GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

Network Address Translation – A real solution?

Rafael Garcia

April 2, 2001.

Abstract

NAT has been considered as one of the common methods to hide real IP addresses and ports to the public area. There exist a hidden cost to use this technology method in the functionality of certain technologies, and may vary depending on the NAT environment used.

This document tries to explain the different methods used by NAT (traditional NAT, bi-directional NAT, Twice NAT and NAPT), the limitations, and the possible solutions (ALG-Application Level Gateways) to keep them functional and secure.

Introduction

Imagine the world with a worldwide network where every imaginable application can be shared on line. It's name: Internet. But this dream comes with a possibility of compromising confidence, availability and integrity. This is when talk about Security is required.

Security must cover not only protection of environment, but also deployability, solving problem orientation and suitability to the Internet environment.

We know the origin of Internet, and we know that it never had planned to be a secure network since 1969 when Arpanet appeared. The new tasks for improve security as well as better functionality for Internet made in 1991 contained in RFCs 1883-1886, and accepted into the Internet Standards Track until ending 1995, better know as Ipv6 still being as a new dream an costly away to an immediately implementation, so we still needing the effectiveness of the security tools around our all dream.

NAT Environments

Basically NAT (RFC 1631) is a routing scheme connecting Intranet and Internet in a transparent way. This basic idea is applied due to the lack of IP address available after the big explosion of Internet and also used as one-way traffic filter, restricting sessions from externals to see the internal devices.

RFC 2663 specify the four NAT common environment configurations. With traditional NAT, the session is initiated only by the internal host, which goes only unidirectional to the outside host.

A bi-directional NAT server (or two-way NAT), use a DNS application level gateway (ALG) to do translations from name to IP addresses and TCP/UDP mappings. In this scheme, fully qualified names from hosts in the private and public networks are assumed as unique side to side. So once a connection is established in either side, NAT is available to map the private network address to a globally unique address in a static or dynamic way, allowing inbound and outbound sessions.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Twice NAT modifies source and destination addresses for packets in a NAT session. This method is basically used when conflicts in the address space occurs for both source and destination network address. In addition to the translation of source address for outbound packets, the NAT server maps the external network host's registered IP address to another unique private IP address.

The last method in this article will be NAPT (Network address and port translation), which translate source, destination ports and checksum values in TCP/UDP headers. NAPT allows NAT servers to modify the transport identifiers in a way that is transparent for upper layers. The biggest issue of this method is when IP payload and port is encrypted, so there is no way to decrypt the payload by the NAT server.

Limitations.
Unfortunately not all the applications works transparently with NAT, and also those carrying IP addresses and TCP/UDP port information inside their payloads must use ALGs for both inbound and outbound sessions. One of the first applications that fail to use NAT is the authentication packets used by some existing security protocols.

Another immediate limitation is related to the layer in which NAT is working. If we are taking the translation in the network and transport layer, once NAT does the change in addresses and ports it has to recalculate the checksum in the packet header. This means if you are using encryption there will be problems using signed or modification-proof function.

For example, IPSec (RFC 2401,2402,2406) uses two mechanisms in the header. One is used to ensure data integrity (AH- authentication header), and one for encapsulating (ESP- encapsulating security payload). Neither NAT nor ALG can translate in this condition, because there is no way to build again the AH, due to there is no way to decrypt the secret source and destination hosts once the modification take place.

IPSec has two ways to handle key exchange and management: manual and automated keying. The most required protocol for on-demand creation of a security association (SA) for automated key is the IKE (Internet Key Exchange). An SA and IPSec are used together to create the algorithms and the key exchange method to encrypt source and destination end points, and for this reason NAT cannot modify such values.

An alternative to IKE is simple key management for IP also knew as SKIP (RFC 2409). This is basically used as encryption method for VPN. SKIP uses packet-oriented keys transmitted in-line. As consequence NAT can translate the IP header with no issues, but if you are using NAPT then it is impossible to translate the payload because it is encrypted.

In socket layer protocols like Secure Socket Layer (SSL) and Transport Layer Security (TLS), encapsulates the transport layer for programming and manages a logical connection between two endpoints to simplify access to underlying layers. These protocols are designed to provide end-to-end security over Internet.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

SSL intercepts messages transmitted from the application layer and fragments them into blocks. Then compress the data before applying the message authentication code, encrypts the messages and transmit the result to the transport layer. So on SSL doesn't use IP or port to verify the message, and then is transparent for NAT and NAPT.

TLS is considered the successor of SSL. It verifies user identification without depending on IP or Port information, which let it pass through NAT and NAPT.

