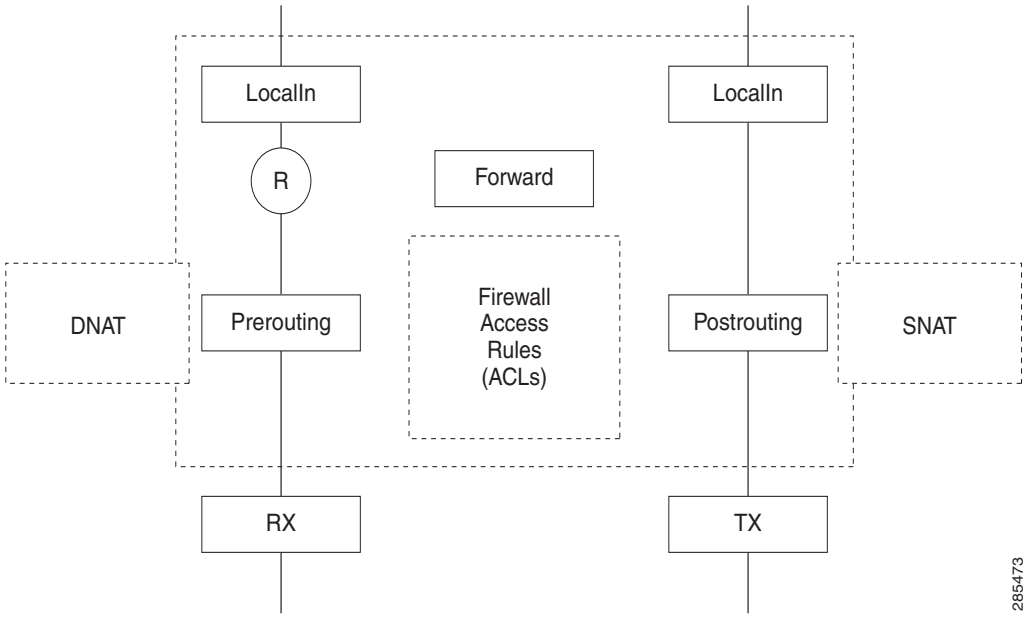
Network Address Translation (NAT) enables private IP networks to connect to the Internet. NAT replaces a private IP address with a public IP address, translating the private addresses in the internal private network into legal, routable addresses that can be used on the public Internet.

The ISA500 supports Port Forwarding, Static NAT, Dynamic PAT, Advanced NAT and Port Triggering translation methods. These features can be used for different deployment scenarios as defined and illustrated in this document.

How Packets Flow through Different Services

It is important to understand the packet flow on the ISA500 to properly configure different functionalities. Figure 1 shows the packet flow for various services. As illustrated, DNAT (Destination NAT) is performed when the packet arrives from an interface before a forwarding decision (Prerouting) is made. Subsequently, SNAT (Source NAT) is performed after a forwarding decision is made (Postrouting).

Figure 1 ISA500 Packet Flow



Applying ACL Rules

On the ISA500, NAT only defines the WAN IP addresses and port translations. To allow traffic to flow between the different zones you must configure firewall rules to control the inbound and outbound traffic. These are also referred to as Access Control Lists (ACLs).

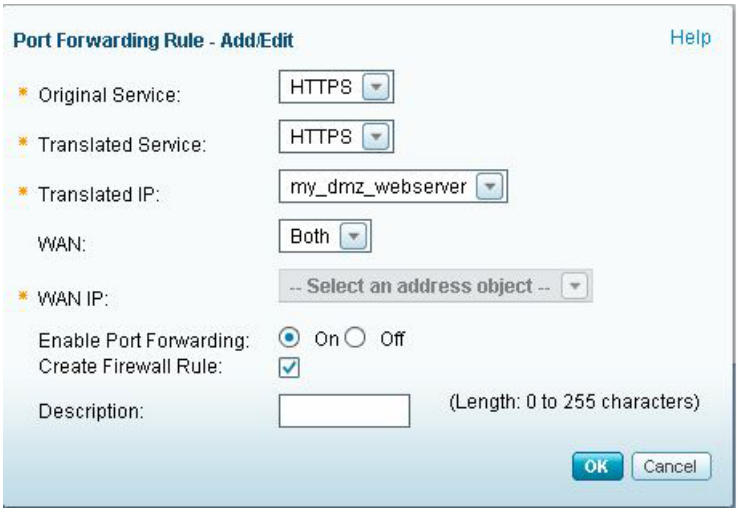
By using the ISA500 Configuration Utility, you can automatically create ACL rules for port forwarding that correspond to the NAT rules.These rules are easy to configure and are less prone to configuration errors. However, if you are using Static NAT or Advanced NAT to open an internal server to the Internet, you must create a rule manually.

Automatically Generating a Rule

To automatically generate a rule:

Step 1. Choose **Firewall > NAT > Port Forwarding**.

Step 2. From the Port Forwarding Rules page, click **Add**.



Step 3. Specify the new rule information.

Step 4. Click the **Create Firewall Rule** box.

Step 5. Click **OK** to save your settings.

The new port forwarding rule is added and an ACL rule is automatically created.

NOTE You cannot modify or delete an automatically generated ACL rule after it's created, or move the rule to increase or decrease its priority in the ACL table.

