Penggunaan *Firewall* Metode *Access Control List* Sebagai Blok Situs dan *Fitering File Transfer Protocol* pada PT Indoraya Makmur Abadi

Aziz Setyawan Hidayat [1)*)], Agus Salim [2)], Yana Iqbal Maulana [3)], Pas Mahyu Akhirianto [4)]

[1)] Teknik Komputer, Universitas Bina Sarana Informatika PSDKU Kota Tegal
[2)] Sistem Informasi, Universitas Bina Sarana Informatika
[3)] Teknologi Informasi, Universitas Bina Sarana Informatika
[4)] Teknik Elektro, Universitas Bina Sarana Informatika
[*)]**Correspondence author**: aziz.aiz@bsi.ac.id , Tegal, Indonesia
DOI: https://doi.org/10.37012/jtik.v10i2.2310

Abstrak

PT Indoraya Makmur Abadi merupakan sebuah perusahaan yang bergerak di bidang telekomunikasi. Teknologi perangkat-perangkat jaringan yang dimiliki oleh perusahaan ini pun sangat mumpuni akan adaptasi perkembangan telekomunikasi yang sangat tinggi. PT Indoraya Makmur Abadi sudah terdapat sistem metode VLAN (*Virtual Local Area Network*) yang membagi beberapa logic jalur koneksi berdasarkan VLAN tersebut. VLAN ini digunakan untuk mengamankan data atau informasi dari satu bagian atau divisi terhadap bagian atau divisi lain agar tidak dapat discanning. Selain itu juga jika salah bagian terkena virus atau worm atau trojan atau lainnya, maka dengan adanya VLAN bagian atau divisi ini akan secara otomatis mengisolasi hanya bagian atau divisi tersebut saja yang terjangkit dan tidak akan menyebar ke bagian atau divisi lainnya. Untuk keamanan jaringan koneksi internet hirarki perangkat setelah modem langsung terhubung ke Router, ini merupakan sebuah metode pencegahan agar koneksi internet dapat lebih dimanajemen pada router. Didalam penelitian ini pembahasan mengenai permasalahan yang dihadapi oleh PT Indoraya Makmur Abadi berupa Tidak adanya blok situs konten dewasa yang diberlakukan diperusahaan, pemblokan ini berguna untuk mengefektifkan bandwidth dalam hal pemanfaatannya. Dan pembatasan akses koneksi pada client dengan memfilter data, agar data yang masuk dan keluar jaringan dapat dikenali dan dijamin keabsahannya pada saat koneksi ke FTP Server pada internet.

Kata Kunci: Firewall; Access Control List; FTP Server

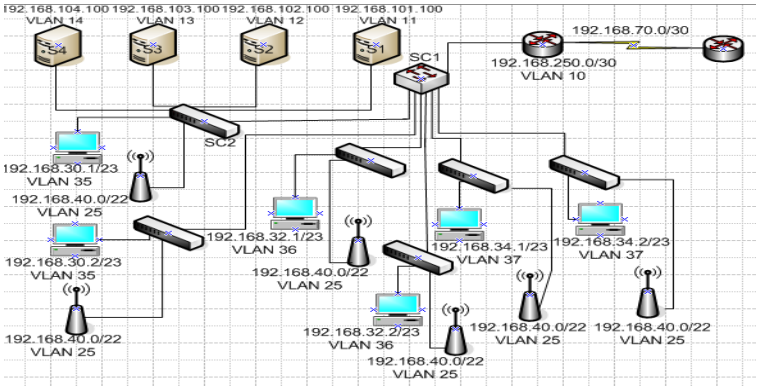
Abstract

PT Indoraya Makmur Abadi is a company operating in the telecommunications sector. The network equipment technology owned by this company is also very capable of adapting to very high telecommunications developments. PT Indoraya Makmur Abadi already has a VLAN (Virtual Local Area Network) method system which divides several connection path logic based on the VLAN. This VLAN is used to secure data or information from one section or division against another section or division so that it cannot be scanned. Apart from that, if one part is infected with a virus or worm or trojan or something else, then with the VLAN this part or division will automatically isolate only that part or division that is infected and it will not spread to other parts or divisions. For network security, the device hierarchy internet connection after the modem is directly connected to the router, this is a prevention method so that the internet connection can be better managed on the router. In this research, there is a discussion of the problems faced by PT Indoraya Makmur Abadi in the form of the absence of adult content site blocks implemented in the company. This blocking is useful for making bandwidth more effective in terms of its utilization. And limiting connection access to clients by filtering data, so that data entering and leaving the network can be recognized and its validity guaranteed when connecting to an FTP Server on the internet.

