FUDMA Journal of Sciences (FJS)
ISSN online: 2616-1370
ISSN print: 2645 - 2944
Vol. 3 No. 3, September, 2019, pp 264 –269

CORPORATE NETWORK SECURITY USING EXTENDED ACCESS CONTROL LIST (ACL) IN A SIMULATION ENVIRONMENT

[*1]Aliyu Rabiu Karmanje, [2]Olanrewaju Oyenike Mary, [3]Shamsuddeen Falalu

[1]Maxair Ltd, Kano, Nigeria
[2]Computer Science Department, Federal University Dutsinma, Katsina, Nigeria
[3]Independent National Electoral Commission, Abuja, Nigeria

Corresponding Author's Email: aliyukarmanje@gmail.com

ABSTRACT
Routers (sometimes gateways) are important devices in internetworks. Routers play the task of interconnecting and partly securing network devices by forwarding packets from source address to destination address. Security on routers is achieved by determining whether packets to be forwarded are authorized to get to their desired destination. This action can be carried out by exploiting misconfigured ACL (Access Control List). ACL is a list of rules that determine whether and how to forward or discard a packet on a network i.e. it filters packets. ACL can also be used for implementing network policies such as NAT (Network address Translation). A correct ACL configured on a router examines each packet to determine whether to forward or drop the packet, this decision is based on the rules specified within the access lists leading to secure network and packet flow. In corporate organizations sometimes there is an interconnection between various LANs but not all devices are allowed to access a device on particular LAN because of the nature of the resources on that device, hence in such scenario ACL is a good choice when looking for the appropriate tool to control the device access. In this paper we have designed a model of a corporate network with 3 Local Area Networks (LANs), and packets traverse the devices on the LANs). After applying the correct ACL configurations on the LAN 2 Router access is restricted on LAN 2 server, which now only receives packets from an authorized device, this greatly enhances the security of the LAN.

Keywords **–** Ping of Death, Zombie, DoS, DDoS, Smurf Attack.

INTRODUCTION

Cisco .Inc initiated the idea of access-lists in the routing world, and hence the feature has existed on devices prior to IOS version 10.3. Access-lists have been used to support a wide variety of protocols, but protocols for IPv4 are undoubtedly the most familiar. Acting primarily as packet filters, these configuration features can act on a number of criteria. In most cases, there are two actions that access-lists take, permit, which allows the packet to pass, and deny, which drops the packet (Balchunas, 2014).

Cisco provides Access Control Lists (ACLs) to control traffic flow from one interface to the other in a network or between networks. ACL also performs other tasks such as restricting telnet, filtering routing information and prioritizing WAN traffic with queuing (Suman and Agrawal, 2016).

ACL is of two types:

- ***Numbered ACL:*** Unique number is assigned to each ACL.
- ***Named ACL:*** Unique name is assigned to each ACL.

Each of the above ACLs can be implemented as:

- ***Standard ACL:*** ACL is applied on destination router. It *permits* or *deny* the packet on the basis of source addresses only.
- ***Extended ACL:*** ACL is applied on source router. It permits or deny the packet on the basis of source as well as destination addresses.

ACL is created in the global configuration mode. After creating the basic group of ACL commands, there is need to activate them (Cisco Systems). For traffic filtering between interfaces, ACL needs to be activated in Interface specific-configuration Mode (Rinehart, 2013). Hence, the direction of filtering the traffic is classified into: inbound and outbound.

If a single host is to be permitted or denied into a network the syntax is:
permit/deny <source IP address> <wildcard mask>
e.g. permit/deny 192.168.10.10 0.0.0.255

If a single network is to be permitted or denied into a network the syntax is:
permit/deny <Network ID> <wildcard mask>
e.g. permit/deny 192.168.10.0 0.0.0.255

If the whole network is to be permitted or denied, the syntax is:
permit/deny 255.255.255.255 255.255.255.255
or *permit/deny any any*

Wild Card Masks

IP access-lists use wildcard masks to determine two things:

1. Which part of an address must match exactly
2. Which part of an address can match any number

This is as opposed to a subnet mask, which tells what part of an address is the network (subnet), and what part of an address is the host. Wildcard masks look like inversed subnet masks (Velte and Velte, 2014). Consider the following address and wildcard mask: Address: 172.16.0.0 Wild Card Mask: 0.0.255.255. Table 1 shows the wildcard mask of network Classes A. B and C.