Manually Generating a Rule

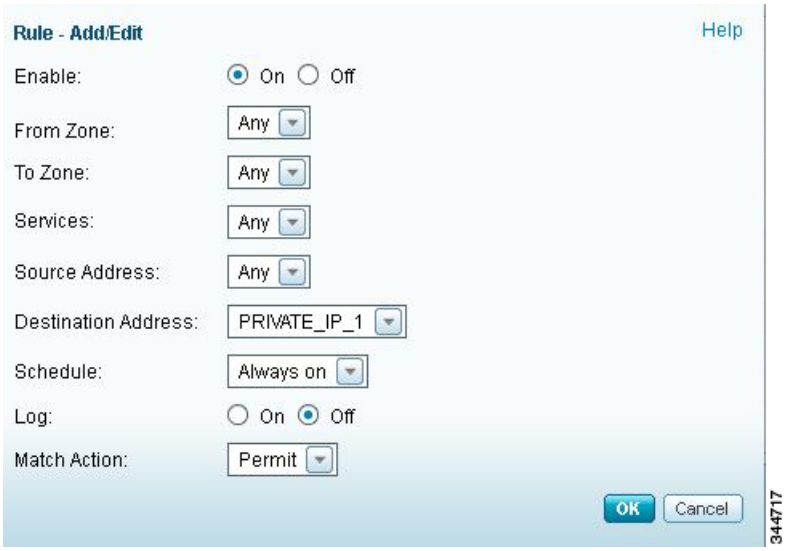
NOTE Unclick the **Create Firewall Rule** box in the Port Forwarding Add - Edit page before you begin.

Step 1. Choose **Firewall > NAT > Static NAT**.

Step 2. Enter the static rule information and click **OK**. The new static NAT rule is added to the Static NAT Rules table.

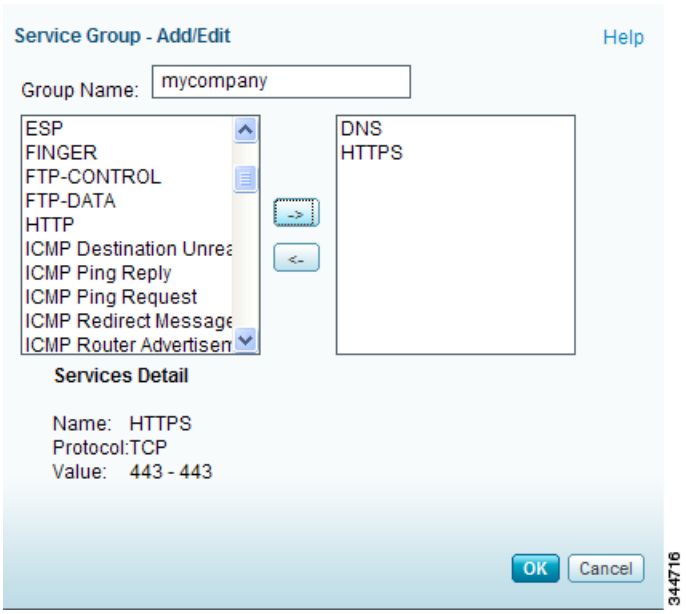
Step 3. Click the pencil icon next to the rule that you just created.

Step 4. From the Static NAT Rule Add/Edit window, click the **Create Rule** link to add a new firewall rule. You can set this rule to allow or deny traffic, and apply it to a specific zone, service, IP address, or time of day.



Step 5. Click **OK** to save your settings.

NOTE If you are creating multiple ACL rules, you can simplify this process by creating a service group from the **Networking > Service Management** page. This allows you to group common applications into a service group which is treated as single service.



Configuring Port Forwarding

You can use port forwarding to open up certain ports or services on the WAN interface (such as web servers, FTP servers and email servers), and forward them to an internal computer or server. Port forwarding is a form of destination NAT and is performed before a forwarding decision is made by the ISA500.

We recommend using port forwarding if you have a web server or email server that you host on the DMZ or LAN and want to allow access from the public Internet (Firewall > NAT > Port Forwarding). You can then create an ACL to allow traffic between the two zones.

For example: you host a web server (192.168.100.10) on the DMZ zone and only have one public IP address (10.0.0.1) that you want to expose to the public as your HTTP server address. You can create a rule to translate any requests to the public IP (10.0.0.1) on port 80 to the internal host (192.168.100.10) on port 80. Or, you can forward a range of ports, such as the public IP address (port 80 to 85) to the private IP address (port 100 to 105).

NOTE You can port forward a range of services as a single service object, but cannot port forward a service object group. For more information, see the *Cisco ISA500 Series Integrated Security Appliances Administration Guide* at: www.cisco.com/go/isa500resources.

How to Configure Port Forwarding to Access Internal Services

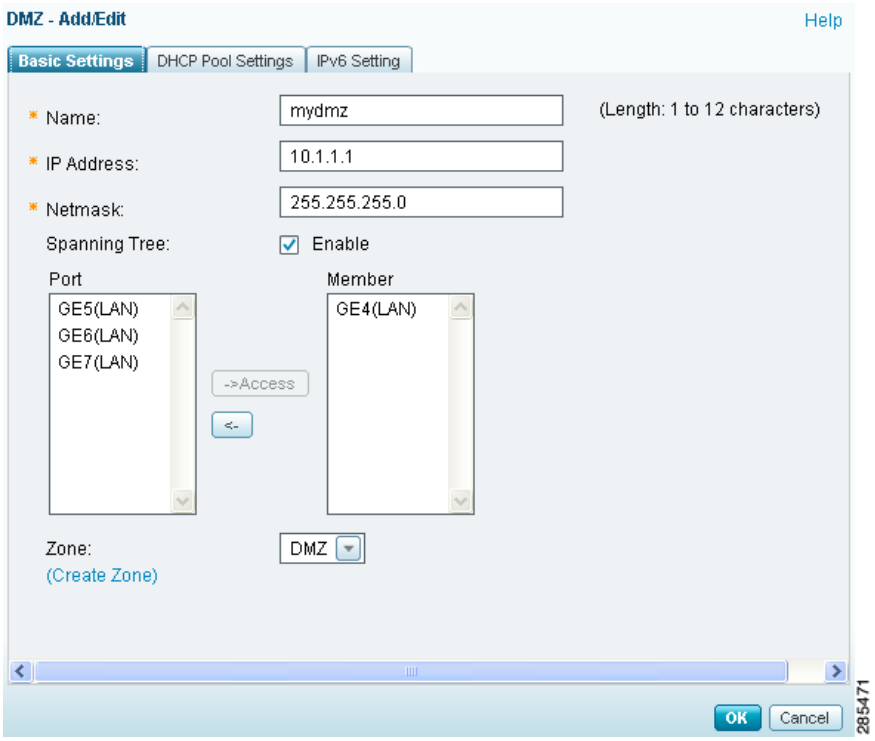
Scenario: Use a Single WAN interface or Dual WAN interface to open the SMTP server to the Internet.

