Global Information Assurance Certification Paper

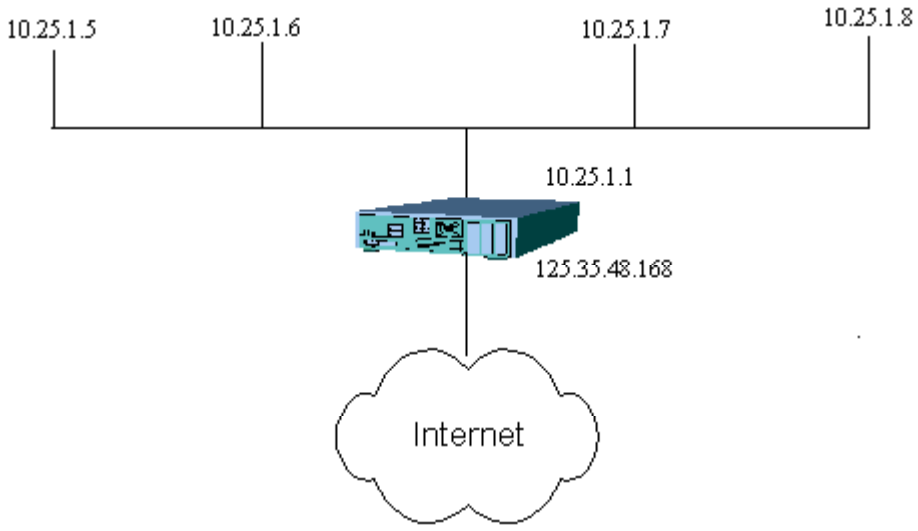
Network Address Translation
Bryan McLaughlin
September 10, 2000

What is Network Address Translation

Network Address Translation (NAT) is a routing scheme devised to provide an immediate solution to the world shortage of Internet Protocol addresses (IP addresses), as well as address network security, and facilitate the ease and flexibility of network administration. In a nutshell, NAT provides a means for privately addressed networks to connect to public networks such as the Internet.

NAT is not a new concept, as the RFC was written in 1994. NAT has gained more popularity recently with the explosion of the Internet and scarcity of registered address classes.

NAT is the translation of an IP address used within one network to a different IP address known within another network. This is easier to understand by referring to the following diagram:



The NAT enabled router has an IP address of 10.25.1.1 for the inside network and an address of 125.35.48.168 for the outside network. Anytime a host on the inside network (10.25.1.0) makes a request to the outside network (the Internet in this instance) NAT will translate the 10.25.1.0 address to 125.35.48.168. From the inside looking out, the machines can access any host on the external network directly, while from the outside looking in it appears that all in and outbound traffic is originating from the single IP address on the router.

How does NAT work

NAT starts by setting up an internal translation table of all inside IP addresses that will be sending packets through the NAT enabled router. Next it sets up a table of port numbers to use on the outside IP addresses. When the inside network sends packets to the outside network the NAT router performs the following steps:

1. It records the source IP address and source port number in the appropriate translation table.

2. It replaces the IP address of the packet with its own (outside) IP address.

3. It assigns a specific port number to the outgoing packet, enters that into the translation table, and replaces the source port number with this.

4. It recalculates the IP and TCP checksums and verifies for integrity.

5. It must also convert any application packet that contains reference to the inside IP address that is being translated, to reference the new, outside IP address.

When the response packet comes back to the NAT enabled router, it checks the packet's destination port number. If this matches a source port number assigned in the translation table, it finds the inside IP source address that was assigned this port number. When it finds a match it rewrites the destination port number and IP address with the original source IP and port used for the packet on the inside that initiated the connection. Then it transmits the packet to the inside host for which it was intended.

There are two modes of NAT; static NAT, and dynamic NAT. In static NAT, the IP addresses on the inside network are mapped on a one-to-one basis with IP addresses on the outside network. Dynamic NAT uses a single IP address on the outside network. Each variation has its specific advantages and disadvantages but for this article they are outside the scope and will not be discussed.

Security Implications of using NAT

Many people forget that the Internet introduces serious threats to anyone who connects to it. The Internet is non-discriminatory; hackers, crackers, and script kiddies will probe any and all computers connected to the Internet regardless of the nature of the connection or sensitivity of the information on the connected device.

An adage about the Internet that is misunderstood or simply unknown is "*when you connect to the Internet the Internet is connected to you"*. This simply means that when you are connected to the Internet, any user on the net can connect to your system. This is a scary thought, now throw in the increasing popularity of high speed, "always on",

Internet connections and the level of concern multiplies.

Many companies rely on firewalls to defend against the threats of the Internet. Firewalls are devices that monitor network traffic and determine based on destination IP, source IP, destination port number, source port number, or other header information which traffic will be allowed to pass through the firewall and into the inside network. The main disadvantage to firewalls is that the rule sets that dictate passage are difficult to write and maintain. Most home users and small businesses do not have the expertise or time to setup and maintain a secure firewall. A poorly maintained firewall provides a false sense of security and almost guarantees a break-in.

NAT can provide the same level of protection as a firewall at a reduced cost and requiring far less technical expertise. NAT provides network security as a by-product of the translation process. Through translation, NAT hides the internal network IP addresses so that external parties only see the external address. Since the actual IP addresses of hosts on the inside network are never broadcast externally there is nothing to hack or spoof.

NAT supports the concept that it is much easier to guard a single point of entry than it is to guard many points of entry. Properly written address translators make it impossible for a person on the outside to mount an attack against inside hosts without first compromising the NAT router itself. Hence, it is easier to protect the NAT router than the entire network.

Ease of Network Administration

NAT can greatly ease the administration of a network in that it allows for unlimited growth as the non-routable address schemes can be used on the inside network, companies do not have to try to conserve address space or attempt to purchase additional address space. NAT also assists in connecting disparate networks. If your company merges with another, NAT can be used to facilitate the communication between the two networks. NAT can even be used to connect two networks that use the same IP addressing schemes (i.e. both networks use the 10.2.1.0 address space).

Conclusion

As I have shown, Network Address Translation can ease burden of the scarcity of registered IP addresses by allowing organizations to use the non-routable addresses on their inside networks. NAT also provides firewall like security by hiding the inside network and disallowing any unwanted connections. NAT can also ease network administration by allowing greater flexibility for growth and the connection of foreign networks.

References

"Network Address Translation."
URL: http://www.vicomsoft.com/knowledge/reference/nat.html

Egevang K., Francis P., "The IP Network Address Translator (NAT)" RFC 1631, May 1994. URL: ftp://ftp.rfc-editor.org/in-notes/rfc1631.txt

"Network Address Translation White Paper."
URL: http://work.home.net/whitepaper/natwpaper.html

Mittelstaedt, Ted. "Network Address Translation." The Network Community, August 1997. URL: http://www.computerbits.com/archive/9708/lan9708.htm

Vepstas, Linas. "Linux Network Address Translation." November 1998.
URL: http://linas.org/linux/load.html