International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 03 | Mar 2020 www.irjet.net p-ISSN: 2395-0072

IMPLEMENTATION OF NETWORK SECURITY AND TRAFFIC FILTERING USING ACCESS CONTROL LIST

R.Suganthi[1], V.Nivetha[2], D.Narmadha[3] , O.R.Meenakumaari[4]

[1]Associate professor, Electronics and communication Engg. Panimalar Institute of Technology, Chennai, India
[2,3,4]B.E. Electronics and communication Engg. Panimalar Institute of Technology, Chennai, India

---

Abstract - *Nowadays we are living in modern society, where we use internet everywhere and major issue faced by corporate world is the security. This project provides the network security where authorized persons are allowed to access the network and unauthorized persons are denied. This methodology is implemented using Access Control List in VLAN.*

Key Words*: *Network security, IP address, Access control list, VLAN, router, host .

1.INTRODUCTION

Basically ACL is sequence or group of statements which permit or deny access to the network and perform packet filtering to control the network traffic. The third layer of the OSI model transfer the packets. The packets contain source address, destination address and so on . The packets are matched with the conditional statement specified in the ACL. By matching this condition the network security is achieved. Router is used to route the packet to the destination based on the static routing. In Static routing the configuration is done manually to the routers. In this project router permits or denies the access to the server using IP address. Here we combine ACL and VLAN to provide better security for the LAN network and to improve the QOS. VLAN is a group of LAN network which provides security for each single LAN network and also increases the overall performances of the network. VLAN is formed by interfacing the network elements to the ports of the switches.

2. TYPES OF ACL

We probably know that ACL there are different types of ACL is present. We have types based on the versions of IP version4, IP version6, Appletalk etc., IP version 4 access control lists into two different types, standard and extended.

2.1 STANDARD ACL:

Checks source IP address. Permits or denies the entire protocol. The IP address is 1-99. The main disadvantage in standard is that we cannot remove single line of coding, if there is error in the coding whole program should be rewritten.

2.2 EXTENDED ACL:

Extended ACL is used to filter packets on cisco packet tracer based on source and destination IP address 100–199. Extended ACL provides more flexibility and matching traffic than standard ACL

2.3 TYPES OF STANDARD AND EXTENDED ACL:

- Numbered Access Control List
- Named Access Control List

2.3.1 NUMBERED ACL:

Numbers between 1 and 99, 1300 and 1999. In the command section the numbered is given as the command instead of using names.

Syntax:
router(config)#**access-list** *access-list-number* {**permit** | **deny**}{*source* [*source-wildcard*] | **host** *hostname* **| any**
E.g: Router(config)# access-list 1 permit 11.0.3.0 0.0.0.255

2.3.2 NAMED ACL:

The only difference between numbered and named is the name, number is not given in the statement. Names are easier to remember for commands than the numbers.

Syntax :
Router(config)# ip access-list standard name_of_ACL
E.g- Router(config)# ip access-list standard Charles

3. IP ADDRESSING

The IP address is the network layer address. A unique IP address required for each host and network components that communicate using TCP/IP. Each IP address network id and host id. The network id identifies the systems that are available on the same physical network id which is bounded by the IP routers. Host id indentifies the workstation, server, routers, or other TCP/IP host within a network.

3.1 SUBNET MASK

The subnet mask is used to differentiate the network prefix and host id.

Host A: 158.80.164.100 255.255.0.0

Host B: 158.80.164.101 255.255.0.0

Network id:158.80.164.100

Subnet mask: 255.255.0.0

3.2 WILDCARD MASK

Wildcard masking in access list is used for address filtering. This indicates whether the IP address has to be check or ignore by comparing it with the address of the packets in the access list. A wildcard mask is 0 the bits are matched and if it is 1 the bits are not matched. If the wildcard mask is not assigned to the access list by default it is assumed as implicit wildcard mask 0.0.0.0 means all bits must be matched.

3.3 IPSEC PROTOCOL

The IPSEC protocol provides a secured network protocol suite that authenticates and encrypts the data packets. The IPSEC protocol ensures confidentiality and integrity of data communication over a public IP network. IPSEC can encrypt data between devices like

- Router to router
- Pc to router
- Pc to server
- Firewall to router

4. EXPERIMENTAL SETUP

The CISCO PACKET TRACER 6.2 is the user friendly software tool used to analyze the network behavior . The packet tracer is the supplement to the physical system. The physical system involves Switches, Routers, PC'S, Server. The packet tracer allows the user to design their network, allow to discover their network behavior and enable them to identify the error and troubleshooting . The physical network is designed in the Packet tracer by connecting the network components. Then the Routers are configured but writing the commands in the CLI. The IP address is assigned to the host and server. Based on the commands configured on the Router the host can be allowed or denied. The VLAN is created in the existing LAN network and configured on the Switches and Routers.

