APPLICATION OF ACCESS CONTROL LIST FOR NETWORK SECURITY AT CISCO ROUTER AS A FIREWALL

Diky Heryanto, Salma Azizah*

S1 Teknik Komputer, Fakultas Ilmu Komputer, Universitas Amikom, Yogyakarta, Indonesia

*salma.azizah@students.amikom.ac.id

ABSTRACT

The provision limiting access to network users is one of the defensive action system from cyber attacks that can occur through a network connected to the user. Installation ACL device the router can be a firewall, where each incoming and outgoing packets will be matched with a list of existing entries, and then will proceed preconfigured actions

Keywords: Access Control List, Firewall, Cisco, Router, Packet Filtering.

INTRODUCTION

Connection from a network into a bridge connecting a device with other devices to interact in the network. Each device in the network will have an IP address (Internet Protocol), as well as when sending a message to someone certainly in need of an address which is the goal of the IP messaging has become an address of a destination device. Because each user connected in a network can communicate with other users connected on the same network it is a gap that is used by an attacker to attack users who are on the network. Therefore we need a protection on the network, as well as blocking access restrictions port which can be a gap for the attacker is one way to address the problem. By restricting users to access some port only, it is useful to minimize the attack on the network. Application of ACL (Access Control List) on router can be a protective firewall, only allow packets in accordance with the provisions are allowed to pass through.

LITERATURE REVIEW

A firewall is needed to safeguard important data from hacker attacks on the company's internal network. Firewall as an important defense on the network can protect the flow of data on a network. In that study chose Cisco Asa 5510 Series as a firewall because it has a fairly sophisticated features such as, remote access, Intrusion Prevention, Content Security, Unified Communications, Botnets, and other features that support this research [1]. Cisco routers contained in Access Control List as a security facility to filter incoming and outgoing data. Access Control can be implemented through hardware in embedded on the device router Cisco, namely IP Access Control List. In using the ACL there are rules that have to be made to do filtering data packets through the lines of the rules in the ACL. To filter the data packets in interfaces can be done through two directions, namely ACL inbound to filter incoming data packets through interfaces and ACL outbound to filter the data packets to be out of interface [2].

In previous research administrator network computers are expected to apply the Access Control List IP network security systems such as firewalls, strengths and weaknesses of what is contained in the package filtering firewall using IP Access Control List. The findings contained in these studies have provided a better understanding of computer network administrator at execution packet filtering firewall with Cisco IP ACL and understand the potential security vulnerability [2]. Setting the ACL on a layer internetwork be one way to close the security gap, the ACL is used to allow or reject the package of host with a specific purpose. ACL contained in the rules and conditions that determine and define the process network traffic at router whether the packet will be forwarded or not [3]. Utilizing the access list feature on Cisco routers can be used to enhance network security. Such access is used to determine any party which may or may not access information or network devices that exist in the computer network [4].

Securing computer networks become very important today. Application of firewall be the first step to anticipate the attack exploits that attack specific computer security. By utilizing Cisco Router device into one of the benefits of firewall implementations [5]. Packet filtering check which packages are to be transferred between computers on the Internet [6]. Made framework for analyzing automatically ACL that will simplify the task of network administrators in the verification of company's security policy [7]. By using a firewall can support multiple security policies. A firewall is also configured to be utilized packet filtering and utilizing the results cache for bypass package that will come [8]. A study proposes to optimal packet filtering though most prefer to use deterministic techniques and not exploittraffic [9].

RESEARCH METHODS

Researchers used a research method by conducting experiments on simulated network implementations with Cisco's Packet Tracer software version 7.2.2 on Windows operating systems research 10. Flow is illustrated by the diagram flow chart in Figure 1.

