ISSN No. 0976-5697

Volume 7, No. 3, May-June 2016

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

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)

Dr. Mohita
North west institute of engg.& tech,
Dhudike (Moga)
Mohita_cse@northwest.ac.in

Abstract: Internet is a default communication channel for business and is growing worldwide. With this expansion of internet, secure data communication between multiple sites connected via public channels is very important. For this purpose virtual private network is the most widely used tunnel. NAT let an organization to use public network to convey private data by using strong authentication & encryption techniques. 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. To contain growth of routing overhead, an Internet Service Provider obtains a block of address space from an address registry, and then assigns to its customers addresses from within that block based on each customer's requirement. 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 this research work, secure connections are developed using Network Address Translation (NAT).

Keywords: NAT, IP, ISP, LAN.

I .INTRODUCTION

NAT (Network Address Translation) is a mechanism where a device performs modifications to the TCP/IP address/port number of a packet and maps the IP address from one realm to another (usually from private IP address to public IP address and vice versa). This works by the NAT device allocating a temporary port number on the public side of the NAT upon forwarding outbound packet from the internal host towards the Internet, maintaining this mapping for some predefined time, and forwarding the inbound packets received from the Internet on this public port back to the internal host.NAT devices are installed primarily to alleviate the exhaustion of IPv4 address space by allowing multiple hosts to share a public/Internet address. Also due to its mapping nature (i.e. a mapping can only be created by a transmission from an internal host), NAT device is preferred to be installed even when IPv4 address exhaustion is not a problem (for example when there is only one host at home), to provide some sort of security/shield for the internal hosts against threats from the Internet.

the server in the private network behind the NAT is notified by the third party that the client would like to establish a connection. The server then initiates the connection to the client.[4]
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]

(A) Remote access: Remote access is the ability to connect and gain access to a computer or a network from a remote distance that is physically distributed. In corporations, people at branch offices, telecommuters, and people who are travelling may need access to the corporation's network. It is a Connection to a data-processing system from a remote location, for example through a virtual private network.

(B) Need of Remote access in organizations: for many organizations , remote access is a cost effective replacement for additional hardware. It also helps businesses to obey some legal acts such as family leave etc., which permits

employees to spend time away from the office. Remote access also cut down on costs by reducing the office space requirements.

(C) Remote access methods: nowadays several remote access methods are available.

(2) 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.

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].

II. METHODOLOGY

The Internet Protocol (IP) is the method or protocol by which data is sent from one computer to another on the Internet. Each computer (known as a host) on the Internet has at least one IP address that uniquely identifies it from all other computers on the Internet. When you send or receive data (for example, an e-mail note or a Web page), the message gets divided into little chunks called packets. Each of these packets contains both the sender's Internet address and the receiver's address. Any packet is sent first to a gateway computer that understands a small part of the Internet. The gateway computer reads the destination address and forwards the packet to an adjacent gateway that in turn reads the destination address and so forth across the Internet until one gateway recognizes the packet as belonging to a computer within its immediate neighborhood or domain. That gateway then forwards the packet directly to the computer whose address is specified. Because a message is divided into a number of packets, each packet can, if necessary, be sent by a different route across the Internet. Packets can arrive in a different order than the order they were sent in. The Internet Protocol just delivers them. It's up to another protocol, the Transmission Control Protocol (TCP) to put them back in the right order.

IPv6 includes the capabilities of IPv4 and any server that can support IPv6 packets can also support IPv4 packets.

1. Defining NAT Inside and Outside Interfaces

2 Allowing Internal Users to Access the Internet

3 Allowing the Internet to Access Internal Devices

4 Configuring NAT to Allow the Internet to Access Internal Devices

5 Redirecting TCP Traffic to another TCP Port or Address

6 Using NAT during a Network Transition

7 Using NAT in Overlapping Networks

8 Difference between One-to-One Mapping and Many-to-Many

9 Verifying NAT Operation

III. VIRTUAL PRIVATE NETWORK

Virtual Private Network (VPN) extends a private network across public networks like the internet. It enables a host computer to send and receive data across shared or public networks as if they were an integral part of the private network with all the functionality, security and management policies of the private network. The objective of VPN is to add a level of security to the exchange of data. VPNs securely connect remote users and offices in a cooperate network. As an alternative to using dedicated connections, such as leased line, a “virtual” connection is made between geographically scattered users and networks over a shared or public network, like the internet. Data is transmitted as if it were passing through private connections. This is a seamless connection, in a way that when two nodes are connected via a VPN they will work as if they were both on the same physical network .

