Perancangan Manajemen Jaringan Menggunakan Metode *Network Access Control* di DISKOMINFO Kabupaten Nagekeo

Sesarius Benyamin Meo[1]
[1]Teknologi informasi, STMIK PPKIA Pradnya Paramita, Malang, Indonesia
Korespodensi author: sherymeo08@gmail.com

Info Artikel

Diajukan: 17 September 2020
Diterima: 08 Oktober 2020
Diterbitkan: 15 Oktober 2020

Keywords:
Network Management Design; Network Access Control Method; DISKOMINFO Nagekeo Regency

Kata Kunci:
Perancangan Manajemen Jaringan; Metode Network Access Control; DISKOMINFO Kabupaten Nagekeo

Abstract

The Nagekeo Regency Communication and Information Service Office (DISKOMINFO) which is located in the Civic Center Complex, Lape Village, Aesesa District is an agency responsible for processing information within the government environment. DISKOMINFO Nagekeo Regency has 7 divisions with their respective duties and functions consisting of Head of Service, Secretariat, Technology and Information Sector, Public Information Processing Sector, Public Communication Processing Sector, Government Services Sector, and Functional Positions. Of the seven fields, DISKOMINFO Nagekeo Regency has 19 employees. One of the tasks of DISKOMINFO Nagekeo Regency is to develop Information and Computer Technology (ICT) infrastructure through application development, public service content, and the use of ICT networks to improve public services. Judging from DISKOMINFO's duties, such as carrying out government affairs and supporting tasks in the fields of communications and informatics, the coding field, and the fields of statistics, of course it has managed data, such as software ordering data, regional apparatus organization data, fax document sender data, operator data, and network installation. , with the duties and functions of DISKOMINFO for the regions, there is a huge risk in access rights for irresponsible people. The aim of this research is to build an internet network and limit network access rights at the DISKOMINFO Office in Nagekeo Regency using the access control method. The results and conclusions of this research can help design networks and their security so that the computer network at DISKOMINFO Nagekeo Regency cannot be accessed by users who do not have permission.

Abstrak

Kantor Dinas Komunikasi dan Informatika (DISKOMINFO) Kabupaten Nagekeo yang terletak di Komplek Civic Center, Kelurahan Lape, Kecamatan Aesesa merupakan suatu instansi yang bertanggung jawab atas pengolahan informasi dalam lingkungan pemerintahan. DISKOMINFO Kabupaten Nagekeo memiliki 7 bidang dengan tugas dan fungsinya masing-masing yang terdiri dari Kepala Dinas, Sekretariat, Bidang Teknologi dan Informasi, Bidang Pengolahan Informasi Publik, Bidang Pengolahan Komunikasi Publik, Bidang Layanan Goverment, dan Jabatan Fungsional. Dari ke tujuh bidang tersebut di DISKOMINFO Kabupaten Nagekeo memiliki jumlah karyawan 19 orang. Salah satu tugas DISKOMINFO Kabupaten Nagekeo adalah mengembangkan infrastruktur Teknologi Inormatika dan Komputer (TIK) melalui pengembangan aplikasi, muatan layanan umum, serta pemanfaatan jaringan TIK untuk peningkatan pelayanan publik. Dilihat dari tugas DISKOMINFO seperti melaksanakan urusan pemerintahan dan tugas pembantuan bidang komunikasi dan informatika, bidang persandian, dan bidang statistik, tentunya mempunyai data yang dikelola, seperti data pemesanan software, data organisasi perangkat daerah, data pengirim dokumen faksimili, data operator, dan pemasangan jaringan, dengan tugas dan fungsi dari DISKOMINFO untuk daerah maka sangat resiko dalam hak akses bagi orang yang tidak bertanggung jawab. Tujuan dalam penelitian ini adalah untuk membangun jaringan internet dan pembatasan hak akses Jaringan pada Kantor DISKOMINFO di Kabupaten Nagekeo mengunakan metode access control. Hasil dan kesimpulan penilitian ini adalah dapat membantu merancang jaringan dan keamanannya sehingga jaringan komputer pada DISKOMINFO Kab.Nagekeo tidak dapat di akses oleh pengguna yang tidak memiliki hak akses.

