RANCANG DAN BANGUN SISTEM KEAMANAN JARINGAN DENGAN VIRTUAL LAN DAN ACCES CONTROL LIST PT ELECTRONIC CITY CIPINANG INDAH MALL

Devry Novriandi, Prionggo. H
devrynovriandi@gmail.com, prionggo.hendradi@gmail.com
Fakultas Teknik, Universitas Satya Negara Indonesia

ABSTRAK

Pada sebuah jaringan perusahaan pastinya diperlukan pemberlakuan jaringan yang maksimal dengan biaya lebih efisien dan hemat. Maka dari itu dibutuhkan Virtual Local Area Network (VLAN) yang mana digunakan untuk membuat satu jaringan menjadi banyak jaringan di dalam satu perangkat (switch). Dalam suatu jaringan yang saling terhubung di sebuah perusahaan pastinya membutuhkan beberapa ketentuan yang berlaku supaya jaringan tetap aman dan efisien. Misalnya pada jaringan yang terhubung di perusahaan itu seperti halnya hak akses suatu bagian yang satu ke bagian yang lainnya. Tetapi terkadang, jaringan yang terhubung di perusahaan tidak memikirkan pembatasan akses yang digunakan komputer untuk saling berhubungan. Terutama pada saat bagian perusahaan tertentu yang mempunyai hak akses penuh dan yang tidak mempunyai hak atas hak akses pada sebuah jaringan di perusahaan. Dengan adanya permasalahan yang seperti itu dibutuhkan suatu Access Control List (ACL) yang mana dapat membuat aturan-aturan dalam hak akses yang berbeda-beda di suatu jaringan perusahaan tersebut.
Kata Kunci : Keamanan Komputer, ACL, Jaringan Komputer, Security Network

ABSTRACT

In a *corporate network, it is certainly necessary to apply the maximum network at a more efficient and efficient cost. Therefore, a Virtual Local Area Network (VLAN) is needed, which is used to create a network into many networks on one device (switch). In a network that is connected to each other in a company, of course, it requires several provisions that apply so that the network remains safe and efficient. For example, the network connected in the company is like the access rights of one part to another. But sometimes, connected networks in a company don't think about restricting the access computers use to connect to one another. Especially when certain parts of the company have full access rights and who do not have access rights to a network in the company. With such a problem, an Access Control List (ACL) is needed which can create rules for different access rights in a corporate network.*
Keywords: Computer Security, ACL, Computer Networks, Network Security

PENDAHULUAN

Pada sebuah jaringan perusahaan pastinya diperlukan pemberlakuan jaringan yang maksimal dengan biaya lebih efisien dan hemat. Maka dari itu dibutuhkan Virtual Local Area Network (VLAN) yang mana digunakan untuk membuat satu jaringan menjadi banyak jaringan di dalam satu perangkat (switch). Dalam suatu jaringan yang saling terhubung di sebuah perusahaan pastinya membutuhkan beberapa ketentuan yang berlaku supaya jaringan tetap aman dan efisien. Misalnya pada jaringan yang terhubung di perusahaan itu seperti halnya hak akses suatu bagian yang satu ke bagian yang lainnya. Tetapi terkadang, jaringan yang terhubung di perusahaan tidak memikirkan pembatasan akses yang digunakan komputer untuk saling berhubungan. Terutama pada saat bagian perusahaan tertentu yang mempunyai hak akses penuh dan yang tidak mempunyai hak atas hak akses pada sebuah jaringan di perusahaan. Dengan adanya permasalahan yang seperti itu dibutuhkan suatu Access Control List (ACL) yang mana dapat membuat aturan-aturan dalam hak akses yang berbeda-beda di suatu jaringan perusahaan tersebut.

Pada PT Electronic City Cipinang Indah Mall terdapat jaringan komputer LAN (Local Area Network) yang belum memilki konfigurasi pengaman dengan ACL (Access Control List) sehingga hal ini dapat membuat ketahanan dari pengamanan jaringan komputer menjadi sangat rentan atas tindakan penerobosan yang dapat dilakukan oleh pihak yang tidak berwenang. Dampak yang terjadi sudah dirasakan oleh user. Wawancara telah dilakukan penulis terhadap user & administrator jaringan setempat. Mereka mengeluhkan seperti berbagi data antar user pada jaringan lokal sangat lamban tidak seperti biasanya, sering muncul beberapa error yang disebabkan malware, akses aplikasi POS client server dan aplikasi lainnya dirasakan sangat lamban, Hal tersebut telah mendapat perhatian khusus dari management perusahaan karena berhubungan dengan produktifitas kerja karyawan yang menurun karena masalah tersebut.

