Jurnal Mantik, 5 (3) (2021) 1684 - 1693

Published by:Institute of Computer Science (IOCS)

Jurnal Mantik

Journal homepage: www.iocscience.org/ejournal/index.php/mantik/index

Firewall Design Using Access Control List Method As Data Filtering

Niar Adisty Putra[1], Verry Riyanto[2], Ganda Wijaya[3], Nuraeni Herlinawati[4]

[13] Program Studi Teknik Informatika, Fakultas Teknologi Informasi, Universitas Nusa Mandiri, Indonesia
[24] Program Studi Sistem Informasi, Fakultas Teknik & Informatika, Universitas Bina Sarana Informatika, Indonesia

E-mail: niaradistyputra@gmail.com[1], verry.vry@bsi.ac.id[2], ganda.gws@nusamandiri.ac.id[3]

A R T I C L E I N F O

Article history:

Received: September 23, 2021
Revised: October 18, 2021
Accepted: November 01, 2021

Keywords:

Access Control List,
Filtering Data,
VLAN

A B S T R A C T

The need for real-time information is very important, to get it quickly and even in real time it must be supported by a fast and stable internet network connection. In addition, it must also be able to protect the network connection from all kinds of threats that can interfere with the connectivity of the connection. In implementing the firewall within the company, the concern is the device used, because the implementation of the firewall on each device is different. Utilization of this firewall is used to filter data packets that will enter the network, using the ACL feature. By using ACL data filtering can be done or as a site blocker that is considered unnecessary to be accessed by all clients on the local network. In addition, as security in the local network, the logical division of network groups can be applied using VLANs, the application of VLANs is found on Catalist Switches or Multilayer Switches. As a security for the physical path of the VLAN connection, a special physical connection path is given to important network devices, so that if there is a down or disconnected physical path, it does not interfere with other VLAN connections.

1. Introduction

The need for real-time information is very important, to get it quickly, even in real time, it must be supported by a fast and stable internet network connection. In addition, it must also be able to protect network connections from all kinds of threats that can interfere with the connectivity of the connection. According to Plt. Head of BSSN Pusopskamsinas, Adi Nugroho, released by the newspaper on March 1, 2021, "In 2020, BSSN detected 495,337,202 cyber attacks occurred in Indonesia with the most attacks in the form of trojan malware that can damage a system or steal data.

In implementing the firewall within the company, the concern is the device used, because the implementation of the firewall on each device is different, for example, the Mikrotik Router is different from the firewall implementation on the Cisco Router. The use of this firewall is used to filter data packets that will enter the PT Dayamitra Telekomunikasi network to exit the network and vice versa. So that the PT Dayamitra Telekomunikasi network can ensure that information entering or leaving the network is safe.

Quoted from the BSSN report (National Cyber and Crypto Agency) taken from bssn.go.id is "The National Cyber Security Operations Center (Pusopskamsinas) National Cyber and Crypto Agency (BSSN) recorded 88,414,296 cyber attacks have occurred from January 1 to 12 April 2020. In January 25,224,811 attacks were observed and then in February 29,188,645 attacks were recorded and then in March there were 26,423,989 attacks and up to April 12, 2020, 7,576,851 attacks have been recorded. The peak number of attacks occurred on March 12, 2020 which reached 3,344,470 attacks and after that the number of attacks decreased significantly when the work from home (WFH) policy was implemented in various places. However, during WFH there have been cyber attacks that take advantage of issues related to Covid-19.

Accredited "Rank 4"(Sinta 4), DIKTI, No. 36/E/KPT/2019, December 13th 2019.

The most common type of attack is trojan activity as much as 56% and then followed by information gathering activity (gathering information) as much as 43% of the total attacks, while the remaining 1% are web application attacks.

To be able to carry out its objectives, a firewall has four techniques in controlling access and enforcing the security policies it applies. Originally, firewalls focused on the virtues of controlling services, namely [10]:

a. Service Control, Determine the type of internet service that can be accessed, inbound or outbound. firewalls can filter traffic on the basis of IP address, protocol, or port number; may provide proxy software that receives and interprets each service request before it is passed or it may host the software's own server, such as a Web or mail service.
b. Direction Control, Specifies the direction of certain services in which requests can be initiated and allowed to flow through the firewall.
c. User Control, Control access to users with appropriate services trying to access them. This feature is usually applied to users inside the perimeter firewall (local user). This can also be applied to incoming traffic from external users; the latter requires some form of authentication technology, as provided in Ipsec.
d. Behavior Control, Controlling how certain services are used. For example, a firewall can filter e-mail to remove spam, or allow external access to only part of the information on a local Web server.

