

NETWORK ADDRESS TRANSLATION

.....

Network Address Translation (NAT) allows Security Administrators to overcome IP addressing limitations, allowing private IP-address allocation and unregistered internal addressing schemes.

VPN-1 NGX supports Static and Dynamic (Hide) NAT. Static NAT translates private IP addresses to public IP addresses, when packets exit protected networks. Static NAT translates public IP addresses to private IP addresses, when packets enter protected networks. Dynamic NAT conceals one or more private IP addresses behind one public IP address. The main purpose of Dynamic NAT is to place many hosts with private IP addresses behind one public IP address.

Objectives

Use private IP-address allocation and unregistered internal addressing schemes, to overcome IP addressing limitations:

1. Select the appropriate NAT scheme to meet business requirements.
2. Configure Dynamic/Hide NAT to meet business requirements.
3. Configure Static NAT to meet business requirements.
4. Configure Manual NAT to meet business requirements

▪
▪
▪
▪
▪

Key Terms

- Network Address Translation (NAT)
- Static NAT
- Dynamic (Hide) NAT
- Manual NAT

UNDERSTANDING NETWORK ADDRESS TRANSLATION

.....

Network Address Translation (NAT) was first introduced to the Internet community by RFC 1631. NAT was later refined in RFC 3022, “Traditional IP Network Address Translator (Traditional NAT)”. The abstract for RFC 3022 states:

Basic **Network Address Translation** or Basic NAT is a method by which IP addresses are mapped from one group to another, transparent to end users. Network Address Port Translation, or NAPT, is a method by which many network addresses and their TCP/UDP (Transmission Control Protocol/User Datagram Protocol) ports are translated into a single network address and its TCP/UDP ports. Together, these two operations, referred to as traditional NAT, provide a mechanism to connect a realm with private addresses to an external realm with globally unique registered addresses.

VPN-1 NGX implements both types of traditional NAT, through its Dynamic and Static NAT capabilities.

Enterprises employ NAT for a variety of reasons, including:

- Private IP addresses used in internal networks.
- Limiting external network access.
- Ease and flexibility of network administration.

IP Addressing

In an IP network, each computer is assigned a unique IP address. Because public IP addresses are scarce and expensive, many enterprises choose to use private addresses for their internal networks. The following blocks of IP addresses were set aside for internal-network use in RFC 1918, “Address Allocation for Private Networks”:

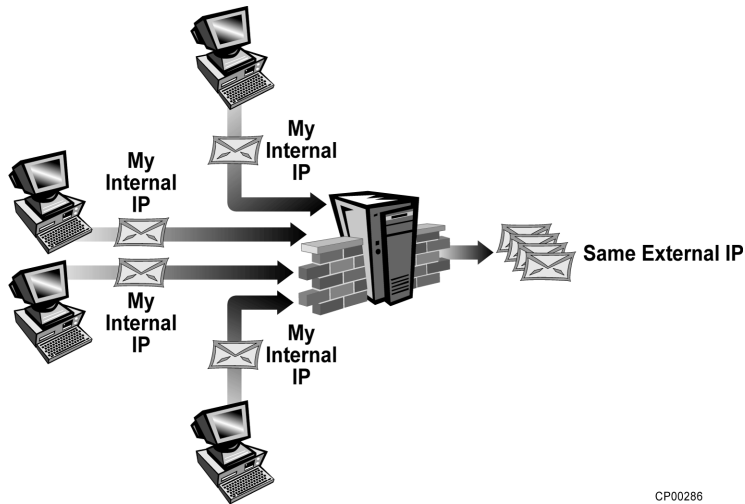
- Class A network numbers:10.0.0.0-10.255.255.255
- Class B network numbers:172.16.0.0-172.31.255.255
- Class C network numbers:192.168.0.0-192.168.255.255



Best practices recommend using only these address ranges for intranets. RFC 1918 addresses cannot traverse public networks.

Dynamic (Hide) NAT

Dynamic (Hide) NAT is used to hide a network, a collection of networks, or a range of IP addresses behind a single IP address. VPN-1 NGX uses dynamically assigned port numbers to distinguish between internal hosts. The defining characteristic of Dynamic NAT is the one-to-many relationship between the hiding IP address and hidden IP addresses. Dynamic NAT is not appropriate for devices offering services to external clients, for example Web servers that must be accessible from the Internet.