NOTE In Dual WAN failover mode, the SMTP server is accessed by its primary WAN IP address. In Load Balancing mode, the server is accessed from either the WAN1 or WAN2 interface.

Step 1. Create a DMZ (Demilitarized Zone). A DMZ is a subnetwork that is located behind the firewall but is open to the public.

a. Choose **Networking > DMZ**.

b. From the DMZs window, click **Add**.

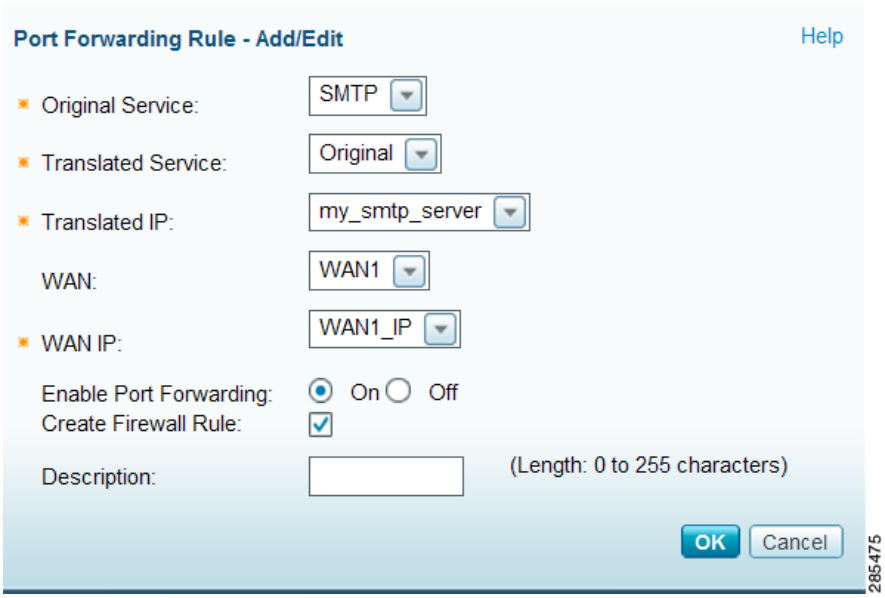


c. Enter the **Name**, **IP Address**, and **Netmask** for the DMZ.

d. Choose a configurable port as the DMZ port and click **OK**.This port connects the SMTP server to the LAN port. In the above example, the DMZ port is identified as GE4 (LAN).

Step 2. Create a port forwarding rule for the SMTP server.

a. Choose **Firewall > NAT > Port Forwarding**. The example below shows a port forwarding rule for a single WAN configuration.



b. Enter the following information:

– **Original Service**: **SMTP** (outside/public service that you want translated).

– **Translated Service**: **Original**. In this example, Original refers to SMTP.

– **Translated IP**: Choose the address of the local SMTP server. In this example, the name of the SMTP server address object is: **my_smtp_server.**

– **WAN**: Choose **WAN1** (Incoming port) for a Single WAN configuration. Choose **Both** for Dual WAN (Load Balancing or Failover mode) configurations. An Internet user can also access the SMTP server by its primary WAN IP address.

– **WAN IP**: Choose **WAN_IP** for a Single WAN configuration. For Dual WAN configurations, this field will be grayed out.

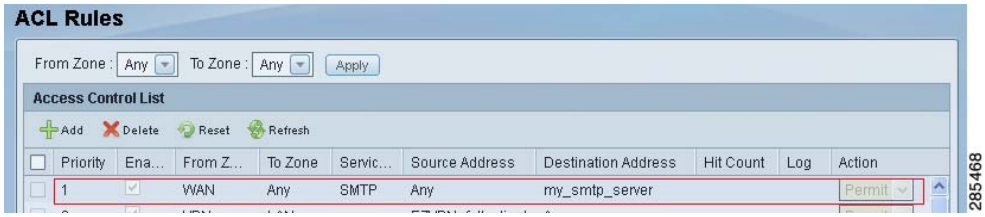
– **Enable Port Forwarding**: Click **On** to enable the port forwarding rule, or click **Off** to create only the port forwarding rule.

– **Create Firewall Rule**: Click this box to automatically create a firewall rule to allow traffic between the zones.

– **Description**: Enter a name for the port forwarding rule.

c. Click **OK** to save your settings.

A firewall rule is automatically created between zones in the **Firewall > Access Control > ACL Rules** page. This rule cannot be modified or deleted.



