Jurnal Sistem Komputer dan Informatika (JSON)
Volume 1, Nomor 2, Januari 2020
e-ISSN 2685-998X
DOI 10.30865/json.v1i2.1920

Implementasi Keamanan Jaringan Komputer *Local Area Network* Menggunakan *Access Control List* pada Perusahaan X

Agung Tri Laksono, M. Alvian Habib Nasution

Fakultas Ilmu Komputer, Program Studi Teknik Komputer, Universitas Amikom Yogyakarta, Sleman, Indonesia
Email: [1] Agung.1998@students.amikom.ac.id, [2] Alvian.nasution@students.amikom.ac.id

Abstrak–Di sebuah Perusahaan X penggunaan internet merupakan sebuah tuntutan bagi para pekerja. Oleh karena itu jaringan internet sangat dibutuhkan di sebuah Perusahaan X. Tidak adanya pembatasan akses dalam penggunaan jaringan internet dapat mengganggu keamanan dan penyalahgunaan jaringan internet, untuk itu dirancang pengaturan dalam jaringan internet tersebut. Salah satu metode yang digunakan yaitu metode *Virtual Local Area Network* (VLAN) *Access Control List* (ACL) yang diterapkan pada Perusahaan X. Metode Vlan *Access Control List* merupakan salah satu teknik permintaan suatu akses jaringan internet atau komunikasi data dan pengiriman sejumlah paket data dari satu komputer ke komputer lainnya. Hasil reset penulis membuktikan bahwa Vlan *Access Control List* dengan metode filtering dan pembagian pengguna koneksi internet dapat menyaring dan mengidentifikasi pengguna yang telah di batasi aksesnya untuk mengakses pengguna yang lain atau ke server di Perusahaan X untuk meningkatkan Keamanan data.

Kata Kunci: *Virtual Local Area Network* (VLAN), *Access Control List* (ACL)

Abstract–In Company X, the use of the internet is a demand for workers. Therefore, an internet network is very much needed in a Company X. The absence of restrictions in the use of the internet network can interfere with the security and misuse of the internet network, for this reason the arrangements in the internet network are designed. One method used is the *Virtual Local Area Network* (VLAN) *Access Control List* (ACL) method that is applied to Company X. The Vlan *Access Control List* method is one of the techniques for requesting an internet network access or data communication and sending a number of data packets from one computer to another. The author resets the results proving that the Vlan *Access Control List* with the filtering and sharing method of internet connection users can filter and identify users who have restricted access to access other users or to servers in Company X to improve data security.

Keywords: *Virtual Local Area Network* (VLAN) , *Access Control List* (ACL)

1. PENDAHULUAN

Banyaknya user yang berada pada Perusahaan X dan tidak adanya pengontrolan hak akses pada setiap user yang ada pada jaringan internet, Masalah ini dapat mengganggu keamanan dan penyalahgunaan jaringan internet sehingga akan menimbulkan segala bentuk resiko.[1] Hal yang akan terjadi jika hak akses setiap user tidak di kontrol seperti pencurian data [2] , user mempunyai akses berlebih terhadap server, user bisa mengupload beberapa file yang berbahaya terhadap server[3].

Dengan akses yang tidak dikontrol kepada pengguna akan mengakibatkan pengguna melakukan penyimpangan di luar kepentingan dari Perusahaan [4]. Untuk menanggulangi permasalahan ini penulis menggunakan *Virtual Local Area Network* (VLAN) dan *Access Control List* (ACL) yang merupakan upaya alternatif untuk mengamankan dan mengontrol akses dari sebuah koneksi jaringan internet [5].

2. METODE PENELITIAN

Metode yang dilakukan oleh penulis dalam melakukan penelitian ini adalah Simulasi Sistem Jaringan tahapan yang dibutuhkan dan analisa kebutuhan kegiatan sebagai berikut:

2.1 Studi Literatur

Merupakan pengumpulan informasi dari literature, dari jurnal tentang permasalahan keamanan jaringan dan pemecahan permasalahan dengan menggunakan *Access Control List.* Metode ini merupakan metode yang dimana pengumpulan referensi yang berkaitan dengan *Virtual Local Area Network* dan *Access Control List* . dengan menganalisa per topiknya . dan kemudian analisis per topiknya untuk memberikan kesimpulan tiap bagian pembahasan.