Table 1: Wildcard Mask

CLASS	*SUBNET MASK*	*WILDCARD MASK*
A	255.0.0.0	0.255.255.255
B	255.255.0.0	0.0.255.255
C	255.255.255.0	0.0.0.255

RELATED WORK

Kaushik et al. (2014) analyzed and simulated a proposed network using Standard ACL and Extended ACL in packet tracer and demonstrates how powerful ACL can be for IP traffic management. One of the drawbacks in the method is the use of standard ACL to carry out the experiment and standard ACL has restrictions over which protocols and what port numbers to restrict.

Zhian (2011) use results of their experiments, for dynamically setting of different types of ACLs to improvise network infrastructure and performance. They discussed and experimented how frequently ACLs should be updated, updates of passive versus active ACL, and how frequently the updates should be downloaded on routers so it does not effect CPU utilization of routers. However the paper does not consider the network throughput, network equipment resource occupation and other factors.

Tomar and Tyagi (2014) present various optimization mechanisms to achieve an optimal ACL which reduces the Packet latency; they also proposed an efficient optimization algorithm to optimize the ACL to enhance network performance. In this work, there is absence of appropriate algorithms and ACL rules applied on the network edge devices.

Bobyshev et al. discuss and experiment on how regularly ACLs should be updated, how updates of passive versus active ACL, and how frequently the updates should be downloaded on routers so it must not affect CPU utilization of routers. They showed how dynamically setting of different types of ACLs can improve network performance. The drawback with this experiment is it centered towards performance evaluation without putting into consideration the security effect of the loads on the devices.

Bansal and Sharma (2016) define how privilege level and access-control mechanism works, how to implement them and how they provide internal security to network. Their research implements such type of mechanisms in all network devices, and an optimized network performance is achieved. However the experiment implements privilege level access control only on layer 3 devices.

METHODOLOGY

PACKET TRACER

Packet Tracer (PT) is virtual networking simulation software developed by Cisco, to learn and understand various concepts in computer networks. Networking devices appear in packet tracer as they look in reality and a student/ researchers can interact with networking devices, customize configurations, model networks etc. With Packet Tracer one can track flow of a packet, when it travels from source to destination, individuals can also learn how to troubleshoot networks. Packet Tracer can also be used to learn networks more clearly by modeling different scenarios (Javid, 2014). Figure 1 shows packet tracer workspace.

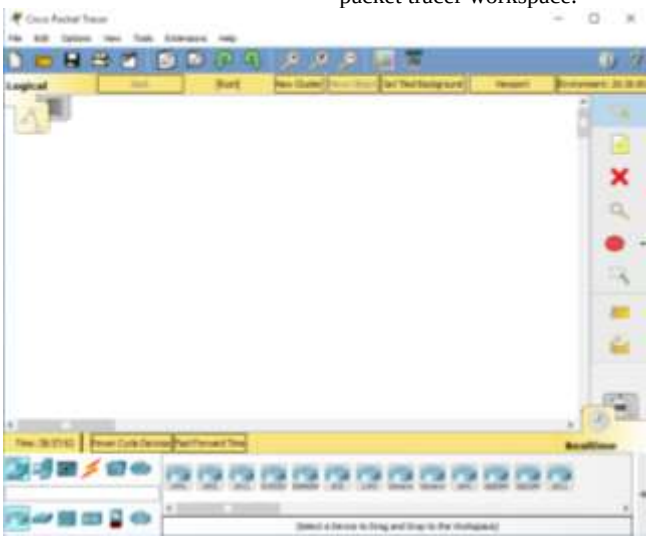

Fig 1: Packet Tracer Workspace

STANDARD ACL

The Standard ACLs filters the source IP address in an IP packet. It is also used to restrict telnet access to the router. ACL number for standard ACL ranges from 1 to 99 and 1300 to 1999. An entry can be created in a standard numbered IP ACL by using the *access-list* command (Cisco Systems)(Todd, 2013). The syntax of this command is:

access-list <ACL_#> <permit/deny> <source_IP address> <wildcard mask>

where,

source_IP address – Specifies the IP address of the source.

