DEVELOPMENT MANAGEMET NETWORK SECURITY PADA PTPN 7 BETUNG

Rica Fuji setiawati[1], Novri Hadinata[2]
Fakultas Ilmu Komputer, Universitas Bina Darma
ricafujisetiawati@gmail.com[1], novri_hadinata@binadarma.ac.id[2]

ABSTRAK

Keamanan jaringan adalah hal yang sangat penting seiring berkembangnya teknologi informasi. Salah satunya adalah PT Perkebunan Nusantara VII Betung yang biasa di sebut dengan PTPN 7 Betung yang merupakan perusahaan yang bergerak pada bidang Minyak Kelapa Sawit. Perusahaan ini telah menerapkan teknologi jaringan komputer namun teknologi jaringan komputer yang sudah ada pada PTPN 7 Betung masih belum maksimal dikarenakan belum adanya pembatasan akses dan filter paket pada masing-masing divisi kerja. Untuk menjaga kerahasiaan informasi dan data yang dimiliki perusahaan tersebut diperlukan sebuah sistem keamanan jaringan komputer. Salah satu sistem keamanan jaringan yang dapat digunakan adalah *access list*. Pada jaringan komputer PTPN 7 Betung terdapat sebuah *Router Cisco* yang tehubung dengan jaringan *internet* kantor pusat. *Router cisco* ini dapat dimanfaatkan fitur *access list* yang dimilikinya untuk meningkatkan keamanan jaringan. *Access list* dapat digunakan untuk menentukan pihak-pihak mana saja yang boleh dan pihak mana saja yang tidak boleh mengakses informasi atau perangkat jaringan yang ada pada jaringan komputer tersebut sehingga keamanan jaringan dapat ditingkatkan.

Kata Kunci : *access list*, keamanan jaringan, PTPN 7 betung.

ABSTRACT

Network security is very important as the development of information technology. One of them is PT Perkebunan Nusantara VII Betung which is commonly referred to as PTPN 7 Betung which is a company engaged in the field of Palm Oil. The company has implemented computer network technology but the existing computer network technology at PTPN 7 Betung is still not optimal due to the lack of access restrictions and packet filters in each work division. To maintain the confidentiality of information and data owned by the company, a computer network security system is needed. One of the network security systems that can be used is the access list. On the PTPN 7 Betung computer network, there is a Cisco Router that is connected to the head office internet network. This cisco router can use its access list feature to improve network security. Access list can be used to determine which parties are allowed and which parties may not access information or network devices that are in the computer network so that network security can be improved.

Keyword: access list, network security, PTPN 7 betung

1. PENDAHULUAN

Keamanan jaringan adalah hal yang sangat penting seiring berkembangnya teknologi informasi. Salah satunya adalah PT Perkebunan Nusantara VII Betung biasa di sebut dengan PTPN 7 Betung merupakan perusahaan yang bergerak pada bidang Minyak Kelapa Sawit. PTPN 7 Betung dibentuk berdasarkan Peraturan Pemerintah Nomor 12 tahun 1996 tanggal 14 Februari 1996 .

Perusahaan ini telah menerapkan teknologi jaringan komputer namun teknologi jaringan komputer yang sudah ada pada PTPN 7 Betung masih belum maksimal dikarenakan belum adanya pembatasan akses dan filter paket pada masing-masing divisi kerja. Untuk memperbaiki dan meningkatkan kualitas jaringan komputer yang ada pada PTPN 7 Betung maka diperlukan *Development Management Network Security* pada perusahaan. Sehingga dapat membatasi akses data seperti mengakses server data, memblock filter virus, dan hanya dapat bekerja pada ruang lingkup yang di batasi sehingga pihak luar tidak dapat mengaksesnya.

Access Control List (ACL) merupakan sebuah metode yang digunakan untuk menyeleksi paket-paket yang keluar masuk network (Muzakir & Ulfa, 2019).

2. METODOLOGI PENELITIAN

2.1 Metode Penelitian

Network Development Life Cycle (NDLC) merupakan suatu metode yang diinginkan dalam mengembangkan atau merancang jaringan infrastruktur yang memungkinkan terjadinya pemantauan jaringan untuk mengetahui statistik dan kinerja jaringan .