Oleh karena masalah tersebut maka penulis tertarik untuk meneliti masalah tersebut dan memberikan solusi dengan dengan penerapan ACL (Access Control List) pada jaringan komputer tersebut sehingga tindakan penerobosan jaringan dapat di minimalisir serta meningkatkan keamanan pada jaringan tersebut.

Tujuan Penelitian

Adapun tujuan dari penelitian ini adalah melakukan Rancang Dan Bangun Sistem Keamanan Jaringan Dengan VLAN *(Virtual Local Area Network)* Dan ACL *(Access Control List)* Pada PT Electronic City Cipinang Indah Mall

Manfaat Penelitian

Penelitian dan rancang bangun ini dapat memberikan manfaat secara khusus untuk user , Tim IT dan Management perusahaan berupa hasil penelitian dan rancang bangun keamanan jaringan VLAN *(Virtual Local Area Network)* Dan ACL *(Access Control List)*, yang mana nantinya dapat dimanfaatkan serta dikembangkan kembali keamanan jaringan yang sudah dibangun.

Metode Penelitian

Penyusunan tugas akhir ini menggunakan metode untuk memperoleh data atau informasi dalam memecahkan permasalahan. Metode yang dilakukan adalah sebagai berikut :

- Metode Observasi

  Dalam metode ini penulis mengadakan pengamatan terhadap objek yang diperoleh pada saat pengerjaan sistem dan pengujian sistem. Dan melakukam pembahasan dengan pembimbing maupun pihak-pihak yang terlibat dalam pelaksanaan tugas akhir ini.

- Metode 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 VLAN *(Virtual Local Area Network)* Dan ACL *(Access Control List)* . dengan menganalisa per topiknya . dan kemudian analisis per topiknya untuk memberikan kesimpulan tiap bagian pembahasan.

- Metode Eksperimental

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 , dan kemudian penulis membuat pembagian-pembagian jaringan untuk Perusahaan 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 dengan menggunakan *Access Control List* (ACL)

Tinjuan Pustaka

Penelitian dan rancang bangun yang dilakukan tidak terlepas dari hasil penelitian – penelitian yang telah dilakukan terdahulu yang merupakan sebagai panduan untuk melakukan penelitian, Antara lain sebagai berikut :

Dari penelitian yang dilakukan oleh Aditya Yuniar, Program Keahlian Teknik Komputer Program Diploma Institut Pertanian Bogor 2014. PENERAPAN ACCESS CONTROL LIST (ACL) PADA JARINGAN VLAN DI PT GOODYEAR INDONESIA TBK

Penelitian ini mempelajari cara implemtasikan access control list (ACL) pada jaringan local area network (VLAN) di PT GoodYear Indonesia TBK. Kofigurasi ACL ini di lakukan untuk blok berdasarkan range alamat IP asal (standard ACL) dan blok berdasarkan range alamat IP tujuan tertentu (extended ACL) dalam alamat-alamat IP yang berada pada jaringan VLAN.

Dari penelitian Agus Didi Purwanto, Mohammad Badrul Teknik Komputer AMIK BSI 2016. IMPLEMENTASI ACCESS LIST SEBAGAI FILTER TRAFFIC JARINGAN (STUDY KASUS PT USAHA ENTERTAINMENT INDONESIA).