With the four techniques mentioned above, a firewall implementation can perform packet filtering, then a set of rules is applied for each incoming and outgoing IP packet and then it can be left to be passed or discarded the packet. Firewalls are usually configured for packet filtering going in both directions (to and from the internal network). Filtering rules are based on the information contained in a network packet, namely [10]:

a. Source IP address: The IP address of the system from which the IP packet originated.
b. Destination IP address:
c. Source and destination transport-level addresses: Transport-level (for example, TCP or UDP) port numbers, which define applications such as SNMP or TELNET
d. IP protocol field: Defines the transport protocol.
e. Interface: For firewalls with three or more ports, the firewall interface packets originate from or the firewall interface packets are destined for".

2. Method

In carrying out the research that has been carried out, the authors use methods in carrying out the process of collecting data and analyzing experimental results which will later be used as material for the preparation of this thesis.

2.1 Method of collecting data

The data collection methods used by the author in conducting this research include:

a. Observation

Observations are made by observing directly in the field to dig up information and observing the concept of data filtering that is running.

b. Interview

Interviews were conducted by asking informants regarding the topology and current network schemes to make it easier to conduct research.

c. Literature Study

The research was also conducted by collecting information related to concepts and theories through the Internet, books, e-books, and several related journal references.

2.2 Research Analysis

Research analysis is carried out by identifying the needs needed to design the Firewall. The required requirements include specifications for hardware (hardware), and software (software) as well as simulations used.

a. Needs Analysis

Equipment needed to design in building a Firewall include: Package Tracer Software Simulator as an illustration of data filtering implementation.

Accredited "Rank 4"(Sinta 4), DIKTI, No. 36/E/KPT/2019, December 13th 2019.

b. Design

Firewall design with Access Control List by forming a tree topology using the Wildcard Mask method, this needs to be done as a filtering host that is given permission for outgoing or incoming connections to the computer network.

c. Testing

At the Firewall stage using the Access Control List, it is done by virtual demonstration using the Packet Tracer simulator.

d. Implementation

Implementation is done by simulating using the Packet Tracer application by adjusting the computer network scheme that is inside.

3. Result and Analysis

3.1 Current Network Schema

a. Network Topology

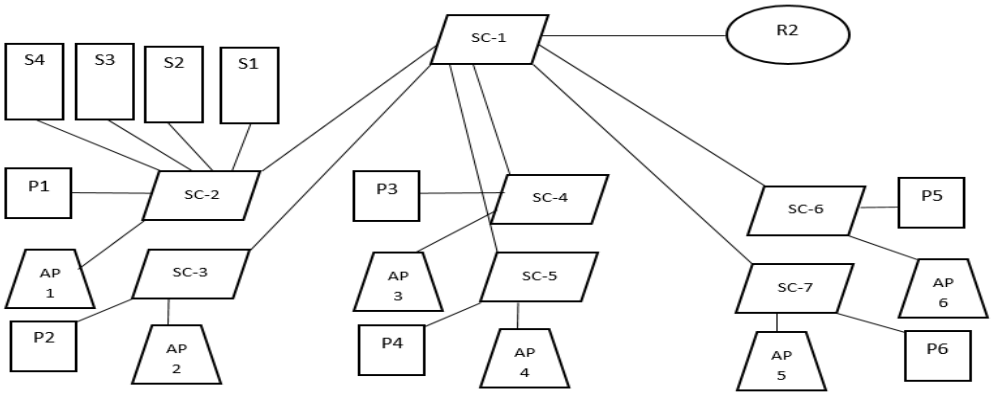

Fig 1. Current Network Topology

In the network topology analysis, the researcher tries to draw a network scheme based on network blocks so that it is easy to understand, before explaining the network topology based on network blocks designed based on the running network scheme, the researcher will explain the blocks used in the above network blocks, including:

1) S is Server2. R is Router
2) SC is a Catalist Switch/Multi layer Switch
3) P is PC
4) AP is Access Point

Next, the author will discuss the network topology analysis used at PT Dayamitra Telekomunikasi. In analyzing the network topology used, the author divides several groups of devices based on the network topology image above, the discussion includes:

a) The first group of computer network devices consists of: Router (R2), Switch Multilayer (SC1), Switch Catalist 2 (SC2), Switch Catalist 3 (SC3), Switch Catalist 4 (SC4), Switch Catalist 5 (SC5), Switch Catalist 6 (SC6), Switch Catalist 7 (SC7). Then the network block image as below:

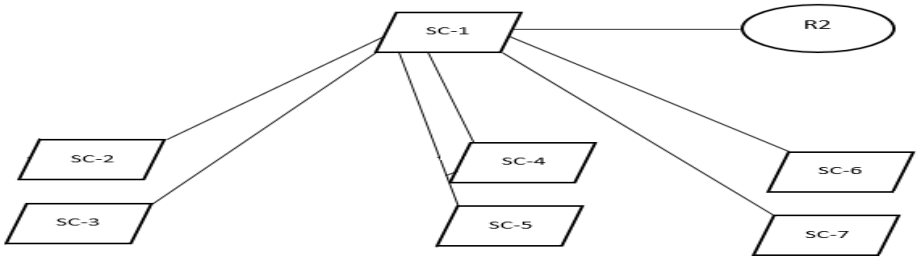

Fig 2. First Computer Network Block Group

Accredited "Rank 4"(Sinta 4), DIKTI, No. 36/E/KPT/2019, December 13th 2019.

Based on the first group of computer network devices, the author analyzes the topology used is the star type, because Switch Catalist 1 (SC1) is the connection center and resembles a star shape (star).

b) The second group of computer network devices consists of: Switch Catalist 2 (SC2), Application Server 1 (S1), Application Server 2 (S2), Application Server 3 (S3), Application Server 4 (S4), PC 1 (P1) and Access Point 1 (AP1). Then the network block image as below:

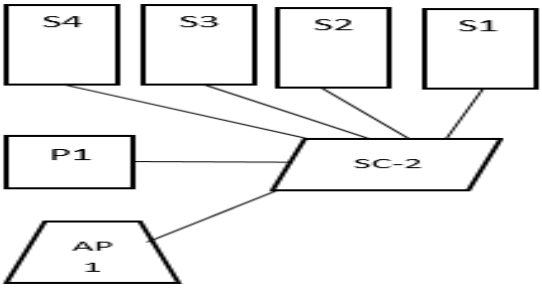

Fig 3. Second Computer Network Block Group

Based on the group of computer network devices, the authors analyze the topology used is a star type, because Switch Catalist 2 (SC2) is the connection center and resembles a star shape (star).

c) The third group of computer network devices consists of: Switch Catalist 3 (SC3), PC 2 (P2) and Access Point 2 (AP2). Then the network block image as below:

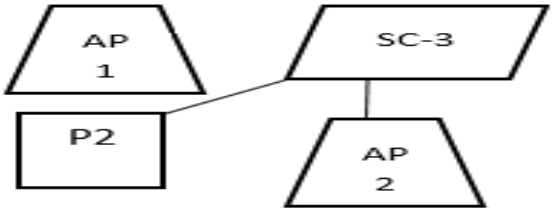

Fig 4. Third Computer Network Block Group

d) The fourth group of computer network devices and so on is almost the same as the Third network group, the author immediately analyzes each fourth computer network group and so on until the eighth network group the author analyzes the topology used is a star topology.

In network analysis, groups of network devices from one to eight form a branch network from a star topology. One of the devices from the network group forms a star topology again. This is evidenced by the first group of computer network devices, Router 2 (R2) being the connection center for other computer network devices in the second group of network devices, as well as the third group of network devices, Multilayer Switch (SC2) being the connection center for other computer network devices in the device group. third network, and so on. So the authors conclude that the overall network topology used by PT Dayamitra Telekomunikasi uses a tree (tree) topology because some network devices that are the center of the first group have branching and branching of the first network device to become the network center in the other group of network devices.

b. Network Schema

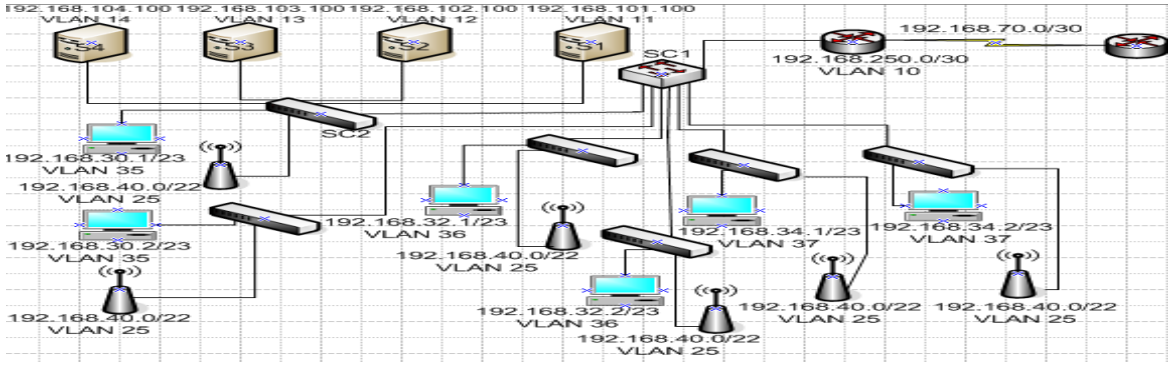

Fig 5. Network Schema

Accredited "Rank 4"(Sinta 4), DIKTI, No. 36/E/KPT/2019, December 13th 2019.

