International Journal of Information System & Technology
Akreditasi No. 36/E/KPT/2019 | Vol. 5, No. 2, (2021), pp. 192-197

Network Security System Analysis Using Access Control List (ACL)

Oris Krianto Sulaiman[1], Darjat Saripurna[2]

[1]Universitas Islam Sumatera Utara, [2]STMIK Triguna Dharma

oris.ks@ft.uisu.ac.id, darjatsaripurna@gmail.com

Abstract

Communication using internet media is a mandatory requirement today to carry out various activities. Communication through the internet will pass through public access, where many people use public access. When communication is in progress, many things can happen before the message reaches its destination. One of them is the occurrence of hacking attempts from irresponsible parties. Therefore, it is necessary to secure the communication process, and many network security methods can be used to secure the communication process in the internet network. Access Control List or ACL is one method that can be used to secure communication in the network. ACL makes it easy to block specific devices and ports to prevent network communication. The results of the ACL implementation have the impact of avoiding access so that not all devices or protocols can access certain communications, thereby increasing network security in the process.

Keywords: *Access Control List (ACL), Network Security, Port Blocking*

1. Introduction

In the development of network communication using internet media, there are many attempts to attack any security holes found [1]–[3]. This network security becomes paramount when the communication process is carried out while using specific applications that are private because these applications contain confidential information that the public should not access. In network security, many ways can be done to fortify the devices that are most often attacked, namely servers [4], [5]. In previous studies, security has been carried out using Firewall Port Security as well as Switch Port Security [6]–[8], And related to research on network communication security using the Access Control List method, several studies combine ACL with VLAN and ACL is used for some instances such as in the company where the researcher conducts research [9]–[11]. In this study, the discussion of ACL is only limited to analysis using two ACL methods, namely Standard IP Access List and Extended IP Access List.

Access Control List (ACL) is a network security method that can limit access rights for connected devices and communicate with each other [11]. ACL is divided into two, namely Standard IP Access List and Extended IP Access List. Standard IP Access List is an ACL method that can filter a device that will access the server. This type of ACL cannot be used to perform special blocks on specific network protocols. Extended IP Access List is an ACL method that can perform particular filtering for specific network protocols on the device. The device cannot communicate if using a particular protocol.

2. Research Methodology

The method used in this analysis is to compare and use each function of:

a) Standard IP Access List
b) Extended IP Access List

The trial was carried out using simulation using Cisco Packet Tracer version 6.2 using a topology.