Dynamic NAT



VPN-1 NGX is able to handle packets from overlapping IP networks coming from different interfaces of the Gateway. When entering the Gateway, these packets are translated to a virtual IP network. When leaving the Gateway, packets are translated to their original IP address.

DYNAMIC PORTS

In Dynamic NAT, IP addresses and ports are modified as traffic traverses a Gateway. As a packet from an internal network passes through a Gateway, the source IP address and port are modified. The source IP address is changed to the hiding address. The source port is changed to a dynamically assigned port, to uniquely identify the connection. The relationship between the dynamically assigned port and the internal IP address is recorded in the Gateway's state tables. When reply packets arrive, the Gateway uses the destination port to determine to which connection the packet belongs, and adjusts the destination port and IP address accordingly.

PORT ASSIGNMENT

Port numbers are dynamically assigned from two pools of numbers:

- 600-1023
- 10,000-60,000

If the original port number is less than 1024, a port number is assigned from the first pool. If the original port number is greater than 1024, a port number is assigned from the second pool. A port number currently in use is not reassigned to a new connection.

The high port range used by Dynamic NAT can be configured using DbEdit, to modify the following properties:

`hide_min_high_port` — Defines the minimum high port used by Dynamic NAT

`hide_max_high_port` — Defines the maximum high port used by Dynamic NAT

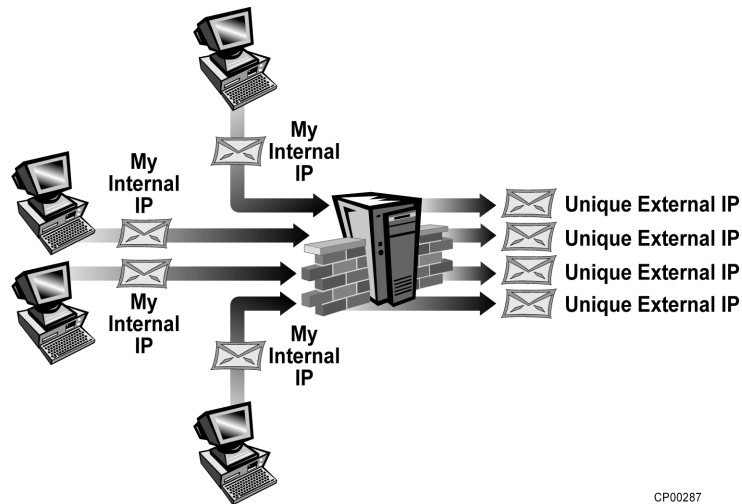
LIMITATIONS

Dynamic NAT cannot be used for protocols that require port numbers remain unchanged, or in situations where an external host must distinguish between internal hosts (based on their IP addresses). A limitation of Dynamic NAT is that all connections must be initiated by hidden hosts.

Static NAT

Static NAT implements a one-to-one relationship between a hidden host and a hiding IP address. Because of this one-to-one relationship, a separate public IP address is required for each hidden host for which a Security Gateway is configured to perform Static NAT.

Static NAT is appropriate when external hosts must be able to contact an internal host, using its IP address. Static NAT connections are recorded in the Gateway's state tables, to permit Stateful Inspection to occur. No port modifications are required for static NAT.



Static NAT

CP00287

CONFIGURING NAT

NGX Administrators configure NAT in three areas:

- Global Properties
- Object properties
- Address-translation rules

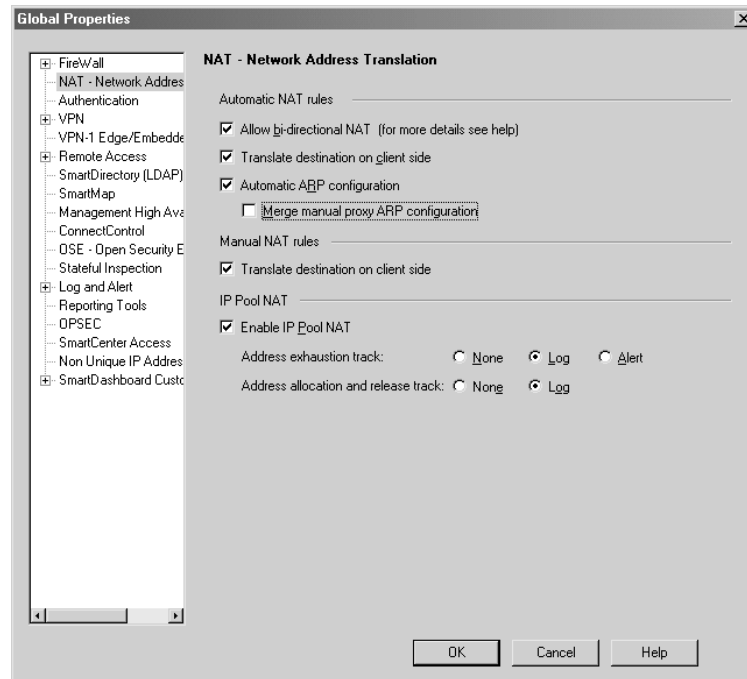
Settings in these areas determine how a Gateway processes packets when NAT is configured. Only automatic NAT rules are covered in this section.



Automatic NAT rules are automatically created from property settings and are appropriate for most installations. In legacy networks where design issues prevent the use of automatic NAT rules, Manual NAT rules may provide solutions.

Global Properties

Several global properties influence how NAT is handled by an NGX Gateway. The figure below shows the default global properties for NAT. Following the figure are detailed descriptions for each property:



Global Properties for NAT

GLOBAL PROPERTIES FOR AUTOMATIC NAT RULES

In most cases, VPN-1 NGX automatically creates NAT rules, based on information derived from object properties. Special circumstances, where it may not be appropriate to use automatic NAT rule creation, are discussed later in this chapter. The following three global properties can be modified to adjust the behavior of automatically created NAT rules on a global level:

- Bi-directional NAT
- Destination translation on client side
- Automatic ARP configuration



All check boxes for NAT Global Properties are checked by default in new installations. Check boxes are cleared by default, when upgrading from previous versions of VPN-1.

Allow bi-directional NAT — If more than one automatic NAT rule matches a connection, both rules are matched. If Allow bi-directional NAT is selected, a Gateway will check all NAT rules to see if there is a source match in one rule, and a destination match in another rule. The Gateway will use the first matches found, and apply both rules concurrently.

Translate destination on client side — For packets from an external host that are to be translated according to Static NAT rules, translate destination IP addresses in the kernel nearest the client:

This property only applies to a limited subset of packets. For this property to apply, a packet must be sent from an external host to an internal host for whom a Gateway is performing Static NAT. For new installations, this property is enabled by default, to prevent conflicts between anti-spoofing and NAT. For upgrades, this property is disabled by default, to maintain compatibility with earlier versions of VPN-1.

NON-UNIQUE ADDRESS RANGES

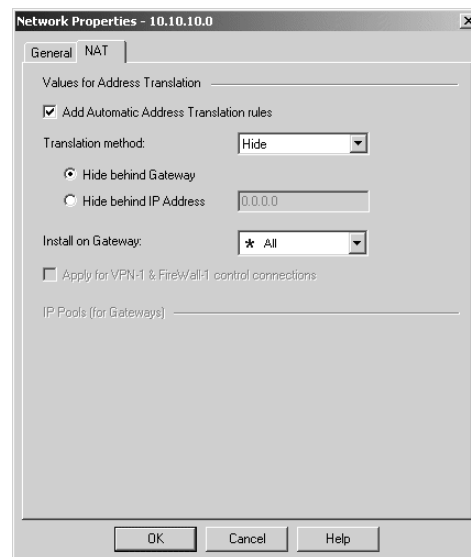
All addresses not listed in the Non-Unique Address Ranges screen will be considered unique addresses. The address ranges reserved for private intranets (RFC 1918) are listed by default. Administrators may add additional addresses to accommodate legacy networks with non-RFC 1918 compliant private addressing schemes. Listed addresses are used by SmartMap and the Automatic Topology Discovery Feature.