Protocols such RPC uses three different UDP ports to set up a session, and the packets exchanged between the RPC client and server during the setup process contain IP address and port information. As a result, protocols that utilize RPC will have an underlying layer fail when using NAT.

Regarding voice over IP, H.323 uses multiple control sessions to negotiate the IP addresses and port numbers for successive H.235 authentication and real-time audio and video sessions. When passing through NAT server, the successive session fail because the server doesn't know the payload (encoded), which include addresses and port numbers.

The session initiation protocol (SIP) and media gateway control protocol (MGCP) are key application layer protocols for voice over IP. Both use the session description protocol (SDP) to derivate the real-time transport protocol (RTP) address and port number for voice communication, in consequence the same effect from H.323 is present in these cases.

Popular protocols like SMTP and POP3, can work in a NAT environment because they don't include IP addresses in the data payload. But, version four of the Internet message access protocol (IMAP4) uses an authentication mechanism like Kerberos and S/key for accessing e-mail or bulletin boards for mail servers. In this case, like IP address and port information is not contained in that process then NAT works fine if the authentication servers are in the public side.

Finally, FTP doesn't work in a traditional NAT or NAPT environment, although their authentication commands does. NAT by itself is not available to understand the encapsulated information contained in the commands PORT and PASV where IP address and port numbers are set up for connection. In addition fragmentation takes place, the fragments must to be reassembled before NAT can be performed.

Possible Solutions

Application level gateway (ALG) is usually used as next step in NAT process. When the traffic is routed by the NAT this is then forwarded to the ALG. This understands the request and does the required translations to perform a connection. If the session comes from outside, then the ALG must be integrated with the NAT to allow the session to pass through the server.

This scheme allows also forwarding ports for simple protocols in fixed ports. This allows forwarding packets for certain port to dedicated servers, where NAT is used as a virtual server that distributes the traffic among server farms. This solution is not providing security

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

in the way, especially when NAT and ALG are outside the trusted boundary. Another issue in this scheme is the fact that performance timings are increased by the ALG, degrading considerably the throughput for the border router and NAT server.

Unfortunately ALG doesn't works in all the cases when NAT is not useful. In the IKE process is no way to decrypt the headers because the process made in the encryption algorithm where ALG is not part of the process, and the same applies when using SKIP and NAPT is used.

In the case of RPC, ALG can't resolve the problem completely, because some RPC packets contain encrypted information and cannot be modified by the NAT server. But for those packets not encrypted, ALG brings a good solution for this protocol.

For voice over IP, exist an ALG called H.323 proxy, which placed between caller and destination host, to prepare NAT for the successive sessions. This solution applies as well for the SIP and MGCP protocols.

Also for FTP an especial ALG is needed. In this case the name of this ALG is FTP ALG also called FTP proxy. This is used to analyze the payloads in order for FTP to work with traditional NAT, NAPT or bi-directional NAT servers. Basically this proxy understands and interprets the addresses managed in the PORT and PASV commands. In the same way this ALG maintains and TCP/UDP state information to modify and reassemble fragmented packets. If the replaced packet is longer than the original, ALG splits it and modify the sequence numbers.

Authentication

Authentication protocols usually need DNS-ALG or port-forwarding servers to aid the pass through a NAT. Kerberos uses a combination of packet encryption, based in credentials depending on the time, and trusted third party to provide secure authentication. When a client initiates a request to a ticket-granting server, authentication server or destination server located in a public network, address translation can be performed transparently. If this request is made to any server in a private network instead the public network, then the DNS-ALG or port-forwarding technology is required for succeed in the authentication through the NAT server.

In other hand, Radius (dial-in user service protocol) carries authentication, authorization and configuration information between a network-access server (NAS) and a shared authentication server. The network-access works as a Radius client, so it sends the user information to the server. At this point the connection between the client and Radius server is authenticated without using IP address, in consequence the process is not affected using NAT. As well as Kerberos, of the Radius server is in a private network, then DNS-ALG or port forwarding must be used.

One time password mechanism like S/Key limits the use of any password to a single communication session. Using this protocol, when a user logs in, the S/Key server issues a challenge consisting in number and string characters, then the user calculate it and returns

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

the answer. The packets used by S/Key doesn't contain IP or Port information, so on NAT is transparent.

Security in Electronic Commerce

One of the most popular solution to secure transactions and payments in Internet-based commerce is the secure electronic transaction (SET). This solution require that holders and merchants have a certificate from a trusted certificate authority prior to any transaction is made. Public key cryptosystem and the certificates used bring a securely way to transmit data over Internet. The payload doesn't contain IP addresses or port information, let it works under all NAT environments.