ISSN : 2580-7250

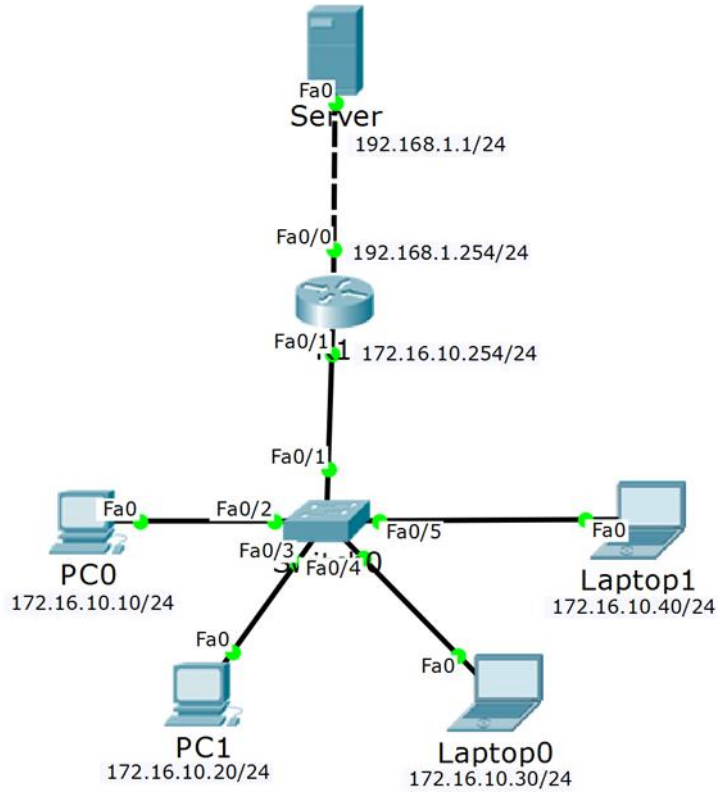


Figure 1. Network Topology

Table 1. Table Addressing

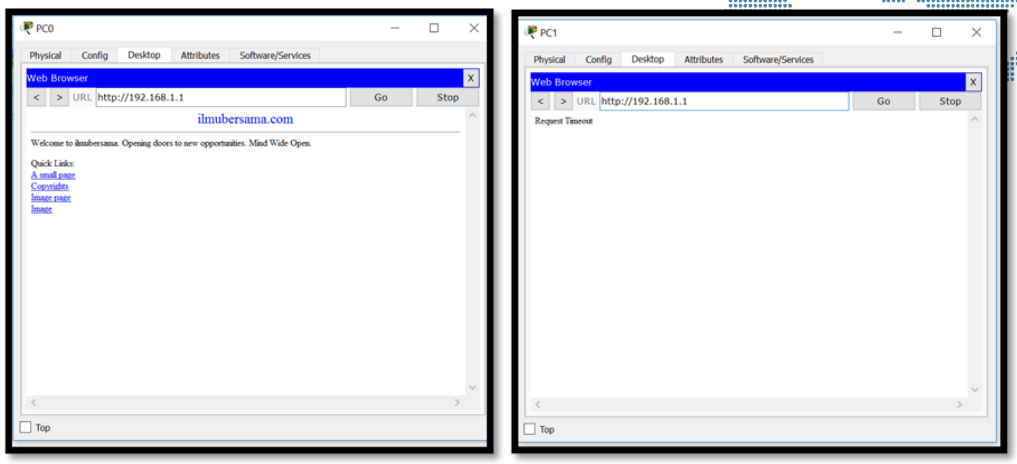
Device	Interface	IP Address	Subnetmask	Default Gateway
Server	NIC	192.168.1.1	255.255.255.0	192.168.1.254
R1	NIC fa 0/0	192.168.1.254	255.255.255.0	N/A
	NIC fa 0/1	172.16.10.254	255.255.255.0	N/A
Switch0	N/A	N/A	N/A	N/A
PC0	NIC	172.16.10.10	255.255.255.0	172.16.10.254
PC1	NIC	172.16.10.20	255.255.255.0	172.16.10.254
Laptop0	NIC	172.16.10.30	255.255.255.0	172.16.10.254
Laptop1	NIC	172.16.10.40	255.255.255.0	172.16.10.254

The topology uses servers, routers, switches and PCs and laptops connected to or connected. Each IP address is adjusted to the data contained in the IP address table.

3. Result and Discussion

The first test of network security will use the Standard IP Access List method. Standard IP access lists use ACL numbers 1-99; Standard IP access lists only use source IP addresses in IP packets as the conditions tested. All decisions are made based on the source IP address. In this scenario, only PC0 using the IP address 172.16.10.10 will communicate with the server that has the IP address 192.168.1.1. Access list used is access-list 1 by allowing (permit) host 172.16.10.10.

The results of this test use communication from PC0 to the server using a web browser.



(a) (b)

Figure 2. (a) PC0 Akses Server (b) PC1 Akses Server

Figure (a) shows the results when PC0 accesses the server, PC0 can connect, as evidenced by the sciencebersama.com web display that appears in PC0's browser. Figure (b) is the result when PCs other than PC0 cannot access the server, as evidenced by the browser display, which only displays request timeouts. This happens because the access control provided is only available on PC0, so that other PCs cannot be connected. If analyzed using ICMP, it will be seen that PC0 gets a reply from the server, while PC1 will get a Destination Host Unreachable (DHU) reply which means the server does not respond to PC1's request.