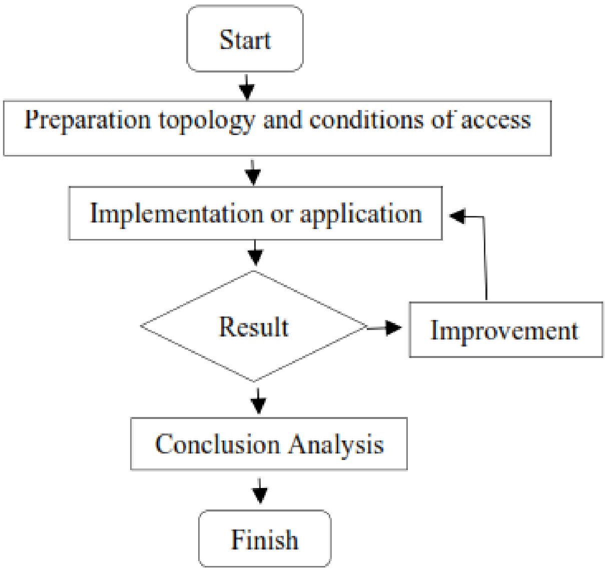

Start
Preparation topology and conditions of access
Implementation or application
Result
Improvement
Conclusion Analysis
Finish

Figure 1 Flowchart Research

A. Desain of Network Topology

The design of the network topology below as a test of the application ACL as in Figure 2.

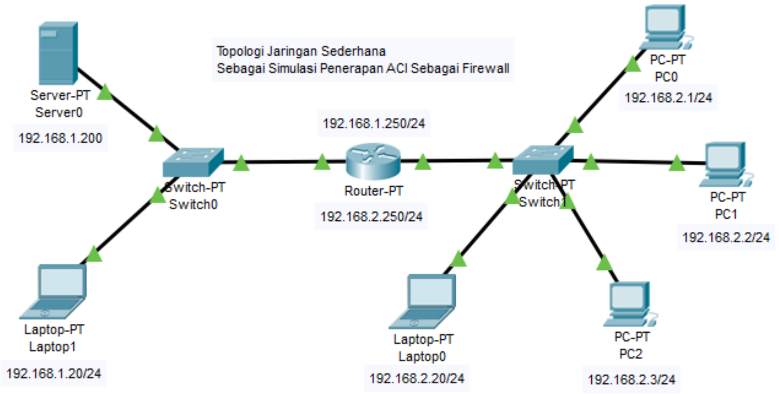


Figure 2 Network Topology

Figure 2 is based on network topology devices used in the simulation comprises:

Table 1. List of required device

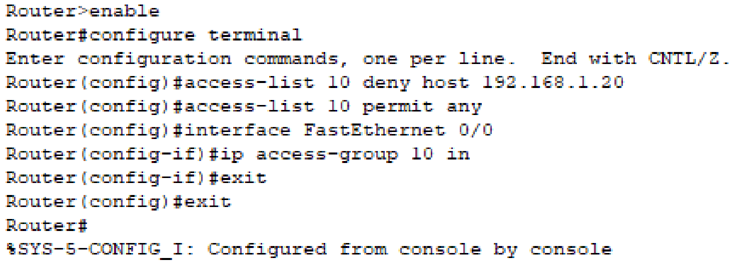
Device	Amount
Server	1
Router	1
Switch	2
PC / Laptop	5

B. Access Restrictions

Before performing an admin access restrictions must know beforehand what is needed by user who will use device The order to access according to the needs required [10].

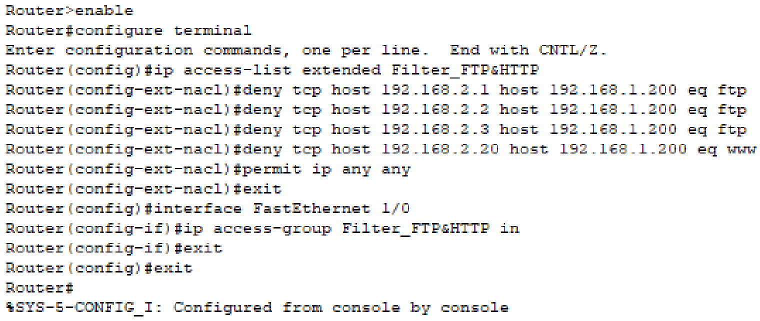
C. Configuration

ACL configuration for standard where device 2 laptop can’t communicate with device network 192.168.2.0/24. Standard ACL configuration commands shown in Figure 3.



```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#access-list 10 deny host 192.168.1.20
Router(config)#access-list 10 permit any
Router(config)#interface FastEthernet 0/0
Router(config-if)#ip access-group 10 in
Router(config-if)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
```