Keywords: *Firewall; Access Control List; FTP Server*

PENDAHULUAN

Di dalam skema jaringan pada PT Indoraya Makmur Abadi sudah memenuhi kaidah serta standar jaringan yang berlaku, karena PT Indoraya Makmur Abadi mengedepankan teknologi dan jaringan komputer yang handal baik dari sisi *hardware* maupun *software*. Pengelola aset pada PT Indoraya Makmur Abadi akan selalu *mengupdate* perkembangan teknologi untuk memperlancar dan mempercepat proses *transfer*, *sharing* data, *email*, dan keamanan jaringan.



Gambar 1. Gambar Skema Jaringan PT Indoraya Makmur Abadi

Berikut ini analisis detail skema jaringan pada PT Indoraya Makmur Abadi:

1. Koneksi internet yang ada didalam Jaringan komputer pada PT Indoraya Makmur Abadi menggunakan perangkat modem berjenis ADSL (*Assymmetric Digital Subscriber line*) yang terdapat pada lantai 27. Modem ini difungsikan selain koneksi ke internet digunakan juga untuk menghubungkan Router 2 (R2), didalam koneksinya modem ini terdiri dari :
   a. 3 buah port RJ 11, pada port 1 RJ 11 dihubungkan ke ISP menggunakan kabel fiber, sedangkan port 2 RJ 11 dihubungkan ke pesawat telepon dan port 3 RJ 11 masih belum digunakan.
   b. 4 buah port RJ 45, pada port 1 RJ 45 dihubungkan ke Router 2 (R2) dan port 2 RJ 45 sampai dengan port 4 RJ 45 belum digunakan dan masih kosong.
2. Bersumber dari modem koneksi internet berjalan pada jaringan komputer PT Indoraya Makmur Abadi. Dengan kecepatan *speed download* dan *upload* ISP *Up To* 100 Mbps.

3. Pada perangkat berikutnya adalah Router yang difungsikan sebagai pusat kontrol jaringan. Router yang terdapat pada PT Indoraya Makmur Abadi, adalah sebagai berikut :

   Router terdapat pada lantai 27 dan mempunyai 4 buah port FastEthernet dan 3 buah port serial. Berikut ini koneksi yang ada didalam Router :

   a. 3 buah port Gigaethernet digunakan untuk menghubungkan ke perangkat modem pada port 0 Gigaethernet, sedangkan port 1 Gigaethernet digunakan untuk menghubungkan perangkat Switch Catalist 1 (SC1), dan 1 buah port Gigaethernet masih belum digunakan.
   b. 3 buah port Serial digunakan untuk menghubungkan ke kantor cabang-cabang pada PT Indoraya Makmur Abadi.

4. Perangkat berikutnya adalah 4 buah Server (S1-S4) yang difungsikan sebagai server-server aplikasi. Server-server ini mengakomodir proses bisnis yang dilakukan oleh PT Indoraya Makmur Abadi, antara lain adalah :

   a. Network Planning
   b. Jasa Penyewaan Menara Telekomunikasi (Makro dan Mikro)
   c. Jasa Penyewaan BTS Hotel dan IBS
   d. Jasa Penyewaan Genset untuk BTS
   e. Jasa Pemeliharaan Site

   Dari 5 (lima) point proses bisnis tersebut diakomodir di dalam 4 (buah) aplikasi yang setiap aplikasinya ditempatkan pada sebuah server.

5. Switch Catalist dan Switch Multilayer adalah perangkat berikutnya yang ada di dalam PT Indoraya Makmur Abadi. Switch catalist ini digunakan untuk membuat metode VLAN pada jaringan komputer PT Indoraya Makmur Abadi. Switch catalist yang ada berjumlah 6 (enam) buah dan 1 (satu) buah perangkat Switch Multilayer, yaitu :

   a. Switch Multilayer (SC1) terletak pada lantai 27, Switch ini sebagai core atau pusat VLAN-VLAN yang ada didalam jaringan. Switch ini memiliki memiliki 24 port FastEthernet dan 2 port GigaEthernet, sedangkat port-port yang digunakan adalah:
      1) Port 2 FastEthernet menghubungkan Switch Catalist 3 (SC3) lantai 25 dan dijadikan VTP dengan metode Trunk untuk VLAN 25 dan VLAN 35.