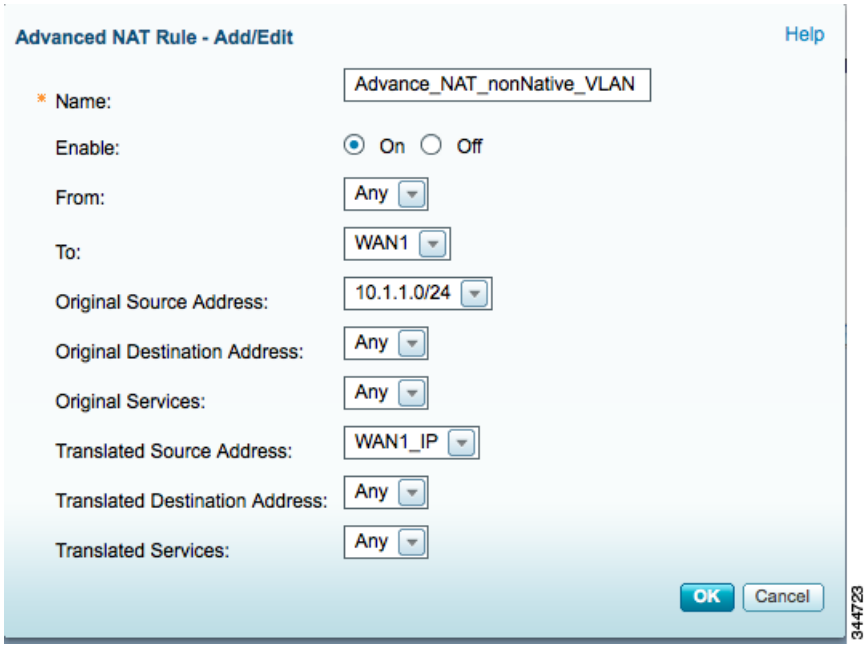
IP Aliases: Assigning Multiple IP Addresses to a WAN Interface

With Port Forwarding, Static NAT, and Advanced NAT you can configure a single WAN interface to be accessible through multiple WAN IP addresses by binding additional IP address to the WAN port.

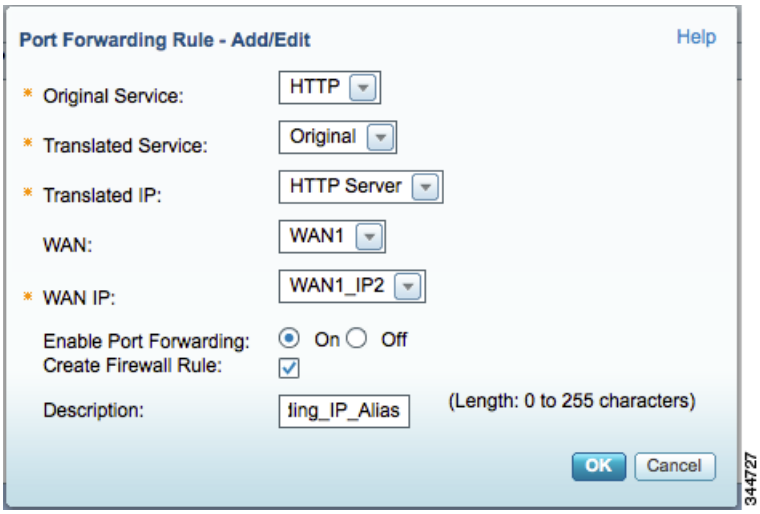
Scenario. The inbound interface (**From**) is set to a WAN port but the original destination IP address (**Original Destination Address**) is different than the primary IP address of the selected WAN port.

For example, you host an HTTP server (192.168.75.20) on your LAN. Your ISP provided you with a static IP address (1.1.1.3) that will be exposed to the public as your HTTP server address. You want to allow the Internet user to access the internal HTTP server by using the specified public IP address.

Solution. Assume that the IP address of the WAN1 port is (1.1.1.2) and you are assigned another public IP address (1.1.1.3.) Create a host address object (192.168.75.20) called HTTPServer and a host address object (1.1.1.3) called WAN1_IP2. From the **Firewall > NAT > Advanced NAT** page, configure an advanced NAT rule as follows to open the HTTP server to the Internet:



This is an example of the same scenario configured by using port forwarding.



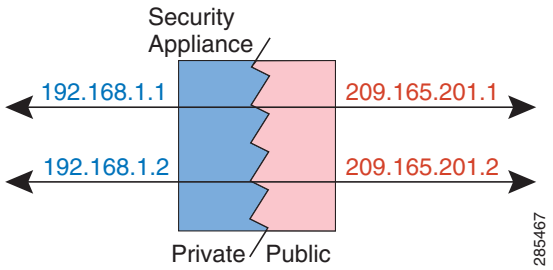
Configuring Static NAT

Static NAT (also referred to as one-to-one NAT) allows you to define static NAT rules to perform one-to-one static mapping from one IP address or subnet to another IP address or subnet without port address translation. Because the mapped address is the same for each consecutive connection, static NAT allows bidirectional connection initiation, both to and from the host (if an ACL exists that allows it).

Static NAT is typically used when you have multiple public IP addresses and want to translate one of the addresses to a fixed local address, that is, to expose an internal host to the internet. Static NAT requires one public IP address for each mapping to a private IP address. You cannot map a public IP address to more than one private IP address.

Figure 2 shows a typical static NAT scenario. The translation is always active so both real and remote hosts can initiate connections.

Figure 2 Static NAT Scenario

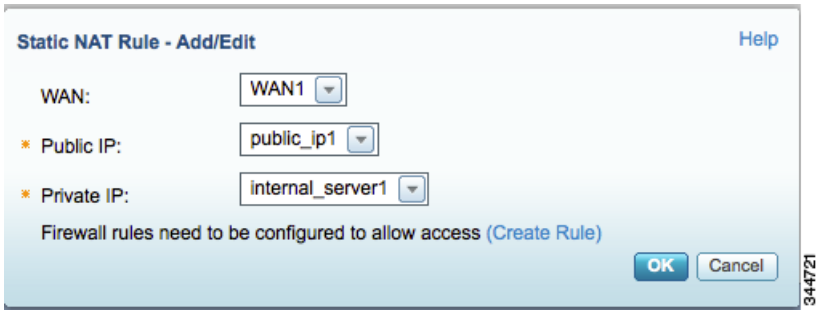


Scenario: You are hosting a server on a DMZ that provides multiple services with private IP address (192.168.100.10) and public IP address (10.0.0.2). You want to translate all incoming traffic to the public address to the private address.

