ISSN No. 0976-5697

Volume 6, No. 7, September-October 2015

International Journal of Advanced Research in Computer Science

REVIEW ARTICLE

Available Online at www.ijarcs.info

Secured and Controlled Network Traffic with Load Balancing using IP-Tables

Talwinder kaur
M.tech(CSE)
North west institute of engg. & tech.
Dhudike (Moga)

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

Abstract : There are two IP addresses for a typical home network: one for local devices to connect to across the local area network (LAN), another for the external or wide area network (WAN) Internet connection. A virtual private network (VPN) is a method for the extension of a private network across a public network, such as the Internet. It enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network, and thus are benefiting from the functionality, security and management policies of the private network. The aim of this method of course is to balance the traffic so as to avoid the congestion.

***Keywords*:** Load balancing, IP network, VPN, NAT.

(1) INTRODUCTION

A default IP address is normally set to internal LAN, private number for example, 192.168.1.1 for their internal IP address. No matter the brand of router, its default internal IP address is listed in the manufacturer's documentation. This IP address can be changed by Administrators during router setup or at any time later. These private LAN-IP address remains fixed, unless someone manually changes it. The external WAN-IP address of the router is set when the router connects to the Internet service provider. This address can also be viewed on the router's administrative console.

Alternatively, the WAN-IP address can be found by a Web-based IP address lookup service—such as WhatIsMyIPAddress.com—from any computer on the home LAN. Load balancing is an important component in improving the efficiency of distributed systems because it distributes an even workload over all the processors. [1]

Load balancing is a process of reassigning the total load to the individual nodes of the collective system to make resource utilization effective and to improve the response time of the job. Simultaneously removing a condition in which some of the nodes are over loaded while some others are idle.[2] Network Load Balancing uses fully distributed software architecture. An identical copy of the Network Load Balancing driver runs in parallel on each cluster host. The drivers arrange for all cluster hosts on a single subnet to concurrently detect incoming traffic for the cluster's primary IP address. [3]

Firewalls A firewall is a security device that can be a software program or a dedicated network appliance. The main purpose of a firewall is to separate a secure area from a less secure area and to control communications between the two. It is a protective system that lies between computer network and the Internet. Firewall prevents unauthorized use and access to your network. The job of a firewall is to carefully analyze data entering and exiting the network based on your configuration. It ignores information that comes from unsecured, unknown or suspicious locations. A firewall plays an important role on any network as it provides a protective barrier against most forms of attack coming from the outside world. Firewalls can perform a variety of other functions, but are chiefly responsible for controlling inbound and outbound communications on anything from a single machine to an entire network.

IP-tables In network security, use of IP Tables is becoming very important. In any campus network, IP-tables can share private networking to simulate the network traffic isolation. In the present study, real implementation of IP-tables is done to improve the security and controlling the network traffic.

It further improves the bandwidth usage for Compute intensive applications and load balance the network traffic over multiple internet service providers using virtual private network (VPN).
Load balancing in the network may results
1) Reduced Congestion in the network.
2) Reduced packet loss and packet delay.
3) Increased overall efficiency of the network.

(2) SOFTWARE FIREWALLS

A software firewall protects computer from outside attempts to control or gain access computer and prevents unwanted access to the computer over a network connection by identifying and preventing communication over risky ports. For individual home users, the most popular firewall choice is a software firewall. Software firewalls are installed on computer (like any software) and can customize it; allowing some controls over its function and protection

features. Many software firewalls have user defined controls for setting up safe file and printer sharing and to block unsafe applications from running on your system. Additionally, software firewalls may also incorporate privacy controls, web filtering and more.

Software firewalls, also sometimes called personal firewalls, are designed to run on a single computer. These are most commonly used on home or small office computers that have broadband access, which tend to be left on all the time.

Computers communicate over many different recognized ports, and the firewall will tend to permit these without prompting or alerting the user. For example, computers access Web pages over port 80 and use port 443 for secure Web communications. A home computer would expect to receive data over these ports. However, a software firewall would probably block any access from the Internet over port 421, over which it does not expect to receive data. A software firewall also allows certain programs on the user's computer to access the Internet, often by express permission of the user. Some software firewalls also allow configuration of trusted zones. These permit unlimited communication over a wide variety of ports. This type of access may be necessary when a user starts a VPN client to reach a corporate intranet.

