ISSN No. 0976-5697

Volume 6, No. 8, Nov-Dec 2015

International Journal of Advanced Research in Computer Science

REVIEW ARTICLE

Available Online at www.ijarcs.info

Network Address Translation for Inbound Connections in Paradigm of Private Network

Manjinder singh
M. Tech (CSE)
North west institute of engg.& tech.,
Dhudike(Moga)

Mohita Garg
North west institute of engg.& tech.
Dhudike (Moga)

Abstract: Information Technology has begun to implement Network Address Translation (NAT) and private addressing for our open-use networks. This technology allows several computers to share one public Internet address at the same time. Only a single IP address is required to represent one or more computers to the rest of the world. . Libraries are subscribing online journals and books more and more these days. To access the digital material outside the IP restricted area, NAT is essential to designed in such a fashion to have secure and reliable connectivity.

keywords: NAT, IP, RIP.

(1) INTRODUCTION

Network Address Translation (NAT) allows a network to use private IP addresses that are not routed over the Internet. Private IP address schemes allow organizations to limit the number of publicly routed IP addresses they use, reserving public addresses for Web servers and other externally accessed network equipment. NAT allows administrators to use one public IP address for all of their users to access the Internet - the firewall is "smart" enough to send the requests back to the requesting workstation's internal IP.
NAT also allows users inside a network to contact a server using a private IP while users outside the network must contact the same server using an external IP. In addition to port and IP address rules, firewalls can have a wide variety of functionality. Firewalls are vital to network management. Without this control over computer and network access, large networks could not store sensitive data intended for selective retrieval. Network address translation (NAT), web server load balancing, and redirecting traffic to transparent proxies all share a common feature: they involve a level of indirection in the meaning of IP addresses and port numbers, and can be implemented by rewriting those values in IP headers and payloads. [1]

(2) TYPES OF NAT

Unidirectional NAT
NAT was designed assuming that a client-server (request-response) communication would begin with a datagram sent from the local network to the global one. For this reason, the first type of NAT is sometimes called Unidirectional, Outbound or Traditional NAT. In this type request-response starts from local to global network.

Bidirectional NAT
Enhanced NAT versions that allow devices on the outside network initiate a transaction with one of the machines in the local network. This type of NAT is called Bidirectional NAT, Two-Way NAT or Inbound NAT. All of these convey the concept that it allows transactions in both ways.

(3) ADDRESSING TERMINOLOGY

NAT Address Terms Based on Device Location (Inside | Outside)
(A) Inside Address: The address of any device on the organization`s private local network that is using a NAT.
(B) Outside Address: Any address that refers to the public Internet (Everything outside the local network).
NAT Address Terms Based on Datagram Location (Local | Global)
(A) Local Address : The address that appears in a datagram in the inside network whether it refers to an inside or outside address.
(B) Global Address: The address that appears in a datagram in the outside network whether it refers to an inside or outside address**.**

Translation is the process by which an internal, private address is converted to an external public address. Some or all of the traffic leaving the internal network will have the IP header of the packets modified before leaving the external interface of edge NAT device. This process is described in the original request for comments or RFC.
Associated with Document is RFC 1597 which describes private Addressing. Three address ranges are removed from the public IP address space:

Private Address Ranges
192.168.0.0/24
172.16.0.0 – 172.31.255.255/16
10.0.0.0/8 [2]

Note that the address space defined is extremely limited.[3] While this RFC does not address NAT specifically, network address translators use these addresses for internal hosts. As transmissions are routed in the outbound direction, the

source IP address from one of these address ranges is modified to be that of the outside interface of the NAT device. When using a single NAT device, this outside address will be part of the public address space of the Internet. Upon returning, the translation process is done in reverse. Critical to this process is the translation table maintained on the NAT device. This table maintains the mapping between the original inside source IP address and port to the outside address and port assigned by the NAT device.

It is important to realize that in addition to this translation, the NAT device is handling routing functions. A NAT box **N** has a public IP address for its interface connecting to the global Internet and a private address facing the internal network [2]. In SOHO networks these devices are also known as home gateways. They can be deployed as stub networks or provide routing for larger topologies using routing protocols such as RIP. NAT is a very important aspect of firewall security. It conserves the number of public addresses used within organization, and it allows for stricter control of access to resources on both sides of the firewall. There are three devices that typically perform NAT. These are routers, firewalls and proxy servers.

(5) METHODOLOGY

Network address translation (NAT) is a methodology of remapping one IP address space into another by modifying network address information in Internet Protocol (IP) datagram packet headers while they are in transit across a traffic routing device. The usage of Network Address Translation (NAT) devices is very common among the devices such as computers, laptops and smart phones connecting to the Internet. Hosts within enterprises that use IP can be partitioned into three categories:

Category 1: hosts that do not require access to hosts in other enterprises or the Internet at large; hosts within this category may use IP addresses that are unambiguous within an enterprise, but may be ambiguous between enterprises.

Category 2: hosts that need access to a limited set of outside services (e.g., E-mail, FTP, net news, remote login) which can be handled by mediating gateways (e.g., application layer gateways).

For many hosts in this category an unrestricted external access may be unnecessary and even undesirable for privacy/security reasons. Just like hosts within the first category, such hosts may use IP addresses that are unambiguous within an enterprise, but may be ambiguous between enterprises.

Category 3: hosts that need network layer access outside the enterprise (provided via IP connectivity); hosts in the last category require IP addresses that are globallyunambiguous.

(6) CONCLUSION

Since privately addressed nodes on a network do not have a presence on the Internet, there has to be a method by which these addresses are translated to globally routable numbers. This translation service is provided by NAT, which allows packets to be sent and received from outside the local network. In the paradigm of digital arena, Libraries are modernizing the way of reading and accessing the information at the door steps of user. Libraries are subscribing online journals and books more and more these days. Publishers are providing user based and IP based authentications. To access the digital material outside the IP restricted area, NAT is essential to designed in such a fashion to have secure and reliable connectivity. In the present work, an attempt is made to develop the secure connection for digital services.

(7) REFERENCES

[1] Prof. S. G. Anantwar1, Miss. Ujjwala Kharkar2 1,2Information Technology, S.G.B.A.U. Amravati, Maharashtra, Indi**a.**

[2] A Retrospective View of Network Address Translation Lixia Zhang, University of California, Los Angeles.

[3] Bruce H. Hartpence and Daryl G. Johnson. A Re-examination of Network Address Translation Security, Networking, Security and Systems Administration Department, Golisano College of Computing and Information Sciences Rochester Institute of TechnologyRochester, NY, USA.

[4] Lizhuo Zhang; Weijia Jia; Xun Xiao; Bin Dai; Huan Li . Research of TCP NAT Traversal Solution Based on Port Correlation Analysis & Prediction Algorithm.