SETTING UP A LAN CONNECTION WITH PORT SECURITY

Dr. N.Suma, Ph.D., AP/ECE, SNS College Of Engineering
R.Sudharshan, S.Manok Kumar, P.Suresh Kumar, S.Naveen Kumar
DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING
UG Scholar, SNS College of Engineering
Email id: sumasivaravi@gmail.com, sudhars1995@gmail.com, manojece07@gmail.com,
76navinkumar@gmail.com, sureshece2361@gmail.com,

ABSTRACT:

Networking is the practice of interfacing two or more computing devices with each other for the purpose of sharing data. Computer networks are built with a combination of hardware and software. Creating a local area connection with multiple hosts and building communication with multiple sub-networks. Connecting multiple clients to several servers and setting up a working WLAN system. The servers used are configured using DHCP and DNS so that multiple clients can be adhered to in the WLAN system. Inside the private network migrating the existing IPv4 addresses to IPv6 addresses. A secure web server is designed and configured using Linux based OS. Connecting all the required clients to the web server and establishing an efficient private network. Due to port forwarding and packet switching an additional degree of security is obtained. All the packets forwarded in the networks are noted. Using SSL and SSH we create more security and add encryption to the packets sent through the network. For encryption 128-bit AES encryption is used. Hence a LAN connection is configured and required layers of security are added to the system.

Keywords: 1) Private LAN configuration

2) Adding security layers

1. INTRODUCTION:

Providing security for a network has become an important part in the basic architectural designing of the network .Nowadays, many kinds of algorithms are used as security algorithms. This project basically sets up a series of protocols and algorithms to a newly built network inside a campus .The main emphasis of the project is to provide a certain level of security to the network.

This paper configures a LAN connection for a required network system using IPV6 protocol and considers port forwarding for providing intranet work security. A detailed note of all the packets forwarded in the network will be registered and monitored. Any packet coming into the system has its default port number changed, and a non repeating port number is given to each protocol. The proposed system is implemented exclusively for TCP networks. Using SSL and SSH, this paper proposes more security and adds another level of encryption to the packets sent through the network.

The platform used for this project is LINUX .RED Hat LINUX is an open source platform and provides a more secure and highly encrypted operating system compared to windows.The cost of the platform is also considered in selecting LINUX.

2. EXISTING SYSTEM

. In the existing system LAN in the current scenario is using IPv4 address and network is facing multiple issues on load balancing and over loading on jobs. More clusters are formed in the network and delay time is created, possibility of losing the connection is also faced in the current scenario. So it is not efficient to perform more complex task on the network.

The current version of Internet Protocol known as IPv4 had not undergone any drastic changes in it's design since Request for

Comments (RFC) 791, published in 1981. Since its time of implementing it has proven to be a easily applicable, inter operable and a robust standard and had stood up to the test of a small nwteork to a scaling global utility. However, the design of IPv4 did not anticipate some of the current scenario problems:

The sudden exponential growth of people using the internet and implementing virtually everything through it has exhausted the IPv4 address space. This can be proven by a simple calculation, g Given that an IP address is 32 bits in length, there are 232 actual IP addresses, which are 4.3 billion addresses. Only 3.7 billion of these are actually usable. Many addresses are reserved, such as the research (239–254), broadcast (255), multicast (224–239), private (10, 172.16, and 192.168), and loopback addresses (127). And, of course, many of the usable addresses are already assigned, leaving about 1.3 billion addresses for new growth. As a result, public IPv4 addresses have become relatively scarce, forcing many users and some organizations to use a NAT to map a single public IPv4 address to multiple private IPv4 addresses. Although NATs promote reuse of the private address space, they violate the fundamental design principle of the original Internet that all nodes have a unique, globally reachable address, preventing true end-to-end connectivity for all types of networking applications. Additionally, the rising prominence of Internet-connected devices and appliances ensures that the public IPv4 address space will eventually be depleted.

