NOKIA

A Practical Look at Network Address Translation

A Nokia Horizon Manager White Paper

Part No. WP0018 Rev A

Published November 2003

COPYRIGHT

RESTRICTED RIGHTS LEGEND

IMPORTANT NOTE TO USERS

This software and hardware is provided by Nokia Inc. as is and any express or implied warranties, including, but not limited to, implied warranties of merchantability and fitness for a particular purpose are disclaimed. In no event shall Nokia, or its affiliates, subsidiaries or suppliers be liable for any direct, indirect, incidental, special, exemplary, or consequential damages (including, but not limited to, procurement of substitute goods or services; loss of use, data, or profits; or business interruption) however caused and on any theory of liability, whether in contract, strict liability, or tort (including negligence or otherwise) arising in any way out of the use of this software, even if advised of the possibility of such damage.

Nokia reserves the right to make changes without further notice to any products herein.

TRADEMARKS

030114

Nokia Contact Information

Corporate Headquarters

Web Site	http://www.nokia.com
Telephone	1-888-477-4566 *or* 1-650-625-2000
Fax	1-650-691-2170
Mail Address	Nokia Inc. 313 Fairchild Drive Mountain View, California 94043-2215 USA

Regional Contact Information

Americas	Nokia Inc. 313 Fairchild Drive Mountain View, CA 94043-2215 USA	Tel: 1-877-997-9199 Outside USA and Canada: +1 512-437-7089 email: ipsecurity.na@nokia.com
Europe, Middle East, and Africa	Nokia House, Summit Avenue Southwood, Farnborough Hampshire GU14 ONG UK	Tel: UK: +44 161 601 8908 Tel: France: +33 170 708 166 email: ipsecurity.emea@nokia.com
Asia-Pacific	438B Alexandra Road #07-00 Alexandra Technopark Singapore 119968	Tel: +65 6588 3364 email: ipsecurity.apac@nokia.com

Nokia Customer Support

Web Site:	https://support.nokia.com/		
Email:	tac.support@nokia.com		
Americas		**Europe**	
Voice:	1-888-361-5030 or 1-613-271-6721	**Voice:**	+44 (0) 125-286-8900
Fax:	1-613-271-8782	**Fax:**	+44 (0) 125-286-5666
Asia-Pacific			
Voice:	+65-67232999		
Fax:	+65-67232897		

031014

Network Address Translation

Network Address Translation (NAT) is a technology that is useful to many network administrators because it saves time and money when dealing with network IP addresses. NAT allows a single network device, such as a router or firewall, to act as an agent between the public network space and a private network space. The NAT-enabled agent makes it possible to use a single IP address to represent an entire group of networked computers. NAT also helps network administrators manage the private and public portions of their network because with NAT, administrators can separate the private and public address spaces. The address separation means that NAT makes the physical device in the private network independent of the IP address hosts in the public network. NAT is defined in RFC 3022 [1].

With NAT, an enterprise does not need to register large, expensive IP address blocks from InterNIC. Since address blocks are a limited resource, network address space might not even be available.

Although NAT prevents hosts in the public network from seeing any internal IP addresses, NAT is not a method of securing the private network. At best, NAT can hide, or obscure, network devices. For a network to be secure, you must at least have a firewall at the border of your network.

RFC 1918 [2] describes address allocation for private internets. The authors of this RFC wanted to address “the proliferation of TCP/IP technology worldwide, including outside the Internet itself,” since “an increasing number of non-connected enterprises use this [TCP/IP] technology and its addressing capabilities for sole intra-enterprise communications, without any intention to ever directly connect to other enterprises or the Internet itself.” Essentially, the available IPv4 address space was on the verge of being exhausted in the mid 1990s, but organizations still needed address blocks for their private network spaces. The address blocks listed in Table 1 are reserved for private address space and are not routable on the backbone network.

Table 1 RFC 1918 Freely Available Address Blocks

Address range	CIDR notation
10.0.0.0 - 10.255.255.255	10/8
172.16.0.0 - 172.31.255.255	172.16/12
192.168.0.0 - 192.168.255.255	192.168/16

Classless Inter-Domain Routing (CIDR) is an IP addressing scheme that allocates blocks of Internet addresses to allow summarization into a smaller number of routing table entries. CIDR is defined in RFC 1520 [3].

