Security Considerations Of NAT

Network Address Translation (NAT) is a technology whereby an edge router translates a set of internal addresses into a single exterior facing address. The most common use of NAT is to conserve public address space by assigning "non-routable" RFC 1918 addresses (10/8, 172.16/12, & 192.168/16) behind a NAT device. These addresses are not routable across the Internet but are within an organization's boundary. When working as expected, the internal hosts are not directly addressable from unsolicited connections outside of the NAT device. While NAT does have a useful purpose, it is too often incorrectly regarded as a security feature. ITSS and ITCom do not recommend using NAT as a network protection mechanism.

Deployment

NAT does not have a clearly defined failure mode. If the device is improperly configured or unexpectedly fails, there is no guarantee that internal hosts will not be reachable by a savvy attacker. Many early implementations of NAT were vulnerable to this sort of direct addressing by a network-adjacent attacker. Specifying the destination MAC address of an internal host, the NAT device would forward the packet without asking any questions.

Since NAT is often deployed in conjunction with a firewall, the features offered by each are often blurred. A firewall gives fine-grained access control to the internal hosts and has a very clear "fail-closed" mode. Firewalls are designed to block network traffic, NAT acts only as a translator. As such, firewalls offer real network security benefits that NAT does not. In most cases a firewall without NAT has all the security properties and flexibility a network needs.

Information Gathering

Contrary to popular belief, NAT does not necessarily hide the identity of hosts behind it. Using passive analysis of TCP/IP and application-layer protocols, it's possible to gain very detailed information about the internal network. Subtleties in the TCP/IP stack allow anyone who can see external traffic to fingerprint the operating systems of internal hosts. Differences in initial TCP sequence numbers, IP options, and IP IDs are more than enough information to enumerate hosts on the internal network. NAT only superficially hides internal hosts.

Beyond gaining information about the operating systems in use behind the NAT device, a savvy attacker can also deduce the internal network architecture. Since NAT only operates at the IP level, an attacker could use low IP time-to-live values to solicit ICMP TTL Exceeded messages and gain detailed information about the internal routing infrastructure. Using these techniques, an attacker can gain almost as much information as if there was no NAT device.

Side-Effects

Because NAT compartmentalizes an entire network, debugging network problems and investigating security incidents becomes more difficult. In the case of a large network with a centralized monitoring

facility such as the University, this is a significant problem. For instance, UMNet's Hackfinder scripts use packet header data at the border routers to heuristically determine compromised hosts. With NAT in place, the actual source of the infection is impossible to determine since an entire network appears to be one source IP address. In this case, real-world functionality is lost.

NAT significantly complicates network configuration. The classic example is the "double NAT" problem -- how do you connect two hosts each behind NAT? Port-forwarding is a solution, but in a large environment, it has its own problems. If you have NAT configured to use one external address you are limited to one service per well-known port. For instance, you'd only be able to run one web server from port 80 since it can only be forwarded to one host. NAT significantly reduces the flexibility of your network.

Many network protocols operate bidirectionally, notably FTP. When a host connects to a FTP server and retrieves a file, it is transferred across a separate TCP connection that is initiated from the server. When the client is behind NAT, the NAT device must watch the FTP connection for signs that the new connection is about to be created and retranslate it to the appropriate host. The NAT device must explicitly support each bidirectional protocol that is required, commonly FTP, H.323, SIP, IPSEC, and IRC.

Deploying NAT also reduces VPN configuration options. Connecting two NAT installations which both use private addresses becomes exponentially more difficult if the address spaces overlap. An internal host would not know whether the address 10.0.0.1 is local or remote. If a subset of hosts using NAT wish to use a VPN, NAT traversal (NAT-T) is required.

Using NAT with routable address space still exhibit most of these problems.

Conclusions

The well-known security adage "security through obscurity is no security at all" is certainly applicable to NAT. IPv6, whose biggest initial win is a significant increase of address space, has no concept of NAT since no additional security is gained. In a significantly large network environment, NAT creates more problems than it solves. NAT multiplies the level of complexity to any network. With only one real benefit, it's difficult to justify the return on investment of deploying NAT. Consider the ramifications to the current and potential network architecture when evaluating NAT.

As such, ITSS and ITCom only recommend deploying NAT when there are no alternatives available. A network with public addresses protected by a firewall satisfies all the concerns addressed above while maintaining a secure environment.

Resources

- Private IP Network Numbers
    - http://www.itcom.itd.umich.edu/backbone/umnet/privateIP.html
- UMnet Administration - Hackfinder Information
    - http://www.itcom.itd.umich.edu/backbone/umnet/Hackfinder.html
- NHS Information Authority Statement on Network Address Translation and Private Addressing in the NHSnet

  - http://www.nhsia.nhs.uk/nhsnet/pages/connecting/ipaddresses/network_address_translation_and_private_addressing.pdf

- RFC 1631 - The IP Network Address Translator (NAT)
  - http://www.rfc-editor.org/rfc/rfc1631.txt
- RFC 1918 - Address Allocation for Private Internets
  - http://www.rfc-editor.org/rfc/rfc1918.txt
- RFC 2775 - Internet Transparency
  - http://www.rfc-editor.org/rfc/rfc2775.txt
- RFC 2993 - Architectural Implications of NAT
  - http://www.rfc-editor.org/rfc/rfc2993.txt
- IPsec-NAT Compatibility Requirements
  - http://ftp.ist.utl.pt/pub/drafts/draft-aboba-nat-ipsec-04.txt
- The Trouble with NAT
  - http://www.cisco.com/en/US/about/ac123/ac147/ac174/ac182/about_cisco_ipj_archive_article09186a00800c83ec.html
- IPSec NAT-T is not recommended for Windows Server 2003 computers that are behind network address translators
  - http://support.microsoft.com/?kbid=885348
- Security gateway and 6bone connection
  - http://www.kame.net/newsletter/19990706/
- A Technique for Counting NATted Hosts
  - http://www1.cs.columbia.edu/~smb/papers/fnat.pdf
- Passive OS Fingerprinting
  - http://lcamtuf.coredump.cx/p0f.shtml