ISSN: 2503-054X
Vol. 8 No: 2, Oktober 2023

Proteksi Jaringan Menggunakan Access Control List pada Local Area Network

1st Wahyudi
Program Studi Sistem Informasi, Universitas Horizon Indonesia
Jl. Pangkal Perjuangan By Pass No.1 Karawang 41316
wahyudi.01.stmik@krw.horizon.ac.id

2nd Dedih
Program Studi Sistem Informasi, Universitas Horizon Indonesia
Jl. Pangkal Perjuangan By Pass No.1 Karawang 41316
dedih.horizon.krw@horizon.ac.id

Abstrak – Asset berupa data dan informasi saat ini sangatlah penting untuk dilindungi, diperlukan suatu cara guna menjaga keamanan data yang dimilikinya. Untuk menjaga keamanan terhadap ancaman dari luar kiranya diperlukan perlindungan yang cukup mumpuni untuk melindungi seluruh data dan informasi yang terdapat didalamnya. Banyak perusahaan yang telah menjadikan teknologi informasi menjadi hal terpenting dalam menunjang seluruh aktifitasnya . Salah satu keamanan dibidang teknologi informasi adalah dengan membatasi akses pada jariangan *Local Area Network* (LAN). Hal tersebut dapat dilakukan dengan memanfaatkan *feature* keamanan dasar yang terdapat pada *router Cisco* yaitu *Access Control List* (ACL). ACL memiliki kemampuan untuk melakukan *filtering* terhadap *traffic* seperti membatasi trafik jaringan, mengatur aliran trafik, memutus jenis *traffic* mana yang diperbolehkan atau tidak diperbolehkan masuk dalam jaringan dan mampu memberikan keamanan untuk akses kejaringan. Cara kerja dari ACL sendiri selalu membaca setiap pernyataan secara berurutan dari atas ke bawah dan kemudian memutuskan untuk menerima atau menolak sesuai dengan apa yang telah didefinisikan didalam pernyataan. Dalam melakukan penelitian ini menggunakan aplikasi *Cisco Packet Tracer* 7.1 yang sudah banyak digunakan untuk membangun *prototype* jaringan dan mensimulasikannya.

Kata Kunci – Keamanan jaringan , LAN, *Access Control List*, Trafik.

I. PENDAHULUAN

Peran internet semakin penting dalam kehidupan sosial, ekonomi dan politik di dunia global saat ini. Setiap tahun internet semakin berpengaruh dalam kehidupan manusia. Tak dapat disangkal bahwa teknologi ini telah mengubah peradaban dunia dengan cepat. Pengguna internet diseluruh dunia baik perngkat *mobile* maupun *fixed* terus mengalami peningkatan. Berdasarkan laporan *International Telecommunication Union* (ITU) yang merupakan badan Perserikatan Bangsa-Bangsa (PBB) jumlah pengguna internet di dunia pada tahun 2018 mencapai 3,9 miliar melebihi setengah dari populasi dunia. Kenaikan jumlah pengguna juga terjadi di Indonesia. Menurut hasil survei Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) pada tahun 2018 jumlah pengguna internet di Indonesia sebesar 171,1 juta, naik sebesar 27,9 juta dari tahun sebelumnya yang berjumlah 143,2 juta. Diprediksi bahwa pada tahun 2019 dan seterusnya jumlah pengguna internet akan terus meningkat, terutama dengan selesainya proyek jaringan palapa RING yang akan meningkatkan keandalan koneksi internet di seluruh indonesia [1]. Perkembangan internet yang begitu pesat saat ini berpotensi pada terciptanya peluang timbulnya kejahatan dibidang teknologi informasi khusus pencurian informasi dan data penting. Pencurian data dan informasi telah terjadi lama sebelum adanya internet. Semua ini terjadi sebelum istilah '*cyber'* digunakan secara luas. Menurut data yang dikeluarkan oleh Badan Siber dan Sandi Negara (BSSN) pada tahun 2021, tercatat bahwa terjadi sebanyak 1.637.937.022 *anomaly traffic* di Indonesia. *Anomaly traffic* paling banyak terjadi pada bulan Desember 2021 yang mencapai 242.066.168 dan *MyloBot* menjadi *top traffic anomaly cyber-attack* di tahun 2021 yang mencapai 730.946.448 kasus [2]. *Cybercrime* merupakan kejahatan yang berada pada dunia maya, kemajuan pada teknologi informasi seperti internet ini dapat digunakan sebagai tindakan illegal sebelumnya serta beberapa illegal baru [3]. Kejahatan *cyber* menargetkan pencurian informasi pribadi, perusahan atau pemerintahan. *Cybercrime* menekankan pentingnya jaringan computer dalam kehidupan, serta fakta bahwa

ISSN: 2503-054X
Vol. 8 No: 2, Oktober 2023

data kita tidak pernah aman di jaringan internet [4]. Oleh karena itu diperlukan suatu langkah atau strategi untuk dapat mencegah terjadinya kejahatan tersebut.