c. IP Address

There are several IP Address segments that are used in the running network scheme, whether it is experiencing subnetting or not. The following IP address segment is used:

Table 1
List of IP addresses

No	IP Address	Device	Information
1.	192.168.40.0/22	Access Point	Used as a network WiFI
2.	192.168.30.0/23	Client/PC	Used as a connection Client/PC
3.	192.168.32.0/23	Client/PC	Used as a connection Client/PC
4.	192.168.34.0/23	Client/PC	Used as a connection Client/PC
5.	192.168.101.0/24	Server 1	Application
6.	192.168.102.0/24	Server 2	Application
7.	192.168.103.0/24	Server 3	Application
8.	192.168.111.0/24	Server 4	Application
9.	192.168.249.8/29	Router	As a Peer to Peer Router connection with Multilayer Switch (SC1)

d. Network Security

On a running network system, the network security used is as follows:

1) There is a VLAN (Virtual Local Area Network) method system that divides several logical connection paths based on the VLAN. This VLAN is used to secure data or information from one part or division against another part or division so that it cannot be scanned. In addition, if one part is affected by a virus or worm or trojan or other, then with the VLAN this part or division will automatically isolate only that part or division that is infected and will not spread to other parts or divisions.
2) There is IP Address management, this can be seen based on the IP Address used, some have experienced subnetting. This is enabled so that the IP Address used is limited and not extensive or not much so that the user cannot change the IP Address at will.
3) For the security of the hierarchical internet connection network after the modem is directly connected to the router, this is a preventive method so that the internet connection can be better managed on the router. Because router devices have features to do more network management compared to modems.
4) In terms of network security Hotspot or WiFI there is filtering or MAC Address filtering. Only MAC addresses that have been registered with the IT Division can use this Hotspot or WiFI network.

3.2 Problem

The network system that runs consists of 3 floors, which is the subject of research after doing research there are main problems including:

a. The connection of the VLAN line on the Catalist 2 Switch (SC2) to the Multilayer Switch (SC1) uses one cable connection, the connection is a VTP Trunk. This is very risky if one cable experiences a connection interruption or is disconnected which could have been caused by being bitten by a rodent or by a natural disaster such as a lightning strike this will result in 4 servers, some clients and one access point will not connect to the network,
b. Limitation of internet connection access rights connected to the system on each client with various divisions or sections free to connect. Should be limited to access to each user who only has an interest in accordance with the responsibilities and work needs based on the section or division.

3.3 Solution

To solve the problem, the researcher tries to propose several views, including:

a. To provide access to VLAN lines contained in vital network devices such as servers, it should not be combined with other devices. So if there are problems handling maintenance can be done quickly. So the VTP connection that connects the Catalist 2 Switch (SC2) with the Multilayer Switch uses the VTP Access method. So there is a separation of the server VLAN lines with other devices that become one in Switch Catalist 2 (SC2).
b. Activate the firewall by using the Access Control List method, limiting connection access on the client by filtering data, so that data entering and leaving the network can be recognized and its validity guaranteed when connecting to an FTP Server on the internet.

Accredited "Rank 4"(Sinta 4), DIKTI, No. 36/E/KPT/2019, December 13th 2019.

3.4 Proposed Network Design

To be able to filter incoming and outgoing data, requires an Access Control List method or also known as ACL. This ACL is a feature contained in Cisco Routers, and in this study the author tries to implement an Extended type ACL with an id number between 100 to 199. Because the extended firewall type ACL can filter the specifics of the data you want to filter in more detail.