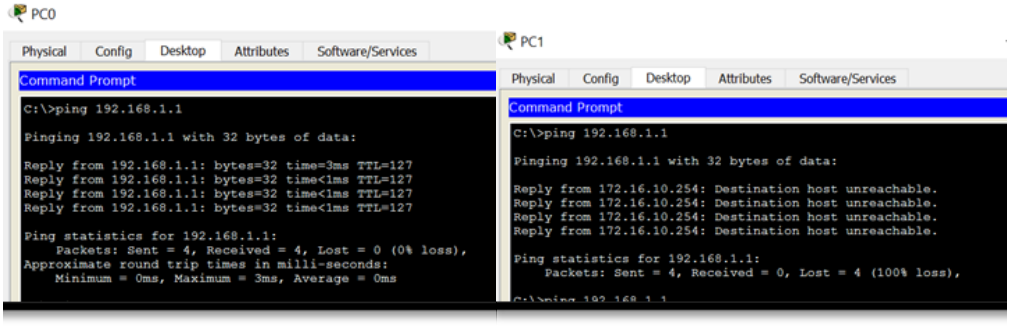


Figure 3. ICMP Testing

The second trial of this network topology is network security using the Extended IP access lists method. This method uses ACL numbers 100-199. Extended IP access lists check for specific source and destination addresses, such as checking for specific UDP/TCP/IP protocols and destination ports. In this trial, ICMP packets (ping) from PC0 to the server cannot be performed, but server access via browser (HTTP) can be committed. Then the Laptop0 device cannot access the HTTP protocol, but the ICMP protocol (ping) can be accessed. The access list used is 100.

R1(config)#access-list 100 deny icmp host 172.16.10.10 host 192.168.1.1
R1(config)#access-list 100 deny tcp host 172.16.10.30 host 192.168.1.1 eq 80
In this case, it can be interpreted that the router will block the ICMP protocol from PC0 (172.16.10.10) to the Server (192.168.1.1). The following command stops the HTTP protocol from Laptop0 (172.16.10.30.) to the Server (192.168.1.1). It can be seen a summary of the Extended IP access lists on this router is as follows.

interface FastEthernet0/0

```
ip address 192.168.1.254 255.255.255.0
duplex auto
speed auto
!
interface FastEthernet0/1
ip address 172.16.10.254 255.255.255.0
ip access-group 100 in
duplex auto
speed auto
……..
access-list 100 deny icmp host 172.16.10.10 host 192.168.1.1
access-list 100 deny tcp host 172.16.10.30 host 192.168.1.1 eq www
access-list 100 permit ip any any
```

To prove Extended IP access lists, PC0 will communicate to the server using the ICMP protocol and check the HTTP protocol from the web browser on PC0.

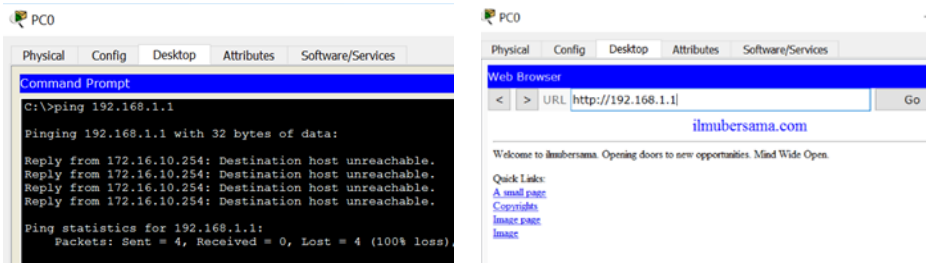


Figure 4. PC0 ICMP and Browsing Testing

In the picture, it can be seen that when PC0 tries to communicate to the server using the ICMP protocol, it gets a Destination Host Unreachable (DHU) reply, which means the server does not respond to PC0 requests. Still, if PC0 tries to communicate using the HTTP protocol from a web browser, then PC0 can connect to the server. This can be proven from the display of the Sainsbersama.com website, which can be accessed from PC0.

The same thing is proven from the results of Extended IP access lists Laptop0. When Laptop0 tries to communicate to the server using the ICMP protocol, the server responds to requests from Laptop0. This is evidenced by the presence of a replay message in the ping results. Meanwhile, when Laptop0 tries to communicate using the HTTP protocol through a web browser, the HTTP packet is blocked. This can be proven from the web display not showing on the server.

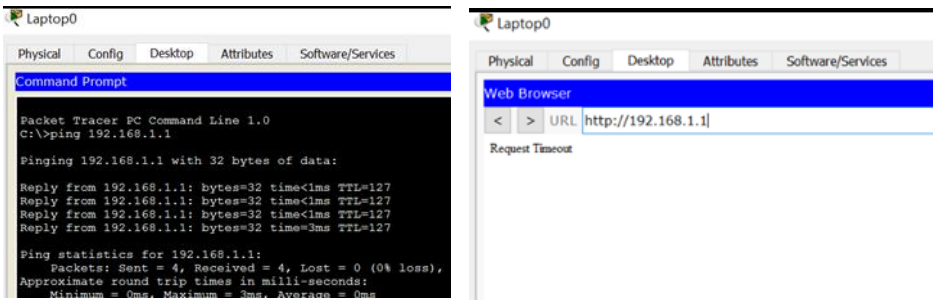


Figure 5. Laptop0 ICMP and Browsing Testing

4. Conclusion

Network communication security is an essential part. Therefore the use of ACLs *is* a priority to prevent cyber attacks. In the trial of the simulation, it can be concluded that the use of the Standard IP Access List method in the ACL can block users with all devices. Still, if you want to be specific to block certain ports so that they cannot access the destination device, in this case, the server, you can use the Extended method. IP Access List allows devices to connect, but some access can be blocked based on blocked ports.