2) Port 3 FastEthernet menghubungkan Switch Catalist 4 (SC4) yang terletak pada lantai 26, port ini digunakan sebagai VTP dengan metode Trunk untuk VLAN 25 dan VLAN 36.
3) Port 4 FastEthernet menghubungkan Switch Catalist 5 (SC5) yang terletak pada lantai 26, port ini digunakan sebagai VTP dengan metode Trunk untuk VLAN 25 dan VLAN 36.
4) Port 5 FastEthernet menghubungkan Switch Catalist 6 (SC6) yang terletak pada lantai 27, port ini digunakan sebagai VTP dengan metode Trunk untuk VLAN 25 dan VLAN 37.
5) Port 6 FastEthernet menghubungkan Switch Catalist 7 (SC7) yang terletak pada lantai 27, port ini digunakan sebagai VTP dengan metode Trunk untuk VLAN 25 dan VLAN 37.
6) Port 10 FastEthernet menghubungkan Switch Catalist 2 (SC2) yang terletak pada lantai 25, port ini digunakan sebagai VTP dengan metode Trunk untuk VLAN 25, VLAN 35, VLAN 11, VLAN 12, VLAN 13 dan VLAN 14.
7) Port 1 GigaEthernet menghubungkan Router yang terletak pada lantai 27, port ini digunakan sebagai VTP dengan metode Trunk untuk VLAN 10.

b. Switch Catalist 2 (SC2) terletak pada lantai 25, Switch Catalist ini mengelola VLAN 25 yang berisi perangkat Access Point 1 (AP1) menggunakan port 1 Gigatehernet sebagai penghubungnya dan beberapa Client atau PC 1 (P1) VLAN 35 sebagai penghubung port 1 FastEthernet sebagai penghubungnya, VLAN 11 server aplikasi 1 menggunakan port 11 Fasethernet, VLAN 12 server aplikasi 2 menggunakan port 12 Fasethernet, VLAN 13 server aplikasi 3 menggunakan port 13 Fasethernet, VLAN 14 server aplikasi 4 menggunakan port 14 Fasethernet, koneksinya kabel jaringan. Switch ini terhubung ke Switch Multilayer (SC1) menggunakan port 10 Fastethernet yang difungsikan sebagai VTP Trunk dari VLAN yang ada di Switch ini.
c. Switch Catalist 3 (SC3) terletak pada lantai 25, Switch Catalist ini mengelola VLAN 25 yang berisi perangkat Access Point 2 (AP2) menggunakan port 1 Gigaethernet dan beberapa Client atau PC 2 (P2) VLAN 35 menggunakan port 1

sampai 20 Fasethernet, koneksinya kabel jaringan. Switch ini terhubung ke Switch Multilayer (SC1) menggunakan port 2 Gigaethernet yang difungsikan sebagai VTP Trunk dari VLAN yang ada di Switch ini.

d. Switch Catalist 4 (SC4) terletak pada lantai 26, Switch Catalist ini mengelola VLAN 25 yang berisi perangkat Access Point 3 (AP3) menggunakan port 1 Gigaethernet dan beberapa Client atau PC 3 (P3) VLAN 36 menggunakan port 1 sampai dengan 10 Fasethernet, koneksinya kabel jaringan. Switch ini terhubung ke Switch Multilayer (SC1) menggunakan port 2 Gigaethernet yang difungsikan sebagai VTP Trunk dari VLAN yang ada di Switch ini.
e. Switch Catalist 5 (SC5) terletak pada lantai 26, Switch Catalist ini mengelola VLAN 25 yang berisi perangkat Access Point 4 (AP4) menggunakan port 1 Gigaethernet dan beberapa Client atau PC 4 (P4) VLAN 36 menggunakan port 1 sampai dengan 10 Fasethernet, koneksinya kabel jaringan. Switch ini terhubung ke Switch Multilayer (SC1) menggunakan port 2 Gigaethernet yang difungsikan sebagai VTP Trunk dari VLAN yang ada di Switch ini.
f. Switch Catalist 6 (SC6) terletak pada lantai 27, Switch Catalist ini mengelola VLAN 25 yang berisi perangkat Access Point 5 (AP5) menggunakan port 1 Gigaethernet dan beberapa Client atau PC 5 (P5) VLAN 37 menggunakan port 1 sampai dengan 10 Fasethernet, koneksinya kabel jaringan. Switch ini terhubung ke Switch Multilayer (SC1) menggunakan port 2 Gigaethernet yang difungsikan sebagai VTP Trunk dari VLAN yang ada di Switch ini.
g. Switch Catalist 7 (SC7) terletak pada lantai 27, Switch Catalist ini mengelola VLAN 25 yang berisi perangkat Access Point 6 (AP6) menggunakan port 1 Gigaethernet dan beberapa Client atau PC 6 (P6) VLAN 37 menggunakan port 1 sampai dengan 10 Fasethernet, koneksinya kabel jaringan. Switch ini terhubung ke Switch Multilayer (SC1) menggunakan port 2 Gigaethernet yang difungsikan sebagai VTP Trunk dari VLAN yang ada di Switch ini.