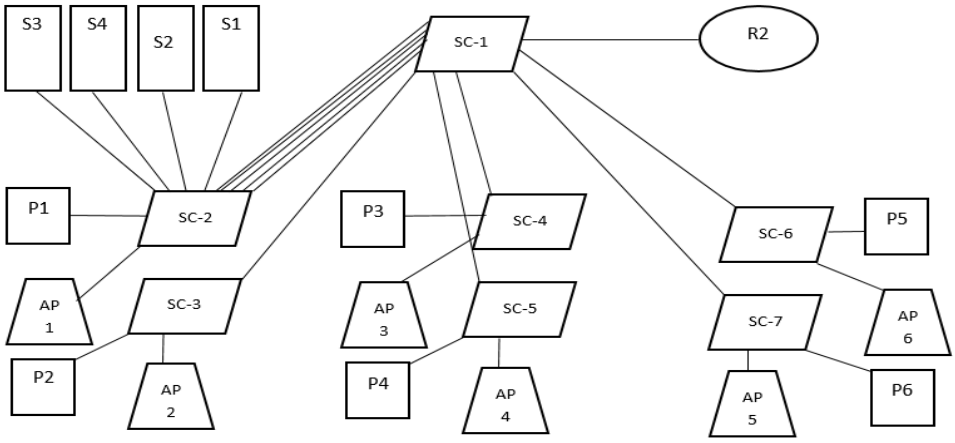

Fig 6. Proposed Network Topology

The proposed network topology does not change the current topology, because the researchers are trying to explore the capabilities of each existing device so that it is more optimal in keeping the business processes running even though there are problems. In the problem, the researcher tries to analyze if there is a connection interruption with the disconnection of the cable transmission media that connects SC 2 (Switch Catalist) with SC 1, it will result in connections to the server all existing network devices are not connected. Therefore, it is necessary to take a connection path one by one because each server has a virtual path that is different from one another. So the author of each virtual server path has one cable connection so that if there is interference with the disconnection of one cable it does not interfere with the connection to other servers. The other device is a router which is in the network topology given the initiation of R2 (Router 2). This is so that the router on the backbone network can filter every incoming or outgoing data packet and can also block a website that is considered harmful or dangerous if one of the existing clients connects to the website. Examples are video-based websites, or movie sites that can reduce the available bandwidth.

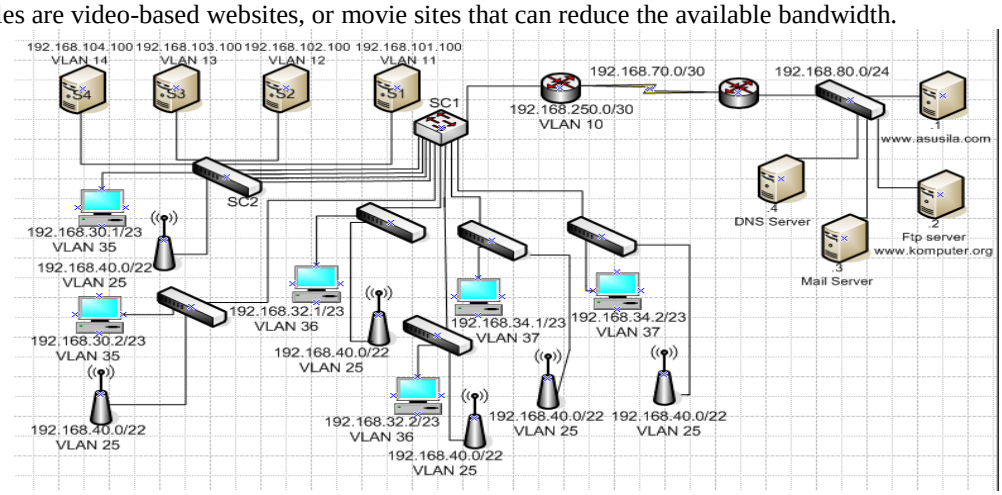

Fig 7. Proposed Network Schema

In the form of the network scheme that the author designed, the Switch Catalist (SC 2) device that connects application servers with each server has a different virtual path, namely VLAN 11 for server 1, VLAN 12 for server 2, VLAN 13 for server 3 and VLAN 14 for server 4. The author tries to design with a network scheme adding 4 cable connections so that the cable that connects SC2 to SC1 is 5 cable connections. The 5 (five) immune connections I use 1 connection as a VLAN Client1 connection line, 1

Accredited "Rank 4"(Sinta 4), DIKTI, No. 36/E/KPT/2019, December 13th 2019.

connection as a VLAN Server 1 connection line, 1 connection as a VLAN Server 2 connection line, 1 connection as a VLAN Server 3 connection line, 1 connection as a VLAN connection line Server 4. With VTP Access (Virtual Trunking Protocol) method. Furthermore, the device that is being developed is Router 1, on the router device there is an Access Control List (ACL) feature. With the extended ACL method, the author tries to build a firewall that is useful for filtering data packets that are on a server that is connected to a router opposite Router 1 (R1).

3.5 Proposed Network Security

For the proposed network security system, an addition is made in the form of activating a firewall using the Access Control List (ACL) feature. By filtering incoming and outgoing data packets. In addition to filtering, the author also adds blocking of internet access on a site that is considered detrimental, besides that the researcher limits access to clients who can make internet connections with full access or not.