SSH encryption protocol version 4.2 is currently being used and it has certain bugs in PAM fixes and portability related bugs which are verified in the later versions.Also port security is not enabled in the existing design. By adding port security, we add a extra layer of security to the switching network. The MAC address of a host generally does not change. If a specific host will always remain connected to a specific switch port, then the switch can filter all other MAC addresses on that port using Port Security. Port Security supports both statically mapping MAC addresses, and dynamically learning addresses from traffic sent on the port.

Disadvantage:

- Not able to handle large amount of traffic
- Restricted security
- Limited number of users inside the private network.

3. PROPOSED SYSTEM:

In the proposed system, all the IPv4 addresses are migrated to IPv6 addresses. Configuration of new enhanced policies and methods has been introduced. Securing the ports and port forwarding will implemented. Web servers will be working with HTTPS (SSL). Instead of using TELNET, all the communication ports will be using SSH. Generating Certificates and Keys with Advanced Encryption Standard (AES) with 128-bit encryption method will be used.

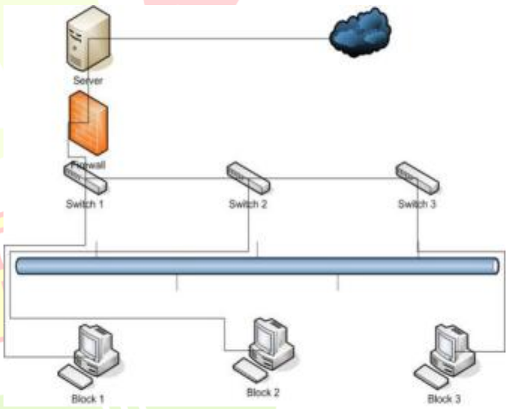
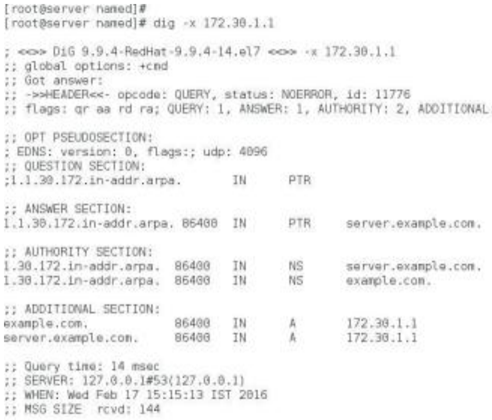


Figure: 3.1 Simplified block diagram of the setup.

3.1 Domain Name Server (DNS) Configuration and Administration

The proposed work uses Linux as a DNS server and hence the configuration of DNS tables for the services is to be done using the BIND 8.x package which comes as a standard with the Red Hat distribution. Red Hat versions 5.1 used to come with BIND 4.x package and hence need to be upgraded. The BIND RPM package is oinstalled and the configuration file is converted into the new format..To enable DNS services, Configure the "/etc/hosts" file as needed.The "/etc/named.conf" file should be configured to point to your DNS tables. Now DNS tables are set up in the "var/named/" directory as configured in "etc/named.config". It is made sure that named daemon is running and is started from the "/etc/rc.d/init.d/named" file.



```
[root@server named]#
[root@server named]# dig -x 172.30.1.1

; <<>> DiG 9.9.4-RedHat-9.9.4-14.el7 <<>> -x 172.30.1.1
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 11776
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 3

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;1.1.30.172.in-addr.arpa.        IN      PTR

;; ANSWER SECTION:
1.1.30.172.in-addr.arpa. 86400  IN      PTR     server.example.com.

;; AUTHORITY SECTION:
1.30.172.in-addr.arpa.  86400   IN      NS      server.example.com.
1.30.172.in-addr.arpa.  86400   IN      NS      example.com.

;; ADDITIONAL SECTION:
example.com.            86400   IN      A       172.30.1.1
server.example.com.     86400   IN      A       172.30.1.1

;; Query time: 14 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Wed Feb 17 15:15:13 IST 2016
;; MSG SIZE  rcvd: 144
```