Acknowledgments

Thank you to UPT TIK Medan State University for facilitating the lab for case trials in this article.

References

[1] I. Anugrah and R. H. Rahmanto, "Sistem Keamanan Jaringan Local Area Network Menggunakan Teknik De-Militarized Zone," *PIKSEL : Penelitian Ilmu Komputer Sistem Embedded and Logic*, vol. 5, no. 2, pp. 91–106, 2018, doi: 10.33558/piksel.v5i2.271.

[2] D. B. Rendro, Ngatono, and W. N. Aji, "Analisis Monitoring Sistem Jaringan Komputer Menggunakan Software Nmap," *PROSISKO: Jurnal Pengembangan Riset dan Observasi Sistem Komputer*, vol. 7, no. 2, pp. 108–115, 2020.

[3] Z. Munawar, M. Kom, and N. I. Putri, "Keamanan Jaringan Komputer Pada Era Big Data," *Jurnal Sistem Informasi-J-SIKA*, vol. 2, no. 1, pp. 1–7, 2020.

[4] S. Ramadhani, U. Sultan Syarif Kasim Alamat, J. Koto Kociak Kecamatan Latina Payakumbuh Sumatera Barat, J. H. Soebrantas Kelurahan Simpang Baru No, and K. Tampan, "Analisis Sistem Keamanan Web Server Dan Database Server Menggunakan Suricata," *Seminar Nasional Teknologi Informasi Komunikasi dan Industri*, vol. 0, no. 0, pp. 2579–5406, 2017, [Online]. Available: http://ejournal.uin-suska.ac.id/index.php/SNTIKI/article/view/3368.

[5] M. I. S. Aryo Nur Utomo, ST, M.Kom1, "Implementasi Sistem Keamanan Server Menggunakan Honeypot Dan Raspberry Pi Terhadap Attacker," *Jurnal Rekayasa Informasi*, vol. 7, no. 2, pp. 71–77, 2018.

[6] S. Sudaryanto, "Implementation Port Security for Security Systems Network at the Computing Laboratory of Adisutjipto College of Technology," *Conference SENATIK STT Adisutjipto Yogyakarta*, vol. 4, 2018, doi: 10.28989/senatik.v4i0.239.

[7] A. Sutiman, Gunawan, "Firewall Port Security Switch Untuk Keamanan Jaringan Komputer Menggunakan Cisco Router 1600S Pada Pt. Tirta Kencana Tata Warna Sukabumi," *CONTEN (Computer and Network Technology)*, vol. 1, no. 1, pp. 13–22, 2021.

[8] O. K. Sulaiman, "Analisis Sistem Keamanan Jaringan dengan Menggunakan Switch Port Securitu," *Computer Engineering, System And Science*, vol. 1, no. 1, pp. 9–14, 2016.

[9] A. sopian Ahmad Fitriansyah, Alarik Andreansyah, "Penerapan Static Vlan Dan Access List," vol. 5, no. 2, pp. 1–6, 2019, [Online]. Available: http://journal.thamrin.ac.id/index.php/jtik/article/view/176/120.

[10] C. E. Suharyanto, "Analisis Penggunaan Access Control List (Acl) Dalam Jaringan Komputer Di Kawasan Batamindo Industrial Park Batam," vol. 2, no. 2, pp. 122–128, 2019, doi: 10.31227/osf.io/8mt59.

[11] M. Ariq Istiqlal, L. O. Sari, and I. T. Ali, "Perancangan Sistem Keamanan Jaringan TCP/IP Berbasis Virtual LAN dan Access Control List," *Jom FTEKNIK*, vol. 3, no. 1, pp. 1–9, 2016.

Authors

Oris Krianto Sulaiman, Lecturer at Universitas Islam Sumatera Utara, focus and scope research computer network communication.