Solution: Create a static NAT rule and add a firewall rule to allow the specified services to permit traffic between the zones. See **Applying ACL Rules**, page 2.

If you have only one public IP address, you can use port forwarding to forward a service/port to one of the internal IP address as follows:

Step 1. Create a static NAT rule from the **Firewall > NAT > Static NAT > Static NAT Rule - Add/Edit** page.



In this example, the Public IP address (public_ip1) is 10.74.10.11. The Private IP address (internal_server1) is 192.168.75.11.

With this rule, traffic from the destination address (192.168.75.11) to the Internet is translated to (10.74.10.11), however, by default, traffic from the untrusted zone to the trusted zone is not permitted.

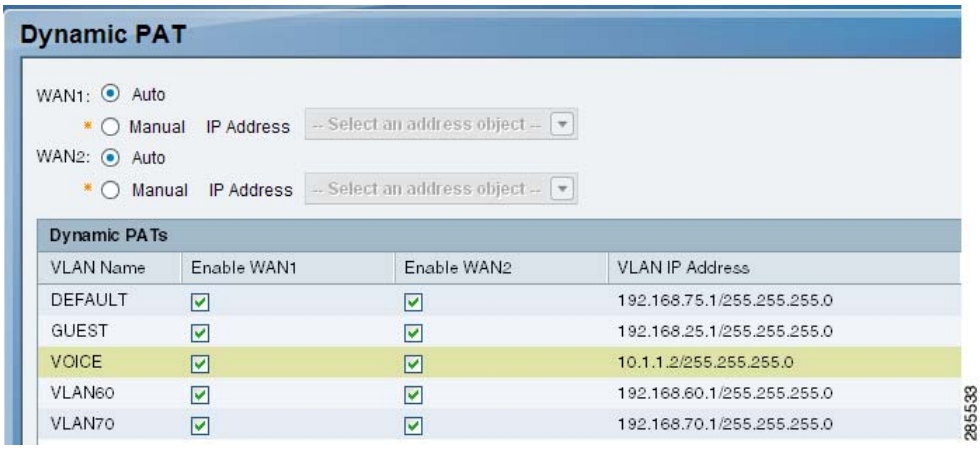
Step 2. Create a firewall rule to allow Internet users to access the SMTP service on 192.168.75.11.

Step 3. Repeat step 1 and 2 to create multiple one-to-one mappings.

Configuring Dynamic PAT

You can use Dynamic Port Address Translation (Dynamic PAT) to establish connections from a private network to public network. Dynamic PAT translates multiple private addresses to one or more public IP address.

Step 1. Choose **Firewall > NAT > Dynamic PAT**.



Step 2. Select the PAT IP address for each WAN port.

In this example, WAN1 and WAN2 are set to **Auto**, which automatically uses the IP address of the WAN port as the translated IP address.

If you select **Manual**, choose a single public IP address or a network address as the translated IP address. If the address object is not available, choose **Create a new address** to create a new address object.

Step 3. Choose one of the following to translate multiple private IP addresses of a VLAN to one or more mapped IP addresses.

- **Enable WAN1**: Translates all IP addresses of the selected VLAN into the public IP address specified on the WAN1 port.
- **Enable WAN2**: Translates all IP addresses of the selected VLAN into the public IP address specified on the WAN2 port.
- **VLAN IP Address**: Subnet IP address and netmask of the selected VLAN.

Step 4. Click **Save** when you are finished.

Configuring Advanced NAT

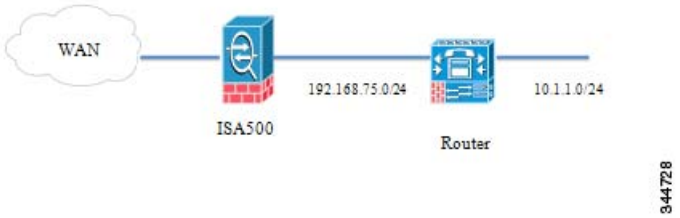
This section describes the different type of NAT methods that you can configure by using Advanced NAT. It includes the following sections:

- Forwarding Traffic from Non-Native VLANs to the Internet
- Configuring Policy NAT
- Using NAT Hairpinning

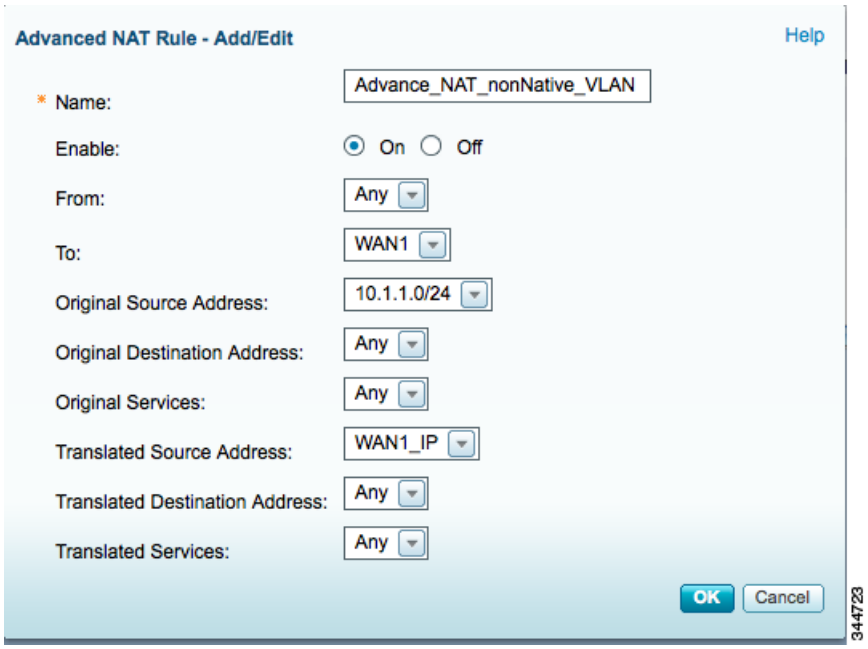
NOTE You can configure up to 16 advanced NAT rules on the ISA500.