The table shown below[9], mention the basic protocols used in network, transport and session layers and say if the NAT environment can work with it. Also mentioned the reason of failure in each case and if is possible to get solution using the ALG.

	NAT Environments					
Protocols	NAT	Two-way NAT	Twice NAT	NAPT	Reason for failure	ALG as Solution
Layer 3&4						
PPTP	Y	Y	Y	Y	N/A	N/A
L2TP	Y	Y	Y	Y	N/A	N/A
IKE	N	N	N	N	Encrypted IP address	No
SKIP	Y	Y	Y	N	Encrypted Port number	No
SSL	Y	Y	Y	Y	N/A	N/A
TLS	Y	Y	Y	Y	N/A	N/A
Layer 5						
RPC	N	N	N	N	1. Dynamic port numbers 2. Encrypted IP address and port number	1. Yes 2. No
Kerberos	Y	Y	Y	Y	N/A	N/A
Radius	Y	Y	Y	Y	N/A	N/A
S/Key	Y	Y	Y	Y	N/A	N/A
H.323	N	N	N	N	Dynamic IP address and port numbers	Yes
SIP	N	N	N	N	Dynamic IP address and port numbers	Yes
MGCP	N	N	N	N	Dynamic IP address and port numbers	Yes
SET	Y	Y	Y	Y	N/A	N/A
FTP	N	N	N	N	IP address and port number in FTP commands	Yes (FTP-ALG)
SMTP	Y	Y	Y	Y	N/A	N/A
POP3	Y	Y	Y	Y	N/A	N/A
IMAP4	Y	Y	Y	Y	N/A	N/A
SSH	Y	Y	Y	Y	N/A	N/A

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Conclusion

NAT can be considered as a great solution to attack problems related with the lack of IP addresses in Ipv4. But at the same time is a limitative technology with big security issues that sacrifice confidence and integrity in such protocols based in Network and Transport methods as well as protocols that works in the session layer where negotiation and encryption over IP and port address are realized.

In the front of the conventional process of cracking systems and the future of quantum computer where the numbers of transactions are highly increased, algorithms and IKE will become as the first barrier against confidence and integrity compromise. In this scenario NAT will become a problem. NAT must find some formula to be working together with encryption devices to allow the transparent routing and the encryption in the same process while Ipv6 resolve at least the basic lake of addresses.

The security issue in NAT environments is key for the success of this technology. Although NAT can work in a transparent way with some secure protocols such SSL, TLS, SET, SSH, and authentication protocols such Kerberos, Radius and S/Key, and gives some secure certain to the admin of NAT servers, more secure algorithms and new encryption methods to hide all the real information can't be used in a NAT environment. The future in this area is based in new standards and Ipv6.

In the meanwhile is important to choose the right configuration scheme for NAT in combination of security tools around it, not just to maintain the routing functionality, but also apply at least the basic steps of security around it.

Sources and References

1. – Foreman, Timothy. "Network Address Translation Not a Security Panacea", 9 Nov 2000. URL:http://www.sans.org/infosecFAQ/firewall/net_add2.htm

2. – McLaughlin, Bryan. "Network Address Translation ", 10 Sep 2000. URL:http://www.sans.org/infosecFAQ/firewall/net_add.htm

3.- Faughnan, John. "NetBIOS over TCP/IP with Network Address Translation on the Cisco 675", 4 Jul 2000. URL:http://www.labmed.umn.edu/~john/netbios.html

4. – Egevang, "The IP Network Address Translator (NAT)", May 1994. URL:http://www.ietf.org/rfc/rfc1631.txt

5. –Srisuresh, "IP Network Address Translator (NAT) Terminology and Considerations ", Aug 1999, URL:http://www.ietf.org/rfc/rfc2663.txt

6. – Kessler, Gary. "IPv6: The Next Generation Internet Protocol ", 1 Ago 2000. URL:http://www.vtac.org/Tutorials/ipv6_exp.html

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

7. - Dave," Encryption and You", 23 Ago 1995.
URL:http://web.syr.edu/~dbgrandi/crypto.htm

8. – Harkins," The Internet Key Exchange (IKE)", Nov 1998.
URL:http://www.ietf.org/rfc/rfc2409.txt

9. - Shieh, Shiuh-Pyng, Ho Fu-Shen, Huang Yu-Lun and Luo Jia-Ning. "Network Address Translators: Effects on Security Protocols and Applications in the TCP/IP stack." IEEE Internet Computing. vol. 4, no. 6(November/December 2000): 42-49

© SANS Institute 2000 - 2002, Author retains full rights.