2.2 Praktik simulasi

Melakukan praktik simulasi dan mempelajari perangkat virtual dan perangkat fisik yang saling berkaitan dengan solusi yang akan diimplementasikan oleh penulis dengan menggunakan *software cisco Packet Tracer* . tahapan praktik simulasi ini , perancangan implementasi dengan menggunakan *software* simulasi sistem jaringan komputer yaitu *cisco packet tracer*, yang dimana penulis membuat sebuah topologi jaringan komputer dari Perusahaan X , dan kemudian penulis membuat pembagian-pembagian jaringan untuk Perusahaan X yang dimana pembagian ini untuk mencegah user dari luar yang ingin masuk ke dalam system atau tidak sembarangan user dari luar masuk dan mengakses sistem dari Perusahaan X dengan menggunakan *Access Control List* (ACL) .

Submitted: **04/01/2020**; Accepted: **09/01/2020**; Published: **25/01/2020**

Jurnal Sistem Komputer dan Informatika (JSON)
Volume 1, Nomor 2, Januari 2020
e-ISSN 2685-998X
DOI 10.30865/json.v1i2.1920

Alamat IP yang di konfigurasi ACL di sesuaikan dengan hak aksesnya yang dimana pada tahapan ini dilakukannya pembagian hak akses bagi user atau client, konfigurasi dilakukan dengan menggunakan dengan menggunakan *standard* ACL dan *extended* ACL, Konfigurasi standard ACL dengan mengkonfigurasi *source IP Address* yang ada pada router dan untuk *extended* ACL mengacu pada destination *IP Address* pada perangkat router dan alamat-alamat IP yang berada pada VLAN. Tahapan akhir dari metode ini yaitu berupa pengujian hasil konfigurasi pada tahapan implementasi . pengujian ini dilakukan dengan mencoba melakukan akses dari client atau user yang di blok dengan menggunakan *Access Control List* dari *source IP Address* (*standard* ACL)dan dari user yang di blok dari *destination IP address* (extended ACL).

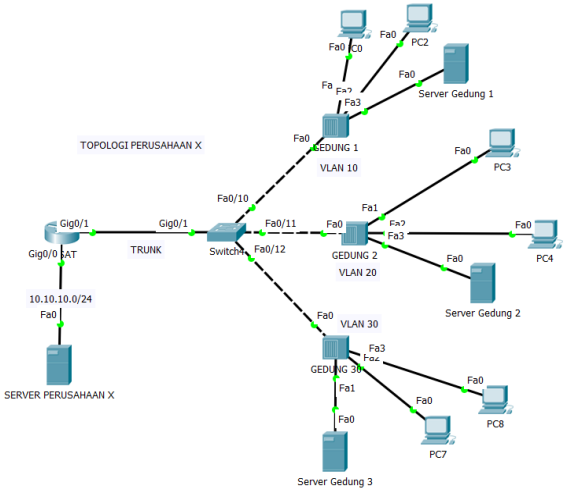
3. HASIL DAN PEMBAHASAN

Pada tahapan praktik simulasi dilakukan pendataan alamat *source* IP dan *destination* IP yang dimana akan diterapkan di *Access Control List.* Alamat IP yang akan diterapkan pada *Access Control List* seperti di tabel 1.1 dapat dilihat bahwa terdapat sepuluh alamat IP sumber (*Source* IP) dan ada sepuluh alamat IP tujuan (*Destination* IP)dan terdapat sepuluh *service* yang dapat di akses oleh masing-masing client dan server. Ketika dikonfigurasi *Access Control List* yang ber *type* hak aksesnya "*permit"* alamat IP sumber (*Source* IP) dan alamat IP tujuan (*Destination* IP) dapat saling terhubung dan dapat mengakses *service* tambahan seperti FTP dan TFTP, ketika *Access Control List* dikonfigurasi dengan type hak akses *"deny"* dengan alamat IP sumber (*Source* IP) dan alamat IP tujuan (*Destination* IP) maka aksesnya akan di filter atau dihentikan akan tetapi dengan menggunakan *Access Control List Extended* dapat menggunakan *service* contoh menggunakan type hak akses *"deny"* dengan memfilter sebuah service ftp maka client tidak dibolehkan mengakses FTP dan koneksi terhadap alamat IP tujuan (*Destination* IP) tidak akan terhubung jika menggunakan *type* (*Outbound*) namun jika menggunakan type (*inbound*) maka client tidak bisa mengakses FTP namun client dapat mengakses koneksi dari alamat IP tujuan (*Destination* IP) yaitu hanya dapat mengakses *Internet Control Message Protocol* (ICMP) saja.