Salah satu bentuk permasalahan yang sering ditemukan jaringan komputer adalah sering terjadi serangan-serangan terhadap jaringan komputer dengan maksud dan tujuan yang berbeda. Dengan latar belakang tersebut dibutuhkan suatu tindakan untuk melakukan proteksi terhadap jaringan komputer yang dimiliki seperti pengaturan keamanan jaringan dengan cara mengontrol trafik yang masuk dan keluar dengan memanfaatkan fitur yang terdapat pada router yang biasanya digunakan untuk koneksi ke internet atau koneksi antar jaringan. Adapun fitur tersebut adalah *Access Control List (ACL).*

II. TINJAUAN PUSTAKA

A. *Access Control List (ACL)*

Access Control List (ACL) adalah metode keamanan jaringan yang dapat membatasi akses untuk perangkat berhubungan dan berkomunikasi satu dengan yang lainnya.[5]. ACL adalah daftar aturan yang menentukan pengguna atau sistem mana yang diberikan atau ditolak aksesnya ke objek atau sumber daya sistem tertentu. ACL dapat dipasang di router yang bertindak sebagai filter, mengelola lalu lintas mana yang dapat mengakses jaringan [6]. ACL digunakan untuk mengkontrol perizinan ke sistem computer atau jaringan computer juga digunakan untuk memfilter trafik yang masuk dan keluar dari perangkat tertentu seperti jaringan *gateway* atau perangkat *endpoint* yang pengguna akses secara langsung. ACL juga dapat membantu memperbaiki pengatur traffic untuk meningkatkan efisien jaringan dan memberi kontrol pada *administrator* jaringan atas pengguna di sistem dan jaringan komputer. ACL juga dapat digunakan untuk meningkatkan keamanan jaringan dengan mencegah lalu lintas berbahaya.

ACL dapat dikategorikan berdasarkan cara mereka mengidentifikasi trafik yaitu *standard* ACLs memblokir atau mengizinkan seluruh rangkaian protocol menggunakan alamat IP sumber dan *Extented* ACLs dimana pemblokiran dan pengizinan trafik jaringan berdasarkan serangkaian karakteristik yang lebih berbeda yang mencakup alamat IP sumber dan tujuan serta nomor port , bukan hanya alamat sumber [6].

B. Cara kerja ACL

Access Control List (ACL) berisikan perintah kontrol akses yang berisi perizinan dan informasi dimana pengguna akan diberikan izin atau ditolak. Jika informasi sudah mempunyai izin, maka pengguna yang telah diberi hak akses tersebut dapat mengakses yang tentunya telah dikontrol oleh kontrol akses tersebut. Dibutuhkan *administrator* untuk mengamankan data serta mengendalikan hak atas data apa saja yang boleh diakses serta kapan data tersebut bisa diakses. Secara sederhana ACL ialah suatu standar keamanan.

Metode kerja ACL sendiri merupakan senantiasa membaca tiap list atau daftar dengan metode sequential ataupun berurut dari atas ke dasar. Ketika terdapat paket informasi, ACL akan membaca serta menyamakan tiap daftar yang telah dibuat. Jika kondisi sesuai dengan yang terdaftar pada kontrol akses, maka data dapat diteruskan untuk memperoleh hak akses. Tetapi apabila kondisi tidak sesuai dengan yang terdaftar pada kontrol akses maka paket tidak dapat memperoleh akses

C. Tipe Access Control List (ACL)

Menurut Ben Lutkevich [6], ada dua tipe dasar ACL:

1. *File System* ACLs mengelola akses ke file dan direktori. ACL memerintahkan OS untuk memberikan ijin akses pengguna pada sistem dan hak istimewa setelah sistem diakses.
2. *Network ACLs* mengelola akses jaringan dengan memberikan instruksi ke jaringan switch dan router yang menentukan jenis trafik yang diizinkan untuk berinteraksi dengan jaringan. ACL ini juga menentukan izin pengguna dalam jaringan. *Administrator* jaringan menetapkan aturan ACL dalam jaringan. Dengan cara ini, ACL berfungsi mirip dengan *firewall*.