After creating the standard ACL, it must be activated on the routers interface. The IP access-group command activate the ACL on the interface. The following steps are followed to activate the standard numbered ACL:

i. Log into the router.
ii. Switch to the privileged mode
iii. Switch to the configured mode.

iv. Type *interface type slot/port* to configure on the router's port.

v. Type *ip access-group ACL_# in/out* to activate the standard numbered ACL on the configured interface.

EXTENDED ACL

Extended access control lists can evaluate many of the other fields in the layer 3 and layer 4 headers of an IP packet. They can evaluate source and destination IP addresses, the Protocol field in the Network layer header, and the port number at the Transport layer header. This gives extended access lists the ability to make much more granular decisions when controlling traffic. Extended access list numbers range from 100 to 199. The 2000–2699 range is also available for extended IP access lists.

Steps to create and implement Extended ACL:

i. Creating

access-list <100-199> <deny/permit> <main protocol> <source address> <source wilcardmask> <destination address> <destination wilcardmask> <operator> <sub protocol>

ii. Assigining

interface <name and number>
ip access-group <acl number> <in/out>

NETWORK DESIGN AND CONFIGURATION

i. Network Modeling

Modeling the network using packet tracer platform, network devices like routers, switches and various virtual links were used for connection. In the network, Routing Information Protocol (RIP) was implemented as the primary routing protocol that enables the network devices to intercommunicate from different networks. Figure 2 is the design of the modeled network.

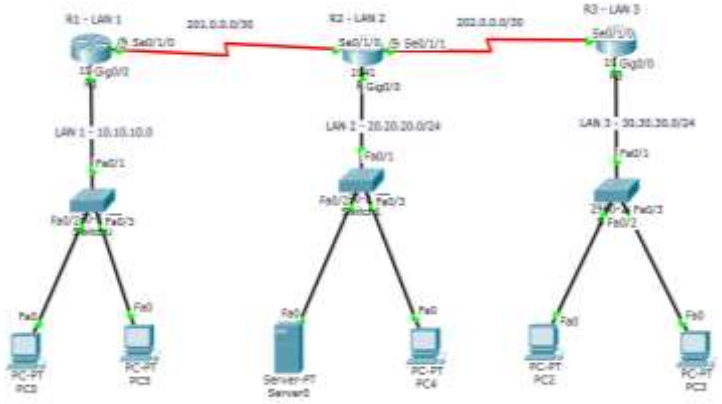

Fig. 2: Network Topology

Fig. 2: is the design of an internetwork with 3 local area networks connected by 3 routers, the networks are LAN 1, LAN 2 and LAN 3. In this scenario the devices on LAN 1 and LAN 3 are restricted access to LAN 2 devices, hence all traffic directed to LAN 2 Server from LAN 1 and LAN 3 is discarded, and other traffics are allowed access.

The configuration applied on router 2 is:

```
R2>en
R2#show running-configuration
Building configuration...

Current configuration : 962 bytes
!
!
hostname R2
!
!
!
interface GigabitEthernet0/0
ip address 20.20.20.1 255.255.255.0
ip access-group 101 out
!
interface Serial0/1/0
ip address 201.0.0.2 255.255.255.252
!
interface Serial0/1/1
ip address 202.0.0.2 255.255.255.252
!
!
router rip
version 2
```

```
network 20.0.0.0
network 201.0.0.0
network 202.0.0.0
no auto-summary
!
!
access-list 101 deny ip any host 20.20.20.2
access-list 101 permit ip any any
!
!
End
```

After applying the above configurations on the routers, the network traffic behaves as shown in Fig. 3.