Dari penelitian ini, penulis bermaksud mengimplementasikan acces list sebagai filter traffic jaringan PT Usaha Entertainment Indonesia. Dengan melihat topologi jaringan berjalan saat ini, lalu lintas data di jaringan tersebut sangat padat, dan dalam segi keamanan filter data, terlihat tidak adanya batas akses antara jaringan kantor pusat dan jaringan kantor cabang. Dalam hal ini tidak adanya filter data apakah data tersebut di perbolehkan masuk pada jaringan atau tidak. Hal inilah yang akan menciptakan celah yang bisa menimbulkan ketidakamanan pada jaringan komputer. Trafic filtering tidak lain merupakan sebuah teknik untuk mengontrol trafik-trafik yang diforward ke dan dari sebuah jaringan melintasi router. Fungsi ini melibatkan perancangan policy-policy keamanan. Pada implementasinya traffic filtering ini akan di rancang untuk membentuk environment firewall. Karena hal tersebut di atas penulis merasa pada PT Usaha Entertainment Indonesia perlu membangun dan mengimplementasikan serta mengembangkan jaringan komputer dan mengusulkan suatu rancangan jaringan dengan implementasi metode access control list.

Dari penelitian Muhamad Syakir, Sistem Komputer STIKOM SURABAYA 2016 PERANCANGAN DAN IMPLEMENTASI ACCES CONTROL LIST DAN VLAN PADA PT EXPERT DATA VOIECE SOLUTION.

Dalam perancangan Cisco Router penulis belajar cara implementasi pembatasan hak akses lalu lintas jaringan. Pada umumnya untuk merancang jaringan dibutuhkan pembatasan akses yang mana dapat menghubungkan, mengijinkan dan memblokir akses dari jaringan satu ke yang lainnya. Maka dari itu dibutuhkan Access Control List (ACL) untuk membuat pembatasan hak akses dari jalur

Jaringan Komputer

Jaringan komputer adalah sekelompok komputer otonom yang saling berhubungan dengan menggunakan protokol komunikasi sehingga dapat saling berbagi informasi, aplikasi dan perangkat keras secara bersama sama. Jaringan komputer juga dapat diartikan sebagai gabungan antara teknologi komputer dan teknologi telekomunikasi. Gabungan teknologi ini menghasilkan pengolahan data yang dapat didistribusikan, mencakup pemakaian database, software aplikasi dan peralatan hardware secara bersamaan(Ahmad, 2016).

Tujuan membangun jaringan komputer adalah membawa informasi secara tepat tanpa adanya kesalahan dari sisi pengirim (Transmitter) menuju ke sisi penerima (Receiver) melalui media komunikasi (Sukmaaji dan Rianto, 2016) Menurut (Sukmaaji dan Rianto, 2016) dalam buku mereka

yang berjudul Jaringan Komputer menyatakan bahwa beberapa manfaat yang terdapat pada jaringan komputer sebagai berikut:

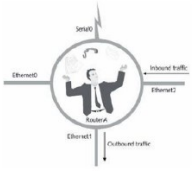
- Pengguna dapat saling berbagi printer dengan kualitas tinggi, dibanding menggunakan printer kualitas rendah dimasing-masing meja kerja. Selain itu, lisensi perangkat lunak jaringan komputer dapat lebih murah dibandingkan lisensi stand-alone terpisah untuk sejumlah pengguna sama.
- Jaringan komputer membantu mempertahankan informasi agar tetap handal dan up-to-date. Sistem penyimpanan data terpusat yang dikelola dengan baik memungkinkan banyak pengguna mengakses dara dari berbagai lokasi yang berbeda dengan hak akses yang bisa diatur bertingkat.
- Jaringan komputer membantu mempercepat proses berbagi data (data sharing). Transfer data pada jaringan komputer lebih cepat dibandingkan dengan sarana berbagi lainnya.
- Jaringan komputer memungkinkan kelompok kerja berkomunikasi dengan lebih efisien, yaitu dengan penyampaian pesan secara elektronik misalnya system penjadwalan, pemantauan proyek dan konferensi online yang bertujuan mambantu tim bekerja lebih efektif.