ACL juga dapat dikategorikan berdasarkan cara mereka mengidentifikasi trafik :

ISSN: 2503-054X
Vol. 8 No: 2, Oktober 2023

1. *Standard ACL* dipakai ketika sebuah trafik dilakukan filtering berdasarkan jenis dari trafik yang berasal dari suatu host atau jaringan. *Filtering* hanya sebatas IP address dan tidak dapat dilakukan untuk memfiltering protocol atau port suatu jariangan.untuk diijinkan atau ditolak.
2. *Extended ACL* , berbeda dengan *Standard ACL* , *Extended ACL* dapat digunakan untuk melakukan *filtering* trafik yang lebih spesifik. Kita dapat menentukan trafik untuk protocol dan port apa yang akan dijinkan atau ditolak. Lebih dari itu *extended* ACL juga dapat digunakan untuk menentukan tujuan dari trafik tersebut.

D. Penomoran dan Penamaan ACL

Semua *access list* harus diidentifikasi menggunakan nama atau nomor, Penamaan *access list* lebih mudah penerapannya dibandingkan dengan penomoran karena kita dapat menentukan nama yang mudah diingat atau berkaitan dengan kegiatan. Penamaan *access list* dapat mendukung fitur yang tidak terdapat pada penomoran.

Beberapa jenis penomoran ACL yang digunakan untuk penomoran untuk mengkonfigurasi ACL dan yang paling umum digunakan adalah *Standard* IP 1 -99 dan 1300 – 1999 dan *Extended* IP 100 -199 dan 2000 – 2999.

E. *Secure Network Life Cycle*

Konsep keamanan dalam konteks tata kelola teknologi informasi, kepatuhan, manajemen resiko dan dengan membangun arsitektur keamanan yang baik dan penerapan *system design life cycle* (SDLC) dapat menghasilkan proses yang lebih murah dan efektif jika dibandingkan dengan menambahkan SDLC kedalam sistem operasional [7].

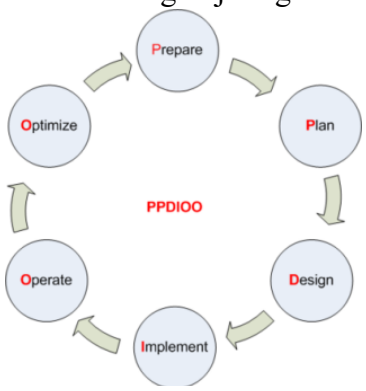
SDLC mencakup lima fase :

1. Inisiasi
2. Akuisisi dan pengembangan
3. Implementasi
4. Operasi dan pemeliharaan
5. Disposisi

Masing-masing dari ke lima fase ini mencakup serangkaian langkah-langkah keamanan minimum yang perlu dilaksanakan secara efektif kedalam sistem keamanan selama proses pengembangan berlangsung.

III. METODE PENELITIAN

Dalam proses mengembangkan dan mendesign jaringan menggunakan framework yang sudah yang sudah banyak digunakan yaitu PPDIOO (*Prepare, Plan, Design, implement, Operate dan Optimize)* [8] yang merupakan metode perancangan jaringan yang dikembangkan oleh Cisco atau biasa disebut sebagai *life cycle* layanan jaringan Cisco yang dirancang untuk membangun jaringan dan perkembangnya.



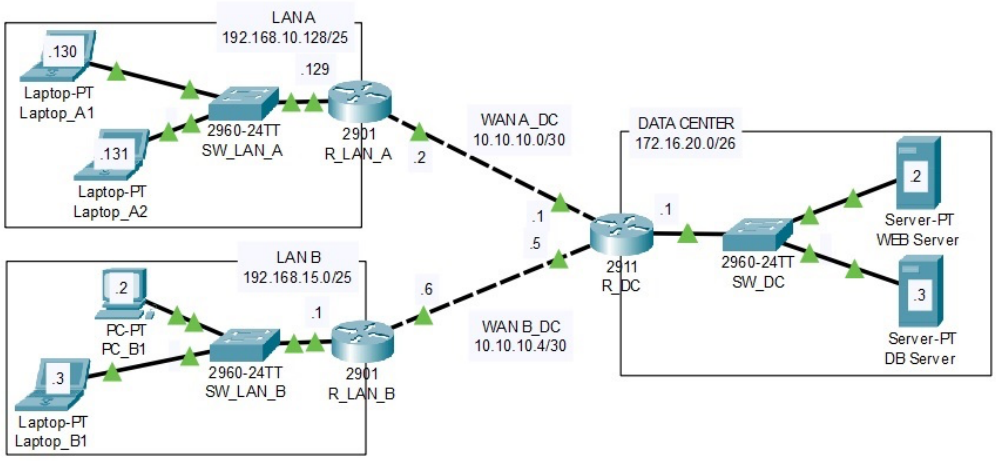
Gambar 1. *Life Cycle* PPDIOO [8]