1. *Analysis*

Langkah pertama yang di lakukan ialah analisis awal, analisis jaringan, analisis jaringan fisik awal, dan analisis topologi jaringan.

2. *Design*

Pasa tahap design ini penulismembuat gambar design topologi jaringan, pada topologi jaringan ini akan memberikan gambaran seutuhnya dari kebutuhan yang ada

3. *Simulation Prototype*

Pada *simulation prototype* akan membuat bentuk simulasi menggunakan tools *packet tracer* untuk melihat kinerjar awal dalam sebuah jaringan dan sebagai bahan presentasi

4. *Implementation*

Implementasi adalah tahapan yang sangat penting untuk menentukan berhasil atau tidaknya suatu *project*.

5. *Monitoring*

Untuk memonitoring jaringan komputer berjalan sesuai keinginan dan tujuan awal.

6. *Management*

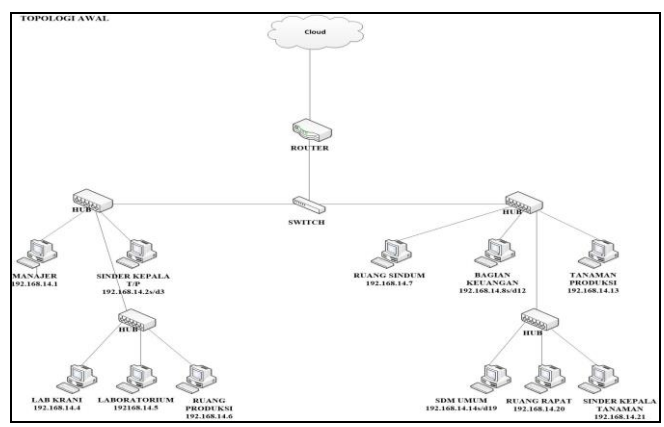
Manajemen dibuat untuk mengatur agar sistem yang telah dibangun dapat berjalan dengan baik atau tidak.

2.3. Rancangan Pengembangan

1. Analisis Awal

a. Analisis Jaringan

Gambar di bawah ini merupakan gambar topologi awal pada PTPN 7 Betung.



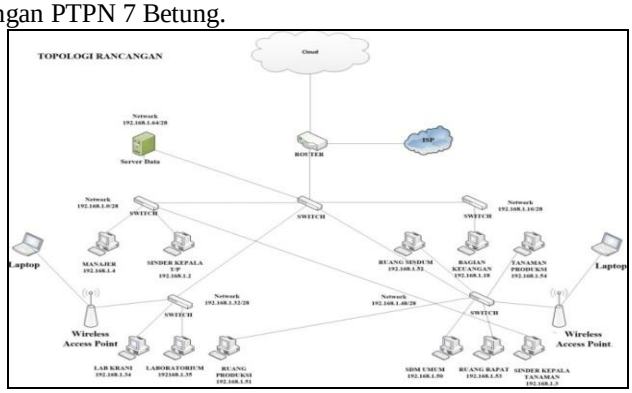
Gambar 1. Topologi Jaringan Baru

Jaringan pada PTPN 7 Betung menggunakan topologi jaringan bertingkat dimana setiap *switch* akan terhubung langsung dengan *hub* dan juga terhubung dengan user lainnya untuk mencapai keseluruh bagian divisi kerja PTPN 7 Betung.

Konektifitas jaringan pada PTPN 7 Betung Juga sering terputus ini dikarenakan topologi jaringan yang digunakan tidak dengan melakukan pemusatan jaringan di satu titik terlihat pada gambar topologi di atas dimana konektifitas pada ruangan lain terhubung secara seri dari jaringan ruangan yang lain.

1. Desain Topologi Jaringan

Desain topologi jaringan baru dilakukan sebagai upaya pengembangan jaringan komputer PTPN 7 Betung. Berikut adalah topologi baru yang dibuat oleh penulis sebagai usulan pengembangan jaringan PTPN 7 Betung.