VLAN

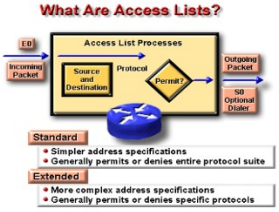
VLAN (Virtual Local Area Network) adalah sebuah LAN sebagai kelompok device terdapat dalam konfigurasi (menggunakan software manajemen) sehingga saling berkomunikasi yang seolah-olah terhubung dengan jaringan yang sama walaupun secara fisikal mereka berada pada segmen dalam LAN yang berbeda. VLAN dibuat lebih pada koneksi logikal yang lebih fleksibel dan dapat membagi jaringan ke dalam beberapa subnetwork serta mengijinkan banyak subnet dalam jaringan yang menggunakan switch yang sama. VLAN merupakan fungsi logik dari sebuah switch yang berfungsi membagi jaringan LAN ke dalam beberapa jaringan virtual. Dapat memudahkan administrator jaringan saat membagi secara logik group workstation secara fungsional yang tidak dibatasi oleh batasan lokasi merupakan Implementasi VLAN dalam jaringan

ACL (Access Control List)

Access Control List biasa disebut dengan Access list adalah pengelompokan paket berdasarkan kategori. Access list bisa sangat membantu ketika membutuhkan pengontrolan dalam lalu lintas network. access list menjadi tool pilihan untuk pengambilan keputusan pada situasi ini. Penggunaan access list yang paling umum dan paling mudah untuk dimengerti adalah penyaringan paket yang tidak diinginkan ketika mengimplementasikan kebijakan keamanan. Sebagai contoh kita dapat mengatur access list untuk membuat keputusan yang sangat spesifik tentang peraturan pola lalu lintas sehingga access list hanya memperbolehkan host tertentu mengakses sumber daya WWW sementara yang lainnya ditolak. Dengan kombinasi access list yang benar, network manajer mempunyai kekuasaan untuk memaksa hamper semua kebijakan keamanan yang bisa mereka ciptakan. (Rochmad, 2015).

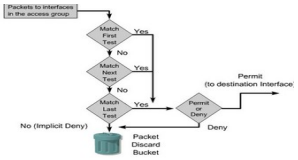


Gambar 1 - Implementasi Router



Gambar 2 - Ketentuan ACL

Untuk mengetahui bagaimana cara kerja ACL lihat gambar di bawah ini :



Gambar 3 - Cara kerja ACL

Tipe dari ACL, yaitu: Standard ACL dan Extended ACL Dua metode digunakan untuk identifikasi Standard dan Extended ACL:

- Numbered ACL: Menggunakan sebuah nomor sebagai identifikasi.
- Named ACL: Menggunakan deskripsi nama ataunomor untuk identifikasi.

IdentifikasiACL

- Nomor Standard ACL IPv4 (1-99) dengan Range Tambahan (1300- 1999).
- Nomor Extended ACL IPv4 (100-199) dengan Range Tambahan (2000-2699).

Named ACL bisa digunakan untuk identifikasi IP Standard dan Extended ACL dengan sebuah alpha numeric string (nama)

- Standard ACL

  Standard ACL hanya menggunakan alamat sumber IP di dalam paket IP sebagai kondisi yang ditest. Semua keputusan dibuat berdasarkan alamat IP sumber. Ini artinya, standard ACL pada dasarnya melewatkan atau menolak seluruh paket protocol. ACL ini tidak membedakan tipe dari lalu lintas IP seperti WWW, telnet, UDP, DSP.
- Extended ACL

  Extended ACL bisa mengevalusai banyak field lain pada header layer 3 dan layer 4 pada paket IP. ACL ini bisa mengevaluasi alamat IP sumber dan tujuan, field protocol pada header network layer dan nomor port pada header transport layer. Ini memberikan extended ACL kemampuan untuk membuat keputusan-keputusan lebih spesifik ketika mengontrol lalu lintas.

Jenis Lalu Lintas ACL

1. Inbound ACL

   Ketika sebuah ACL diterapkan pada paket inbound di sebuah interface ,paket tersebut diproses melalui ACL sebelum di-route ke outbound interface. Setiap paket yang ditolak tidak bisa di-route karena paket ini diabaikan sebelum proses routing diabaikan.
2. Outbond ACL

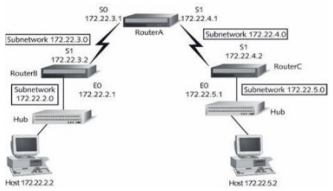
   Ketika sebuah ACL diterapkan pada paket outbound pada sebuah interface, paket tersebut di-route ke outbound interface dan diproses melalui ACL malalui antrian.