Figure 3 Configuration Standard ACL



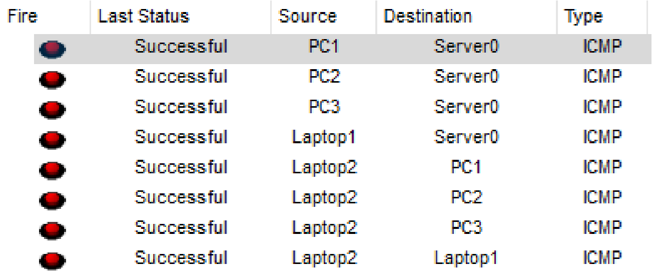
```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#ip access-list extended Filter_FTP&HTTP
Router(config-ext-nacl)#deny tcp host 192.168.2.1 host 192.168.1.200 eq ftp
Router(config-ext-nacl)#deny tcp host 192.168.2.2 host 192.168.1.200 eq ftp
Router(config-ext-nacl)#deny tcp host 192.168.2.3 host 192.168.1.200 eq ftp
Router(config-ext-nacl)#deny tcp host 192.168.2.20 host 192.168.1.200 eq www
Router(config-ext-nacl)#permit ip any any
Router(config-ext-nacl)#exit
Router(config)#interface FastEthernet 1/0
Router(config-if)#ip access-group Filter_FTP&HTTP in
Router(config-if)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
```

Figure 4 Configuration Extended ACL

Then to the configuration extended in the provision of ACLs configured are each PC 1, PC 2, PC 3 can access to the HTTP server but can't access to the FTP server, while the laptop one can access to the FTP server but can't access to the HTTP server. For extended ACL configuration is shown in Figure 4.

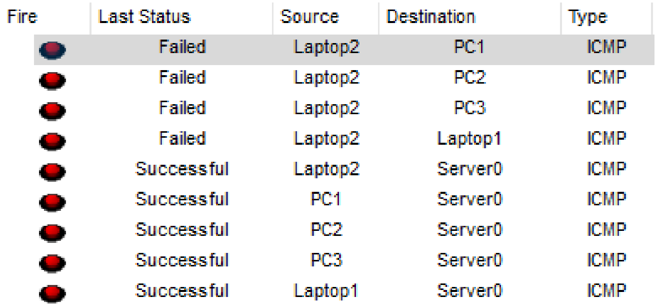
RESULTS AND DISCUSSION

After experimenting with applying ACL in router with the terms previously described experimental analysis before and after configuration configure can be seen in Figure 5 that before configured each device can't interact without any restrictions. But after ACL applied Figure 6 can be seen that device network 192.168.2.0/24 is not sending an ICMP packet to a laptop 2 and laptop 2 can't make deliveries packet yet still be able to communicate with the server. Can be seen in Figure 7 to Figure 10 displays the results of the application of the ACL under the provisions of any PC on the network can access the network 192.168.2.0/24 HTTP server but can't access the FTP server and laptops in the network 192.168.2.0/24 can login access to the FTP server but do not have access to the HTTP server.



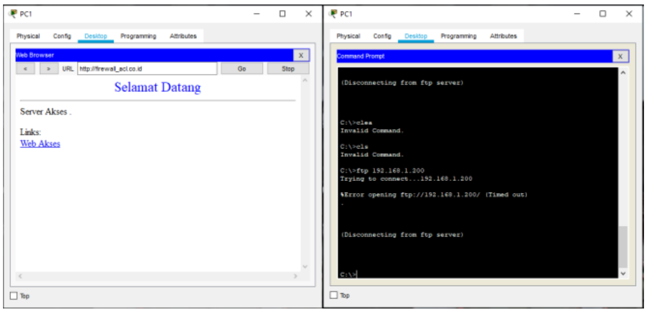
Fire	Last Status	Source	Destination	Type
●	Successful	PC1	Server0	ICMP
●	Successful	PC2	Server0	ICMP
●	Successful	PC3	Server0	ICMP
●	Successful	Laptop1	Server0	ICMP
●	Successful	Laptop2	PC1	ICMP
●	Successful	Laptop2	PC2	ICMP
●	Successful	Laptop2	PC3	ICMP
●	Successful	Laptop2	Laptop1	ICMP