Gambar 2. Topologi Jaringan Baru

a. Desain IP *Address*

Untuk desain IP *Address* baru pada jaringan komputer PTPN 7 Betung penulis menggunakan metode pembagian segmen CIDR (*Classless Inter-Domain Routing*) disesuaikan dengan kebutuhan komputer yang ada, tabel IP *Address* dapat dilihat tabel di bawah ini :

Tabel 1. Desain Alokasi IP *Address*

No	Nama	Network	Range IP Adrress	Host	Broadcast
1	Manajer, Sinder Kepala T/P, Sinder Kepala Tanaman	192.168.1.0/28	192.168.1.1 – 192.168.1.14	4	192.168.1.15
2	Keuangan	192.168.1.16/28	192.168.14.17– 192.168.14.30	5	192.168.1.31
3	Laboratorium	192.168.1.32/28	192.168.1.33– 192.168.1.46	2	192.168.1.47
4	Ruang Sindum, Ruang Rapat, SDM Umum, Ruang Produksi	192.168.1.48/28	192.168.1.49– 192.168.1.62	9	192.168.1.63
5	Server	192.168.1.64/28	192.168.1.65 – 192.168.1.78	1	192.168.1.79

b. Perancangan Keamanan Jaringan

Perancangan keamanan dilakukan dengan membatasi akses dan aliran data pada masing-masing divisi sesuai dengan kebutuhan dan peraturan yang disesuaikan dengan keinginan PTPN 7 Betung ini agar terjaminnya keamanan aliran data yang ada, rancangan keamanan dapat dilihat tabel dibawah :

Tabel 2. Perancangan Keamanan

No	Nama Divisi	Akses dan Aliran Data yang di izinkan	Akses dan Aliran Data yang tidak di izinkan
1	Manajer, Sinder Kepala T/P, Sinder Kepala Tanaman, Sinder Kepala	1. Melakukan akses *server* data 2. Akses *Internet* 3. Akses *Telnet*	1. Akses ke Divisi lain selain ke Divisi keuangan
2	Laboratorium	1. Melakukan akses *server* data 2. Akses *Internet*	1. Akses *Youtube.com* dan *Facebook.com* *2. Telnet Router* 3. Akses ke Divisi lain
3	Ruang Sindum, Ruang Rapat, SDM Umum, Ruang Produksi,	1. Melakukan akses server data 2. Akses *Internet*	1. Akses Youtube.com dan *Facebook.com* 2. Telnet *Router* 3. Akses ke Divisi
4	Bagian Keuangan	1. Melakukan akses *server* data 2. Akses *Internet*	1. Akses ke Divisi lain selain Manajer 2. Telnet Router 3. Akses *Internet*

c. Perancangan Manajemen Jaringan

Manajemen jaringan dilakukan agar memudahkan operator dalam melakukan pengawasan jaringan, beberapa konfigurasi untuk memudahkan manajemen jaringan adalah pembuatan VLAN (*Virtual Local Area Network*) , konfigurasi DHCP (*Dynamic Host Configuration Protokol*) dan Manjemen *Bandwidth*, berikut merupakan *manajemen* jaringan yang diusulkan oleh penulis :

1. Perancangan VLAN

Perancangan VLAN dibuat berdasarkan jumlah divisi, *server* data dan *Branch Manajer* diamana keseluruhan memiliki 5 bagian yang juga terdiri dari 5 *segment* IP *address* yang sudah di rancang, berikut tabel penamaan dan nomor VLAN yang di rancang oleh penulis.