Wildcard Masking

Wildcard masking digunakan bersama ACL untuk menentukan host tunggal, sebuah jaringan atau range tertentu dari sebuah atau banyak network. Untuk mengerti tentang wildcard, kita perlu mengerti tentang blok size yang digunkan untuk menentukan range alamat. Beberapa blok size yang berbeda adalah 4, 8, 16, 32, 64.

Ketika kita perlu menentukan range alamat, kita memilih blok size selanjutnya yang terbesar sesuai kebutuhan. Sebagai contoh, jika kita perlu menentukan 34 network, kita memerlukan blok size 64. jika kita ingin menentukan 18 host, kita memerlukan blok size 32. jiak kita perlu menunjuk 2 network, maka blok size 4 bisa digunakan. Wildcard digunakan dengan alamat host atau network untuk memberitahukan kepada router untuk difilter. Untuk menentukan sebuah host, alamat akan tampak seperti berikut 172.16.30.5 0.0.0.0 keempat 0 mewakili setiap oktet pada alamat. Dimanapun terdapat 0, artinya octet pada alamat tersebut harus persis sama. Untuk menentukan bahwa sebuah octet bisa bernilai apa saja, angka yang digunakan adalah 255. sebagai contoh, berikut ini adalah

subnet /24 dispesifikasikan dengan wildcard: 172.16.30.0 0.0.255 ini memberitahukan pada router untuk menentukan 3 oktet secara tepat, tapi oktet ke- 4 bisa bernilai apa saja.



Gambar 4 - Contoh Jaringan Yang Terhubung

Standard Access List

Standard IP ACL memfilter lalu lintas network dengan menguji alamat sumber IP didalam paket. Kita membuat standard IP ACL dengan menggunakan nomor ACL 1-99 atau 1300-1999(expanded range). Tipe ACL pada ummnya dibedakan berdasarkan nomor yang digunakan ketika ACL dibuat, router akan mengetahui tipe syntax yang diharapkan untuk memesukkan daftar. Dengan menggunakan nomor 1-99 atau 1300-1999, kita memberitahukan kepada router bahwa kita ingin membuat IPACL, jadi router akan mengharapkan syntax yang hanya menspesifikasikan alamat sumber IP pada baris pengujian. Banyak range nomor ACL pada contoh dibawah ini yang bisa kita gunakan untuk memfilter lalu lintas pada jaringan kita (protocol yang bisa kita terapkan ACL bisa tergantung pada versi IOS kita) :

Tabel 5 - Perbedaan Standard dan Extended

TIPE ACL	NUMBER RANGE / IDENTIFIER
Standard	1-99, 1300-1999
Extended	100-1999, 2000-2699

Contoh Standard ACL untuk menghentikan user tertentu mendapatkan akses ke LAN Department Finance. Pada gambar, router mempunyai 3 koneksi LAN dan 1 koneksi WAN ke internet. User pada LAN Sales tidak boleh mempunyai akses ke LAN finance, tapi mereka boleh mengakses internet dan Department Marketing. LAN Marketing perlu mengakses LAN Finance untuk layanan aplikasi Pada router yang digambar, standard IP ACL berikut dikonfigurasi :

Lab_A#config t
Lab_A(config)#access -list 10 deny 172.16.40.0 0.0.0.255
Lab_A(config)#access-list 10 permit any

Sangatlah penting untuk diketahui bahwa perintah any sama halnya dengan menggunakan wildcard masking berikut :

Lab_A(config)#access-list 10 permit 0.0.0.0 255.255.255.255

Karena wildcard mask menyatakan bahwa tidak ada oktet yang diperiksa, setiap alamat akan sesuai dengan kondisi test. Jadi fungsi ini sama dengan penggunaan kata any. Saat ini, ACL dikonfigurasi untuk menolak alamat sumber dari LAN sales yang mengakses LAN finance, dan memperbolehkan dari akses yang lain. Tetapi untuk diingat, tidak ada tindakan yang diambil sampai akses list diterapkan pada arah yang spesifik. Tetapi dimana ACL ini seharusnya ditempatkan? Jika kita menempatkannya pada E0, kita mungkin akan mematikan juga interface Ethernet karena semua peralatan LAN Sales akan ditolak akses kesemua network yang terhubung ke router.