ISSN: 2503-054X
Vol. 8 No: 2, Oktober 2023

Berdasarkan gambar 1 diatas maka dalam melakukan penelitian ini dilakukan beberapa tahapan yaitu [9]:

1. Persiapan / *Prepare*
   Meliputi persiapan di tingkat organisasi, seperti menentukan strategi jaringan dan menentukan model bisnis yang sesuai dengan jaringan yang akan dibangun.
2. Perencanaan / *Plan*
   Perencanakan meliputi merencanakan kebutuhan jaringan, melakukan analisis permasalahan dan perencanaan waktu pengerjaan projek.
3. Desain / *Design*
   Desain jaringan harus dibuatkan secara detail, seperti menggunakan aplikasi untuk mendesain topologi jaringan dan aplikasi *cisco packet tracer* untuk mensimulasikan koneksi pada jaringan atau yang lainnya.
4. Implementasi / *Implement*
   Implementasi harus dilakukan berdarakan rencana dan desain yang sudah dibuat..
5. Operasi / *Operate*
   Operasi jaringan meliputi konfigurasi jaringan sesuai dengan perencanaan yang telah dibuat sebelumnya dan memonitor kondisi jaringan.
6. Optimisasi / *Optimize*
   Optimisasi meliputi mengatasi kelemahan yang ada seperti mencari kelemahan dari jaringan, meningkatkan performa jaringan, dan menjaga agar jaringan tetap stabil.

Adapun rancangan topologi untuk mengimplementasikan ACL adalah sebagai berikut :



Gambar 2. Rancangan Topologi Jaringan

No	Lokasi	IP Address
1	LAN A	192.168.10.128/25
2	LAN B	192.168.15.0/25
3	LAN Data Center	172.16.20.0/26
4	WAN A_DC	10.10.10.0/30
5	WAN B_DC	10.10.10.4/30

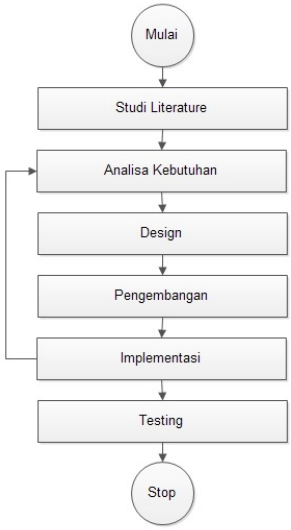
Tabel 1. Alokasi IP Address

Skenario Pengujian Keamanan :

1. LAN A tidak diperbolehkan mengakses Web Server tapi dapat mengakses FTP Server
2. LAN B tidak diperbolehkan mengakses FTP Server tapi dapat mengakses Web Server
3. Data Center dapat mengakses LAN A dan LAN B

ISSN: 2503-054X
Vol. 8 No: 2, Oktober 2023

A. Diagram Kerja Penelitian



Gambar 3. Alur Kerja

Alur kerja ini dibuat untuk mempermudahkan dalam merancang dan mengimplementasikan penelitian ini.

B. Studi Literatur

Dalam merancang jaringan ini metode yang dilakukan berupa pengumpulan data yang terkait dengan keamanan jaringan. Pengumpulan data dilakukan dengan cara mencari materi rujukan terkait dengan keamanan jaringan menggunakan ACL yang terdapat pada router cisco dan beberapa referensi lainya baik dari berbagai buku, jurnal, internet dan pengalaman penulis sendiri.