Tabel 1. Pengalamatan IP

NO	TYPE AKSES	SOURCE/RANGE IP	DESTINATION IP	SERVICE
1	Permit	192.168.10.5	10.10.10.5	ftp,tftp
2	Permit	192.168.20.5	10.10.10.5	ftp,tftp
3	Permit	192.168.30.5	10.10.10.5	ftp,tftp
4	Deny	192.168.10.2-3	10.10.10.5	ftp
5	Deny	192.168.20.2-3	10.10.10.5	ftp
6	Deny	192.168.30.2-3	10.10.10.5	ftp

Data Alamat IP yang terdapat pada Tabel 1 tersebut dapat digambarkan menjadi sebuah topologi Gambar 1 dibawah ini. Pada Gambar 1 terdapat tiga gedung dan di masing-masing gedung terdapat satu server kemudian terdapat dua client dan juga terdapat Router PUSAT yang di dalamnya terdapat Server Perusahaan X, di dalam topologi tersebut telah di konfigurasi dengan sesuai instruksi dari Tabel 1.



Gambar 1. Topologi Perusahaan X X

Pada tahap implementasi dilakukan tiga tahap konfigurasi. *Virtual Local Area Network* (VLAN), Inter-VLAN dan *Access Control List* (ACL) untuk mendaftarkan alamat IP untuk management VLAN atau ACL

Submitted: **04/01/2020**; Accepted: **09/01/2020**; Published: **25/01/2020**

Jurnal Sistem Komputer dan Informatika (JSON)
Volume 1, Nomor 2, Januari 2020
e-ISSN 2685-998X
DOI 10.30865/json.v1i2.1920


```
!
interface GigabitEthernet0/1.10
 encapsulation dot1Q 10
 ip address 192.168.10.1 255.255.255.0
 ip access-group vlan10 in
!
interface GigabitEthernet0/1.20
 encapsulation dot1Q 20
 ip address 192.168.20.1 255.255.255.0
 ip access-group vlan20 in
!
interface GigabitEthernet0/1.30
 encapsulation dot1Q 30
 ip address 192.168.30.1 255.255.255.0
 ip access-group vlan30 in
!
```

Gambar 2. Konfigurasi VLAN

```
ip classless
!
ip flow-export version 9
!
!
ip access-list extended vlan10
 permit tcp host 192.168.10.5 host 10.10.10.5 eq ftp
 deny tcp host 192.168.10.3 host 10.10.10.5 eq ftp
 deny tcp host 192.168.10.2 host 10.10.10.5 eq ftp
 permit tcp host 192.168.10.5 host 10.10.10.5 eq tftp
ip access-list extended vlan20
 deny tcp host 192.168.20.2 host 10.10.10.5 eq ftp
 deny tcp host 192.168.20.3 host 10.10.10.5 eq ftp
 permit tcp host 192.168.20.5 host 10.10.10.5 eq ftp
 permit tcp host 192.168.20.5 host 10.10.10.5 eq tftp
ip access-list extended vlan30
 deny tcp host 192.168.30.2 host 10.10.10.5 eq ftp
 deny tcp host 192.168.30.3 host 10.10.10.5 eq ftp
 permit tcp host 192.168.30.5 host 10.10.10.5 eq ftp
 permit tcp host 192.168.30.5 host 10.10.10.5 eq tftp
!
```