Two VPN technologies that are being used are:
Site-to-site VPN - A site-to-site VPN allows multiple offices in fixed locations to establish secure connections with each other over a public network such as the Internet. It also provides extensibility to resources by making them available to employees at other locations.

Remote Access VPN - A remote-access VPN allows individual users to establish secure connections with a remote computer network. These users can access the secure resources on that network as if they were directly plugged in to the network's servers[3].

IV. RESULTS & DISCUSSIONS

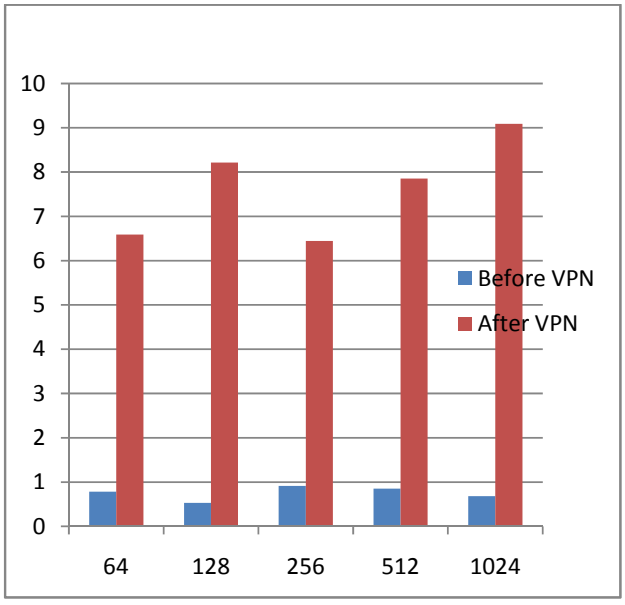
The implementation of Network Address Translation is carried out to access the digital material outside the IP restricted area. All the graphs and tables reported in this chapter depict the performance of VPN under various conditions with the use of NAT. As a general goal, the performance of implemented VPN is evaluated based on parameters like throughput and RTT. For all the graphs represented in this chapter, the RedHat-server virtual machine is being referred to as A and RedHat-Client virtual machine is referred to as B.

Results for RTT

The following values show the average RTT obtained before VPN and after VPN

Size(Bytes)	Before VPN(ms)	After VPN(ms)
64	0.782	6.592
128	0.531	8.217
256	0.916	6.444
512	0.853	7.856
1024	0.683	9.089

RTT before and after VPN from NodeA to NodeB

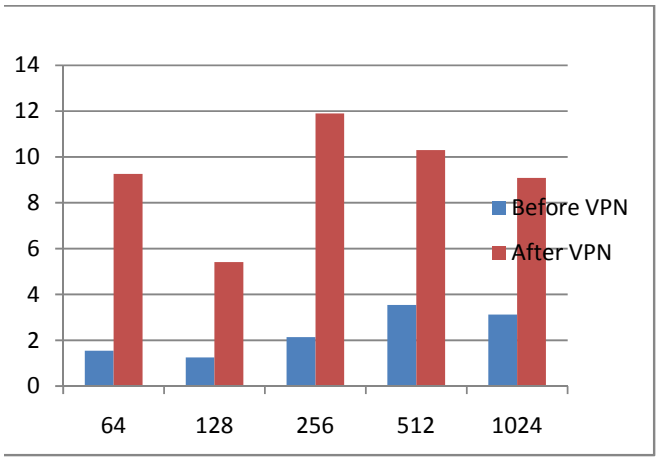


RTT before and after VPN from NodeA to NodeB

The following values show the average RTT obtained before VPN and after VPN with different packet sizes from node B to node A.