6. Akses point Aruba 303 digunakan sebagai koneksi wireless pada jaringan komputer PT Indoraya Makmur Abadi. Akses point yang digunakan sebanyak 6 buah akses point dengan pembagian setiap lantai 25 sampai dengan lantai 27 terdiri dari 2 buah

perangkat. Ini difungsikan sebagai penguat signal yang ada pada setiap lantainya. SSID atau nama wifi yang digunakan mitratel, jadi semua perangkat akses point hanya sebagai pembroadcast SSID atau nama wifi pada setiap lantainya. Setiap perangkat akses poin yang ada disetiap lantai 25 sampai lantai 27 menggunakan port GigaEthernet 2 sebagai penghubung ke setiap Switch Catalist (SC2 sampai dengan SC7). Sebagai sistem keamanan yang digunakan oleh AP agar terhubung ke perangkat Laptop atau Notebook atau Handphone dan lainnya harus didaftarkan terlebih ke divisi IT yaitu MAC Address yang ada di dalam perangkat-perangkat tersebut diatas.

7. *Client* yang ada didalam PT Indoraya Makmur Abadi terdiri dari 2 macam yaitu PC atau komputer desktop dan Laptop atau notebook. Koneksi yang digunakan oleh PC atau komputer desktop menggunakan jaringan kabel, sedangkan client berupa laptop atau notebook menggunakan jaringan wireless atau hotspot yang ada di tiap lantainya.
8. Media transmisi yang digunakan ada 2 macam penggolongan yang digunakan, yaitu :
   a. Wireless atau nirkabel, yang digunakan pada koneksi akses point dan perangkat wireless lainnya, seperti: handphone, tablet, atau laptop pada setiap laintainya yaitu lantai 25 sampai dengan lantai 27.
   b. Kabel, yang digunakan pada jaringan komputer PT Indoraya Makmur Abadi terdiri dari beberapa macam, yaitu:
      1) Kabel Fiber dengan konektor SJ, media transmisi ini digunakan untuk menghubungkan perangkat modem ke ISP.
      2) *Unshield Twisted Pair* (UTP), sebagian besar koneksi perangkat jaringan komputer pada PT Indoraya Makmur Abadi menggunakan media transmisi ini. Tetapi yang membedakannya adalah pengurutan kabel UTP tersebut terbagi menjadi 2 macam, yaitu:
         a) Kabel UTP Cross dengan konektor RG 45, digunakan untuk menghubungkan Switch Multi Layer (SC1) ke perangkat Switch Catalist 2 (SC2) sampai dengan Switch Catalist 7 (SC7).
         b) Kabel UTP Straight dengan konektor RG 45, digunakan untuk menghubungkan Router (R) dengan Switch Catalist (SC), Switch Catalist

(SC) dengan Akses Point, Switch Catalist (SC) dengan Server (S), Switch Catalist (SC) dengan PC (P).

9. Sedangkan ip address yang digunakan pada PT Indoraya Makmur Abadi, sebagai berikut :

Tabel 1. IP Address PT Indoraya Makmur Abadi

No	IP Address	Perangkat	Keterangan
1.	192.168.40.0/22	Access Point	Digunakan sebagai Jaringan WiFI pada setiap lantai 25-27
2.	192.168.30.0/23	Client/PC	Digunakan sebagai koneksi Client/PC pada Lant 25
3.	192.168.32.0/23	Client/PC	Digunakan sebagai koneksi Client/PC pada Lant 25
4.	192.168.34.0/23	Client/PC	Digunakan sebagai koneksi Client/PC pada Lant 25
5.	192.168.101.0/24	Server 1	Aplikasi
6.	192.168.102.0/24	Server 2	Aplikasi
7.	192.168.103.0/24	Server 3	Aplikasi
8.	192.168.111.0/24	Server 4	Aplikasi
9.	192.168.249.8/29	Router	Sebagai koneksi Peer to Peer Router dengan Switch Multilayer (SC1)

Sedangkan dari segi keamanan pada jaringan PT Indoraya Makmur Abadi, sebagai berikut:

Pada PT. Dayamitra Telekomunikasi pada sistem jaringan komputernya menggunakan sistem keamanan jaringan di mulai dari:

1. Pada PT Indoraya Makmur Abadi sudah terdapat sistem metode VLAN (*Virtual Local Area Network*) yang membagi beberapa logic jalur koneksi berdasarkan VLAN tersebut. VLAN ini digunakan untuk mengamankan data atau informasi dari satu bagian atau divisi terhadap bagian atau divisi lain agar tidak dapat discanning. Selain itu juga jika salah bagian terkena virus atau worm atau trojan atau lainnya, maka dengan adanya VLAN bagian atau divisi ini akan secara otomatis mengisolasi hanya bagian atau divisi tersebut saja yang terjangkit dan tidak akan menyebar ke bagian atau divisi lainnya.
2. Sudah adanya manajemen IP Address ini terlihat berdasarkan IP Address yang digunakan beberapa sudah ada yang mengalami subnetting. Ini difungsikan agar IP Address yang digunakan secara terbatas dan tidak luas atau tidak banyak sehingga tidak dapat user mengganti-ganti IP Address seamaunya sendiri.
3. Untuk keamanan jaringan koneksi internet hirarki perangkat setelah modem langsung terhubung ke Router, ini merupakan sebuah metode pencegahan agar koneksi internet dapat lebih dimanajemen pada router. Karena perangkat router yang memiliki feature

untuk melakukan manajemen jaringan secara lebih dibandingkan dengan modem.

4. Dari segi keamanan jaringan Hotspot atau WiFI pada PT Indoraya Makmur Abadi menggunakan pemfilteran atau penyaringan MAC Address. Hanya MAC Address yang sudah terdaftar pada Divisi IT dapat menggunakan jaringan Hotspot atau WiFI ini.

Didalam penelitian ini berdasarkan segi keamanan yang terjadi permasalahan tentang pembangunan firewall, yaitu:

1. Tidak adanya blok situs konten dewasa yang diberlakukan diperusahaan, pemblokan ini berguna untuk mengefektifkan bandwidth dalam hal pemanfaatan, dikarenakan jika salah pegawai mengakses situs dewasa dan menjalankan video pada situs tersebut, maka bandwidth akan banyak tersedot.
2. Pembatasan akses koneksi pada client dengan memfilter data, agar data yang masuk dan keluar jaringan dapat dikenali dan dijamin keabsahannya pada saat koneksi ke FTP Server pada internet.

METODE

Firewall merupakan sebuah sistem pengaman jadi Firewall bisa berupa apapun baik hardware maupun software. Firewall dapat digunakan untuk melakukan Filter paket-paket dari luar dan dalam jaringan di mana ia berada. Firewall secara umum adalah melindungi jaringan dari dalam maupun sisi luar router lewat port-port mana saja yang tersedia. Kata firewall jika diterjemahkan secara bahasa adalah “dinding api”. Firewall maksudkan untuk melindungi perangkat router dan client-client yang terhubung dengannya. Umumnya firewall dibuat untuk melindungi network internal (LAN) terhadap berbagai gangguan atau serangan yang berasal dari luar (Internet). Konsep firewall dalam konteks jaringan komputer mengambil gagasan dasar dari firewall (tembok penahan api) sebuah perangkat fisik yang dipasang di gedung-gedung. Tujuan utama pemasangan firewall fisik ini pada gedung-gedung adalah mencegah menjalarnya api dari sumbernya ke area di belakang firewall. Di kompleks- kompleks apartemen, misalnya, jika antara tiap-tiap unit apartemen dibatasi oleh sebuah firewall, maka api kebakaran yang timbul di salah satunya tidak akan menjalar degan mudah ke unit-unit yang bersebelahan karena terhalang firewall. Untuk dapat menjalankan

tujuannya, sebuah firewall mempunyai empat teknik dalam mengontrol akses dan menegakkan kebijakan keamanan yang diterapkannya. Secara original, firewall terfokus pada keutamaan dalam mengontrol pelayanan, yaitu:

1. Dalam kasus ini wildcard yang digunakan di dalam ACL merupakan lawan dari subnet mask yang digunakan pada alamat IP host/clien, maka semua alamat IP host/clien akan diproses. Subnet mask yang digunakan pada alamat IP host/clien adalah 255.255.0.0 sedangkan wildcard yang digunakan adalah 0.0.255.255. Bahwa terlihat nilai Byte pertama dan kedua subnet mask 255.255 sedangkan nilai Byte pertama dan kedua Wildcardmask adalah 0.0 maka dapat dikatan bahwa NetID pada alamat IP tersebut akan diproses. Sedangkan prosesnya adalah melihat perintah sebelumnya yaitu “deny tcp”.
2. Perintah “deny” adalah menolak, jadi perintah ini berfungsi sebagai penghalang dan tidak diberikan izin untuk dapat melewati interface router. Nah apa yang ditolak ?
3. Setelah perintah “deny” adalah nama aplikasi yaitu “tcp”. Aplikasi tersebut kepanjangannya adalah Transmission Control Protocol. Didalam aplikasi tcp terdapat beberapa paket data yaitu ftp, pop3, smtp, telnet dan www.
4. Sedangkan Wildcardmask 0.0.255.255 berfungsi sebagai pemilih atau penentu alamat IP segmen apa saja yang akan ditolak (deny). Dilihat dari Wildcard mask yang digunakan adalah Byte ke 1 (pertama) sampai dengan Byte ke 2 merupakan angka “0” (null). Ini menandakan bahwa 2 Byte sebagai alamat Net ID yang dideklarasikan akan ditolak. Disini 2 Byte tersebut merupakan alamat NetID, jadi dapat ditarik kesimpulan bahwa Net ID 172.16.0.0 akan ditolak dan akhirnya semua host/client pada Net ID tersebut juga akan ditolak atau tidak diizinkan untuk mengakses ftp server.

Audit firewall menawarkan banyak manfaat:

1. mengidentifikasi kesalahan konfigurasi : kesalahan konfigurasi firewall adalah penyebab umum kerentanan keamanan. audit rutin dapat membantu mengidentifikasi kesalahan konfigurasi ini dan segera memperbaikinya.

2. memastikan kepatuhan: pemeriksaan firewall reguler dapat membantu memastikan bahwa firewall dikonfigurasi sesuai dengan kebijakan keamanan internal dan persyaratan peraturan eksternal.
3. meninjau dan menyempurnakan aturan: seiring berjalannya waktu, aturan firewall dapat menjadi ketinggalan jaman atau tidak relevan. Berikan kesempatan untuk meninjau aturan tersebut dan menghapus atau memperbarui aturan yang tidak lagi memenuhi kebutuhan organisasi.
4. perubahan dokumen: audit firewall membuat catatan historis perubahan konfigurasi dan aturan firewall, yang dapat membantu dalam pemecahan masalah atau investigasi di masa mendatang.

Access Control List

Access control list (ACL), merupakan pengelompokan paket berdasarkan kategori. Access Control List (ACL) bisa sangat membantu ketika membutuhkan pengontrolan dalam lalu lintas network. Access control list menjadi tool pilihan untuk pengambilan keputusan pada situasi ini. Access Control List (ACL) sederhananya digunakan untuk mengijinkan atau tidak paket dari host menuju ke tujuan tertentu. Access Control List (ACL) terdiri atas aturan-aturan dan kondisi yang menentukan trafik jaringan dan menentukan proses di router apakah nantinya paket akan dilewatkan atau tidak. Penggunaan access Control list (ACL) yang paling umum dan paling mudah untuk dimengerti adalah penyaringan paket yang tidak diinginkan ketika mengimplementasikan kebijakan keamanan.

Access Control list terdapat dua macam identitas, yaitu :

1. ACL Standard

Daftar akses IP standar hanya menguji alamat sumber paket (kecuali untuk dua pengecualian). Karena daftar akses standar menguji alamat sumber, mereka sangat efisien dalam memblokir lalu lintas yang dekat dengan tujuan. Ada dua pengecualian ketika alamat dalam daftar akses standar bukan alamat sumber:

a. Pada daftar akses VTY keluar, ketika seseorang mencoba melakukan telnet, alamat dalam entri daftar akses digunakan sebagai alamat tujuan dan bukan sebagai alamat sumber.
b. Saat memfilter rute, Anda memfilter jaringan yang diiklankan kepada Anda, bukan alamat sumbernya.

2. ACL Extended

Daftar akses yang diperluas bagus untuk memblokir lalu lintas di mana saja. Daftar akses yang diperluas menguji alamat sumber dan tujuan serta data paket IP lainnya, seperti protokol, nomor port TCP atau UDP, jenis layanan (ToS), prioritas, tanda TCP, dan opsi IP. Daftar akses yang diperluas juga dapat memberikan kemampuan yang tidak dapat diberikan oleh daftar akses standar, seperti berikut ini:

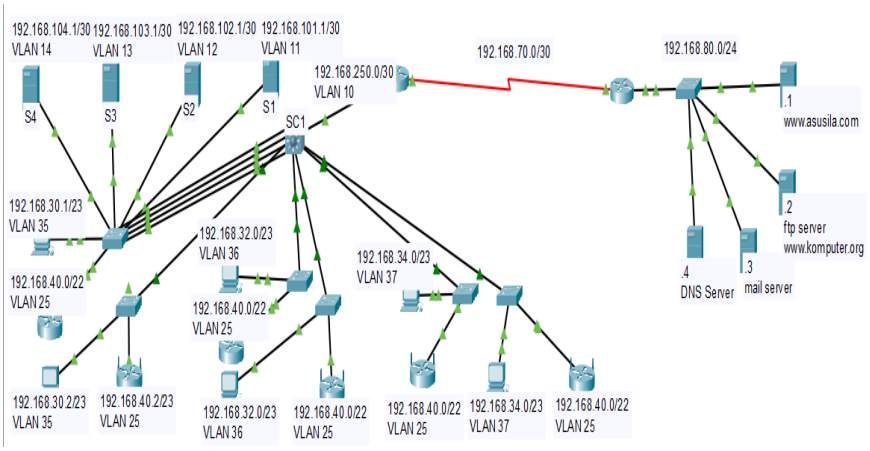
- Memfilter Pilihan IP
- Memfilter flag TCP
- Memfilter fragmen paket yang bukan awal (lihat modul “Menyempurnakan Daftar Akses IP”)
- Entri berbasis waktu (lihat "Daftar Akses Berbasis Waktu" dan modul “Menyempurnakan Daftar Akses IP”)

File Transfer Protocol

Protokol FTP adalah sebuah protocol yang menyediakan sebuah server dan client agar dapat mengirimkan file atau mengambil file dari server maupun dari client dalam sebuah jaringan computer. Dan FTP ini merupakan salah satu implementasi dari file server.Pada jaringan komputer dengan sistem ini, file ditempatkan secara terpusat sehingga apabila komputer pengguna rusak karena virus atau sebab lain, data tetap terjamin dengan aman karena disimpan di server, sehingga mengurangi faktor risiko penyalahgunaan data. Selain itu, setiap pengguna akan mendapatkan username dan password yang harus dimasukkan saat mengakses file atau data di file server.

HASIL DAN PEMBAHASAN

Untuk dapat memfilter data yang masuk maupun yang keluar dari jaringan PT Indoraya Makmur Abadi memerlukan sebuah metode *Access Control List* atau yang disebut juga dengan ACL. ACL ini merupakan sebuah feature yang terdapat dalam Router Cisco, dan dalam penelitian ini penulis mencoba mengimplementasikan ACL dengan jenis Extended dengan nomer id antara 100 sampai dengan 199. Karena dengan ACL berjenis extended firewall dapat memfilter spesifik dari data yang ingin difilternya lebih detail.



Gambar 2. Skema Usulan Jaringan PT Indoraya Makmur Abadi

Topologi jaringan yang diusulkan tidak merubah yang saat ini ada didalam jaringan PT Indoraya Makmur Abad, karena penulis mencoba lebih menggali kemampuan dari salah perangkat yang ada didalam PT Indoraya Makmur Abadi agar lebih maksimal dalam menjaga proses bisnis yang dijalankan tetap berjalan walaupun terjadi permasalahan. Pada permasalahan penulis mencoba menganalisis jika terjadi gangguan koneksi dengan terputusnya media transmisi kabel yang menghubungkan SC 2 (Switch Catalist) dengan SC 1 akan mengakibatkan koneksi untuk ke server semua perangkat jaringan yang ada di dalam PT Indoraya Makmur Abadi tidak terkoneksi. Maka diperlukan jalur koneksi satu persatu karena setiap server mempunyai jalur virtual yang berbeda satu sama lainnya. Maka penulis setiap jalur virtual Server memiliki satu buah koneksi kabel agar jika terjadi gangguan dengan terputusnya salah satu kabel tidak mengganggu koneksi ke server lainnya.

Perangkat lainnya adalah Router yang didalam topologi jaringan penulis berikan inisiasi R2 (Router 2). Hal ini bertujuan agar *router* pada jaringan *backbone* dapat menyaring

setiap paket data yang masuk maupun yang keluar dan juga dapat memblok sebuah website yang dianggap merugikan atau berbahaya jika salah client yang ada pada PT Indoraya Makmur Abadi melakukan koneksi ke website tersebut. Contohnya adalah website situs-situs porno, atau situs film yang dapat mengurangi bandwdith yang ada didalam PT Indoraya Makmur Abadi.