Forwarding Traffic from Non-Native VLANs to the Internet

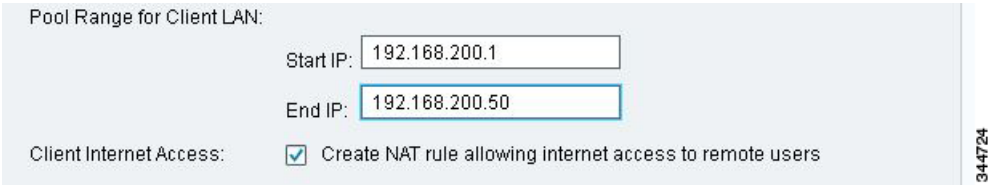
Scenario 1: To allow hosts that are not in local VLANs of the ISA500 to access the Internet. In this scenario, another router is located behind the ISA500 in a Dual WAN configuration. To accomplish this task you will need to create two Advanced NAT rules on the ISA500.



To allow **Router interface2 subnet** to access the Internet, create an advanced NAT rule as follows:



For SSL VPN Remote User Access or IPsec Remote Access, the NAT rule for the IP address in the VPN IP pool is automatically created when you enable **Client Internet Access** on the VPN Configuration page. These rules cannot be edited or changed. If you want to modify a rule, you must disable this option.

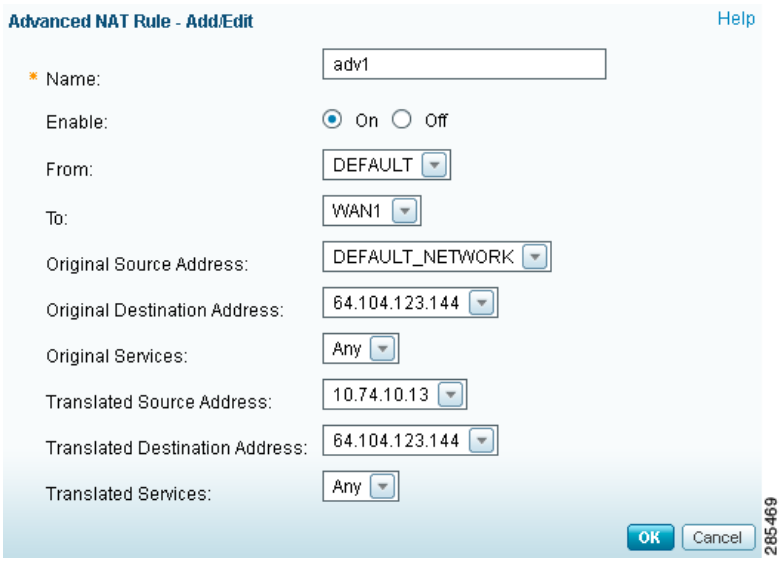


Configuring Policy NAT

Policy NAT/PAT translates the IP address of packets passing through the ISA500 only if those packets match a defined criterion or policy. You can define the policy by identifying interesting traffic based on the source IP Address, destination IP Address, source port and destination port. If the traffic matches the defined entries, then the original source or destination address can be translated to a different address.

Scenario 2 (Policy NAT): The ISA500 has two public IP addresses (10.74.10.12) and (10.74.10.13). When the default VLAN hosts accesses the Internet server (64.104.123.144), the IP address is translated to (10.74.10.13); otherwise it is translated to (10.74.10.12).

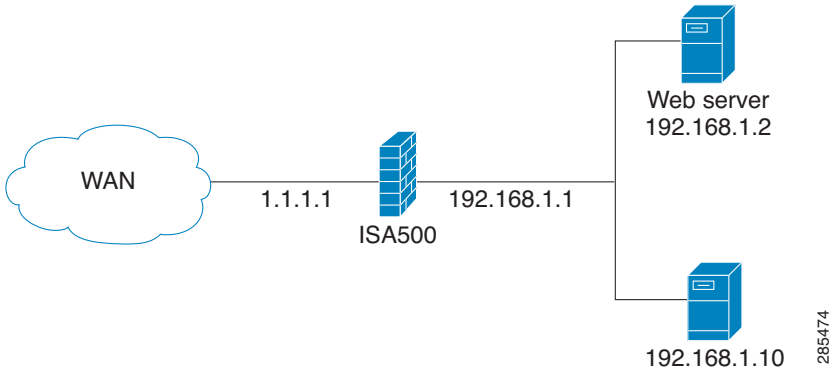
Solution: Create two advanced NAT rules (**Networking > NAT > Advanced NAT**) as follows:



Using NAT Hairpinning

NAT hairpinning, also referred to as NAT loopback, allows the hosts at the LAN side to access internal servers by using its external IP address (public IP address). Figure 3 shows an example NAT hairpinning scenario using advanced NAT.