Cara mensitasi artikel:
S. B. Meo, "Perancangan Manajemen Jaringan Menggunakan Metode Network Access Control di DISKOMINFO Kabupaten Nagekeo," *Jurnal Teknologi Informasi: Teori, Konsep, dan Implementasi (JTI-TKI)*, vol. 11, no. 2, pp. 74–78, October 2020, doi: 10. 36382/jti-tki.v11i2.500

PENDAHULUAN

Saat ini jaringan internet semakin meningkat kegunaannya dikalangan masyarakat. Mulai dari kalangan sekolah, kantor, perusahaan maupun masyarakat biasa sudah menggunakan sistem jaringan komputer. Tujuannya agar *user* dapat saling berkomunikasi antara satu dengan yang lainnya. Hal ini memicu orang-orang yang tidak

bertanggungjawab untuk melakukan hal-hal yang dapat mengganggu sistem keamanan komunikasi data dalam sebuah jaringan. Misalnya saja mencuri informasi, atau sekedar iseng-iseng saja [1]

Sistem keamanan jaringan komputer saat ini menjadi hal penting untuk diterapkan. Banyak organisasi yang telah menjadikan teknologi informasi sebagai bahagian penting dalam menunjang aktifitasnya. Akses pengguna yang tidak dibatasi menjadi ancaman bagi sebuah organisasi, karena banyak data dan informasi penting yang tersebar dalam perangkat jaringan komputer di organisasi tersebut dapat disusupi oleh pihak yang tidak berwenang. Salah satu usaha yang dapat dilakukan adalah dengan menerapkan *extended access list* yang merupakan salah satu bagian dari metode *access control list*. *Extended access list* dapat menyaring lalu lintas data suatu jaringan dengan mengontrol apakah paket-paket tersebut dilewatkan atau dihentikan. *Extended access list* juga dapat menjamin keamanan untuk setiap komputer sehingga jalur komunikasi serta hak akses setiap komputer dapat berjalan dengan baik. *Extended access list* memungkinkan penyaringan berdasarkan sumber atau alamat tujuan, protokol yang dipilih, port yang digunakan, dan apakah koneksi sudah ditetapkan agar dapat melakukan filter terhadap paket data yang melewati jaringan [2].

Kantor Dinas Komunikasi dan Informatika (DISKOMINFO) Kabupaten Nagekeo yang terletak di Komplek Civic Center, Kelurahan Lape, Kecamatan Aesesa merupakan suatu instansi yang bertanggung jawab atas pengolahan informasi dalam lingkungan pemerintahan. Dinas ini memiliki 7 bidang dengan tugas dan fungsinya masing-masing yang terdiri dari Kepala Dinas, Sekretariat, Bidang Teknologi dan Informasi, Bidang Pengolahan Informasi Publik, Bidang Pengolahan Komunikasi Publik, Bidang Layanan Goverment, dan Jabatan Fungsional. Dari ke tujuh bidang tersebut memiliki jumlah karyawan 19 orang. Salah satu tugasnya adalah mengembangkan infrastruktur Teknologi Inormatika dan Komputer (TIK) melalui pengembangan aplikasi, muatan layanan umum, serta pemanfaatan jaringan TIK untuk peningkatan pelayanan publik. Berdasarkan tugas seperti melaksanakan urusan pemerintahan dan pembantuan bidang komunikasi dan informatika, bidang persandian, dan bidang statistik, tentunya mempunyai data yang dikelola, seperti data pemesanan software, data organisasi perangkat daerah, data pengirim dokumen faksimili, data operator, dan pemasangan jaringan. Dalam melakukan pertukaran maupun pengolahan data sangat memerlukan jaringan internet dengan keamanannya yang bertujuan agar setiap data yang dikelolah secara internal tidak dapat di akses oleh orang lain. Dalam hal ini agar setiap pertukaran data dan pengolahannya dapat terjaga maka jaringan internet perlu adanya sebuah keamanan yang berguna agar dapat melindungi setiap data yang dikelolah secara internal dapat terjaga sehingga tidak dapat di akses oleh pihak luar.