Tabel 3 VLAN

No	Ruangan	No VLAN
1.	Manajer, Sinder Kepala, Sinder Kepala Tanaman	11
2.	Keuangan	12
3.	Laboratorium	13
4.	Ruang Sindum, Ruang Rapat, SDM Umum, Ruang Produksi	14
5.	Server	15

2. Perancangan DHCP (*Dynamic Host Configuration Protokol*)

Pada desain DHCP, penulis akan merancang pada *router* utama untuk memberikan *default gateway* dari tiap-tiap *vlan* di masing-masing divisi kerja dan melakukan konfigurasi *Dinamic Host Configuration Protocol* (DHCP) yang berfungsi untuk memberikan IP dinamis ke semua PC, Laptop, dan *Smartphone* yang terhubung ke jaringan

3. *Simulation Prototyping*

1. **Konfigurasi VLAN Pada *Switch* Utama**

Pada *Switch* Utama ini merupakan *switch* sentral yang menghubungkan *switch-switch* lain ke *Router Cisco*, maka disini penulis akan mengkonfigurasi VTP *server*, VLAN ID, RSTP, *Trunk Link, Access Lins* dan *Show* VLAN yang sudah di konfigurasi.

```
Switch_Utama#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z
Switch_Utama(config)#hostname Switch_Utama
Switch_Utama(config)#vlan 11
Switch_Utama(config-vlan)#name Manajer
Switch_Utama(config-vlan)#vlan 12
Switch_Utama(config-vlan)#name Keuangan
Switch_Utama(config-vlan)#vlan 13
Switch_Utama(config-vlan)#name Laboratorium
Switch_Utama(config-vlan)#vlan 14
Switch_Utama(config-vlan)#name umum
Switch_Utama(config-vlan)#vlan 15
Switch_Utama(config-vlan)#name Server
```

Gambar 3. Konfigurasi Vlan Pada *Switch* Utama

a. **Konfigurasi *Access List* Pada *Router Cisco***

Pada konfigurasi *Access list* penulis menggunakan *access list standard* dan juga *access list extended* dimana nomor *access list* 11 untuk *interface telnet*, nomor *access list* 10 untuk pembatasan akses ke jaringan manajer, *access list* 12 untuk pembatasan akses ke jaringan bagian keuangan dan *access list* .

1. Konfigurasi *Access List Telnet* Pada *Router Cisco*

Access list telnet ini hanya mengizinkan *user* pada ruangan Manajer untuk mengakses *telnet router* sedangkan ruangan lainnya tidak diizinkan.

```
Router_PTPN7(config)#access-list 11 permit 192.168.1.0
0.0.0.15
Router_PTPN7(config)#access-list 11 deny any
Router_PTPN7(config)#line vty 0 4
Router_PTPN7(config-line)#access-class 11 in
Router_PTPN7(config)#
```

Gambar 4. Konfigurasi *Access List Telnet* Pada *Router Cisco*

2. Konfigurasi *Access List* Pada *Subinterface* Jaringan Manajer

Pada perintah *access list* di bawah ini penulis menggunakan *access list standard* 10 ini tidak mengizinkan jaringan ruangan lain untuk berkomunikasi dengan jaringan ruangan manajer kecuali pada jaringan ruangan bagian keuangan dan *server*.

```
Router_PTPN7(config)#access-list 10 permit 192.168.1.16
0.0.0.15
Router_PTPN7(config)#access-list 10 deny 192.168.1.32
0.0.0.15
Router_PTPN7(config)#access-list 10 deny 192.168.1.48
0.0.0.15
Router_PTPN7(config)#access-list 10 permit any
Router_PTPN7(config)#interface GigabitEthernet0/0.11
Router_PTPN7(config-if)#ip access-group 10 out
```

Gambar 5. Konfigurasi *Access List* Pada *Subinterface* Jaringan Manajer

3. Konfigurasi *Access List* Pada *Subinterface* Jaringan Bagian Keuangan

Pada perintah *access list* di bawah ini penulis menggunakan *access list standard* 12 ini tidak mengizinkan jaringan ruangan lain untuk berkomunikasi dengan jaringan ruangan bagian keuangan kecuali pada jaringan ruangan jaringan manajer dan *server*.

```
Router_PTPN7(config)#access-list 12 permit 192.168.1.0
0.0.0.15
Router_PTPN7(config)#access-list 12 deny 192.168.1.32
0.0.0.15
Router_PTPN7(config)#access-list 12 deny 192.168.1.48
0.0.0.15
Router_PTPN7(config)#access-list 12 permit any
Router_PTPN7(config)#interface GigabitEthernet0/0.12
Router_PTPN7(config-if)#ip access-group 12 out
```