4.1 VLAN IN ACCESS CONTROL LIST

CODING:

R0 CONFIGURATION

Interface fa0/0.1

Encapsulation dot1Q 10

Ip address 10.1.1.10 255.255.255.0

Interface fa0/0.2

Encapsulation dot1Q 20

Ip address 20.1.1.10 255.255.255.0

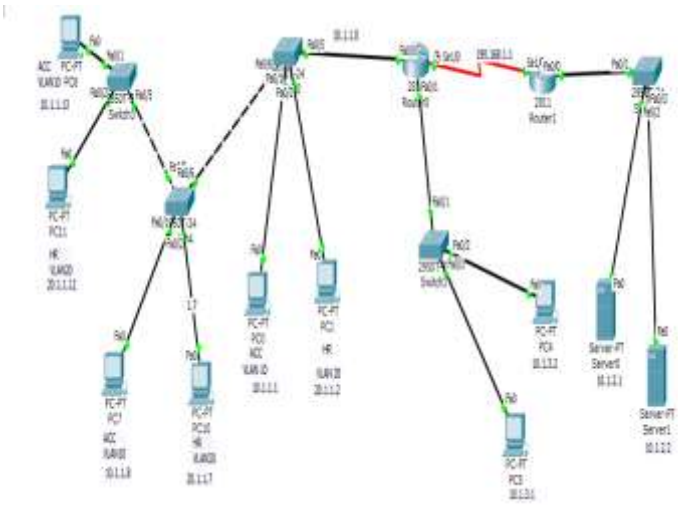

FIG1: VLAN SETUP

R1 CONFIGURATION

R1#

R1#Conf t

Enter configuration commands, one per line. End with CNTL/Z

R1(config)#int fa0/0

R1(config-if)#ip access-group namedstdacl out

R1(config-if)#end

R1#wr

R1#Conf t

Enter configuration commands, one per line. End with CNTL/Z

R1#(Config0#ip access-list standard namedstdacl

R1#(Config-std-nacl)#no 100

R1#(Config-std-nacl)#no 110

R1#(Config-std-nacl)#no 120

R1#(Config-std-nacl)#end

R1#

%SYS-5-CONFIG_I: Configured from console by console

Wr

Building configuration.....

[OK]

R1#sh access-lists

Standard IP access list namedstdacl

10 deny host 10.1.1.1

100 permit host 20.1.1.2

40 deny host 10.1.1.8

120 permit host 20.1.1.12

60 deny host 10.1.1.13

80 deny host 10.1.3.2

70 deny host 10.1.3.1

90 permit any

Now you can observe the seq no 100,110,120 is removed. Now permit 20.1.1.2, 20.1.1.12, 20.1.1.17 with same sequence number.

R1#

R1#Conf t

Enter configuration commands, oner per line. End with CNTL/Z

R1(config)#ip access-list standard namedstdacl

R1(config-std-nacl)#100 permit 20.1.1.2

R1(config-std-nacl)#110 permit 20.1.1.7

R1(config-std-nacl)#120 permit 20.1.1.12

R1(config-std-nacl)#end

R1#

%SYS-5-CONFIG_I: Configured form console by console

Wr

Building configuration.....

[OK]

R1#sh access-lists

Standard IP access list namedstdacl

10 deny host 10.1.1.1

100 permit host 20.1.1.2

40 deny host 10.1.1.8

120 permit host 20.1.1.12

60 deny host 10.1.1.13

110 permit host 20.1.1.7

80 deny host 10.1.3.2

70 deny host 10.1.3.1

90 permit any

R1#

Check connectivity from 20.1.1.2, 20.1.1.12, 20.1.1.7 to access the server.