Beberapa penelitin sebelumnya yang telah membahas keamanan jaringan komputer telah dilakukan oleh: [3], dalam penelitian yang berjudul "Analisis dan Design Keamanan Jaringan Komputer Dengan Metode Network Develoment Life Cicle (Studi Kasus Universitas Telkom)". Keamanan jaringan komputer merupakan hal yang tidak terpisahkan dalam jaringan komputer. Keamanan jaringan komputer yang tidak dirancang dengan baik dapat menyebabkan kebocoran data, pelanggaran privasi, hingga kerugian finansial. Oleh karena itu, dibutuhkan rancangan keamanan jaringan komputer yang dapat memenuhi kebutuhan dari pengguna layanan jaringan komputer. Penelitian ini bertujuan untuk mendesain keamanan jaringan komputer dengan obyek penelitian adalah Universitas Telkom dengan menggunakan Network Develoment Life Cicle (NDLC). Hasil penelitian yang diperoleh berdasarkan metode yang digunakan, simulasi dibutuhkan dalam pengujuain untuk memastikan bahwa desain usulan dapat memenuhi keutuan pengguna. Jika hasil simulasi mampu untuk memenuhi keutuhan dari pengguna, maka rancangan ususlan keamanan data center dapat dikatakan berhasil.

Simanjuntak, Cosmas, dan Jamilah, (2017:122)[4], dalam penelitian yang berjudul "Analisis Penggunaan Access Control Dalam Jaringan Komputer Di Kawasan BatamIndo Industrial Park (BATAMINDO Industrial Park Batam)". Router menyediakan kemampuan untuk menyaring traffic, seperti memblokir traffic Internet, dengan Access Control. Access Control adalah suatu rentetan list dari suatu statemen perijinan atau penolakan yang di aplikasikan kepada alamat-alamat jaringan atau layer protokol paling atas. Tujuan dari penelitian ini yaitu untuk mengetahui pengaruh access control dalam jaringan di Kawasan Batamindo Industrial Park Batam. Metode yang digunakan dalam penelitian ini adalah metode deskriptif. Sampel yang digunakan sebanyak 101 karyawan IT di Batamindo Industrial Park Batam. Dan di peroleh rumusan masalah dari penelitian ini yaitu untuk menentukan bagaimana manfaat penggunaan *access control*. Hasil penelitian yang diperoleh adalah *access control list* dipersepsikan bermanfaat, Maka dengan penelitian ini penulis dan Karyawan IT di Perusahaan dapat mengetahui bahwa penggunaan access control sangat penting dalam jaringan komputer di Kawasan BATAMINDO Industrial Park Batam.

Peneliti [2], yang berjudul "Extended Access List untuk Mengendalikan Trafik Jaringan" Access control. Keamana jaringan komputer saat ini menjadi hal penting untuk diterapkan. Banyak organisasi yang telah menjadikan teknologi informasi sebagai bagian penting dalam menunjang aktivitasnya. Akses pengguna yang tidak dibatasi menjadi ancaman bagi sebuah organisasi, karena banyak data dan informasi penting yang tersebar dalam perangkat jaringan komputer di organisasi tersebut dapat disusupi oleh pihak yang tidak berwenang. Salah satu usaha yang dapat dilakukan adalah dengan menerapkan extended access list yang merupakan salah satu bagian dari metode *access control list*. Extended access list dapat menyaring lalu lintas data suatu jaringan dengan mengontrol apakah paket-paket tersebut dilewatkan atau dihentikan. Extended access list juga dapat menjamin keamanan untuk setiap komputer sehingga jalur komunikasi serta hak akses setiap

komputer dapat berjalan dengan baik. Extended access list memungkinkan penyaringan berdasarkan sumber atau alamat tujuan, protokol yang dipilih, port yang digunakan, dan apakah koneksi sudah ditetapkan. Tulisan ini membahas penerapan extended access list dalam jaringan supaya dapat melakukan filter terhadap paket data yang melewati jaringan. Penerapannya menggunakan software Packet Tracer 6.1.1 untuk membuat prototipe jaringan dan mensimulasikannya. Sehingga nanti dapat diterapkan pada jaringan yang sebenarnya. List yang dibangun pada penelitian ini diterapkan untuk protokol antara lain: TCP (WWW, FTP, Telnet, SMTP, POP3), UDP (DNS), dan ICMP (Ping). Hasilnya didapatkan extended access list yang dikonfigurasi pada router dalam topologi penelitian ini mampu melakukan filter terhadap paket yang melewati jaringan. Hasil konfigurasinya sangat spesifik, sehingga penerapan hak akses permit dan deny dapat dilakukan sesuai dengan aturan dan skenario yang dirancang.