3.6 Application Design

In this proposed network, the writer divides some of the main material proposed in this research, including:

A. Change the Virtual Trunking Protocol (VTP) connection from Trunk mode to VTP Access mode.

The author's reason is that if there is a cable transmission medium connecting SC 1 (Switch Catalist) with SC 2 as the Trunk method VTP which is on the 26th floor, it is disconnected (because it is eaten by rodents, or because of nature being struck by lightning and other reasons) it will not interfere with the connection. Other VLANs (VLAN 35, VLAN 25, VLAN 11, VLAN 12, VLAN 13, and VLAN 14).

The following is the proposed configuration design that the author did:

Table 2
Proposed VTP Access Method Design

Perangkat	Port	Keterangan
Switch Catalist 2 (SC2) – Switch Catalist (SC1)	FastEthernet 0/10	Koneksi VTP Metode Access untuk VLAN 35
	FastEthernet 0/11	Koneksi VTP Metode Access untuk VLAN 11
	FastEthernet 0/12	Koneksi VTP Metode Access untuk VLAN 12
	FastEthernet 0/13	Koneksi VTP Metode Access untuk VLAN 13
	FastEthernet 0/14	Koneksi VTP Metode Access untuk VLAN 14
	FastEthernet 0/15	Koneksi VTP Metode Access untuk VLAN 25

Source: Research Object (2021)

a. Configure Catalist 2 (SC2) Switches

```
SC2(config)#int fa0/10
SC2(config-if)#swi mod acc
SC2(config-if)#swi acc vlan 35
SC2(config-if)#exit
SC2(config)#int f0/1
SC2(config-if)#swi mod acc
SC2(config-if)#swi acc vlan 11
SC2(config-if)#exit
SC2(config)#int f0/12
SC2(config-if)#swi mod acc
SC2(config-if)#swi acc vlan 12
SC2(config-if)#exit
SC2(config)#int f0/13
SC2(config-if)#swi mod acc
SC2(config-if)#swi acc vlan 13
SC2(config-if)#exit
SC2(config)#int f0/14
SC2(config-if)#swi mod acc
SC2(config-if)#swi acc vlan 14
SC2(config-if)#exit
SC2(config)#int f0/15
SC2(config-if)#swi mod acc
```


Accredited "Rank 4"(Sinta 4), DIKTI, No. 36/E/KPT/2019, December 13th 2019.

```
SC2(config-if)#swi acc vlan 25
SC2(config-if)#exit
SC2(config)#
```

b. Configure Catalist 1 (SC1) Switch

```
SC1(config)#int fa0/10
SC1(config-if)#swi mod acc
SC1(config-if)#swi acc vlan 35
SC1(config-if)#exit
SC1(config)#int f0/1
SC1(config-if)#swi mod acc
SC1(config-if)#swi acc vlan 11
SC1(config-if)#exit
SC1(config)#int f0/12
SC1(config-if)#swi mod acc
SC1(config-if)#swi acc vlan 12
SC1(config-if)#exit
SC1(config)#int f0/13
SC1(config-if)#swi mod acc
SC1(config-if)#swi acc vlan 13
SC1(config-if)#exit
SC1(config)#int f0/14
SC1(config-if)#swi mod acc
SC1(config-if)#swi acc vlan 14
SC1(config-if)#exit
SC1(config)#int f0/15
SC1(config-if)#swi mod acc
SC1(config-if)#swi acc vlan 25
SC1(config-if)#exit
SC1(config)#
```

In this proposed network, the researcher analyzes that there are several sections or divisions that can access a system that should not be allowed to connect. For example, the Marketing division cannot access a File Transfer Protocol (FTP) server located on the internet. Researchers consider this ftp server provided for use in the field. What important data is in the field such as: reporting on the BTS soil structure, the location or field of BTS installation and others. The Marketing division or division is in the IP Address segment owned by clients on the 26th Floor, which is 192.168.32.0/22.

1) The following is the proposed configuration design:

```
Router(config)#acc 101 deny ip any host 192.168.80.1
Router(config)#acc 101 deny tcp 192.168.32.0 0.0.1.255 host 192.168.80.2 eq ftp
Router(config)#acc 101 permit ip any any
```

2) View the ACL 101 configuration on Router 1:

```
Router(config)#do sh acc 101
Extended IP access list 10
deny ip any host 192.168.80.1
deny tcp 192.168.32.0 0.0.1.255 host 192.168.80.2 eq ftp permit ip any any
```

3.7 Network Testing

With the VTP Access method, researchers argue that managing existing networks is because the existing VLAN connection line has 1 cable line so that if there is a problem in one of the VLANs, you can immediately identify the problem based on the cable connection that connects Switch Catalist 1 (SC1) with Switch Catatlist. 2 (SC2). Time management in handling obstacles is faster.