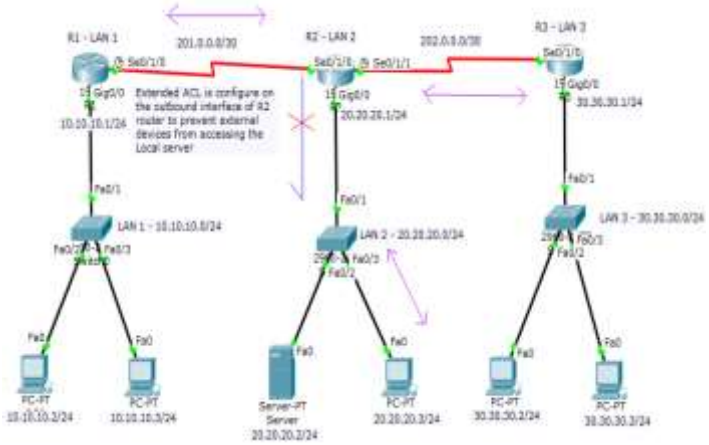

Fig. 3: Configured Network

After applying the correct Extended ACL configurations on Router 2 outboud interface (Gigabit Interface 0/0) all packets sent to Server from outside LAN 2 are dropped immediately they reached the interface. This provides a security mechanism for access restriction to the Server on LAN 2 and also increase the overall Quality of Service on the network.
The IP address used in the 3 LANs is shown in Table 2

Table 2: IP Address of the LANs

LAN	***IP Address Range***
1	*10.10.10.1/24*
2	*20.20.20.0/24*
3	*30.30.30.0/24*

I. RESULTS

After the Extended ACL configuration is applied on router 2 the network traffic analyzed is in Figure 4.

```
Packet Tracer PC Command Line 1.0
C:\>ping 20.20.20.2

Pinging 20.20.20.2 with 32 bytes of data:

Reply from 201.0.0.2: Destination host unreachable.
Reply from 201.0.0.2: Destination host unreachable.
Reply from 201.0.0.2: Destination host unreachable.
Reply from 201.0.0.2: Destination host unreachable.

Ping statistics for 20.20.20.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 20.20.20.3

Pinging 20.20.20.3 with 32 bytes of data:

Request timed out.
Reply from 20.20.20.3: bytes=32 time=15ms TTL=126
Reply from 20.20.20.3: bytes=32 time=14ms TTL=126
Reply from 20.20.20.3: bytes=32 time=16ms TTL=126

Ping statistics for 20.20.20.3:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 14ms, Maximum = 16ms, Average = 15ms
```

Fig. 4: PC0 (LAN 1) to LAN 2

In Fig. 4 ICMP echo packets from PC0 on LAN 1 cannot reach the Server (20.20.20.2) on LAN 2, but ICMP echo packets from the same PC can reach PC4 (20.20.20.3) on LAN 2.

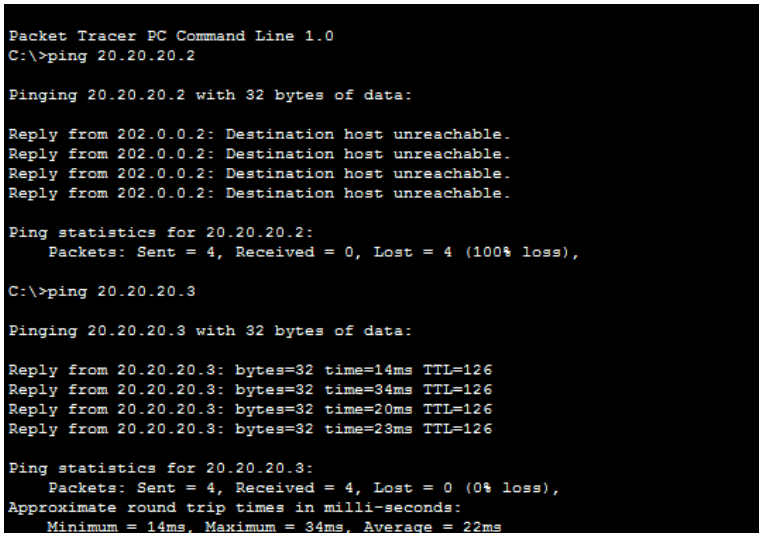

Fig. 5: PC5 (LAN 3) to LAN 2

In Fig. 5 ICMP echo packets from PC5 on LAN 3 cannot reach the Server (20.20.20.2) on LAN 2, but ICMP echo packets from the same PC can reach PC4 (20.20.20.3) on LAN 2.