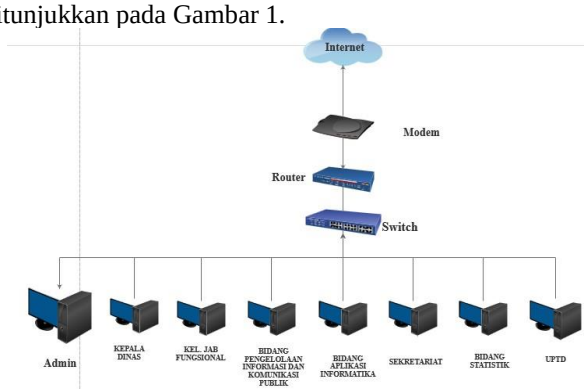
Penelitiam oleh [5], dalam penelitian yang berjudul "Perancangan Dan Analisis Keamanan Jaringan Nirkabel Dari Serangan DDOS (*Distributed Denial Of Service*) Berbasis Honeypot" Masalah keamanan komputer merupakan faktor yang sangat penting untuk diperhatikan dan dikelola dengan baik oleh sistem administrator, banyak sekali cara yang ditempuh untuk menghalangi seseorang/ perusahaan untuk dapat memberikan layanan yang optimal. Namun seringnya jaringan server mengalami gangguan karena diserang yang disebabkan oleh serangan jenis DDoS, gangguan tersebut bisa berupa kegagalan sistem, *halt*, *error request* bahkan kerusakan *hardware server*. Hal inilah yang terjadi di ruang server PDAM Tirta AlBantani. Dengan membuat sistem keamanan jaringan server menjadi aman dari serangan DDoS, sistem memberikan keamanan bagi server agar tidak adanya penyerangan dari DDoS. Sehingga dengan diterapkannya sistem *honeypot*, dengan membuat satu server sebagai korban dengan membangun sistem honeypot komputer server dan keamanan jaringan yang lain akan terlindungi, karena penyerang melihat target seolah-olah itu adalah OS target yang bisa diserang, padahal itu adalah sistem *honeypot* yang sengaja dibuat untuk menampung dan meladeni penyerang. Tentunya dengan sistem ini, dapat meningkatkan keamanan jaringan wireless, dan dapat melindung server dari gangguan serangan jenis apapun termasuk jenis serangan DDoS.

Penelitian oleh [6], dalam penelitian yang berjudul "Pembatasan Akses Jaringan Internet Pada Clearos Menggunakan Metode Access Control List". Permintaan untuk penggunaan internet dirasakan oleh para pekerja. Karenanya sangat dibutuhkan sekali jaringan internet di sebuah perusahaan. Tidak adanya batasan dalam penggunaan koneksi internet dapat mengganggu keamanan jaringan dan penyalahgunaan jaringan, karena dirancang pengaturan akses internet. Salah satu metode yang digunakan adalah *Access Control List metode* yang diterapkan ke *ClearOS Server*. *Metode Access Control List* adalah salah satu teknik permintaan data akses koneksi dan transmisi paket data dari satu komputer ke komputer lainnya. Hasil penelitian ini membuktikan bahwa ClearOS[7]–[11] dengan metode penyaringan berdasarkan Access Control List dapat memfilter identifikasi. Perangkat berdasarkan akun pengguna dan pemilihan permintaan layanan data berdasarkan alamat situs web yang dikunjungi.

Pada artikel ini peneliti menawarkan keamanan jaringan menggunakan metode access control yang merupakan salah satu metode dalam mengamankan jaringan internet yang dapat mengontrol jalur komunikasi jaringan serta dapat mengijinkan atau menolak setiap pengguna yang akan mengakses jaringan.

METODE PENELITIAN

Pada penelitian ini perancangan jaringan tree pada DISKOMINFO Kabupaten Nagekeo Topologi seperti ditunjukkan pada Gambar 1.



Gambar 1. Topologi jaringan

A. *Perancangan*

Perancangan Topologi jaringan pada DISKOMINFO dengan adanya access control sebagai media yang berfungsi untuk menerima atau menolak perangkat yang nantinya berhak atau tidak untuk mengakses jaringan pada DISKOMINFO. Nantinya *Access Contorl*[12] akan di konfigurasikan pada router. Sistem access control ini terdiri dari PC Admin, router dan switch. Obyek perancangan jaringan dan keamanannya dapat dijabarkan sebagai berikut: 1) Modem, modem digunakan sebagai media perantara antar komputer client dengan jaringan internet melalui line kabel untuk mengakses internet, dimana terdapat permintaan sinyal ke operator untuk mengalirkan paket data ke client. 2) Switch, Switch ini akan digunakan sebagai media penghubung antar router dan User yang nantinya terhubung pada jaringan internet yang sudah di konfigurasikan oleh admin pada router. 3) Router, Router berfungsi konfigurasi jaringan internet dan access control untuk mengizinkan atau menolak perangkat yang akan mengakses jaringan pada Kantor DISKOMINFO Kabupaten.