Gambar 6. Konfigurasi *Access List* Pada *Subinterface* Jaringan Bagian Keuangan

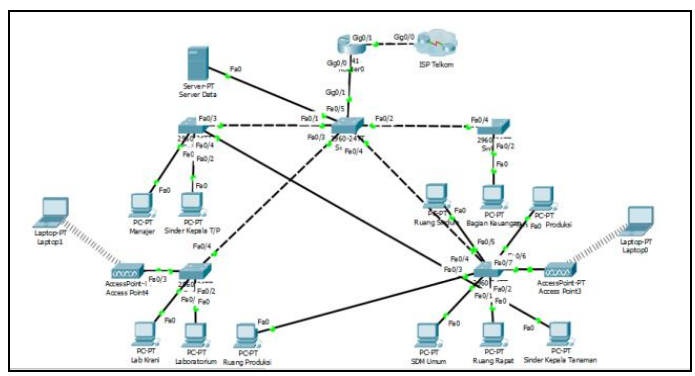
4. HASIL DAN PEMBAHASAN

4.1. Hasil Penelitian

Setelah melakukan tahapan-tahapan dari metode *Network Development Life Cycle* (NDLC) untuk mengembangkan jaringankomputer di PTPN 7 Betung yang meliputi analisis awal, desain topologi jaringan, *simulation prototyping* dan dokumentasi serta *testing*.

1. Hasil Desain Topologi

Penulis akan memberikan sketsa *blueprint* tentang hasil pengembangan jaringan komputer pada PTPN 7 Betung sebagai berikut.



Gambar 7. Desain Topologi Jaringan

2. Perbandingan Jaringan Lama dan Baru

Adapun perbandingan antara jaringan lama dan jaringan baru yang diperoleh setelah dilakukan pengembangan jaringan komputer pada PTPN 7 Betung yaitu :

Tabel 4. Perbandingan Jaringan lama dan baru

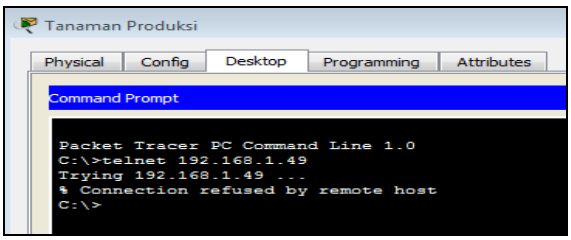
No	Yang Diterapakn	Jaringan Lama	Jaringan Baru
1	*Gateway*	Ada	Ada
2	Keamanan Jaringan	Tidak	Ada
3	Jaringan Lokal (VLAN)	1	5
4	*Access List*	Tidak	Ada
5	*Wifi Access Point*	Tidak	Ada
6	*Server* Data	Tidak	Ada
7	Filter Virus	Tidak	Ada

4.2. Pembahasan

a. Testing Keamanan Jaringan

1. Testing Akses *Router*

Blok akses *router* dilakukan dengan cara membatasi semua *user* pada setiap divisi selain Ruangan Manajer dan Ruangan Sinder Kepala Tanaman untuk mengakses ke *router* melalui *web browser*, pada testing dibawah ini dilakukan tes koneksi ke *router* dari Ruangan Tanaman Produksi, yang termasuk kedalam daftar divisi yang tidak boleh mengakses *router* mikrotik, untuk masuk ke menu *router* menggunakan *webserver* cukup dengan memasukan *gateway* dari Ruangan Produksi yaitu 192.168.1.49. maka akan di dapat hasil seperti gambar dibawah ini:

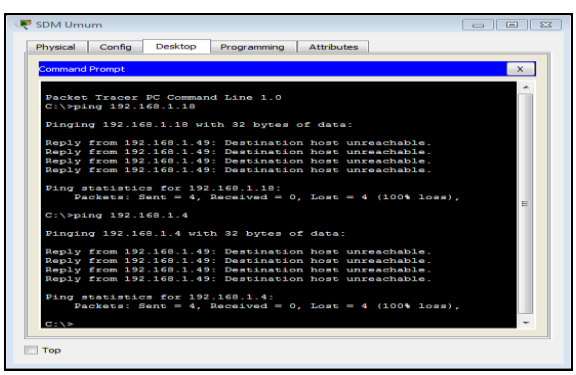


Gambar 8. Tes koneksi Ke Router Mikrotik Dari Divisi Tanaman Produksi

Pada gambar 8 terlihat bahwa koneksi dari divisi Tanaman Produksi ke *router* mikrotik direset, ini karena semua IP *address* dari divisi Tanaman Produksi atau divisi lain selain dari Ruangan Manajer dan Ruangan Sinder Kepala Tanaman tidak dizinkan untuk mengakses *router* dari *web browser*.

2. Testing Akses Ke Divisi Lain

Pada perancangannya pada jaringan lokal hanya Ruangan Manajer dan Ruangan Bagian Keuangan yang boleh melakukan koneksi sedangkan untuk divisi lain seperti Ruangan SDM Umum hanya diizinkan akses ke *server* data.



Gambar 10. Hasil Tes Koneksi dari Manajer dan Ruangan Bagian Keuangan.

Pada gambar diatas menunjukan *reply Destination host unreachable*, ini artinya bahwa IP tujuan tidak dapat dijangkau. Dan koneksi ke IP tujuan tidak dapat dilakukan karena akses ke IP *user* SDM Umum telah dibatasi oleh *router* mikrotik.

5. KESIMPULAN

Adapun kesimpulan yang penulis dapat dari penelitian tugas akhir ini adalah :

1. VLAN dapat meorganisasi jaringan pada ruangan masing-masing seksi sehingga memudahkan *Administrator* dalam perawatan dan menemukan penyebab gangguan apabila terjadi masalah pada jaringan.
2. Dengan adanya *access list* maka keamanan *user* pada masing-masing ruangan dan *server* dapat ditingkatkan karena terdapat pembatasan-pembatasan hak akses.
3. *Router* merupakan perangkat yang terpenting dalam sebuah jaringan, maka dari itu keamanan untuk *router* harus ada, dengan diterapkannya *access list* keamanan *router* bisa ditingkatkan dengan membatasi akses *user* ke *router cisco* (*telnet*).
4. Pemblokiran filter virus pada *access list* maka keamanan user pada masing-masing port dapat di tingkatkan karena terdapat pembatasan-pembatasan hak akses.

6. DAFTAR PUSTAKA

[1] Muzakir, A., & Ulfa, M. (2019). ANALISIS KINERJA PACKET FILTERING BERBASIS MIKROTIK ROUTERBOARD PADA SISTEM KEAMANAN JARINGAN. *Simetris: Jurnal Teknik Mesin, Elektro Dan Ilmu Komputer*, *10*(1), 15–20.

[2] Mochamad, P. (2015). Analisis Dan Desain Keamanan JAringan Komputer Dengan Metode Network Development Life Cycle (Studi Kasus : Universitas Telkom).

[3] Purwanto, A. D., & Badrul, M. (2016). IMPLEMENTASI ACCESS LIST SEBAGAI FILTER TRAFFIC JARINGAN (STUDY KASUS PT. USAHA ENTERTAINMENT INDONESIA), (1), 11.

[4] Rahmawati. (2015). KONFIGURASI KEAMANAN JARINGAN KOMPUTER PADA ROUTER DENGAN METODE ACL'S.

[5] Saputra, B. W. (2015). *RANCANGAN KEAMANAN JARINGAN KOMPUTER DENGAN MEMANFAATKAN ROUTER CISCO DI KANTOR PELAYANAN PAJAK PARATAMA PALEMBANG SEBERANG ULU (SIMULASI DENGAN PACKET TRACER).*

[6] Simanjuntak, P., & Suharyanto, C. E. (2017). ANALISIS PENGGUNAAN ACCESS CONTROL LIST (ACL) DALAM JARINGAN KOMPUTER DI KAWASAN BATAMINDO INDUSTRIAL PARK BATAM, 7.