One more thing about network management is to limit access based on client groups or divisions or parts that are not interested in accessing the system. So that the server that serves the request is not too busy, so that the connection on the client to the server can be isolated which causes the connection to be smoother. And every request to the server, the server will quickly respond to the request.

3.8 Network Management

In this initial test, the writer did the following points that the writer tried to describe.

a. Testing VTP using the Access method.

In Switch Catalist 2 there are several VLANs, namely: VLAN 11 contains application server 1, VLAN 12 contains application server 2, VLAN 13 contains application server 3, VLAN 14 contains application server 4, VLAN 25 contains Access Points, and finally VLAN 35 contains 25th floor clients. As for this test, the author does how the 6 VLAN connection responds to other devices on the network.

b. Testing the filtering of FTP

Server data packets to the Client consisting of several parts or divisions, from the section or division the need for a connection to a different system according to the needs based on the responsibilities of the related division or section. In this study, the author raises the existence of authorization of access to a file system that is on an internet connection in the form of an FTP server to the marketing division or division. The researcher considers that this marketing division or division should not require connection access to an FTP server, because an FTP server is provided for the need for field documents in the installation, organization, repair of BTS (Base Transceiver Station). The client-client network scheme used by the marketing division or division is located on floor 26 with the IP address segment 192.168.32.0/22. While the FTP server is on the opposite LAN Router network with the IP address 192.168.80.2/24. Here, the researcher only filters FTP (File Transfer Protocol) data packets, while other data packets on the FTP server are not filtered. In this test the author will test the connection and call the ftp server on each client.

c. Final Test

In this final network test the author tries to draw conclusions based on the problems raised, including:

1) Change of VTP connection system from Trunk to Access

In accordance with the tests that the author did and show in Figure IV.4 to Figure IV.8 all groups of network devices that you on the 25th floor based on VLAN can connect to all existing devices. So that if one of the existing VLANs is disconnected, the IT division or division can quickly analyze the problems that occur and can easily repair the lost VLAN connection path.

2) Filtering data packets against the FTP server at the client or marketing division.

4. Conclusion

The final conclusion that the author implemented on the network scheme is in the attached image, the existing clients when testing or testing connections using the ping command in the command prompt application to the ftp server have no problems or connect. Likewise, when remotely using the ftp server using the command prompt application, it still connects or succeeds. But when in the marketing division, when remotely using the ftp server using the command prompt application, the request for ftp data packets on the client is blocked or cannot be forwarded, meaning that it does not connect or does not remotely the ftp server. Based on the discussion that has been made by the researcher as follows below:

a. By using VTP (Virtual Trinking Protocol) Access mode, each VLAN that is on a different Switch can be connected, and this Access mode provides a one-way cable connection link for one VLAN to communicate with the same VLAN on a different Switch.
b. By activating the firewall using the Access Control List (ACL) feature, it can be used to block sites that are considered irrelevant to the work needs of the company.
c. By further optimizing the ACL can create access rights on a system that is connected to the internet. So the system can only be accessed on clients who need the system.

5. References

[1] D. B. Rendro, Ngatono, and W. N. Aji, "Analisis Monitoring Sistem Jaringan Komputer Menggunakan Software Nmap," PROSISKO J. Pengemb. Ris. dan Obs. Sist. Komput., vol. 7, no. 2, pp. 108–115, 2020.
[2] J. E. W. Prakasa, "Konsep Dasar jaringan," no. Oktober, p. 106, 2018.
[3] D. Alfurqon and S. Assegaff, "Analisis Dan Perancangan Jaringan Local Area Network Pada Laboratorium Smk Negeri 1 Kota Jambi," J. Manaj. Sist. Inf., vol. 3, no. 3, pp. 1149–1163, 2018.
[4] Y. Faodiansyah, K. Amron, and E. S. Pramukantoro, "Analisis dan Perbandingan Performansi File Sharing Peer-to-Peer Menggunakan Framework JXTA dan Gnutella," J. Pengemb. Teknol. Inf. dan

Accredited "Rank 4"(Sinta 4), DIKTI, No. 36/E/KPT/2019, December 13th 2019.

Ilmu Komput., vol. 2, no. 10, pp. 3771–3778, 2018, [Online]. Available: https://j-ptiik.ub.ac.id/index.php/j-ptiik/article/view/2732/1016.