Figure: 3.2 Checking successful configuration of DNS server

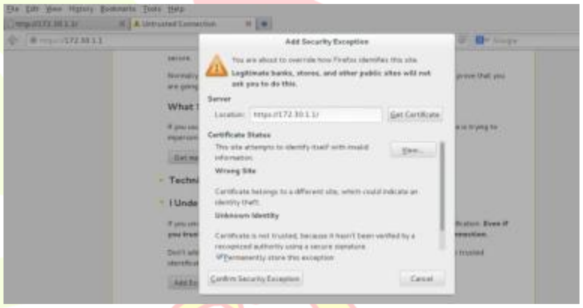
3.2 DHCP Configuration

The DHCP, or Dynamic Host Configuration Protocol, allows an administrator to configure network settings for all clients on a central server.
The DHCP clients request an IP address and other network settings from the DHCP server on the network. The DHCP server in turn leases the client an IP address within a given range or leases the client an IP address based on the MAC address of the client's network interface card (NIC). The information includes its IP address, along with the network's name server, gateway, and proxy addresses,including the netmask.
Nothing has to be configured manually on the local system, except to specify the DHCP server it should get its network configuration from. If an IP address is assigned according to the MAC address of the client's NIC, the same IP address can be leased to the client every time the client requests one. DHCP makes network administration easier and less prone to error.

3.3 SSH Installation and Port Forwarding

Secure Shell is a program to log into another computer over a network, to execute commands in a remote machine, and to move files from one machine to another. It provides strong authentication and secure communications over insecure channels. It is a replacement for rlogin, rsh, rcp, and rdist. SSH version 4.9 is used in the proposed project which fixes important bugs for the previous versio

SSH protects a network from attacks such as IP spoofing, IP source routing, and DNS spoofing. An attacker who has managed to take over a network can only force ssh to disconnect. He or she cannot play back the traffic or hijack the connection when encryption is enabled. When using ssh'sslogin (instead of rlogin) the entire login session, including transmission of password, is encrypted; therefore it is almost impossible for an outsider to collect passwords.


File Edit View History Bookmarks Tools Help
Untrusted Connection
https://172.30.1.1
Get Certificate
View...
Confirm Security Exception
Cancel

Add Security Exception

You are about to override how Firefox identifies this site.
Legitimate banks, stores, and other public sites will not ask you to do this.

Server
Location: https://172.30.1.1/

Certificate Status
This site attempts to identify itself with invalid information.
Wrong Site
Certificate belongs to a different site, which could indicate an identity theft.
Unknown Identity
Certificate is not trusted, because it hasn't been verified by a recognized authority using a secure signature.
☑ Permanently store this exception

Figure 3.3 Adding security encryption SSH

Port forwarding or port mapping is an application of network address translation (NAT) that redirects a communication request from one address and port numbercombination to another while the packets are traversing a network gateway, such as a router or firewall. This technique is most commonly used to make services on a host residing on a protected private internal network available to hosts on the opposite side of the gateway (external network), by remapping the destination IP address and port number of the communication to an internal host. In the proposed project port forwarding is done using Zabbix software; all the ports used by various client systems are monitored and unused port numbers are noted down. Then all the data coming through these ports are redirected to the unused port inside the private network. Hence security is increased as an outside system does not know the port through which the packets are received.

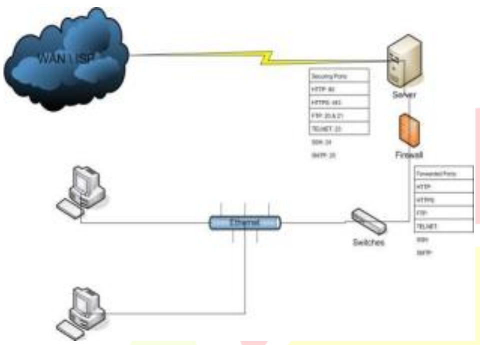
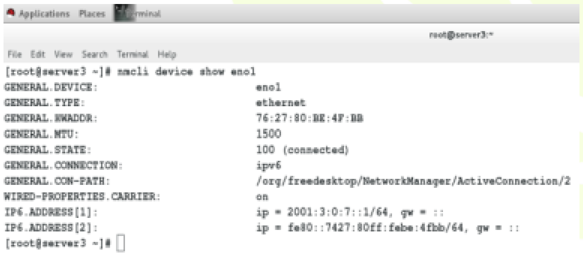