Gambar 3. Konfigurasi AC

Gambar 2 menunjukan konfigurasi pembuatan VLAN disini penulis membuat tiga buah *Virtual Local Area Network* (VLAN) dengan ID 10.20,dan 30 yang akan di terapkan pada *Access Control List (*ACL) Pada gambar 1.2 pada port *FastEthernet*0/10 dimasukan VLAN 10 , pada port *FastEthernet*0/20 dimasukan VLAN 20 , dan pada port *FastEthernet*0/20 dimasukan VLAN 30. Pada gambar 3 merupakan konfigurasi *Access Control List* (AC) disini penulis menggunakan *Extended Access Control List* karena untuk ACL ini merupakan jenis ACL yang keamanan nya sudah teruji , pada gambar 1.3 penulis menggunakan nama ACL dengan nama VLAN 10, VLAN 20 dan VLAN 30 yang dimana di masing ACL terdapat beberapa client yang sudah dapat di filter di ACL VLAN 10 terdapat type ACL deny yang dimana host dari 192.168.10.2 dan 192.168.10.3 tidak dapat mengakses service FTP dari alamat IP tujuan 10.10.10.5. dan terdapat akses permit yang dimana host dari 192.168.10.5 dapat mengakses service FTP dan TFTP pada host 10.10.10.5 yang berada di server Perusahaan X. Pada ACL VLAN 20 terdapat type ACL deny yang dimana host dari 192.168.20.2 dan 192.168.20.3 tidak dapat mengakses service FTP dari alamat IP tujuan 10.10.10.5. dan terdapat akses permit yang dimana host dari 192.168.20.5 dapat mengakses service FTP dan TFTP pada host 10.10.10.5 yang berada di server Perusahaan X .Pada ACL VLAN 30 terdapat type ACL deny yang dimana host dari 192.168.30.2 dan 192.168.30.3 tidak dapat mengakses service FTP dari alamat IP tujuan 10.10.10.5. dan terdapat akses permit yang dimana host dari 192.168.30.5 dapat mengakses service FTP dan TFTP pada host 10.10.10.5 yang berada di server Perusahaan X

Tabel 2. Konfigurasi ACL Berdasarkan Baris

Baris ke -	ACL
1	permit tcp host 192.168.10.5 host 10.10.10.5 eq ftp permit tcp host 192.168.10.5 host 10.10.10.5 eq tftp
2	permit tcp host 192.168.20.5 host 10.10.10.5 eq ftp permit tcp host 192.168.20.5 host 10.10.10.5 eq tftp
3	permit tcp host 192.168.30.5 host 10.10.10.5 eq ftp permit tcp host 192.168.30.5 host 10.10.10.5 eq tftp
4	deny tcp host 192.168.10.2 host 10.10.10.5 eq ftp deny tcp host 192.168.10.3 host 10.10.10.5 eq ftp
5	deny tcp host 192.168.20.2 host 10.10.10.5 eq ftp deny tcp host 192.168.20.3 host 10.10.10.5 eq ftp
6	deny tcp host 192.168.30.2 host 10.10.10.5 eq ftp deny tcp host 192.168.30.3 host 10.10.10.5 eq ftp

Pada Tabel 2 Konfigurasi ACL ini mengacu pada hasil yang dilakukan dari tahapan praktik simulasi yaitu menggunakan *Access Control List extended* yang dimana alamat-alamat IP yang di konfigurasi seperti pada baris pertama sampai baris ke 3 dengan akses *"permit"* untuk konfigurasi , pertama memasukan alamat IP sumber (*Source* IP) dengan di lanjut memasukan alamat IP tujuan (*Destination* IP) dan di lanjut memasukan *service* yang

Submitted: **04/01/2020**; Accepted: **09/01/2020**; Published: **25/01/2020**

Jurnal Sistem Komputer dan Informatika (JSON)
Volume 1, Nomor 2, Januari 2020
e-ISSN 2685-998X
DOI 10.30865/json.v1i2.1920

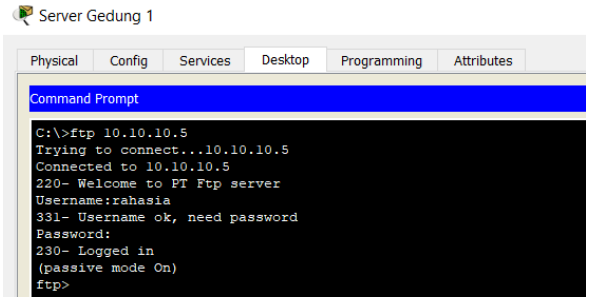
akan di filter yaitu FTP dan TPFT. Di konfigurasi ini yaitu ketika masing-masing server yang ada di Gedung satu ,dua, dan tiga akan mengakses server Perusahaan X dengan service FTP maka aksesnya diijinkan "*permit*" , begitupun sebaliknya ketika server Perusahaan X mengakses FTP dari server yang ada di masing-masing Gedung maka akses akan diijinkan. Selanjutnya Pada baris empat sampai enam dengan akses *"deny"* untuk konfigurasi , pertama memasukan alamat IP sumber (*Source* IP) dengan di lanjut memasukan alamat IP tujuan (*Destination* IP) dan di lanjut memasukan *service* yang akan di filter yaitu FTP. Di konfigurasi ini yaitu ketika masing-masing client atau PC yang ada di masing-masing Gedung ingin mengakses sebuah service FTP dari server Perusahaan X aksesnya tidak diijinkan *"deny"* atau di hentikan karena di filter oleh *Access Control List* , tujuan tidak diijinkan client mengakses server Perusahaan X karena untuk membatasi upload file yang tidak penting atau mengatasi user yang sengaja merugikan Perusahaan X, jadi setiap server Perusahaan X ingin mengambil data dari client dapat melalui server yang berada di masing-masing gedung guna menjaga keamanan sebuah jaringan dan keamanan Perusahaan X.