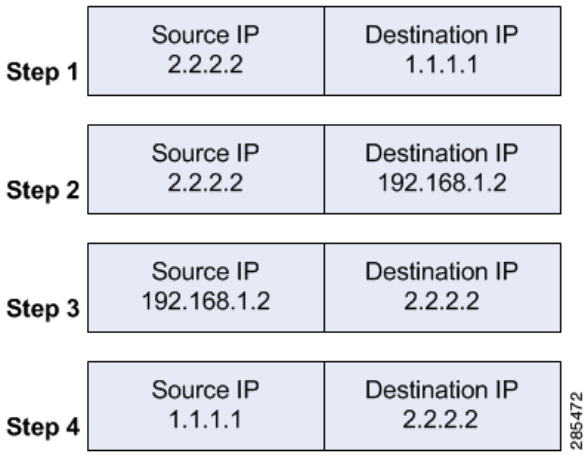
Figure 3 Example of NAT Hairpinning



What Basic NAT Does

Basic NAT is the simplest type of NAT that provides a one-to one translation of IP addresses. For example, when a client on the Internet with IP address (2.2.2.2) establishes a connection to the web server, the ISA500 performs NAT as shown in Figure 4.

Figure 4 Example of Network Address Translation



Step 1. The client sends a packet with source IP address (2.2.2.2) to destination IP address (1.1.1.1) on port TCP/80 to request a web resource.

Step 2. The ISA500 destination NATs the packet to (192.168.1.2) and replaces the destination IP address in the packet. The source IP address (2.2.2.2) remains the same.

Step 3. The server replies to the client's request. The reply packet source IP address is (192.168.1.2) and the destination IP address is (2.2.2.2)

Step 4. The ISA500 determines that the packet is part of a previous connection and undoes the destination NAT. It then places the original destination IP address into the source IP address field. The destination IP address is (2.2.2.2) and the source IP address is (1.1.1.1).

Step 5. The client receives the reply packet it expects and the connection is established.

When to Use NAT Hairpinning

Scenario: When a client on the same internal network as the web server requests a connection to the web server's public IP address, the connection breaks as described in the steps below:

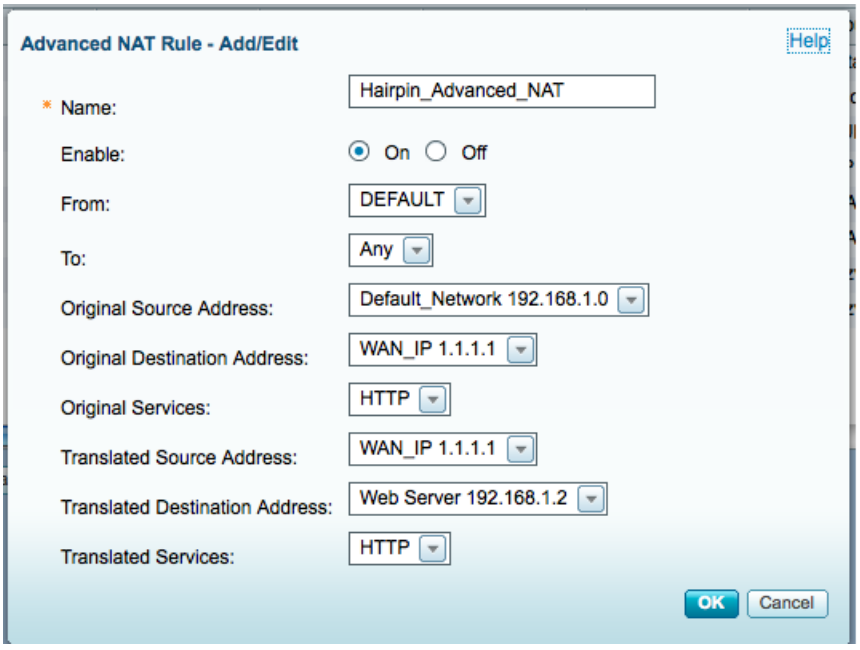
Step 1. The client sends a packet with source IP address (192.168.1.10) to destination IP address (1.1.1.1) on port TCP/80 to request a web resource.

Step 2. The ISA500 translates the destination packet to 192.168.1.2 and replaces the original destination IP address. The source IP address (192.168.1.10) remains the same:

Step 3. The server replies to the client's request. However, the requested source IP address is on the same subnet as the web server. The web server does not send the reply back to the ISA500, but sends it directly to the source IP address (192.168.1.10) in the reply of 192.168.1.2.

Step 4. The client receives the reply packet, but discards it because it expects a packet back from 1.1.1.1, and not from 192.168.1.2. The packet is considered invalid and is not related to any connection the client previously attempted to establish.

Solution: Use NAT Hairpinning. Add a NAT rule (**Firewall > NAT > Advanced NAT**) on the ISA500 to allow all reply traffic to flow through the device as follows. Note that the client and server are on the same subnet.



After you add the new rule, the flow changes to the following:

Step 1. The client sends a packet with source IP address (192.168.1.10) to the destination IP address of (1.1.1.1) on port TCP/80 to request a web resource.

Step 2. The ISA500 translates the packet's destination address (192.168.1.2) and forwards the request to the internal web server. It also translates the packet's source IP address to its WAN interface IP address (WAN1_IP).

Step 3. The web server replies to the request and sends the reply with a source IP address of 192.168.1.2 back to the router's WAN interface IP address (WAN1_IP).

Step 4. The ISA500 determines that the packet is part of a previous connection and undoes both the source and destination NAT. It then places the original destination IP address (1.1.1.1) into the source IP address field and the original source IP address (192.168.1.10) into the destination IP address field.

Step 5. The client receives the reply packet that it expects and the connection is established.

Configuring Port Triggering

Port triggering opens an incoming port for a specified type of traffic on a defined outgoing port. Port triggering is more flexible and secure than port forwarding, because the incoming ports are always open. The ports are open only when a program is actively using the trigger port.