The first address block is a 24-bit block, the second block is a 20-bit block, and the third is a 16-bit block. In pre-CIDR notation, the first block is nothing but a single class A network number, the second block is a set of 16 contiguous class B network numbers, and the third block is a set of 256 contiguous class C network numbers.

Any enterprise that uses IP addresses from the address space defined in RFC 1918 can do so without contacting or paying IANA (Internet assigned numbers authority) or an Internet service provider. Addresses within the private address space are only unique within an enterprise or multiple enterprises that choose to cooperate over this space to communicate with each other in their own private internet.

Static and Dynamic Network Address Translation

Network address translation is categorized into the following general types:

- Static NAT maps a private address to a public address in a one-to-one relationship.
- Dynamic NAT maps a private address to a public address on an as-needed basis.

Dynamic NAT has many subsets. This document concentrates on the dynamic NAT subset called hide NAT, which is the primary dynamic NAT mechanism that the Check Point FireWall-1 application uses. Hide NAT maps all specified private addresses to a single public address. Both static and dynamic NAT affect the services available in the private network from the public network.

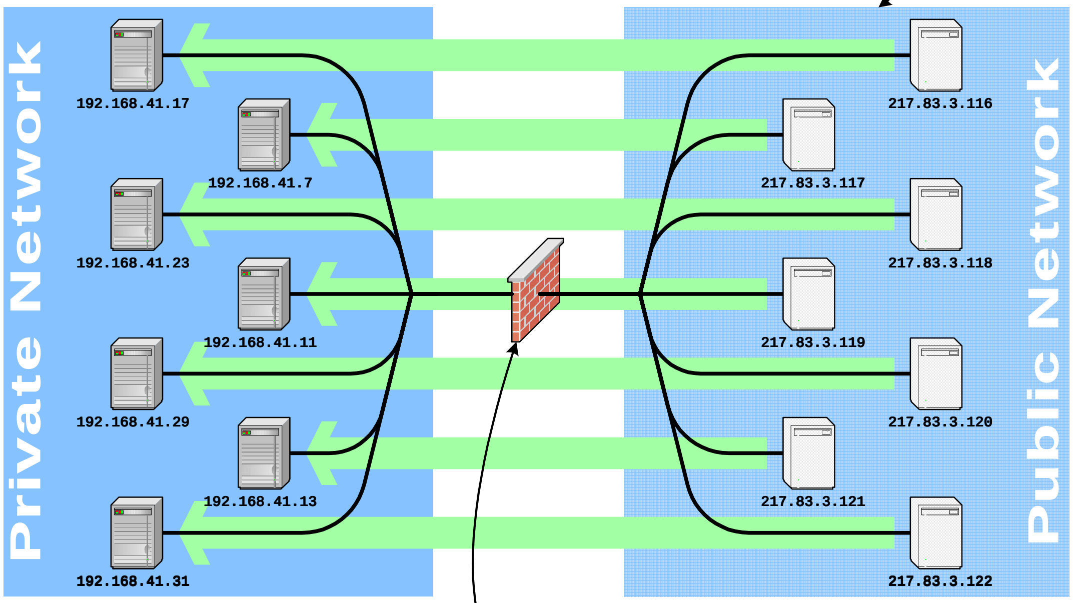
Static NAT

Static NAT (also called inbound mapping) maps a single private network address, which is typically the address of a network server, to a single public network address. Static NAT allows hosts outside of the private network to use a public IP address to access hosts on a private network. Static NAT is a potential security risk. If the network security policy is configured incorrectly, the private network device mapped to the public IP address might be fully exposed to the public network.

Figure 1 illustrates several network servers located on a private network space that have public addresses associated with them through static NAT at the border firewall.

Figure 1 Static NAT Topology Example

These network devices do not physically exist. They are present on the public network by virtue of the Firewall/Router responding to connection requests for these servers and then routing the connection to the appropriate network device in the private network space.

