International Journal of Information & Computation Technology.
ISSN 0974-2239 Volume 4, Number 14 (2014), pp. 1361-1366
© International Research Publications House
http://www. irphouse.com

Access Control List Implementation in a Private Network

Sharat Kaushik[1], Anita Tomar[2,] Poonam[3]

[1] *Department of Computer Science & Engineering, NGFCET, Palwal, Haryana*
[2] *Department of Computer Science & Engineering, NGFCET, Palwal, Haryana*
[3] *Department of Computer Science & Engineering, NGFCET, Palwal, Haryana*

Abstract

With the dramatic growth of internetwork ACL's now become very important for network administrator. ACLs are one of the main features of today's internetwork router. Routers generally check each incoming packet against the rule of the ACL which are defined by the network administrator. These rules decide which network traffic is permitted and which type of network is denied. In this paper we configure a standard ACL in a private network to provide security for the network of the organisation by providing traffic flow control. It makes the router capable for performing the filtering of network packets which travels in or out of the router interfaces to increase the speed & performance of the server. It also restrict network usage by certain users or devices to enhance security. This all experiment with network behaviour is done on the Cisco packet tracer 6.0.1.

Keywords: ACL, cisco, packet tracer, rule, router.

INTRODUCTION

The ACL is basically a sequence or setoff rules also called ACL entries. These rule specify the type of network traffic that can be passed or block through a router. ACLs are deployed at almost all points of entry in a private network and outside internet. So that all the network traffic that is incoming and outgoing packet can be monitored. Different protocols can be used in ACLs like IPX, AppleTalk etc.

A packet is basically contains a limited number of fields such as source or destination port no., IP address, the source and destination protocols type etc. Every packet is matched with the rules of the ACL starting from the first rule and so on until it match with the rule or the last Statement. This matching process decides how to apply the network security.

The structure of a typical rule, using CISCO IOS notation might be:

```
permitip 10.1.2.0 0.0.0.255 host 10.2.2.1 eq http
```

An ACL contains many rules and there can be conflicts between these rules such as redundancy, shadowing etc [1]. So the ACLs must be managed carefully so that the conflicts can be resolved[2].The Rule sets are generally composed of number of rules ranging from tens to five thousand [3].

TYPES OF ACLS

Mainly two types of ACLs can be configure on the routers. These are as follows:

- Standard ACL – This allows or denies packets based on IP address of source. Valid range of standard ACL IDs are from 1 – 99 or also can be a string.
- Extended ACL – This allows or denies packets based on protocol information and also based on IP address of source and destination. Valid range of extended ACL IDs are from 100 – 199 or also can be a string.

Standard ACLs permit or deny packets based on source IP address. You can configure up to 99 standard ACLs. You can configure up to 1024 individual ACL entries on a device. There is no limit to the number of ACL entries an ACL can contain except for the system-wide limitation of 1024 total ACL entries.

Extended ACLs let you permit or deny packets based on the following information:

- IP protocol
- Source IP address or host name
- Destination IP address or host name
- Source TCP or UDP port (if the IP protocol is TCP or UDP)
- Destination TCP or UDP port (if the IP protocol is TCP or UDP)

The ACLs can also be used in filtering route advertisements and also in enforcing network policies such as traffic shaping and NAT(network address translation)[4].

ACCESS LIST SYNTAX

- Standard IP Access List Configuration Syntax[5].

  # access-list access-list-number {permit | deny}source {source-mask}ip access-group access-list-number {in | out}

- Extended IP Access List Configuration Syntax

  #access-list access-list-number {permit | deny}protocol source {source-mask} destination{destination-mask}ip access-group access-list-number {in | out}

- Named IP Access List Configuration Syntax

  #ip access-list {standard | extended} {name |number}

EXPERIMENTAL SETUP

In this the experiment with network behavior is done on the Cisco packet tracer

6.0.1.Cisco Packet Tracer is a powerful network simulation program which allows students to experiment with the network behaviour and enables them to ask “what if” type questions. Packet Tracer acts as a supplement for physical equipment in the classroom as it allowing students to create a computer network with an almost any number of devices, encouraging the practice, discovery and the troubleshooting.

Initially a physical network is created with PCs, routers, switches, server and connections using Cisco packet tracer 6.0.1.Then the routers are configured and route is established by writing command in CLI.At this point all the packets are received by the server.Then standard ACL is created & configured on the router closed to the destination. The standard ACL don’t have any information regarding destination so it must be placed as close to the destination as possible.