B. *Konfigurasi*

Access Control akan dikonfigurasikan oleh admin pada jaringan yang berada satu *router* karena *access control* [13][14][15]mempunyai fitur yang dapat melakukan hak akses bagi pengguna jaringan internet yang terkoneksi pada mikrotik.

Konfigurasi IP *Address* yang dilakukan yaitu yang pertama menambahkan IP address agar terhubung pada ISP internet dan IP Adrress untuh client. Untuk ISP Internet menggunakan IP 192.168.1.22/24 dengan network 192.168.1.0 dan Untuk client menggunakan IP 10.5.50.1/24 dengan network 10.5.50.0. Dalam proses konfigurasi IP address dilakukan juga Konfigurasi server ini menggunakan Mikrotik agar client dapat terhunbung pada jaringan DISKOMINFO Kabupaten Nagekeo. Media pengujian ini menggunakan Winbox sebagai perantara koneksi jaringan DISKOMIFNO Kabupaten Nagekeo. Konfigurasi DNS, pada konfigurasi ini dilakukan setting pada DNS dengan mengisi pada kolom servers yang pertama dengan IP address dari ISP Indihome dan yang kedua menggunakan IP dari google yaitu 8.8.8.8. Konfigurasi Routes, pada konfigurasi routes dilakukan setting dengan menambahkan routes dengan mengisi IP address ISP Indihome pada kolom gateway. Konfigurasi NAT, Konfigurasi NAT dilakukan setting pada firewall dengan menambahkan pada tab NAT. Konfigurasi DHCP Server, Konfigurasi yang dilakukan setting DHCP server agar perangkat client mendapatkan IP address secara otomatis dari server. Pada konfigurasi ini yaitu menentukan IP address dan gateway. Konfigurasi Hotspot, Pada konfigurasi hotspot admin jaringan akan menentukan interface yang akan digunakan sebagai hotspot untuk client, IP address, IP pool, DNS server, DNS name dan user dan password untuk client.

Mikrotik digunakan untuk konfigurasi Access control, Pengaturan akses mikrotik dilakukan agar mikrotik mendaftarkan mac address client yang nantinya terhubung pada jaringan DISKOMINFO Kaupaten Nagekeo. Dengan menghubungkan mikrotik dengan Access control agar admin dapat menentukan client mana yang dapat terhubung ke jaringan DISKOMINFO.

Admin melakukan konfigurasi hotspot pada mikrotik. Admin daftarkan MAC address client yang akan yang menentukan client yang berhak untuk mengakses jaringan di DISKOMINFO Kabupaten Nagekeo. Apabila ada user yang belum terdaftar MAC address ingin mengakses jaringan maka sistem secara otomatis menolak. User yang sudah terdaftar MAC address pada sistem jaringan maka langsung terkoneksi dan mengakses jaringan.

C. Alat dan Bahan

Alat yang digunakan dalam penelitian ini meliputi perangkat keras (*hardware* jaringan) dan perangkat lunak (*software*). Spesifikasi perangkat keras (*hardware* jaringan) dan perangkat lunak (*software*) yang digunakan seperti tertera pada Tabel 1.

Tabel 1. Hardware jaringan

No	Alat	Spesifikasi
1	RAM	2 GB
2	Processor	Intel Celeron 2.16Ghz
3	Graphics	999 MB
4	HDD	500 GB

Sementara itu perangkat lunak yang digunakan untuk melakukan pengujian tertera pada Tabel 2.

Tabel 2 Alat Penelitian / Software

No	*Software*	
1	Sistem Operasi	Micorsoft Windows 8 Mikrotik 6.39.2 (stable)
2	Aplikasi	Winbox 313

D. Pengukuran Statis

Pengukuran yang dilakukan dalam penelitian ini menggunakan simulasi untuk mengukur waktu setelah adanya jaringan internet dan sebelum adanya jaringan internet. Dengan meggunakan jaringan internet ini, *user* yang berada di Kantor DISKOMINFO Kabupaten Nagekeo dapat lebih cepat dalam melakukan pertukaran data. Pengukuran waktu ini digunakan mendeteksi waktu dalam melakukan pertukaran data dari sesudah dan sebelum adanya jaringan internet seperti tertera pada Tabel 3..