One drawback to software firewalls is that they are software running on a personal computer operating system. If the underlying operating system is compromised, then the firewall can be compromised as well. Since many other programs also run on a home computer, malicious software could potentially enter the computer through some other application and compromise the firewall. Software firewalls also rely heavily upon the user making the right decisions.

(3) HARDWARE FIREWALLS

A hardware firewall uses packet filtering to examine the header of a packet to determine its source and destination. This information is compared to a set of predefined or user-created rules that determine whether the packet is to be forwarded or dropped.

Hardware firewalls can be purchased as a stand-alone product but more recently hardware firewalls are found in broadband routers, and should be considered an important part of the system and network set-up, especially for a broadband connection. Hardware firewalls can be effective with little or no configuration, and they can protect every machine on a local network. Most hardware firewalls will have a minimum of four network ports to connect other computers, but for larger networks, business networking firewall solutions are available.

A hardware firewall is placed between a network, such as a corporation, and a less secure area, such as the Internet. Firewalls also can separate more secure networks from less secure networks, such as one corporate location within a larger corporate structure. Versions of hardware firewalls are available to home users who want stronger protection from potential Internet attacks. There are many different default configurations for these devices - some allow no communications from the outside and must be configured, using rules, others (like those available for the home market) are already configured to block access over risky ports. Rules can be as simple as allowing port 80 traffic to flow through the firewall in both directions.

Firewalls are also used for **Network Address Translation (NAT)**. This 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. [4]

(5) METHODOLOGY

IP Tables are based on open source and easy to implement and manipulate according to need of the organization for controlling the traffic for need based applications. **iptables** is a user-space application program that allows a system administrator to configure the tables provided by the Linux kernel firewall (implemented as different Net filter modules) and the chains and rules it stores. Different kernel modules and programs are currently used for different protocols; iptables applies to IPv4, ip6tables to IPv6, arptables to ARP, and ebtables to Ethernet frames. Iptables requires elevated privileges to operate and must be executed by user root, otherwise it fails to function.

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. While NAT devices are generally used in local area networks (LAN), they can also be used just for one computer. In home networks, most Internet Service Providers (ISPs) give Wi-Fi-enabled NAT home gateways to their users. Thus, when users can connect their devices to the Internet, their private Internet Protocol (IP) addresses are hidden on the Internet since they are encapsulated with a public IP address that the NAT provides.

There are other uses for Network Address Translation (NAT) beyond simply allowing workstations with internal IP addresses to access the Internet. In large networks, some servers may act as Web servers and require access from the Internet. These servers are assigned public IP addresses on the firewall, allowing the public to access the servers only through that IP address. However, as an additional layer of security, the firewall acts as the intermediary between the outside world and the protected internal network. Additional rules can be added, including which ports can be accessed at that IP address.

Using NAT in this way allows network engineers to more efficiently route internal network traffic to the same resources, and allow access to more ports, while restricting access at the firewall. It also allows detailed logging of communications between the network and the outside world.

(6) CONCLUSION

IP tables are used for controlling the traffic. By Implementing the IP tables the load can be balanced of the Network traffic which results in Improved, secured and controlled traffic over virtual private network. It further improves the bandwidth usage for Compute intensive applications and load balance the network traffic over multiple internet service providers using virtual private network (VPN).

(7) REFERENCES

[1] Xinyu Zhang1, Yongli Zhao2, Xin Su1, Ruiying He1, Weiwei Wang1, Jie Zhang2 , School of Information and Communications Engineering, (2) State Key Laboratory of Information Photonics and Optical Communication, Beijing University of Posts and Telecommunications, Beijing.7th International ICST Conference on Communications and Networking in China(2012)

[2]An Efficient Distributed Dynamic Load Balancing for Private Cloud Environment,G.Suryadevi ,D.Vijay akumar,R.SabariMuthuKumar,Dr. K .G. Srinivasagan

[3]PG Scholar, Dept of Computer Science and Engineering, National Engineering College, Kovilpatti, Tamilnadu, India.

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

[5] Eddie Kohler, Robert Morris, and Massimiliano Poletto MIT Laboratory for Computer Science