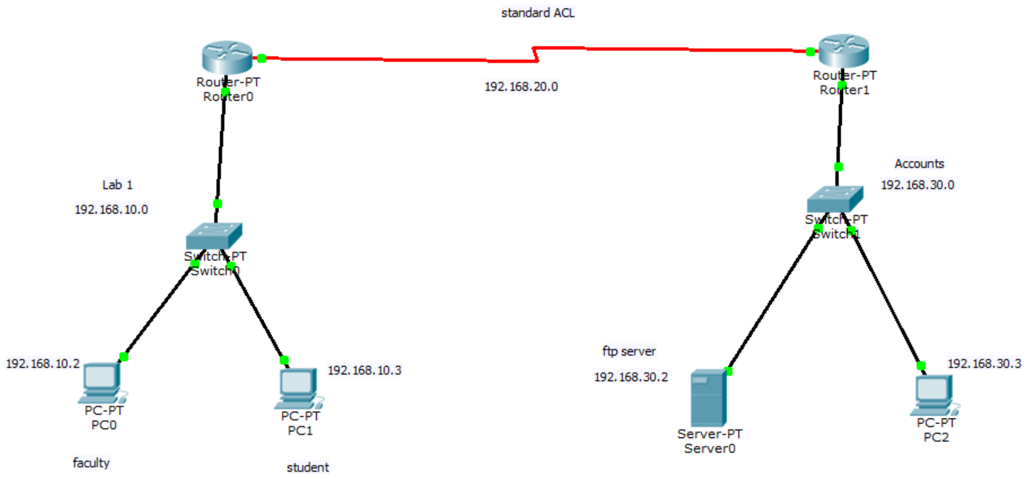


Fig.1 Private network

CREATING & CONFIGURE ACL

- USING THE CLI

```
Router(config)#access-list 1 deny host 192.168.10.3
Router(config)#access-list 1 permit 192.168.10.2
Router(config)#access-list 1 permit any
Router(config)#interface fastethernet 0/0
Router(config-if)#ip access-group 1 out
Router(config-if)#write memory
```

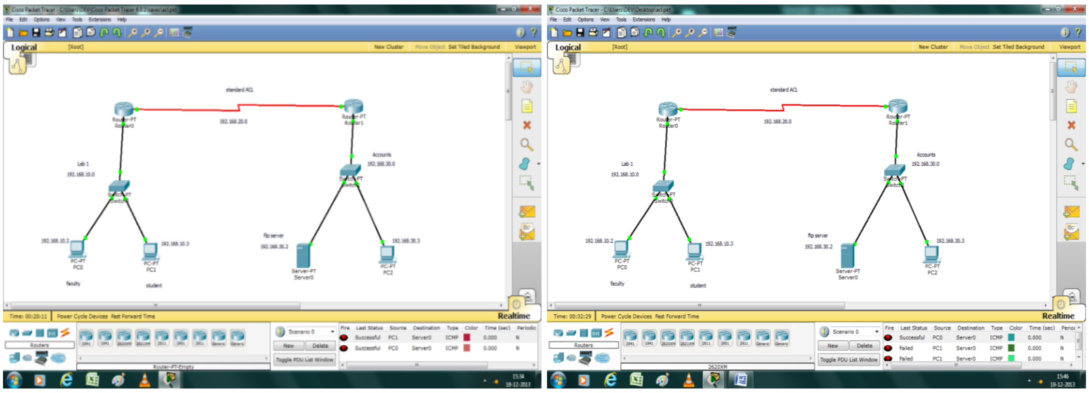
The host <source-ip> | <hostname> parameter makes you able to specify a host IP address or host name. When this parameter is used in ACL rule, there is no need to specify the network mask. A default mask of all zeros i.e. 0.0.0.0 is implied.

The any parameter is used to configures the security policy to match on all the host addresses.

The log argument is used to configure the network device to generate entriesin Syslog and also SNMP traps for those packets which are denied by the access policy.