Figure 5. ICMP Packet Delivery before Configuring ACL



Fire	Last Status	Source	Destination	Type
●	Failed	Laptop2	PC1	ICMP
●	Failed	Laptop2	PC2	ICMP
●	Failed	Laptop2	PC3	ICMP
●	Failed	Laptop2	Laptop1	ICMP
●	Successful	Laptop2	Server0	ICMP
●	Successful	PC1	Server0	ICMP
●	Successful	PC2	Server0	ICMP
●	Successful	PC3	Server0	ICMP
●	Successful	Laptop1	Server0	ICMP

Figure 6. ICMP Packet Delivery after Configuring ACL



http://firewall_acl.co.id

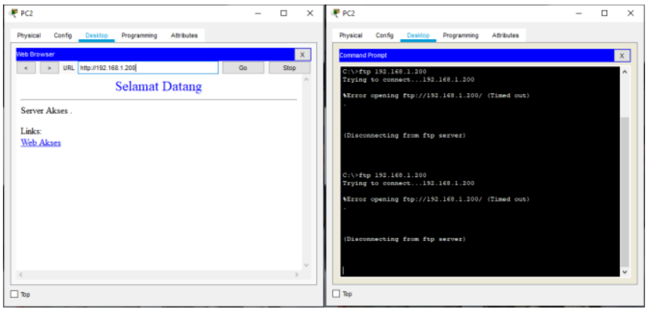
Selamat Datang

Server Akses .

Links:
Web Akses

```
(Disconnecting from ftp server)



C:\>clea
Invalid Command.

C:\>cls
Invalid Command.

C:\>ftp 192.168.1.200
Trying to connect...192.168.1.200

%Error opening ftp://192.168.1.200/ (Timed out)
.



(Disconnecting from ftp server)



C:\>
```

Figure 7. PC 1 access



URL http://192.168.1.200

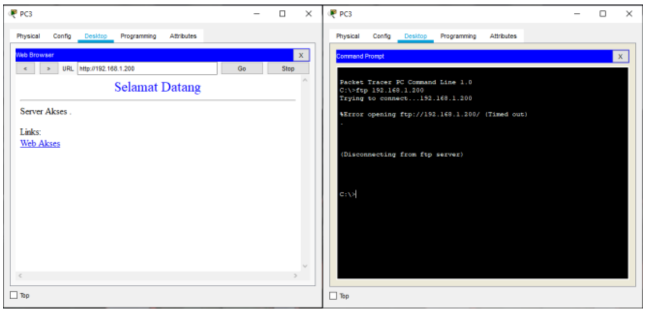
Selamat Datang

Server Akses .

Links:
Web Akses

```
C:\>ftp 192.168.1.200
Trying to connect...192.168.1.200

%Error opening ftp://192.168.1.200/ (Timed out)
.


(Disconnecting from ftp server)



C:\>ftp 192.168.1.200
Trying to connect...192.168.1.200

%Error opening ftp://192.168.1.200/ (Timed out)
.


(Disconnecting from ftp server)
```

Figure 8. PC 2 access



URL http://192.168.1.200

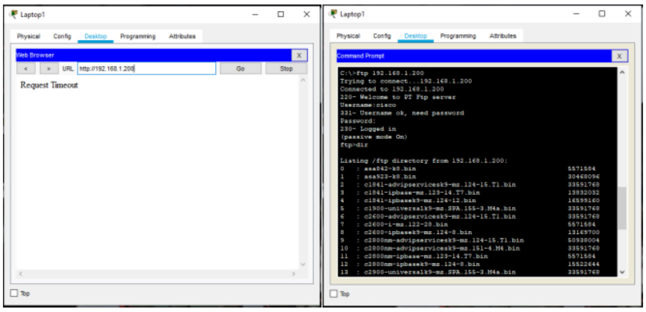
Selamat Datang

Server Akses .