Dynamic NAT Object Configuration

Dynamic NAT can be configured to hide networks using a Security Gateway IP address or another, externally accessible IP address.

DYNAMIC NAT USING SECURITY GATEWAY INTERFACE IP

The following figure illustrates how to configure the NAT properties for a network using a Security Gateway's IP address when dynamically translated.



Dynamic NAT using Security Gateway IP Address

To configure Dynamic NAT with automatic NAT rule creation, check the “Add Automatic Address Translation rules” box on the NAT tab for the network to be hidden. Select Hide from the Translation method menu. Confirm the radio button is in the “Hide behind the interface of the Install on Gateway” option. Clicking OK automatically creates the necessary NAT rules for the object.

The figure below shows the NAT rules automatically created from the object’s NAT properties.

NO.	ORIGINAL PACKET			TRANSLATED PACKET			INSTALL ON	COMMENT
	SOURCE	DESTINATION	SERVICE	SOURCE	DESTINATION	SERVICE		
1	Net_10.10.10.0	Net_10.10.10.0	Any	Original	Original	Original	All	Automatic rule (see the netw data).
2	Net_10.10.10.0	Any	Any	Net_10.10.10.0	Original	Original	All	Automatic rule (see the netw data).

Dynamic NAT using Security Gateway IP Address

Configuring the network object as described above creates two rules in the Address Translation Policy. The first rule prevents translation of packets traveling from the translated object to itself. In the example above, packets whose source and destination are both part of the 10.10.10.0/24 network will not be translated.

The second rule instructs the Security Gateway to translate packets whose source IP address is part of the 10.10.10.0/24 network. This rule translates packets from private addresses to the IP address of the exiting interface of the Security Gateway. If packets exit the Security Gateway’s external interface, source addresses will be translated to the Security Gateway’s external IP address.

Because Dynamic NAT also modifies source ports, there is no need to add another rule for reply packets. Information recorded in a Security Gateway’s state tables will be used to modify the destination IP address and destination port of reply packets.



If Dynamic NAT is configured with the “Hide behind the interface of the Install on Gateway” option selected, the exiting interface will be used. For example, if a host in the hidden network sends traffic to the DMZ, the source IP address of the packets will be translated to the Security Gateway’s DMZ interface IP address.

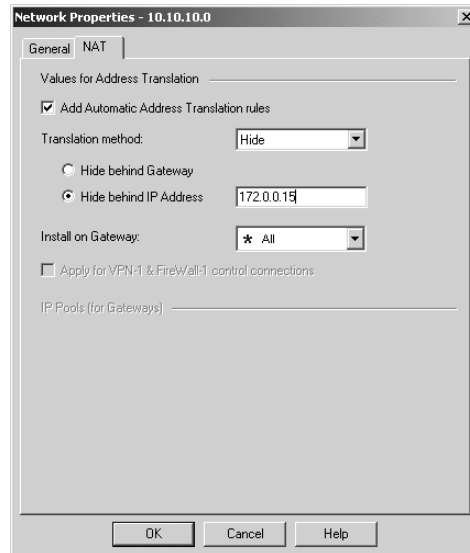


In scenarios where multiple internal networks route traffic through a Security Gateway, the load on the Security Gateway can be reduced. Add manual rules to the Address Translation policy for traffic between internal networks. Specify “Original > Original > Original” in the Translated Packet fields, as in Rule 1 above.

DYNAMIC NAT NOT USING SECURITY GATEWAY INTERFACE IP

Hiding internal addresses behind a Security Gateway’s IP address is not the most secure way to configure Dynamic NAT. Using another, externally accessible IP address for Dynamic NAT is considered best practice.

The following figure illustrates how to configure the NAT properties for a network that will use another, externally accessible IP address when dynamically translated.



Object Configured for Dynamic NAT

For automatic NAT rule creation, NGX makes all necessary route and ARP table entries on the Security Gateway. In the example above, the Security Gateway will process packets destined for 172.0.0.15, even though that IP address is not bound to its interface. For routing to work properly, the address selected to hide internal networks should be on the same subnet as the IP address of the interface where packets will arrive.