3.1 Implementasi

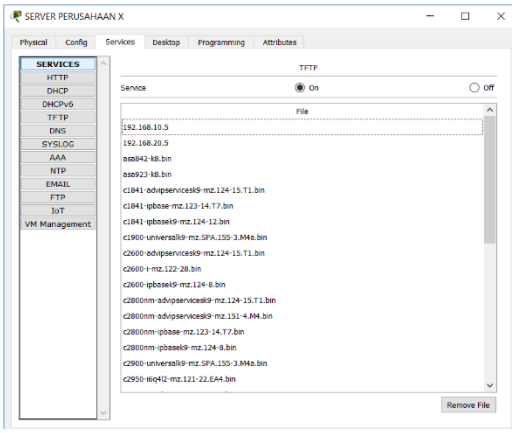
Pada tahapan evaluasi ini dilakukan pengujian dari setiap alamat IP sumber (*Source* IP) dan alamat IP tujuan (*Destination* IP) yang telah di konfigurasi dengan *Access Control List* (ACL). Pengujian ini dilakukan sesuai dengan tahap praktik simulasi yang sudah dijelaskan sebelumnya.

1. Tahap pengujian baris kesatu ACL

Pada gambar 4 dan gambar 5 dalam pengujian ACL , disini terdapat sebuah Server dari Gedung satu dengan host 192.168.10.5 di konfigurasi *Access Control List* dengan menggunakan hak akses "permit" atau diijinkan mengakses sebuah service FTP dan TFTP Fungsinya untuk memudahkan server dari Perusahaan X X atau dari server Gedung 1 berbagi data dan membackup data.



Gambar 4. Pengujian ACL FTP



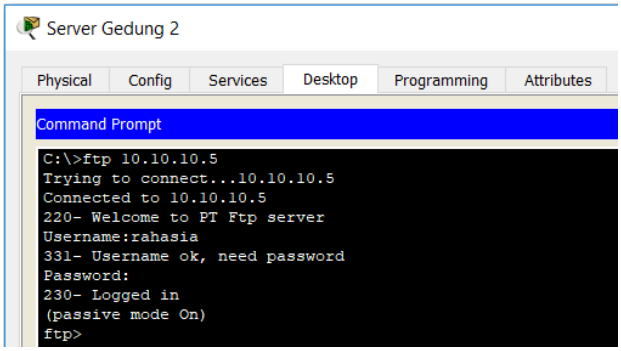
Gambar 5. Pengujian ACL TFTP

2. Tahap pengujian baris kedua ACL

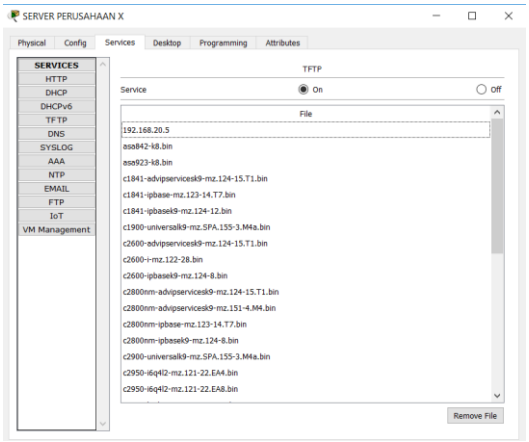
Pada gambar 6 dan 7 dalam pengujian ACL, disini terdapat sebuah Server dari Gedung dua dengan host 192.168.20.5 di konfigurasi *Access Control List* dengan menggunakan hak akses "permit" atau diijinkan mengakses sebuah service FTP dan TFTP Fungsinya untuk memudahkan server dari Perusahaan X atau dari server Gedung 1 berbagi data dan membackup data.