Links:
Web Akses

```
Packet Tracer PC Command Line 1.0
C:\>ftp 192.168.1.200
Trying to connect...192.168.1.200

%Error opening ftp://192.168.1.200/ (Timed out)
.


(Disconnecting from ftp server)



C:\>
```

Figure 9. PC 3 access



URL http://192.168.1.200

Request Timeout

```
C:\>ftp 192.168.1.200
Trying to connect...192.168.1.200
Connected to 192.168.1.200
220- Welcome to PT Ftp server
Username:cisco
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>dir

Listing /ftp directory from 192.168.1.200:
0    : asa842-k8.bin                                    5571584
1    : asa923-k8.bin                                    30468096
2    : c1841-advipservicesk9-mz.124-15.T1.bin           33591768
3    : c1841-ipbase-mz.123-14.T7.bin                    13832032
4    : c1841-ipbasek9-mz.124-12.bin                     16599160
5    : c1900-universalk9-mz.SPA.155-3.M4a.bin           33591768
6    : c2600-advipservicesk9-mz.124-15.T1.bin           33591768
7    : c2600-i-mz.122-28.bin                            5571584
8    : c2600-ipbasek9-mz.124-8.bin                      13169700
9    : c2800nm-advipservicesk9-mz.124-15.T1.bin         50938004
10   : c2800nm-advipservicesk9-mz.151-4.M4.bin          33591768
11   : c2800nm-ipbase-mz.123-14.T7.bin                  5571584
12   : c2800nm-ipbasek9-mz.124-8.bin                    15522644
13   : c2900-universalk9-mz.SPA.155-3.M4a.bin           33591768
```

Figure 10. Laptop1 access

CONCLUSION

There is a list of rules or statements of successive test packets out on the access list. Source IP address, destination IP address, and the protocol is an example of a package that test a variety of specific information using these rules. Packs tested in advance to follow the rule set until certain conditions are met. The package will be submitted to the second row if none fulfilled the first rule. If no appropriate conditions then there are consequences "deny all" [10]

REFERENCES

[1] R. Ocanitra and M. Ryansyah, “Implementasi Sistem Keamanan Jaringan Menggunakan Firewall Security Port pada Vitaa Multi Oxygen,” vol. 7, no. 1, pp. 52–59, 2019.

[2] I. Sutoyo and M. Wahyudi, “KAJIAN PENGGUNAAN PACKET FILTERING FIREWALL,” vol. XI, no. 2, pp. 110–121, 2009.

[3] M. A. Istiqlal, L. O. Sari, and I. T. Ali, “Perancangan Sistem Keamanan Jaringan TCP / IP Berbasis Virtual LAN dan Access Control List,” pp. 1–9, 2011.

[4] S. Juanita and Windarto, “Rancangan sistem informasi peringatan dini bencana banjir,” Pros. Semin. Nas. Multi Disiplin Ilmu Call Papaer UNISBANK Ke-3, vol. 3, pp. 123–129, 2017.

[5] A. S. H, “ADDRESS MENGGUNAKAN METODE ACCESS LIST CONTROL PADA ROUTER CISCO,” vol. III, no. 1, pp. 60–73, 2017.

[6] M. Tur, “Packet filtering by artificial neural network.”

[7] J. Qian, S. Hinrichs, and K. Nahrstedt, “ACLA : A Framework for Access Control List (ACL) Analysis and Optimization,” 2001.

[8] I. Michael, J. Coss, R. L. Sharp, and N. J, “United States Patent (19),” no. 19, 2000.

[9] H. Hamed, A. El-atawy, and E. Al-shaer, “Adaptive Statistical Optimization Techniques for Firewall Packet Filtering,” pp. 1–12.

[10] A. Hikmaturokhman et al., “ANALISIS PERANCANGAN DAN IMPLEMENTASI FIREWALL DAN,” vol. 2010, no. semnasIF, pp. 1–8, 2010.