Keistimewaan Standard Access List

Extended ACL

Extended ACL bisa mengevaluasi banyak field lain pada header layer 3 dan layer 4 pada paket IP. ACL ini bisa mengevaluasi IP sumber dan tujuan, field protocol dalam network header Network Layer dan nomor port pada Transport Layer. Ini memberikan extended ACL kemampuan untuk membuat keputusan – keputusan lebih spesifik ketika mengontrol lalu lintas. Pada contoh Standard ACL, perhatikan bagaimana kita harus memblok semua akses dari LAN Sales ke Department

Finance. Bagaimana jika untuk urusan keamanan, kita membutuhkan Sales mendapatkan akses ke server tertentu pada LAN Finance tapi tidak ke layanan network lainnya ? Dengan standard IP ACL, kita tidak memperbolehkan user mendapat satu layanan sementara tidak untuk yang lainnya. Dengan kata lain, ketika kita membutuhkan membuat keputusan berdasarkan alamat sumber dan tujuan, standard ACL tidak memperbolehkan kita melakukannya karena ACL ini hanya mambuta kaputusan berdasrkan alamat sumber. Tetapi extended ACL akan membantu kita karena extended ACL memperbolehkan kita menentukan alamat sumber dan tujuan serta protocol dan nomor port yang mengidentfikasikan protocol upper layer atau aplikasi. Dengan menggunakan extended ACL kita bias secara efisien memperbolehkan user mengakses ke fisik LAN dan menghentikan host tertentu atau bahkan layanan tertentu pada host tertentu.

Konfigurasi Router

Setting Interface

```
R.Local(config)#int fa0/0
R.Local(config-if)#ip address 192.168.1.1  255.255.255.0
R.Local(config-if)#no shutdown
```

Setting Subinterface Untuk Gateway Vlan Masing-masing

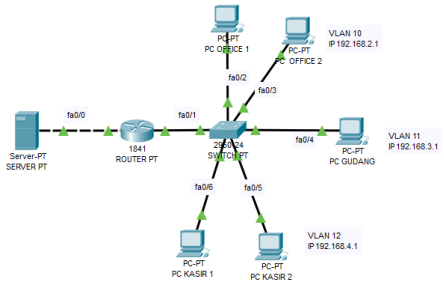
```
R.Local(config-if)#int fa0/1.10
R.Local(config-subif)#encapsulation dot1Q 10
R.Local(config-subif)#ip address 192.168.2.1 255.255.255.0
R.Local(config-if)#int fa0/1.11
R.Local(config-subif)#encapsulation dot1Q 11
R.Local(config-subif)#ip address 192.168.3.1 255.255.255.0
R.Local(config-if)#int fa0/0.12
R.Local(config-subif)#encapsulation dot1Q 12
R.Local(config-subif)#ip address 192.168.4.1 255.255.255.0
```

Setting ACL

Sesuai Topologi di atas sebuah aturan baru di terapkan yakni Layanan HTTP pada Server WWW hanya boleh diakses oleh PC OFFICE. Sementara Layanan FTP pada Server FTP hanya boleh diakses oleh PC OFFICE dan PC GUDANG. Trafik yang lainnya diijinkan dan seluruh client juga tetap bisa melakukan ping ke server.

```
R.Local(config)#access-list 102 deny tcp host 192.168.3.4 host 192.168.1.2 eq www
R.Local(config)#access-list 102 deny tcp host 192.168.4.5 host 192.168.1.2 eq www
R.Local(config)#access-list 102 deny tcp host 192.168.4.6 host 192.168.1.2 eq www
R.Local(config)#access-list 102 deny tcp host 192.168.4.5 host 192.168.1.2 eq ftp
R.Local(config)#access-list 102 deny tcp host 192.168.4.6 host 192.168.1.2 eq ftp
R.Local(config)#access-list 102 permit ip any any
R.Local(config)#int fa0/0
R.Local(config-if)#ip access-group 102 out
R.Local (config-if)#exit
```