The figure below shows the NAT rules automatically created from the object's NAT properties.

NO.	ORIGINAL PACKET			TRANSLATED PACKET			INSTALL ON	COMMENT
	SOURCE	DESTINATION	SERVICE	SOURCE	DESTINATION	SERVICE		
1	Net_10.10.10.0	Net_10.10.10.0	* Any	Original	Original	Original	* All	Automatic rule (see the network data).
2	Net_10.10.10.0	* Any	* Any	Net_10.10.10.0	Original	Original	* All	Automatic rule (see the network data).

Dynamic NAT Using another, Externally Accessible IP Address

Like Dynamic NAT behind a Security Gateway's IP address, configuration for Dynamic NAT using another, externally accessible IP address also creates two rules. The first rule instructs the Security Gateway not to translate traffic whose source and destination is the object for which Dynamic NAT is configured. The second rule translates the source address of packets not destined for the object for which Dynamic NAT is configured.

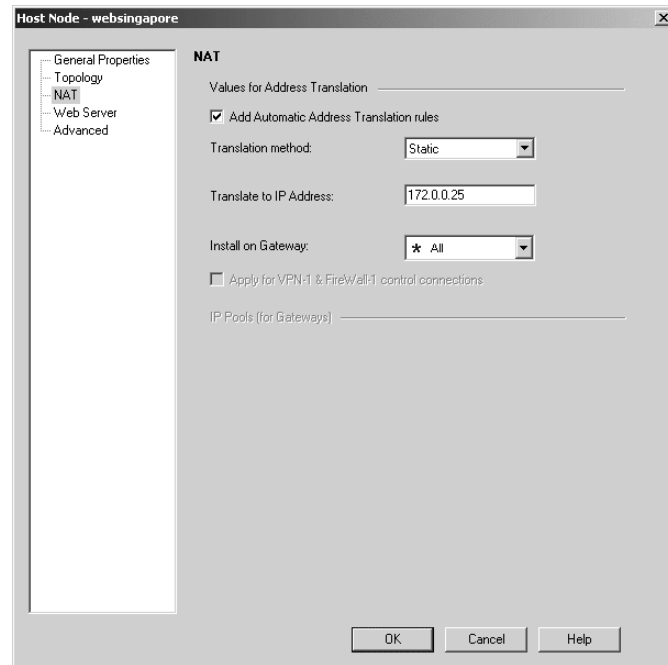


If multiple internal networks can be supernetted into a single network object, there is no need to create Manual NAT rules for internal networks routed through a Security Gateway. For example, if all internal networks are 10.X.X.X/24, an object can be created for 10.0.0.0/8. Configuring Dynamic NAT for the 10.0.0.0/8 object will cause traffic between 10-nets not to be translated, and will still allow translation of packets destined for external sources. The result is fewer rules, and consequently less load on the Security Gateway.

Static NAT Object Configuration

Configuring a Security Gateway to perform Static NAT for a host is similar to configuring a Security Gateway to perform Dynamic NAT using another, externally accessible IP address.

The following figure illustrates how to configure NAT properties, when Static NAT is used to translate a host's IP address.



Object Configured for Static NAT

To automatically configure static NAT rules:

1. Select Add Automatic Address Translation rules.
2. Choose Static from the Translation method menu. Type the public IP address, in the Translate to IP Address field.

For routing to work properly, the translate to IP address must be on the same subnet as the Security Gateway's IP address. When automatic NAT rule creation is used, NGX makes necessary adjustments to the Security Gateway's routing and ARP configuration.

The next figure shows NAT rules automatically created from an object's NAT properties.

NO.	ORIGINAL PACKET			TRANSLATED PACKET			INSTALL ON	COMMENT
	SOURCE	DESTINATION	SERVICE	SOURCE	DESTINATION	SERVICE		
1	websingapore	* Any	* Any	websingapore (\	Original	Original	* All	Automatic rule (see the network data).
2	* Any	websingapore (\	* Any	Original	websingapore	Original	* All	Automatic rule (see the network data).