Submitted: **04/01/2020**; Accepted: **09/01/2020**; Published: **25/01/2020**

Jurnal Sistem Komputer dan Informatika (JSON)
Volume 1, Nomor 2, Januari 2020
e-ISSN 2685-998X
DOI 10.30865/json.v1i2.1920



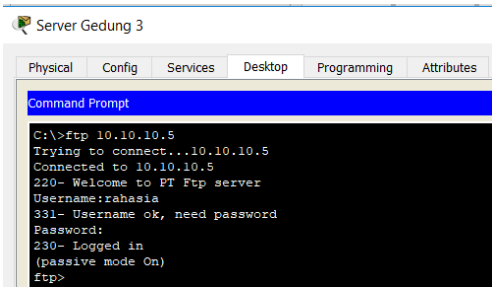
Gambar 6. Pengujian ACL FTP



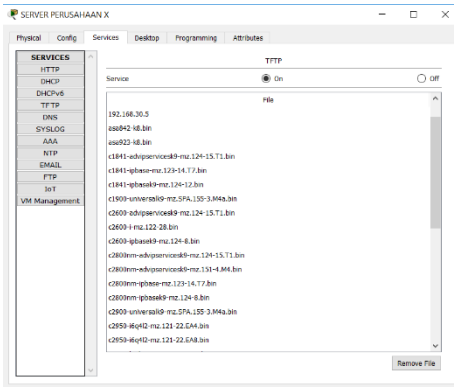
Gambar 7. Pengujuan ACL TFTP

3. Tahap pengujian baris ketiga ACL

Pada gambar 8 dan 9 dalam pengujian ACL , disini terdapat sebuah Server dari Gedung tiga dengan host 192.168.30.5 di konfigurasi *Access Control List* dengan menggunakan hak akses “permit” atau diijinkan mengakses sebuah service FTP dan TFTP Fungsinya untuk memudahkan server dari Perusahaan X atau dari server Gedung 1 berbagi data dan membackup data.



Gambar 8. Pengujian ACL FTP



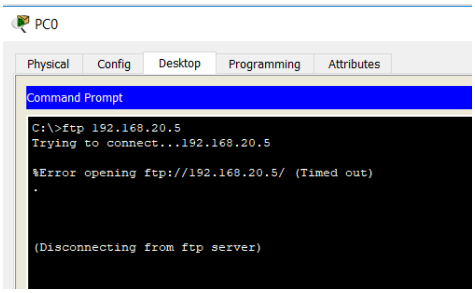
Gambar 9. Pengujian ACL TFTP

Submitted: **04/01/2020**; Accepted: **09/01/2020**; Published: **25/01/2020**

Jurnal Sistem Komputer dan Informatika (JSON)
Volume 1, Nomor 2, Januari 2020
e-ISSN 2685-998X
DOI 10.30865/json.v1i2.1920

4. Tahap pengujian baris keempat ACL

Pada gambar 10 dan dalam pengujian ACL , disini terdapat sebuah client dari Gedung satu dengan host 192.168.10.2-192.168.10.3 di konfigurasi *Access Control List* dengan menggunakan hak akses "*deny*" atau tidak diijinkan mengakses sebuah service FTP Fungsinya untuk keamanan data supaya client tidak bisa upload file sembarangan terhadap server Perusahaan X .



Gambar 10. Pengujian ACL FTP

4. KESIMPULAN

Dari hasil implementasi praktik simulasi yang telah dilaksanakan penulis dapat menyimpulkan bahwa *Access Control List*(ACL) pada jaringan *Virtual Local Area Network* (VLAN) di Perusahaan X sudah berhasil diterapkan. Hal yang dapat dibuktikan dengan melakukan testing terhadap client, mengakses server Perusahaan X dengan hak akses *"deny"* atau tidak diijinkan mengakses Service FTP dari Server Perusahaan X dengan tujuan keamanan data, dan server dari setiap Gedung dapat mengakses Server X terutama service FTP dan TFTP untuk upload dan membackup sebuah data.

REFERENCES

[1] "Penerapan Access Control List (Acl) Pada Karingan Vlan," 2014.
[2] I. Chaidir and R. R. Wirawan, "Pembatasan Akses Jaringan Internet Pada Clearos Menggunakan Metode Access Control List," vol. 4, no. 1, pp. 212–216, 2018.
[3] 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.
[4] P. M. Informatika, "Penerapan Static Vlan Dan Access List," vol. 5, no. 2, pp. 1–6, 2019.
[5] 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, pp. 15–19, 2011.

Submitted: **04/01/2020**; Accepted: **09/01/2020**; Published: **25/01/2020**