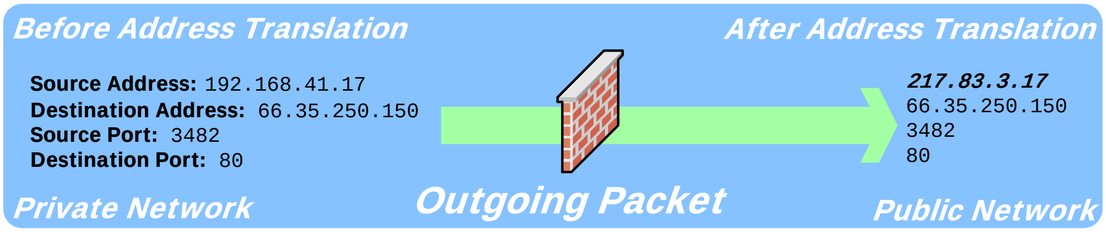


The border Firewall/Router translates the network address of selected network devices. The Firewall/Router responds to a request from the public network for a NAT'd network device and routes the network connection to the correct device. The is an example of Static NAT and demonstrates the one-to-one relationship of this NAT type.

All address translations take place within the policy enforcement point, and the translation process is transparent to both internal and external entities. When hosts from the public network try to contact private network hosts, the packets are either dropped or forwarded to the internal hosts, depending on the security policy.

For an outgoing network transaction, such as in Figure 2, the only change to the packet is the source address, which is translated to the public network address for the shared network device. The destination address, source port, and destination port are not modified.

Figure 2 Static NAT for Outgoing Packets

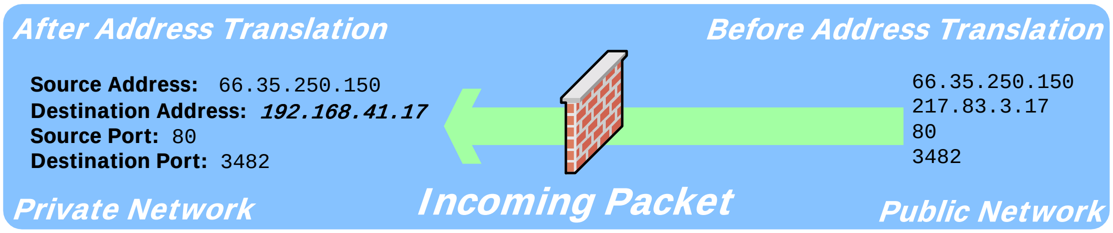


Source Address: 192.168.41.17
Destination Address: 66.35.250.150
Source Port: 3482
Destination Port: 80

217.83.3.17
66.35.250.150
3482
80

For an incoming network transaction, the only change to the packet is the destination address, as shown in Figure 3. The NAT agent on the enforcement point changes the destination address from the public network address to the address that corresponds to the statically translated network device. The source address, source port, and destination port do not change.

Figure 3 Static NAT for Incoming Packets


After Address Translation
Before Address Translation
Source Address: 66.35.250.150
Destination Address: 192.168.41.17
Source Port: 80
Destination Port: 3482
66.35.250.150
217.83.3.17
80
3482
Private Network
Incoming Packet
Public Network

The enforcement point uses a proxy address resolution protocol (ARP) technique to respond to the request for the addresses that use static NAT. One network device, such as a firewall, responds to ARP requests intended for another network device. By impersonating the identity of the targeted network device, the firewall accepts responsibility for routing packets to the true destination.