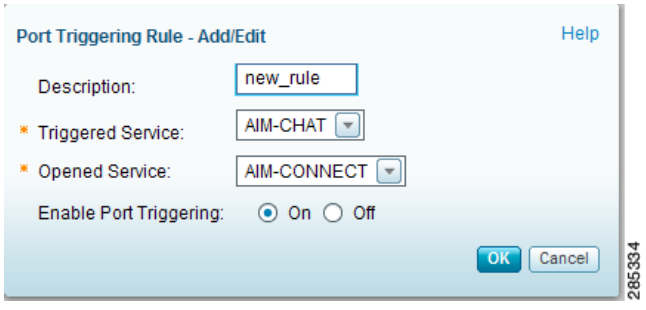
Some applications may specifically require port triggering. These applications require that, when external devices connect to them, they receive data on a specific port or range of ports to function properly. The ISA500 must send all incoming data for that application only on the required port or range of ports. You can specify a port triggering rule by defining the type of traffic (TCP or UDP) and the range of incoming and outgoing ports to open when enabled.

NOTE You can configure up to 15 port triggering rules.

Step 1. Choose **Firewall > NAT > Port Triggering**.

Step 2. To enable a port triggering rule, click the box in the **Enable** column.

Step 3. To add a new port triggering rule, click **Add**.



Step 4. Enter the following information.

- **Description**: Enter the name for the port triggering rule.
- **Triggered Service**: Choose an outgoing TCP or UDP service.

- **Opened Service**: Choose an incoming TCP or UDP service. If the service that you want is not in the list, choose Create a new service to create a new service object.
- **Enable Port Triggering**: Click **On** to enable the port triggering rule, or click **Off** to create only the port triggering rule.

Step 5. Click **OK** to save your settings.

NAT Priority

If there is a conflict between different NAT configurations, the ISA500 does the following:

- For an inbound packet, the ISA500 performs DNAT (before a forwarding decision is made) in this order: **Advanced NAT > Static NAT > Port Forwarding > Port Triggering**.
- For an outbound packet, the ISA500 performs SNAT (after a forwarding decision is made) in this order: A**dvanced NAT > Static NAT > Dynamic PAT**.

For example, if an advanced NAT rule and a port forwarding rule conflict, the Advanced NAT rule takes precedence over the Port Forwarding rule and the Port Forwarding rule is not applied.

Deciding Which NAT Method to Use

Open a single service to the Internet.	Create one port forwarding rule and one ACL.
Open multiple services on multiple servers to the Internet.	Create multiple port forwarding rules and multiple ACLs, or multiple port forwarding rules and one ACL with multiple services.
Open multiple services on a host to the Internet.	Create one static NAT rule and one ACL with multiple services.
Allow internal users to access a service by using its public IP address.	Create one Advanced NAT rule (NAT hairpinning) and one ACL with the service.
Allow non-native VLANs to access the Internet.	Create one Advanced NAT rule.

Frequently Asked Questions

Q. What do I need to know when configuring port forwarding and NAT ACL rules?

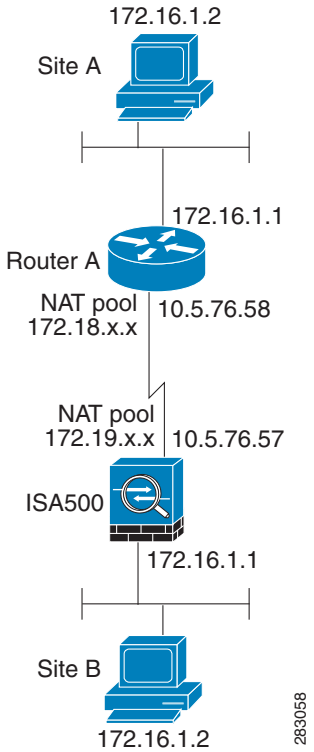
A. Remote management does not work properly with a static NAT mapping internal server to WAN IP address

For example: The ISA500 is configured with WAN IP address (173.39.202.68), LAN host (192.168.75.100), and remote management enabled on http://173.39.202.68:8080. If Static NAT is configured between 192.168.75.100 and 173.39.202.68, you cannot access the ISA500 Configuration Utility from http://173.39.202.68:8080.

Q. How do I configure a Site-to-Site VPN when there are overlapping networks?

A. Figure 5 shows an example of two merging companies that have the same IP addressing scheme. Two routers are connected with a VPN tunnel, and the networks behind each router are the same. For one site to access the hosts at the other site, Network Address Translation (NAT) is used on the routers to change both the source and destination addresses to different subnets.

Figure 5 Two Merging Companies with the Same IP Addressing Scheme



In this example, when host (172.16.1.2) at Site A accesses the same IP-addressed host at Site B, it connects to (172.19.1.2) instead of the actual (172.16.1.2) IP address. When the host at Site B accesses Site A, it connects to a (172.18.1.2) address. NAT on Router A translates any 172.16.x.x address to look like the matching 172.18.x.x host entry. NAT on the ISA500 changes 172.16.x.x to look like 172.19.x.x.

NOTE This configuration only allows the two networks to communicate. It does not allow for Internet connectivity. You need additional paths to the Internet for connectivity to locations other than the two sites; in other words, you need to add another router or firewall on each side, with multiple routes configured on the hosts.

For More Information

Product Resources	Location
Product Documentation	www.cisco.com/go/isa500resources
Cisco Small Business Support Community	www.cisco.com/go/smallbizsupport
Cisco Small Business Support and Resources	www.cisco.com/go/smallbizhelp
Phone Support Contacts	www.cisco.com/go/sbsc
Firmware Downloads	www.cisco.com/go/isa500software
Cisco Partner Central for Small Business (Partner Login Required)	www.cisco.com/web/partners/sell/smb
Cisco Small Business Home	www.cisco.com/smb