Tabel 3 Tabel pengukuran statis

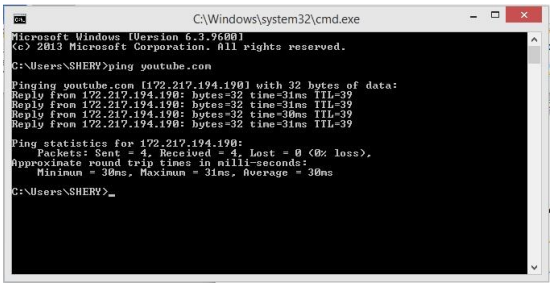
No	Pengukuran	Keterangan
1	Data pendokumentasian data statistik dari seluruh bidang pembangunan Kabupaten	Download/Upload (Mbps)
2	Jaringan	Ping (ms)
3	Efektifitas	Menit

HASIL DAN PEMBAHASAN

Pada tahap ini dilakukan pengujian terhadap sistem yang telah dikonfigurasi untuk mengetahui hasil yang diharapkan. Pengujian yang akan dilakukan yaitu menggunakan satu komputer sebagai *client*. Pengujian ini dilakukan mulai dari uji coba pengujian koneksi internet dan *Access Control.*

A. Pengujian Koneksi Internet

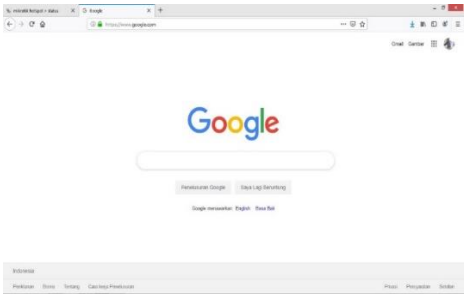
Pertama pengujian dilakukan ping dari *client* terhadap domain www.youtube.com melalui *command promp*, jika hasilnya "*Replay*" maka komputer *client* sudah terhubung dengan Internet, seperti pada Gambar 2.



Gambar 2. Ping *Client* ke youtube.com

Kedua dilakukan pengujian menggunakan *browser* firefox dengan mengetikkan skripsishery.net, jika hasilnya langsung tampil halaman skripsishery.net/ login, untuk mengisi *user* dan *password* menggunakan *mac address* yang sudah di daftarkan. Setelah melakukan *login* maka *client* sudah terhubung ke jaringan internet. Setelah *login* berhasil *client* mengetikkan www.google.com, jika

hasilnya langsung tampil halaman www.google.com maka komputer *client* sudah terhubung dengan Internet seperti ditunjukkan pada Gambar 3.



Gambar 3. *Client Browsing*

B. Pengukuran Kecepatan Internet

Pengukuran terakhir adalah pengukuran keccepatan internet. Pengukuran kecepatan internet menggunakan situs www.speedtest.net. Cara pengukuran kecepatan internet adalah membuka alamat website www.speedtest.net dari komputer *client*, kemudian meenekan tombol "Go", maka komputer *client* akan mengirim *ping test* ke *server* jaringan lalu mengukur kecepatan *download* dan *upload* data, sperti Gambar 4.

Gambar 4. Pengukuran Kecepatan Internet

Gambar 4 menunjukkan hasil test kecepatan internet di kantor, dimana kecepatan download 10,69 Mbps (Mega bit per second) dan kecepatan upload 2,02 Mbps. Data hasil pegujian kecepatan internet sebagaimana terlihat pada Tebel 4

Tabel 4 Pengujian Jaringan Internet

No	Pengukuran	Keterangan
1	Data pendokumentasian data statistik dari seluruh bidang pembangunan Kabupaten	Download (10,69 Mbps) Upload (2,02 Mbps)
2	Jaringan	Ping (5ms)
3	Efektifitas	Sebelum (10-20 Menit) Sesudah (1-2 Menit)

KESIMPULAN

Berdasarkan penelitian yang telah dilakukan maka dapat diambil kesimpulan yaitu penelitian ini dapat membantu terbentuknya suatu jaringan internet serta adanya keamanan jaringann internet sehingga jaringan komputer pada DISKOMINFO Kab.Nagekeo tidak dapat di akses oleh pengguna yang tidak memiliki hak akses.