Size(Bytes)	Before VPN(ms)	After VPN(ms)
64	1.541	9.256
128	1.249	5.413
256	2.133	11.895
512	3.538	10.301
1024	3.123	9.483

RTT before and after VPN from Node B to Node A



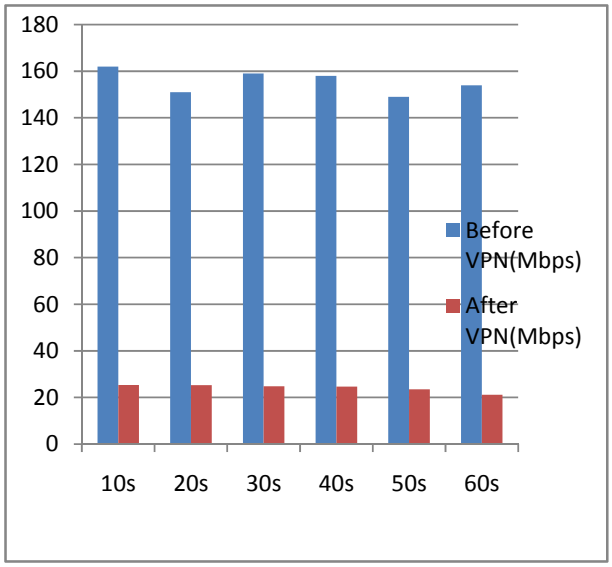
RTT before and after VPN from Node B to Node A

The results obtained show that before the VPN tunnel was established RTT values were found to be low as expected and that there was an increase in delay after the VPN is applied.

Results for throughput

The following values depict the average throughput before and after VPN configuration from node A to node B

Time(seconds)	BeforeVPN(Mbps)	AfterVPN(Mbps)
0-10	162	25.4
10-20	151	25.3
20-30	159	24.8
30-40	158	24.7
40-50	149	23.5
50-60	154	21.2

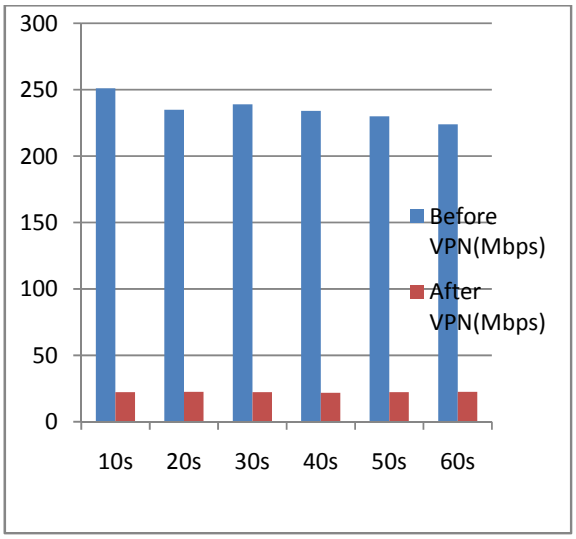


Throughput values before and after VPN configuration from A to B

The following values depict the average throughput before and after VPN configuration from node B to node A

Time(seconds)	Before VPN(Mbps)	After VPN(Mbps)
0-10	251	22.3
10-20	235	22.5
20-30	239	22.3
30-40	234	21.8
40-50	230	22.3
50-60	224	22.5

Throughput values before and after VPN configuration from B to A



Throughput values before and after VPN configuration from B to A

It is clearly evident from the results that there is a drastic decrease in throughput once the VPN tunnel has been established. It is due to the fact that VPN uses several encryption algorithms and hence overhead is more.

V. CONCLUSION

Many organizations across the world use every available physical connection method to link up their individual offices. The goal of this research was to use Network Address Translation for Inbound Connections of Private Network to implement the basic remote access approaches and Implementation of virtual private network based on open source using NAT. The option chosen can be both dedicated digital lines and virtual private network (VPN), which are significantly cheaper than their physical equivalents. In this research work, NAT is implemented to access digital resources.

VI. REFERENCES

[1] Prof. S. G. Anantwar, Miss. Ujjwala Kharkar Information Technology, S.G.B.A.U. Amravati, Maharashtra, India.

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

[3] Virtual Private Network. Ritika kajal, Deepshikha Saini, Kusum Grewal, Software Engineering Computer Science Engineering I T M University I T M University Sector 23-A, Gurgaon

[4] Steven m.bellovin, A technique for counting Nated hosts