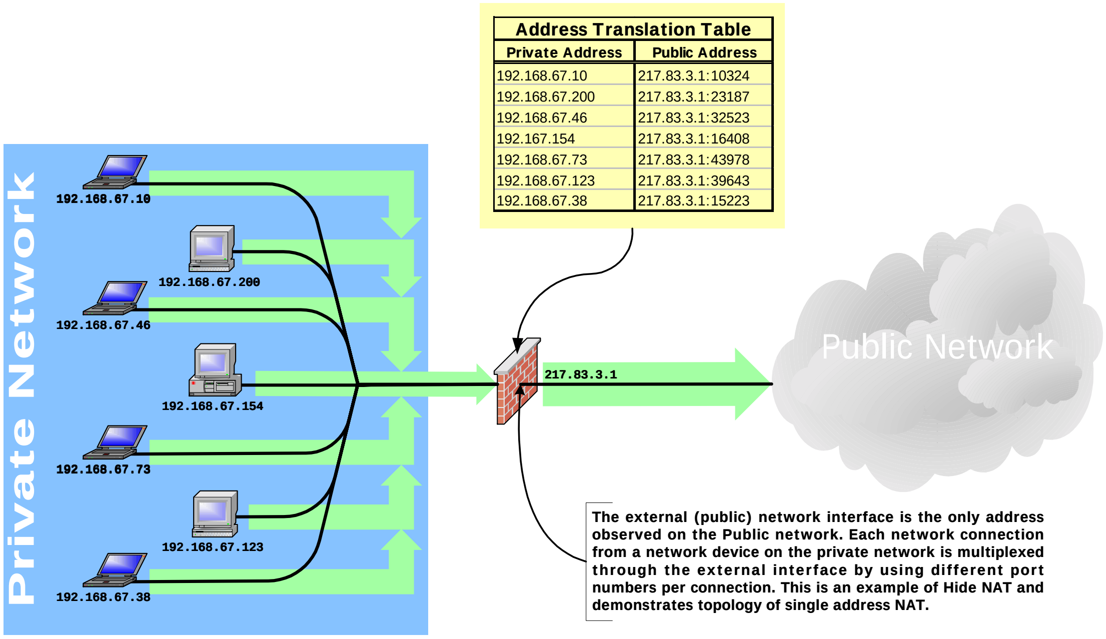
Hide NAT

Hide NAT is a type of dynamic NAT that uses different network source ports to map multiple private addresses to a single public address. This type of address mapping is also known as:

- IP masquerading
- Port address translation
- Single address NAT
- Port-level multiplexed NAT

Regardless of the name, in this type of address mapping, the mapping is not static. In hide NAT, for each session between an internal network device and the public network, the public IP address remains the same, but the source port for each device changes. Figure 4 provides an overview of a network topology that uses hide NAT. The figure also shows an example of the address translation table.

Figure 4 Hide NAT Topology Example



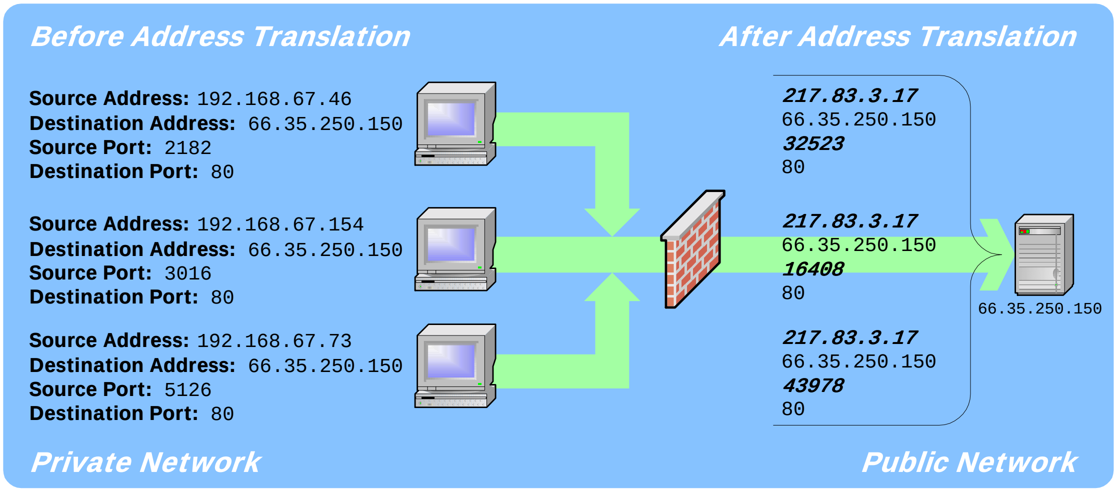
Address Translation Table	
Private Address	**Public Address**
192.168.67.10	217.83.3.1:10324
192.168.67.200	217.83.3.1:23187
192.168.67.46	217.83.3.1:32523
192.167.154	217.83.3.1:16408
192.168.67.73	217.83.3.1:43978
192.168.67.123	217.83.3.1:39643
192.168.67.38	217.83.3.1:15223

The external (public) network interface is the only address observed on the Public network. Each network connection from a network device on the private network is multiplexed through the external interface by using different port numbers per connection. This is an example of Hide NAT and demonstrates topology of single address NAT.

With hide NAT, address translations do not exist in the NAT table of the enforcement point until the enforcement point receives traffic that requires translation. Dynamic translations also have a timeout period. When the period ends, the translations are purged from the translation table, which makes them available for other internal addresses. The timeout period is different for each transport protocol (TCP or UDP) and NAT device.