Figure 3.4 Port Forwarding

3.3 Output:

After adding all the server and client configurations, encryption standards and required certificates, the connection is checked and the following output is obtained.



```
[root@server3 ~]# nmcli device show enol
GENERAL.DEVICE:                         enol
GENERAL.TYPE:                           ethernet
GENERAL.HWADDR:                         76:27:80:BE:4F:BB
GENERAL.MTU:                            1500
GENERAL.STATE:                          100 (connected)
GENERAL.CONNECTION:                     ipv6
GENERAL.CON-PATH:                       /org/freedesktop/NetworkManager/ActiveConnection/2
WIRED-PROPERTIES.CARRIER:               on
IP6.ADDRESS[1]:                         ip = 2001:3:0:7::1/64, gw = ::
IP6.ADDRESS[2]:                         ip = fe80::7427:80ff:febe:4fbb/64, gw = ::
[root@server3 ~]# 
```

Figure 3.4 Final output

RESULTS

With the proposed project a LAN system is designed and connected between various subsystems. The IP, switch and router configurations are done in hyperterminal. A firewall is provided to the network to protect it against viruses, trojans and various other attackers. An AES encryption is added so that data sent over the network are safe and cannot be obtained by miscellaneous users.

Future progress that can be made in this project is that the number of clients can be added. A virtual network topology can be adopted by which space and storage can be greatly reduced. The wired system can be changed to a wireless system for better speed and mobility.

It can be incorporated into a group of mobile devices that can be activated inside a specialized network zone and authorized users can share and manage files within the network in a faster rate. With the help of cloud computing and virtualization this project which is limited within a finite quarters can be expanded between cities or even between counries.

REFERENCES

1. Sung Jun Ban, Hyeonwoo Cho, Chang Woo Lee, and Sang Woo Kim, “Implementation of IEEE 802.15.4 Packet Analyzer”, International Journal of Electrical and Electronics Engineering, May, 2008.
2. Chung-Sheng Li, Yueh-Min Huang, Han-Chieh Chao, "UPnP IPv4/IPv6 Bridge for Home Networking Environment," IEEE Transactions on Consumer Electronics, pp. 1651-1655, vol. 54, no. 4, 2008.
3. Matt Blaze, Joan Feigenbaum, and Jack Lacy, “Decentralized trust management”, In IEEE Symposium on Security and Privacy, pages 164–173, 2010.
4. Jim Owens and Jeanna Matthews,” A Study of Passwords and Methods Used in Brute-Force SSH Attacks” In IEEE Symposium on Security and Privacy, pages 164–173, 2012.
5. Md. KamrulHasan, A.H.M. Amimul Ahsan, and M. Mostafizur Rahman, “IEEE 802.11b Packet Analysis to Improve Network Performance” JU Journal of Information Technology (JIT), Vol. 1, June, 2012.
6. T.-Y. Wu, H.-C. Chao, T.-G. Tsuei, and Y.-F. Li, “A Measurement Study of Network Efficiency for TWAREN IPv6 Backbone”, International Journal of Network Management, vol. 15, no. 6, pp. 411–419, Nov. 2013.
7. Chiranjith Dutta, Ranjeet Singh, ”Sudtainable IPv4 to IPv6 Transition”, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 10, October 2014
8. Priya Bali, “A Detail Comprehensive Review on IPv4-to-IPv6 Transition and Co-Existance

Strategies" International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 4 Issue 4, April 2015