C. Analisa Kebutuhan

1. Lokasi Penelitian
   Lokasi penelitian dilakukan di Laboratorium di kampus STMIK Horizon Karawang.
2. Aturan keamanan Jaringan
   Langkah awal sebelum membangun keamanan ini adalah dengan membuat aturan - aturan atau policy keamanan terlebih dahulu sesuai dengan kebutuhan yang diinginkan oleh pihak kampus. Adapun garis besar policy/aturan yang dibutuhkan adalah sebagai berikut :
   a. Jaringan pada LAN A tidak diperbolehkan mengakses Web Server yang terdapat pada Data Center tetapi dapat mengakses FTP Server.
   b. Jaringan pada LAN B tidak diperbolehkan mengakses FTP Server tapi dapat mengakses Web Server.
   c. Data Center dapat diakses oleh LAN A dan LAN B

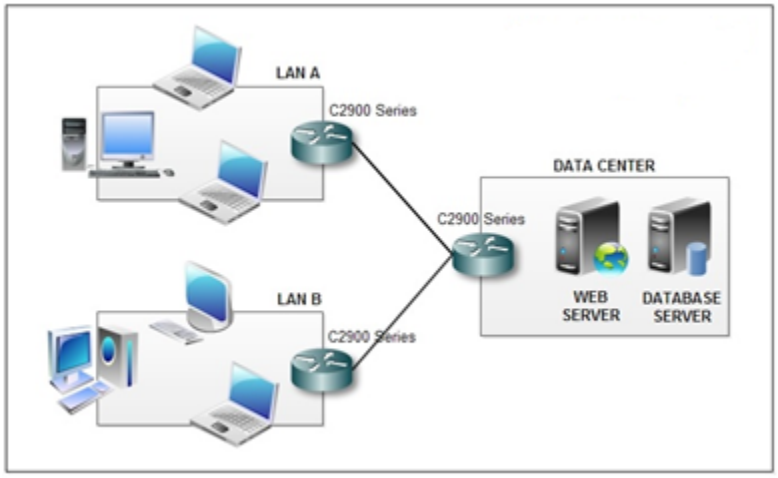
D. Survey Lokasi

Survey lokasi dibutuhkan guna menentukan dimana perangkat-perangkat tersebut akan diletakan, kesiapan dari media tranmisi yang akan digunakan serta infrastuktur lain yang dibutuhkan. Hal tersebut dilakukan guna memperoleh gambaran dan mengidentifikasi setiap kemungkinan yang mungkin terjadi pada saat implementasi seperti kebutuhan dan kendala yang ditemukan.

E. Design

Adapun rancangan design topologinya adalah sebagai berikut :

ISSN: 2503-054X
Vol. 8 No: 2, Oktober 2023



Gambar 4. Rancangan Design Jaringan

Langkah berikutnya adalah membangun jaringan berdasarkan design yang sudah dibuat menggunakan Cisco Packet Tracer (CPT) seperti rancangan design pada gambar 2. Simulasi dengan CPT dilakukan untuk memastikan bahwa konfigurasi yang dibuat berjalan dengan baik sebelum konfigurasi tersebut diimplementasikan pada perangkat sesungguhnya.

IV. HASIL DAN PEMBAHASAN

A. Implementasi

Dalam mengimplementasikan ACL ini , konfigurasi cukup dilakukan hanya di salah satu sisi saja tidak perlu seluruh router dikonfigurasi dalam kasus ini ACL dipasang pada router yang terdapat pada sisi Data Center. Berdasarkan design topologi yang terdapat pada gambar 3 dan alokasi IP address yang terdapat pada table 1, maka konfigurasi router pada sisi Data Center adalah sebagai berikut :

```
!
interface GigabitEthernet0/0
 description R_DC to R_LAN A
 ip address 10.10.10.1 255.255.255.252
 ip access-group 100 in
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 description R_DC to R_LAN B
 ip address 10.10.10.5 255.255.255.252
 ip access-group 110 in
 duplex auto
 speed auto
!
!
access-list 100 deny tcp 192.168.10.128 0.0.0.127 host 172.16.20.2 eq www
access-list 100 permit ip any any
access-list 110 deny tcp 192.168.15.0 0.0.0.127 host 172.16.20.2 eq ftp
access-list 110 permit ip any any
!
```