For a network connection, the Check Point VPN-1/FireWall-1 application changes the source TCP or UDP port of the packet so that it can track the client server traffic throughout the life of the connection more effectively, as shown in Figure 5.

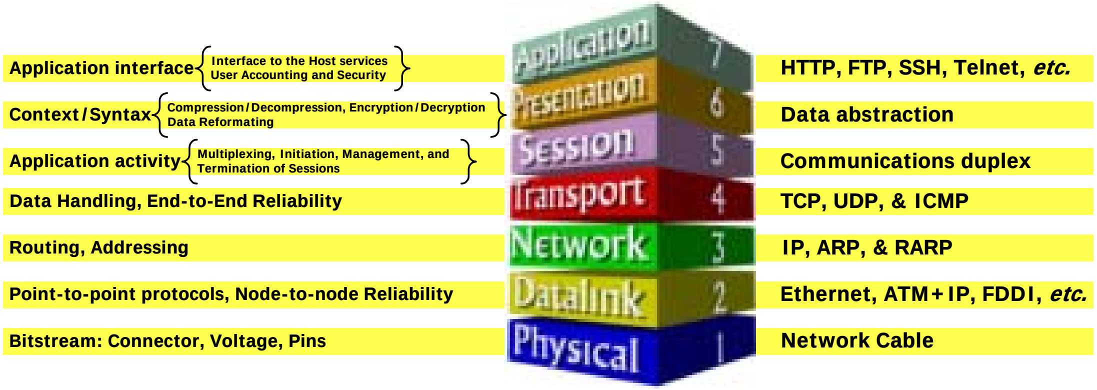
Figure 5 Hide NAT Overloaded Network Connection



NAT As a Proxy

NAT operates at the network layer (layer three) of the OSI network model, which is shown in Figure 6. Since NAT operates below layer four of the OSI model, it is a *fundamental* proxy. A fundamental proxy has no cache, and its only function is to take a network connection and transparently pass it from one side of the network to another.

Figure 6 OSI Reference model


Application interface
Interface to the Host services
User Accounting and Security
Context/Syntax
Compression/Decompression, Encryption/Decryption
Data Reformating
Application activity
Multiplexing, Initiation, Management, and
Termination of Sessions
Data Handling, End-to-End Reliability
Routing, Addressing
Point-to-point protocols, Node-to-node Reliability
Bitstream: Connector, Voltage, Pins
Application 7
Presentation 6
Session 5
Transport 4
Network 3
Datalink 2
Physical 1
HTTP, FTP, SSH, Telnet, etc.
Data abstraction
Communications duplex
TCP, UDP, & ICMP
IP, ARP, & RARP
Ethernet, ATM+IP, FDDI, etc.
Network Cable

A proxy is any device that acts on behalf of another device. For example, a Web proxy acts on behalf of a Web server. Network clients make a requests to the Web proxy, and the Web proxy makes requests to the appropriate Web server on behalf of the network client. The advantage of having a proxy is that the Web proxy can cache commonly accessed sites locally. Local caching reduces outbound traffic, which increases the performance to the Web user.

Unlike a NAT agent, a Web proxy is not a fundamental proxy because it operates at layer four, the transport layer. A Web proxy is more complex than the type of proxy involved with NAT. The Web proxy is not transparent and must be explicitly supported by the clients it represents. The network administrator must configure each client to use the correct proxy. Whenever the configuration changes, the network administrator must reconfigure every client. Also, the proxies that operate at layer four and above are typically slower than fundamental proxies.

Client-Server Communication Through NAT

Nokia Horizon Manager v1.3 uses a client-server architecture that allows the administrator to centralize and secure the server and still maintain a flexible client deployment. Table 2 lists the network protocols that the Nokia Horizon Manager v1.3 client uses to communicate with the Horizon Manager v1.3 server.

Table 2 Nokia Horizon Manager v1.3 Client and Server Network Ports

Port name	Port number	Description
RMI_Server_port	1200/tcp	Client to server communications port
RMI_Server_port	1201/tcp	Server to client communications port
RMI_Registry_port	1210/tcp	RMI registry port
SSL_Server_port	2016/tcp	SSL key exchange port

Table 3 lists the network protocols that the Nokia Horizon Manager v1.3 server uses to communicate with the managed network devices.