[5] Putra, "TOPOLOGI JARINGAN : Pengertian, Macam Macam Topologi & Kelebihan Kekurangannya," Salamadian, 2019, [Online]. Available: https://salamadian.com/topologi-jaringan-komputer/.

[6] M. R. Redi Mulyana, "APLIKASI PENGGAJIAN KARYAWAN BERBASIS CLIENT-SERVER PADA PT RADIO NASIONAL BUANA SUARA," J. Ilm. Ilmu Ekon., vol. 4, pp. 9–15, 2017, [Online]. Available: http://eprints.ummi.ac.id/64/3/Aplikasi Penggajian Karyawan Berbasis Client-Server Pada PT. Radio Nasional Buana Suara.pdf.

[7] I. Efendi, "Apa yang dimaksud dengan server," [Online]. Available: https://www.it-jurnal.com/apa-yang-di-maksud-dengan-server/.

[8] Zakaria, "15 Perangkat Jaringan Komputer Beserta Pengertian," [Online]. Available: https://www.it-jurnal.com/apa-yang-di-maksud-dengan-server/.

[9] Y. Ardian, "Buku Ajar Modul 1 Mikrotik Operating System Jaringan Komputer," Univ. Kanjuruhan Malang - Fak. Teknol. Inf., pp. 1–105, 2015, [Online]. Available: https://repository.unikama .ac.id/378/1/Modul Jarkom ISBN.pdf.

[10] A. Hidayat, "Perancangan Virtual Local Area Network (VLAN) Pada Lab Komputer D-III Sistem Informasi Universitas Muhammadiyah Metro (UM Metro)," Konf. Nas. Sist. Inf., pp. 739–745, 2018, [Online]. Available: http://jurnal.atmaluhur.ac.id/index.php/knsi2018/article/view/442.

[11] Y. D. Noviani, "Analisis Pengembangan Virtual Local Area Network (VLAN) di SMK Asy-Syarifiy Pandanwangi - Lumajang," vol. 02, no. 02, pp. 61–66, 2020, [Online]. Available: https://jurnal.stmik-amikbandung.ac.id/joint/article/download/31/22/105.

[12] M. Sabara and M. Sungkar, "Flashing Interconnecting Operating System (Ios) Pada Router Cisco 1841 Series Untuk Membangun Isp Dengan Sistem Pppoe Pada Client Di Arg Media Data," Power Elektron. J. Orang Elektro, vol. 8, no. 1, pp. 1–4, 2019, doi: 10.30591/polektro.v8i1.1495.

[13] A. Setyawan, "Address Menggunakan Metode Access List Control Pada Router Cisco," J. Tek. Komput. Amik BSI, vol. III, no. 1, pp. 60–73, 2017, [Online]. Available: https://ejournal.bsi.ac.id/ejurnal/index.php/jtk/article/view/1344/1093.

[14] S. Samuel Tampi, S. Raharjo, and M. Sholeh, "PERANCANGAN JARINGAN KOMPUTER PADA RUMAH SAKIT SOEDARSONO DARMOSOEWITO DI BATAM DESIGN OF COMPUTER NETWORK AT SOEDARSONO DAMOSOEWITO IN BATAM Stefanus Samuel Tampi," J. JARKOM, vol. 7, no. 1, pp. 137–152, 2018, [Online]. Available: http://download.garuda.ristekdikti.go.id/article.php?article=975068&val=6284&title=PERANCANGAN JARINGAN KOMPUTER PADA RUMAH SAKIT SOEDARSONO DARMOSOEWITO DI BATAM DESIGN OF COMPUTER NETWORK AT SOEDARSONO DAMOSOEWITO IN BATAM.

[15] J. Pastima Simanjuntak, Cosmas Eko 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.

[16] I. W. D. Alfian Aji Saputra, "Implementasi Access Control List Menggunakan Mikrotik Pada Smk Budi Mulia Tangerang," Jurr n a l I D E A L I S, vol. 1, no. 5, pp. 401–408, 2019.

[17] S. N. M. P. Simamora, N. Hendrarini, E. Lya, and U. Sitepu, "Metode Access Control List sebagai Solusi Alternatif Seleksi Permintaan Layanan Data pada Koneksi Internet," J. Teknol. Inf. Politek. Telkom, vol. 1, no. 1, 2011.

[18] R. R. R. B. Wijonarko, "Implementasi Virtual Local Area Network Dengan Switch," vol. 14, no. 2, pp. 203–210, 2020, [Online]. Available: https://ejournal.nusamandiri .ac.id/index.php /inti/article/view/ 122 5/613.