RESULT ANALYSIS

- Before applying standard ACL:

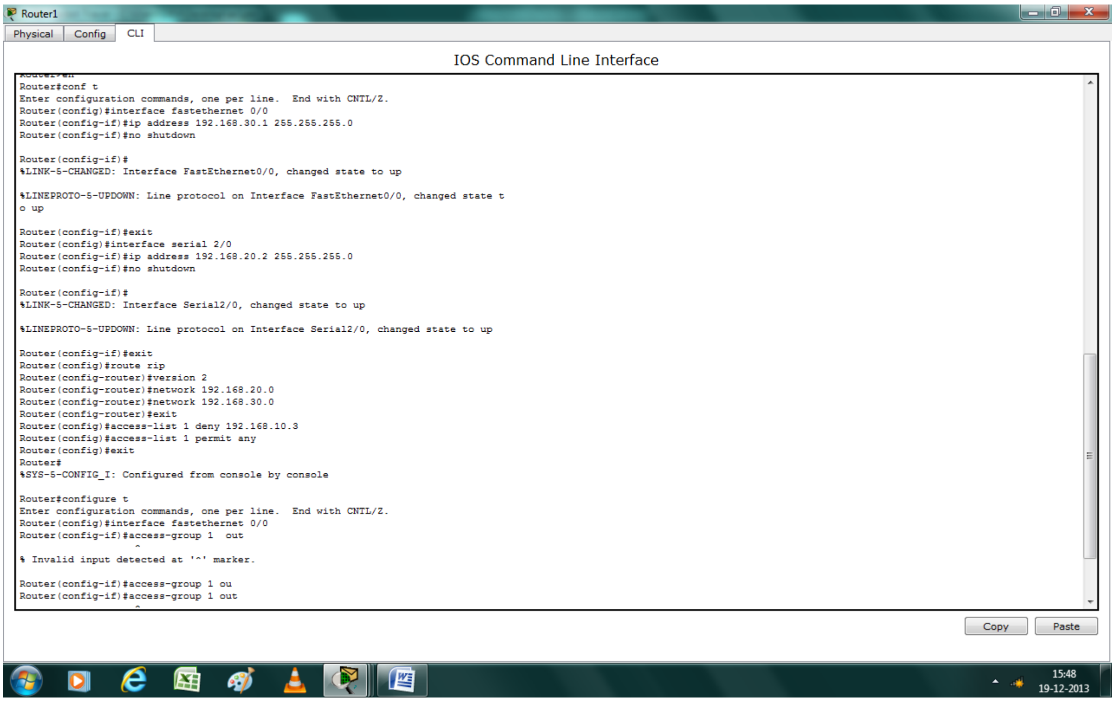


Fire	Last Status	Source	Destination	Type	Color	Time (sec)	Periodic
●	Successful	PC1	Server0	ICMP	🟥	0.000	N
●	Successful	PC0	Server0	ICMP	🟥	0.000	N

Fire	Last Status	Source	Destination	Type	Color	Time (sec)	Periodic
●	Successful	PC0	Server0	ICMP	🟦	0.000	N
●	Failed	PC1	Server0	ICMP	🟩	0.000	N
●	Failed	PC1	Server0	ICMP	🟩	0.000	N