Table 3 Nokia Horizon Manager v1.3 Server and Managed Network Device Protocols

Port name	Port number	Description
Secure shell	22/tcp	Secured managed device communication (ssh and scp)
http	80/tcp	Voyager (unsecured) device access
https	443/tcp	Voyager (secured) device access
ftp	20/tcp, 21/tcp	Unsecured file transfer communication
Telnet	23/tcp	Unsecured managed device command line access

Nokia Horizon Manager is an application that manages network policy enforcement points. All of the network devices that Horizon Manager manages should have routable, or at least reachable, IP addresses. Moreover, the network protocols listed in Table 3 are common network services and are typically allowed on the private network. The network protocols are required for Horizon Manager to manage the network devices.

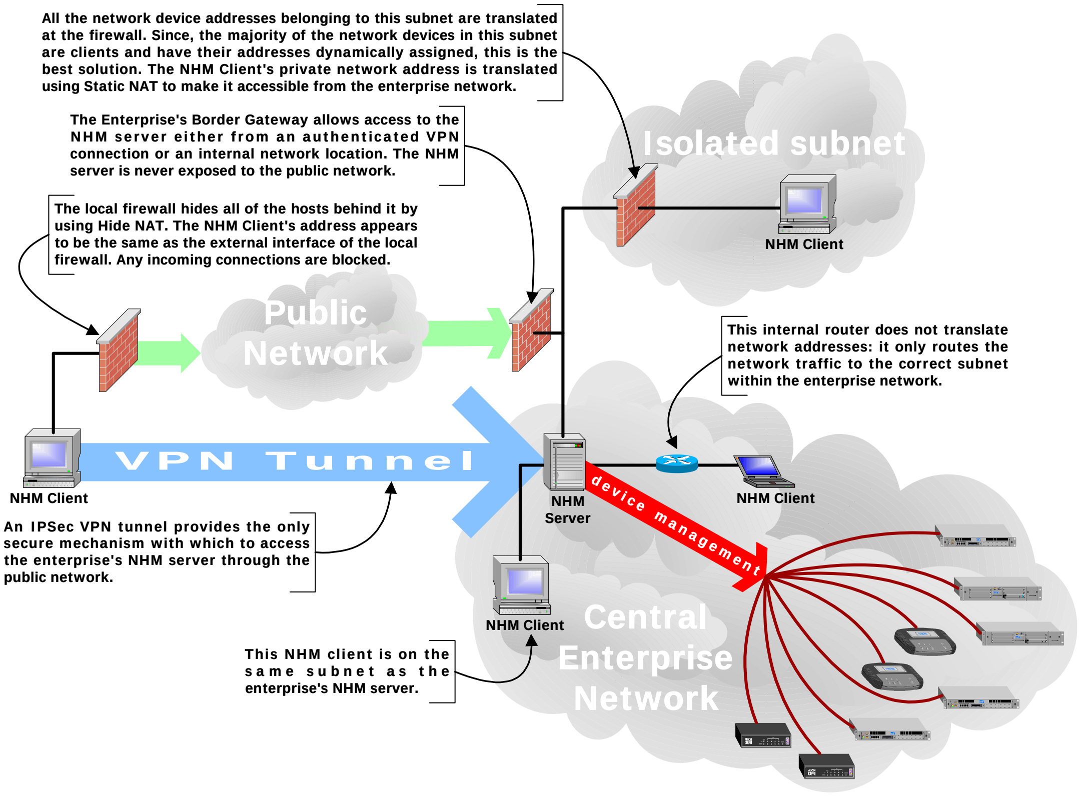
You must add the four network protocols listed in Table 2 to any security policy at intervening policy enforcement points. The RMI_Server_port protocol is a bidirectional communication mechanism, while the RMI_Registry_port and SSL_Server_port network protocols are mono-directional (client to server only). This means that the client or the server can both initiate network communication for the Horizon Manager application.

Note
Communication between the Horizon Manager client and the server is not possible if any intervening gateway uses hide NAT to mask network addresses.

Figure 7 illustrates several potential Horizon Manager client locations with respect to the Horizon Manager server and NAT gateways. The basic configuration has two Horizon Manager clients within the central enterprise network. One Horizon Manager client is on the same subnet as the Horizon Manager server. As long as the enterprise name server can resolve the host names for the Horizon Manager client and the Horizon Manager server, the client-server pair can communicate.