REFERENSI

[1] Simamora.. Metode *Access Control List* sebagai Solusi Alternatif Seleksi Permintaan Layanan Data pada Koneksi *Internt, Jurnal Teknologi Informasi Politeknik Telkom Vol. 1, No. 1*., 2011

[2] Hari Antoni Musril. Extended Access List untuk Mengendalikan Trafik Jaringan, *Jurnal Edukasi dan Penelitian Informatika (JEPIN) Vol. 2, No. 2*. 2016., ISSN 2460-0741.

[3] Mochamad dan Ramadhan.. Analisis dan Design Keamanan Jaringan Komputer di Universitas Telkom Dengan Metode *Network Develoment Life Cicle*. *Jurnal Rekayasa System & Industri -* Vol 2 No 01, 2017

[4] Simanjuntak. dkk. Analisis Penggunaan *Access Control List* (ACL) Dalam Jaringan Komputer Di Kawasan BATAMINDO Industrial Park Batam, *Jurnal ISD Vol.2 No.2*. 2017 eISSN: 2528—

[5] [Sutarti and Khairunnisa, "Perancangan Dan Analisis Keamanan Jaringan Nirkabel Dari Serangan Ddos (Distributed Denial of Service) Berbasis Honeypot," J. PROSISKO, vol. 4, no. 2, p. 8, 2017.

[6] [6] Chaidir dan Wirawan.. Pembatasan Akses Jaringan Internet Pada Clearos Menggunakan Metode Access Control List, Jurnal Teknik Komputer Vol 4, No. 1, 2018, e-ISSN: 2550-0120[7]

[7] A. Gunawan, R. Rahmah, and A. Iskandar, "Rancang Bangun Jaringan Hotspot Menggunakan LINUX ClearOS Dengan Konsep Security Gateway," *JTIM J. Teknol. Inf. dan Multimed.*, vol. 4, no. 4, pp. 272–280, 2023, doi: 10.35746/jtim.v4i4.251.

[8] E. Varianto and M. Badrul, "Implementasi Virtual Private Network Dan Proxy Server Menggunakan Clear Os Pada Pt.Valdo International," *J. Tek. Komput. Amik Bsi*, vol. 1, no. 1, pp. 54–65, 2015.

[9] M. D. S. Lubis and A. Allwine, "Mengatur Akses Internet dan Management Bandwidth Menggunakan Server ClearOs Enterprise v. 5.2: Mengatur Akses Internet dan Management Bandwidth …," *J. Armada …*, no. November 2018, pp. 0–12, 2017.

[10] H. Octavia, "UNJUK KERJA PENERAPAN TEKNOLOGI VoIP PADA JARINGAN VPN (VIRTUAL PRIVATE NETWORK)," *Elektron J. Ilm.*, vol. 5, no. 2, pp. 1–12, 2018, doi: 10.30630/eji.5.2.49.

[11] S. Suhartono and A. R. Patta, "Sistem Pengamanan Jaringan Admin Server Dengan Metode Intrusion Detection System (Ids) Snort Menggunakan Sistem Operasi Clearos," *J. Teknol. Elekterika*, vol. 14, no. 2, p. 145, 2017, doi: 10.31963/elekterika.v14i2.1220.

[12] K. Kredo and P. Mohapatra, "Medium access control in wireless sensor networks," *Comput. Networks*, vol. 51, no. 4, pp. 961–994, 2007, doi: 10.1016/j.comnet.2006.06.012.

[13] W. Wahyudi, "Membangun Proxy Server Cv Global Max Menggunakan Sistem Operasi Linux Blankon 6.0 Ombilin Sebagai Manajemen Akses Jaringan," *Edik Inform.*, vol. 1, no. 1, pp. 63–71, 2017, doi: 10.22202/ei.2014.v1i1.1441.

[14] R. Tourani, S. Misra, T. Mick, and G. Panwar, "Security, Privacy, and Access Control in Information-Centric Networking: A Survey," *IEEE Commun. Surv. Tutorials*, vol. 20, no. 1, pp. 556–600, 2018, doi: 10.1109/COMST.2017.2749508.

[15] B. Carminati, E. Ferrari, R. Heatherly, M. Kantarcioglu, and B. Thurainsingham, "A semantic web based framework for social network access control," *Proc. ACM Symp. Access Control Model. Technol. SACMAT*, pp. 177–186, 2009, doi: 10.1145/1542207.1542237.