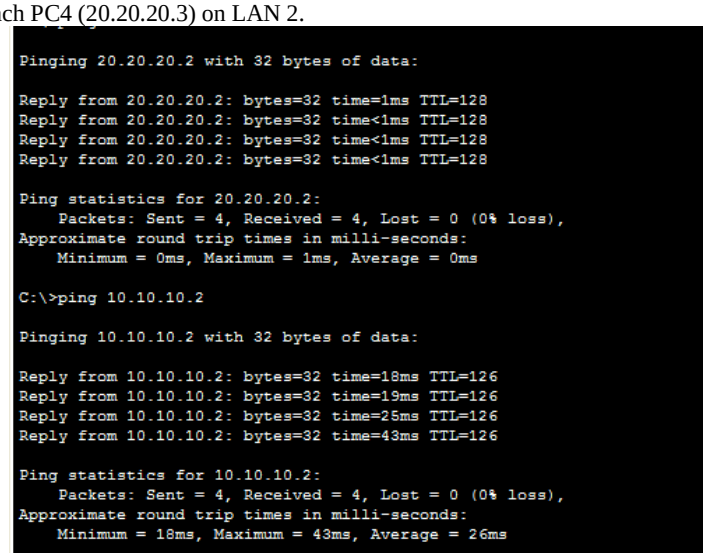

Fig. 6: PC4 (LAN 2)

In Fig. 6 ICMP echo packets from PC4 on LAN 2 can reach the Server (20.20.20.2) on LAN 2, it also can reach PC0 (10.10.10.2) on LAN 1.

From the above figures it can be observed that due to Extended ACL being applied on router 2 which is the gateway of LAN 2, all devices on LAN 1 and LAN 3 cannot exchange packets with the Server on LAN 2 but can communicate with other devices on the same LAN, this gives us the ability to make a servers/ devices that stores sensitive and crucial information of the organization local, which does not need to be accessed by devices outside its LAN.

CONCLUSION

This work demonstrates how ACL can be a great tool to control resource access on corporate networks. Both standard ACL and extended ACL, which are applied on a router, were elucidated. The standard ACL create filters based on source addresses only and are used for server based filtering, whereas extended ACL provide more security by creating filters based on source addresses as well as destination addresses, protocol and port number. The extended ACL in this paper used TCP/IP protocol which restricts access to the local server on LAN 2. Routing Information Protocol (RIP) is used for routing the packets.

In future work, more IP and TCP protocols can be used in extended ACL. Apart from RIP routing protocols, EIGRP, OSPF and BGP routing protocols can be used to route packets.

REFERENCES

Bansal R. and Sharma P. (2016), Implementation of Privilege Level and Access - Control Mechanism for Network Securitv. *International Journal of Advance Research and Innovative Ideas in Education, Vol-2 Issue-4, p 957-962 ISSN(O) - 2395-4396*

Balchunas A. (2014), CCNA Study Guide *v2.71.*

Bobyshev A., DeMar P., Lamore D., Fermilab, and Batavia (n.d), Effect of Dynamic ACL (Access Control List) Loading on Performance of CISCO Routers.

Javid R. (2014), Role of Packet Tracer in learning Computer Networks, *International Journal of Advanced Research in Computer and Communication Engineering Vol. 3, Issue 5, pp 2278-1021 www.ijarcce.com 6508*

Kaushik S., Tomar A, and Poonam (2014), Access Control List Implementation in a Private Network, *International Journal of Information & Computation Technology, Vol. 4, No. 14, pp. 1361-1366.*

Rinehart J. (2013), Demystefying Switch-based ACLs, *Global Knowledge Expert Reference Series of White Papers.*

Suman S. and Agrawal A. (2016), IP Traffic Management With Access Control List Using Cisco Packet Tracer, *International Journal of Science, Engineering and Technology Research (IJSETR) Volume 5, Issue 5,p 1556-1561 ISSN: 2278 – 7798*

Todd T. (2013), Cisco Certified Network Associate Study Guide, Wiley Publishing, Inc., *8th Edition.*

Tomar K. and Tyagi S. S. (2014), Enhancing Network Security And Performance Using Optimized ACLs, *International Journal in Foundations of Computer Science & Technology (IJFCST), Vol.4, No.6 pp 25-35*

Velte A. and Velte T. (2014), Cisco - A Beginner's Guide, McGrawHill Inc, *5th edition.* Cisco Systems Inc. http://www.cisco.com

Zhian L. (2011), Study of Network Optimization Method Based on ACL, Published by Elsevier Ltd. *Selection and/or peer-review under responsibility of [CEIS]. Procedia Engineering Journal, Vol. 15, p 3959-3963*