4.2 OUTPUT

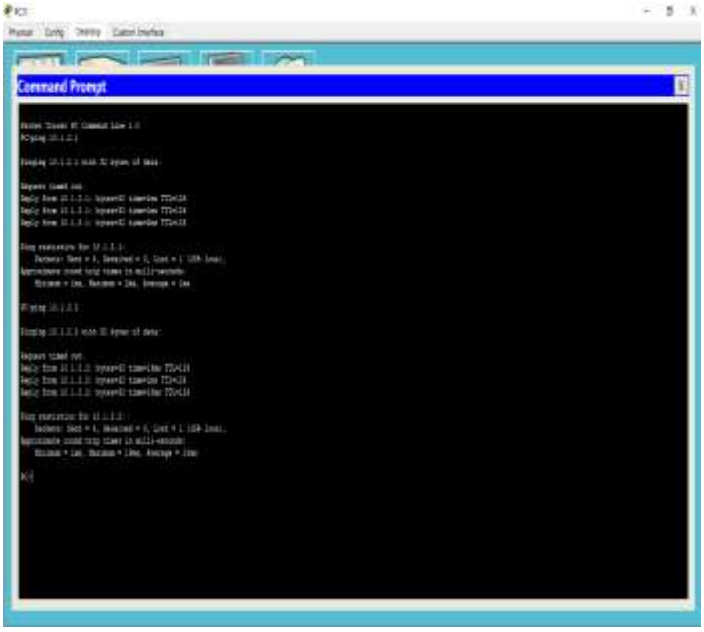

Figure 2 Shows the ping of the server by the HR department

ACL COMMANDS

TABLE1

Command	Description
show ip access-list	Shows only the IP access lists configured on the router
Any	Keyword used to represent all hosts or networks, replaces 0.0.0.0 255.255.255.255 in access list.
Host	Keyword that specifies that an address should have a wildcard mask of 0.0.0.0 (i.e will match only 1 host)
Router >	User EXEC Mode Default mode after booting.
Router #	Privileged EXEC mode Use **enable** command from user exec mode for entering into this mode
Router(config)#	Global Configuration mode Use **configure terminal** command from privileged exec mode
Router(config-if)#	Use **interface <interface name+number>** command from global configuration mode

5. RESULT AND FINDINGS

When an attempt was made to ping router R0 through interface loopback 10.1.1.13,10.1.1.8 10.1.1.1 the ping failed because IP address 10.1.1.13,10.1.1.8 and 10.1.1.1 is denied by applying ACL in VLAN . This blocks the traffic in the LAN network . Figure 2 shows the implementation of ACL in VLAN on R1 by ping test.

6. CONCLUSION

Access Control List are a set of commands configured on a router The routing packets select the optimum path between source and destination. The path selected by the routing protocol. ACLs limit network traffic to increase network performance. ACLs configured on a network provide traffic flow control by restricting the delivery of routing update. It also provides additional security by denying host or IP addresses and is very simple to configure.

7. REFERENCES

[1] *International Nahush Kulkarni1,Harsh Kothari2,Hardik Ashar3, Sanchit Patil published "Access ControlList"- Journal for Research in Applied Science & Engineering Technology (IJRASET) Electronics and Telecommunication Department of K.J SomaiyaCollege of Engineering-Mumbai University.*

[2] *Vishes, Tejas, Tejaswini, Apoorva M Gowda, Siddarth S Bellur, Samarth S Kulkarni, published "Access Control List:Route,filtering and traffic control"- International Journal of Advanced Research in Computer and Communication Engineering (IJARCC) Department of Telecommunication Engineering, BNM Institute of Technology, Bangalore, India*

[3] *Xiao Liu, Brett Holden, and Dinghao WuCollege of Information Sciences and Technology The Pennsylvania State University, published "Automated synthesis of Access Control List" University Park, PA 16802, USA*

[4] *Route Redistribution-A Case Study - ijarcce-www.ijarcce.com/upload/2017/june-17/IJARCCE%2042.pdf*

[5] *Configuring IP Access Lists - Cisco-https://www.cisco.com/c/en/us/support/docs/security/ios.../23602-confaccesslists.html*

[6] *Li Zhu ; Huaqing Mao ; Hang Qin "A Case Study on Access Control Rules Design " 2012 8th International Conference on Wireless Communications, Networking and Mobile Computing.*

[7] *Hirokazu Sayama, Noriaki Yoshiura "Test tool for equivalence of access control list" 2012 14th Asia-Pacific Network Operations and Management Symposium (APNOMS)*

[8] *Kei Wakabayashi ; Daisuke Kotani ; Yasuo Okabe "Traffic-aware Access Control List Reconstruction" 2020 International Conference on Information Networking (ICOIN)*

[9] *Cisco Systems Inc. http://www.cisco.com*

[10] *Sharat Kaushik, Anita Tomar, Poonam, "Access Control List Implementation in a Private Network", International Journal of Information & Computation Technology, Vol.4, No. 14, 2014, pp. 1361-1366*