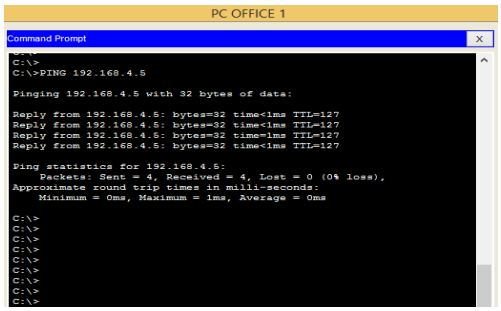
Hasil Konfigurasi



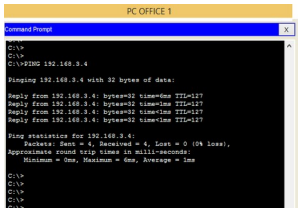
Gambar.5 - Hasil Konfigurasi

Hasil konfigurasi yang diperoleh dari rancangan gambar dan ketentuan sesuai yang tertera di atas antara lain:

1. Komputer dari PC OFFICE dapat melakukan access ke komputer PC GUDANG dan ke PC KASIR



Gambar.6 - Akses PC OFFICE ke PC KASIR



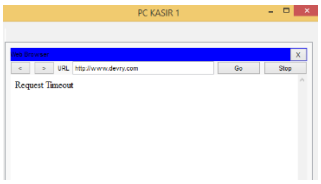
Gambar.7 - Akses PC OFFICE ke PC GUDANG

2. Komputer dari PC OFFICE dapat melakukan access internet

Gambar.8 - Akses PC OFFICE ke Internet

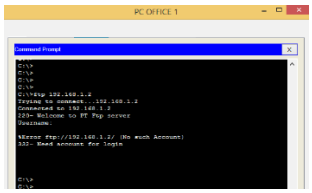
3. Komputer dari PC KASIR dan PC GUDANG tidak dapat melakukan access ke internet.

Gambar.9 - Akses PC GUDANG ke Internet



Gambar10 - Akses PC KASIR ke Internet

4. Komputer dari PC OFFICE dan PC GUDANG dapat melakukan access layanan FTP pada server FTP.



Gambar.11 – Akses layanan FTP PC OFFICE

Kesimpulan

Dari hasil pembahasan laporan Tugas Akhir / Skripsi ini penulis memberikan kesimpulan sebagai berikut:

1. Dengan adanya VLAN, dapat membuat banyak jaringan berbeda dalam satu switch.
2. Dengan adanya VLAN, dapat mempermudah administrator untuk membagi jaringan sesuai divisi pada sebuah perusahaan.
3. Untuk dapat melakukan pembatasan hak akses pada Cisco Router, dibutuhkan konfigurasi ACL.
4. Dengan adanya ACL, dapat membatasi paket-paket yang akan diblok atau yang diijinkan.

Saran

Berdasarkan kesimpulan dan analisis yang dilakukan selama Tugas Akhir, penulis ingin memberikan saran-saran sebagai berikut:

1. Untuk penggunaan VLAN, lebih baik menggunakan selain VLAN 1.
2. Untuk penggunaan VLAN, lebih baik menggunakan jalur trunk sebagai penghemat jalur yang mengarah ke router.
3. Untuk penggunaan ACL, penulis menyarankan untuk menggunakan standart ACL apabila tidak ada batasan secara spesifik seperti : pembatasan HTTP, TCP, WWW, dll.
4. Untuk peletakkan ACL, apabila standart ACL, baiknya diletakkan sedekat mungkin dengan alamat tujuan dan extended ACL, baiknya diletakkan sedekat dengan alamat asal.

DAFTAR PUSTAKA

Manuaba Ida Bagus Verry Hendrawan, dkk. 2012. Evaluasi Keamanan Akses Jaringan Komputer Nirkabel. ISSN 2301 – 415613. JNTETI, Vol. 1, No. 1.

Mentang, Randy, dkk. 2015. Perancangan dan Analisis Keamanan Jaringan Nirkabel Menggunakan Wireless Intrusion Detection System. E-journal Teknik Elektro dan Komputer, Volume 5, No.7: ISSN:2301-8402.

Pujiarto, Bambang, dkk. 2013. Evaluasi Keamanan Wireless Local Area Network Menggunakan Metode Penetration Testing. ISSN 1411-3201, Vol. 14 No.2.

Richard Pangalila, Agustinus Noertjahyana, Justinus Andjarwirawan. 2015. Penetration Testing Server Sistem Informasi Manajemen dan Website Universitas Kristen Petra.