Automatic Rules Created From Object Properties, Static NAT

Configuring an object for automatic creation of static NAT rules adds two rules to the Address Translation policy. For static NAT, both rules are translating rules. Dissecting the rules and examining their fields makes clear the need for two rules.

Address-translation rules are divided into two elements: Original Packet and Translated Packet. The elements of the Original Packet section inform a Security Gateway which packets match the rule. In the example above, packets whose source address belongs to websingapore (10.10.10.2) match the rule. The Translated Packet elements define how the Security Gateway should modify the packet. In the example above, the Security Gateway uses the information in the first rule to change the source address from the private address (10.10.10.2) to the public address (172.0.0.25).

MANUAL NAT

NGX allows Security Administrators to create Manual NAT rules. **Manual NAT** involves more configuration than automatic NAT rule creation, but provides additional flexibility in Rule Base design.

When to Use Manual NAT

Automatic NAT rule creation is appropriate for most installations. Properly configured objects, well-planned networks, and global property settings make Manual NAT rule creation unnecessary for most enterprises. For Security Administrators faced with legacy networks where design issues prevent the use of automatic NAT rules, Manual NAT rules may provide solutions.

Some of the situations where Manual NAT rule creation may be warranted include:

- Instances where remote networks only allow specific IP addresses.
- Situations where translation is desired for some services, and not others.
- Environments where more granular control of address translation in VPN tunnels is needed.
- Enterprises where Address Translation Rule Base order must be manipulated.
- When port address translation is required.
- Environments where granular control of address translation between internal networks is required.
- When a range of IP addresses, rather than a network, will be translated.

Configuring Manual NAT

Manual NAT requires configuration of objects and rules. The amount of configuration varies between Dynamic NAT and Static NAT.

OBJECT CONFIGURATION

Object configuration for Manual NAT does not differ significantly from object creation for Security Policy objects. When using Manual NAT rule creation, the following objects must be created:

Dynamic NAT — Object for hidden networks or range of IP addresses; object for hiding IP address; a Security Gateway object may be used if its IP address will be hiding internal addresses.

Static NAT — Object for private IP address, object for public IP address

RULE BASE CONFIGURATION

Address Translation policy rules have two sections. The first section, Original Packet, specifies the parameters for a match. The second section, Translated Packet, provides instructions for the Security Gateway on how to modify matching packets.

To configure Address Translation policy rules for Dynamic NAT, place the object for the hidden addresses in the Original Packet, Source field. Place the object for the hiding address in the Translated Packet, Source field. A single rule is sufficient for manual Dynamic NAT rules. In most environments, it is also advisable to add a rule above the translation rule preventing translation between internal networks. Place objects for internal networks in the Original Packet, Source and Destination fields. Leave the Translated Packet fields as Original > Original > Original.

Manual NAT for Static NAT normally requires two rules. The first rule translates the source IP address of packets from the protected host. The second rule translates the destination IP address of packets destined for the protected host. Configure the source address-translation rule with the object for the private IP address in the Original Packet, Source field. And configure the object for the public IP address in the Translated Packet, Source field. Configure the destination address-translation rule with the object for the private IP address in the Original Packet, Destination field. And configure the object for the public IP address in the Translated Packet, Destination field.

Special Considerations

When automatic NAT rule creation is used, NGX makes all necessary adjustments to the Security Gateway's ARP and routing tables. Using automatic NAT rule creation also eliminates potential anti-spoofing issues. If Manual NAT rule creation is used, special consideration must be paid to ARP and routing-table entries, and anti-spoofing issues.

ARP

When automatic NAT rule creation is used, Check Point NGX makes all necessary adjustments to the Security Gateway's ARP table. If Manual NAT rule creation is used, the Security Administrator must edit the Security Gateway's ARP table, as follows:

Dynamic NAT, Security Gateway in Translated Packet, Source field — No additional ARP table entries are required.

Dynamic NAT, hiding behind an IP address not assigned to the Security Gateway — Add an ARP table entry to the Security Gateway for the hiding address.

Static NAT — Add ARP table entries to the Security Gateway for all hiding addresses.

For information creating persistent ARP table entries, consult your OS documentation.