Fig.2 Before & after applying standard ACL

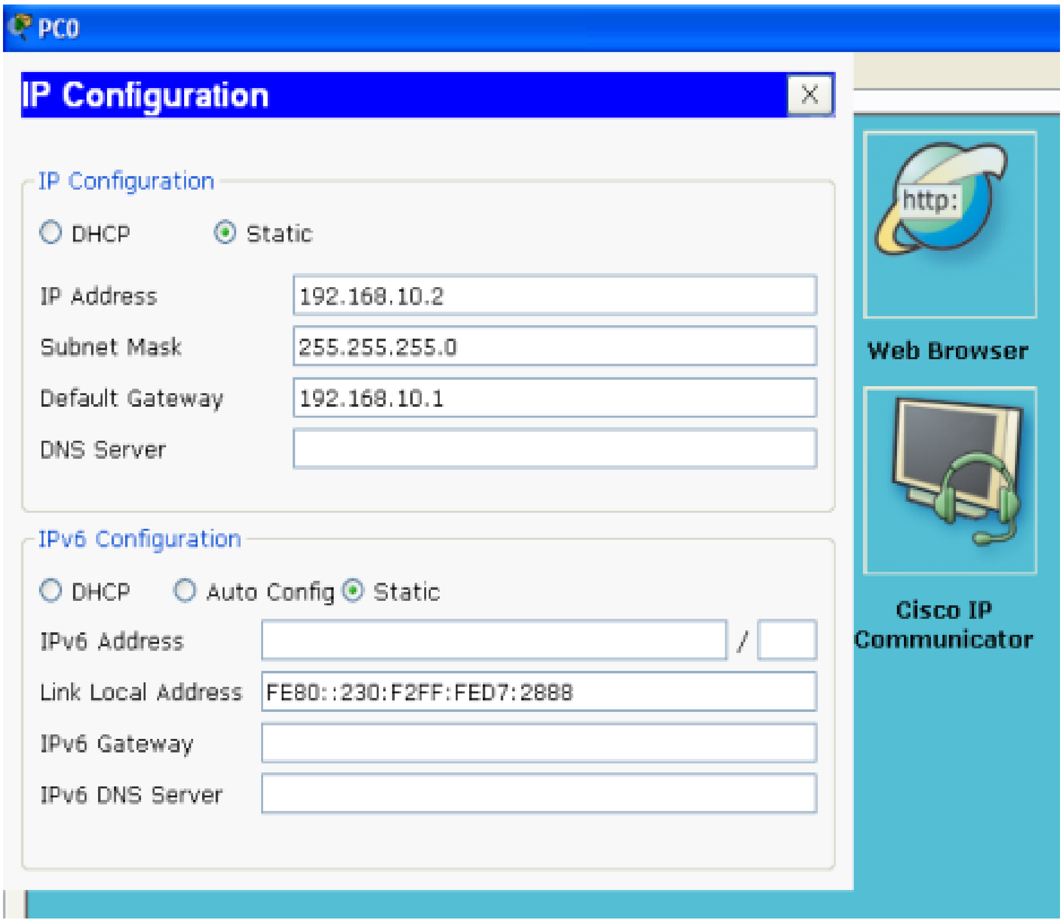
- Define route and configure ACL



```
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface fastethernet 0/0
Router(config-if)#ip address 192.168.30.1 255.255.255.0
Router(config-if)#no shutdown

Router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state t
o up

Router(config-if)#exit
Router(config)#interface serial 2/0
Router(config-if)#ip address 192.168.20.2 255.255.255.0
Router(config-if)#no shutdown

Router(config-if)#
%LINK-5-CHANGED: Interface Serial2/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial2/0, changed state to up

Router(config-if)#exit
Router(config)#route rip
Router(config-router)#version 2
Router(config-router)#network 192.168.20.0
Router(config-router)#network 192.168.30.0
Router(config-router)#exit
Router(config)#access-list 1 deny 192.168.10.3
Router(config)#access-list 1 permit any
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#configure t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface fastethernet 0/0
Router(config-if)#access-group 1  out
                   ^
% Invalid input detected at '^' marker.

Router(config-if)#access-group 1 ou
Router(config-if)#access-group 1 out
```

Fig.3 ACL Configuration

Configuring IPs:



PC0

IP Configuration

IP Configuration

○ DHCP ● Static

IP Address 192.168.10.2

Subnet Mask 255.255.255.0

Default Gateway 192.168.10.1

DNS Server

IPv6 Configuration

○ DHCP ○ Auto Config ● Static

IPv6 Address /

Link Local Address FE80::230:F2FF:FED7:2888

IPv6 Gateway

IPv6 DNS Server

Fig.4 IP Configuration

VII. CONCLUSION

This standard ACL provide security for the network of the organisation by providing traffic flow control. It enables the filtering of network packets flow *in* or *out* of router interfaces and hence increase the speed & performance of the server. It restrict network usage by certain users or devices.

In this experiment the standard ACL is configured on the router. It create filters based on source addresses and are used for server based filtering. In future the more security can be provided by creating filters based on source addresses, destination addresses, protocol, port number and other features and are used for packet based filtering for packets that traverse the network. This all can be done by configuring extended ACL

VIII. REFERENCES

[1] Zhe Chen, ShizeGuo, and RongDuan.Research on the anomaly discovering algorithm of the packet filtering rule sets.In Pervasive Computing Signal Processing and Applications (PCSPA), 2010 First International Conference on, pages 362-366, sept. 2010.

[2] S. Pozo, A.J. Varela-Vaca, and R.M. Gasca. A quadratic, complete, and minimal consistency diagnosis process for firewall acls. In Advanced Information Networking and Applications (AINA), 2010 24th IEEE International Conference on, pages 1037-1046, april 2010.

[3] David E. Taylor.“Survey and taxonomy of packet classification techniques.”ACM Computing Surveys, Vol. 37, No. 3, 2005. Pages 238-275

[4] A. Velte and T. Velte.“Cisco: A Beginner’s Guide”, McGraw-Hill Inc. 3rd edition (2004).

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