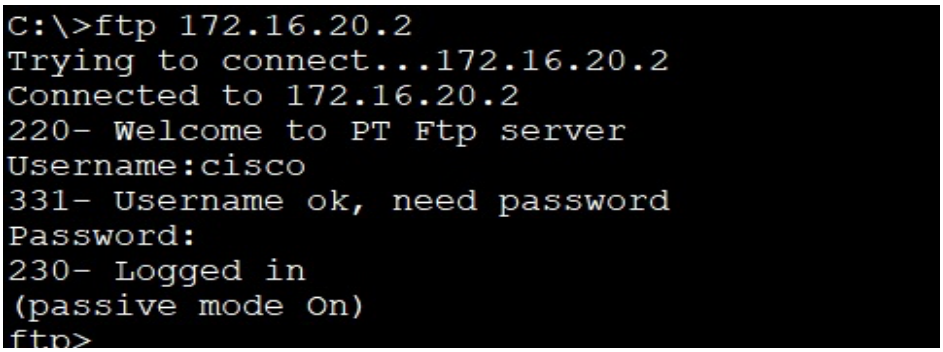
ISSN: 2503-054X
Vol. 8 No: 2, Oktober 2023

B. *Testing*

Hasil test browsing dan ftp yang dilakukan, diperoleh hasil :

1. Test browsing dan ftp dilakukan dari jaringan LAN A dengan mengakses service http dan ftp server yang terdapat pada jaringan Data Center dengan IP 172.16.20.2. Dari hasil pengetesan yang dilakukan didapat hasil sebagai berikut :

Gambar 5. Hasil Test Web Server



Gambar 6. Hasil Test FTP Server

2. Test browsing dan ftp dilakukan dari jaringan LAN B dengan mengakses service http dan ftp server yang terdapat pada jaringan Data Center dengan IP 172.16.20.2. Dari hasil pengetesan yang dilakukan didapat hasil sebagai berikut :

Gambar 7. Hasil Test Web Server

Gambar 8. Hasil Test FTP Server

ISSN: 2503-054X
Vol. 8 No: 2, Oktober 2023

V. KESIMPULAN dan SARAN

A. Kesimpulan

Berdasarkan hasil pengetesan koneksi yang telah dilakukan pada saat testing , maka didapat kesimpulan :

1. Jaringan LAN A tidak dapat mengakses service Web Server pada Data Center dengan IP Server 172.16.20.2 tetapi dapat mengakses FTP Server
2. Jaringan LAN B dapat mengakses service Web Server dan tidak dapat mengakses Service FTP Server

B. Saran

Keamanan jaringan tidak hanya dapat dilakukan dengan menggunakan perangkat software dan hardware tapi juga dapat dilakukan dengan memanfaatkan fitur-fitur yang terdapat di router seperti Acess Control List. Service-service yang dilindungi/diproteksi tidak hanya terbatas pada kedua service (FTP/WEB) diatas tapi juga dapat dikembangkan pada service-service lain.

VI. DAFTAR PUSTAKA

[1] Wicaksono Irawan, Aditya., Yusufianto, Aan., & Agustina, Dwi (2019-2020, Q2)., Laporan Survei Internet APJII. (pp.3)
[2] Id-SIRTII/CC (2021), ‘Laporan Tahunan Monitoring Keamanan Siber (pp. 16-17). BSSN.
[3] Conteh, N. Y. (2021). The dynamics of social engineering and cybercrime in the digital age. In Ethical Hacking Techniques and Countermeasures for Cybercrime Prevention (pp. 144–149). IGI Global.
[4] Palmieri, M., Shortland, N., & McGarry, P. (2021). Personality and online deviance: The role of reinforcement sensitivity theory in cybercrime. Computers in Human Behavior, 120, 106745.
[5] 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.
[6] Lutkevich, Ben (2022)., Access Control List., Available https://www.techtarget.com/searchnetworking/definition/access-control-list ACL#:~:text=An access control list (ACL) is a list of rules,traffic can access the network. (diakses 31 Maret 2022)
[7] Cisco Press (2013)., Network Security Concepts and Policies, Available at : https://www.ciscopress.com/articles/article.asp?p=1998559&seqNum=4#:~:text=The lifecycle approach looks at,methodology in securing our networks. (Diakses 1 April 2022)
[8] Cisco Certified Expert (2022)., Network Design Methodology., Available at : https://www.ccexpert.us/network-design/network-design-methodology.html (diakses : 1 April 2022)
[9] Wahyudi, Ananta Dewi Tania (2022)., ‘Implementasi IPv6 Menggunakan Routing Information Protocol (Studi Kasus: STMIK Horizon Karawang)., http://ejournal.urindo.ac.id/index.php/TI/article/view/1445 ., Jurnal Teknologi Informatika URINDO Vol 8, No.1 (2022)