In Figure 7, there is also a Horizon Manager client behind an internal router in the central enterprise network. Since the internal router does not translate addresses or block any network traffic, the Horizon Manager client and the Horizon Manager server can communicate. Again, the enterprise name server must be able to resolve the host names for the Horizon Manager client and the Horizon Manager server to authenticate each other.

Figure 7 Horizon Manager Client Connections to the Server Through Different NAT Conditions



All the network device addresses belonging to this subnet are translated at the firewall. Since, the majority of the network devices in this subnet are clients and have their addresses dynamically assigned, this is the best solution. The NHM Client's private network address is translated using Static NAT to make it accessible from the enterprise network.

The Enterprise's Border Gateway allows access to the NHM server either from an authenticated VPN connection or an internal network location. The NHM server is never exposed to the public network.

The local firewall hides all of the hosts behind it by using Hide NAT. The NHM Client's address appears to be the same as the external interface of the local firewall. Any incoming connections are blocked.

This internal router does not translate network addresses: it only routes the network traffic to the correct subnet within the enterprise network.

An IPSec VPN tunnel provides the only secure mechanism with which to access the enterprise's NHM server through the public network.

This NHM client is on the same subnet as the enterprise's NHM server.

Another Horizon Manager client in Figure 7 is in an isolated subnet outside of the central enterprise network, but within the enterprise. This subnet contains dynamically assigned RFC 1918 addresses for all the desktop workstations within the subnet. To prevent address collisions with any other part of the enterprise network, the firewall in the subnet uses hide NAT to mask all addresses behind the network interface of the firewall that faces the enterprise.

Hide NAT at the subnet firewall prevents the Horizon Manager client from communicating with the Horizon Manager server. More importantly, hide NAT prevents the Horizon Manager server from connecting to the Horizon Manager client (RMI_Server_port, 1201/tcp). To allow communication between the client and server, you must configure the firewall to statically translate the address of the Horizon Manager client in the isolated subnet.

The Horizon Manager client located outside of the enterprise network requires a VPN tunnel to securely communicate with the enterprise Horizon Manager server. To remain secure, the enterprise Horizon Manager server should never be exposed to the public network. Even though all communication between the Horizon Manager server and any Horizon Manager client is encrypted (128-bit SSL), if hosts on the public network can see the Horizon Manager server, the server becomes a potential target for attack.

If the gateway at the remote site uses hide NAT for the hosts behind it (for example, to maximize network resources), the gateway might drop the Horizon Manager communication protocols. Any gateway between the Horizon Manager client and Horizon Manager server that uses hide NAT blocks Horizon Manager server-to-client communication. When the Horizon Manager client and server communicate through an IPSec VPN tunnel rather than over the public network, the communication is secure, and the traffic between the client and the server is not dropped by any gateways.

Summary

One of the most important reasons to use NAT is that it simplifies network administration. NAT gives you flexibility in assigning internal network IP addresses since it allows you to separate public network spaces from private network spaces. For example, if you move a Web server or FTP server to another host, you only need to change the address mapping at the firewall to reflect the new host. Also, if you make changes to the internal network, you do not need to reconfigure the IP address for each host because the public IP address for each device in the internal network either belongs to the firewall or is associated with external network interface of the firewall.

NAT is also cost-effective. The non-public routable address blocks defined in RFC 1918 can be reused repeatedly without an associated registration cost. With hide NAT you can use a single network device to provide network access for nodes within a private network space.

When you use NAT, make sure you do not block client-server communication for applications like Horizon Manager v1.3.

While NAT is practical, you should never use it as a method to secure a private network. NAT is only capable of hiding network devices, not securing them. The first step in securing the network is to put a firewall at the border of the network.

References

1. RFC 3022: “Traditional IP Network Address Translator (Traditional NAT),” P. Srisuresh, K. Egevang. January 2001. (Obsoletes RFC1631).
2. RFC 1918: “Address Allocation for Private Internets,” Y. Rekhter, B. Moskowitz, D. Karrenberg, G. J. de Groot, E. Lear. February 1996. (Obsoletes RFC1627, RFC1597).
3. RFC 1520: “Exchanging Routing Information Across Provider Boundaries in the CIDR Environment,” Y. Rekhter, C. Topolcic.