Pada bentuk skema jaringan yang penulis rancang, perangkat Switch Catalist (SC 2) yang menghubungkan server-server aplikasi dengan setiap server memiliki jalur virtual yang berbeda yaitu VLAN 11 untuk server 1, VLAN 12 untuk server 2, VLAN 13 untuk server 3 dan VLAN 14 untuk server 4. Penulis mencoba design dengan skema jaringan menambahkan 4 buah koneksi kabel sehingga kabel yang menghubungkan SC2 dengan SC1 sebanyak 5 koneksi kabel. 5 (lima) koneksi kebal tersebut penulis gunakan 1 koneksi sebagai jalur koneksi VLAN Client1, 1 koneksi sebagai jalur koneksi VLAN Server 1, 1 koneksi sebagai jalur koneksi VLAN Server 2, 1 koneksi sebagai jalur koneksi VLAN Server 3, 1 koneksi sebagai jalur koneksi VLAN Server 4. Dengan metode VTP Access (*Virtual Trunking Protocol*).

Selanjutnya perangkat yang dikembangkan kemampuannya adalah Router 1, pada perangkat router terdapat feature *Access Control List* (ACL). Dengan metode ACL extended penulis mencoba membangun sebuah firewall yang berguna menyaring paket data yang berada pada server yang terhubung dengan Router yang berada diseberang Router 1 (R1).

Untuk system keamanan jaringan pada PT Indoraya Makmur Abadi melakukan penambahan berupa pengaktifan firewall dengan menggunakan feature *Access Conrol List* (ACL). Dengan memfilter paket data yang dapat masuk maupun yang keluar dari jaringan PT Indoraya Makmur Abadi . Selain memfilter penulis juga menambahkan pemblokan akses internet pada sebuah situs yang dianggap merugikan (situs porno), selain itu juga penulis membatasi akses client-client yang dapat melakukan koneksi internet secara akses full atau tidak.

Implementasi firewall pada penulisan ini penulis mencoba membuat aturan dengan memblok situs asusila yang berada pada seberang Router 1. Dengan design skema Router yang berada diseberang Router 1 dianggap koneksi internet dan dibawah router tersebut terdapat beberapa server antara lain:

1. Server 1 sebagai web server dengan domain www.asusila.com dan memiliki IP Address 192.168.80.1.
2. Server 2 sebagai ftp server dan web server dengan domain www.komputer.org dan memiliki IP Address 192.168.80.2
3. Server 3 sebagai mail server dengan dan memiliki IP Address 192.168.80.3
4. Server 4 sebagai DNS server dan memiliki IP Address 192.168.80.4.

Konfigurasi pada Router 1 akan memblok situs www.asusila.com sehingga semua perangkat jaringan yang ada di dalam PT Indoraya Makmur Abadi tidak dapat melakukan koneksi ke website tersebut. ACL yang digunakan adalah jenis extended yang memiliki Id ACL 100 sampai dengan 199, dan Id ACL yang digunakan oleh penulis adalah 101. Konfigurasi Router 1 dibawah ini :

1. Konfigurasi Router 1 memblok situs www.asusila.com

   Router(config)#access-list 101 deny ip any 192.168.80.1 0.0.0.0
   Router(config)#access-list 101 permit ip any any
   Router(config)#int g0/0
   Router(config-if)#ip access-group 101 in
   Router(config-if)#exit
2. Melihat konfigurasi ACL 101 pada Router 1

   Router#show access-lists 101
   Extended IP access list 101
   deny ip any host 192.168.80.1
   permit ip any any

Didalam jaringan usulan ini penulis menganalisis ada beberapa bagian atau divisi pada PT Indoraya Makmur Abadi dapat mengakses sebuah sistem yang semestinya divisi atau bagian tersebut sebaiknya tidak boleh melakukan koneksi. Contohnya bagian divisi Marketing tidak dapat mengakses sebuah server File Transfer Protocol (FTP) yang berada pada jalur internet. Penulis menganggap ftp server ini disediakan oleh PT Indoraya Makmur Abadi untuk keperluan di lapangan. Data-data penting apa yang ada dilapangan seperti: reporting struktur tanah BTS, lokasi atau medan pemasangan BTS dan lain-lainnya. Divisi

atau bagian Marketing PT Indoraya Makmur Abadi berada pada Lantai 26 dan kebetulan segmen IP Addrees yang dimiliki client-client pada Lantai 26 adalah 192.168.32.0/22.

1. Berikut design konfigurasi usulannya :

   Router(config)#acc 101 deny ip any host 192.168.80.1

   Router(config)#acc 101 deny tcp 192.168.32.0 0.0.1.255 host 192.168.80.2 eq ftp

   Router(config)#acc 101 permit ip any any

2. Melihat konfigurasi ACL 101 pada Router 1 :

   Router(config)#do sh acc 101

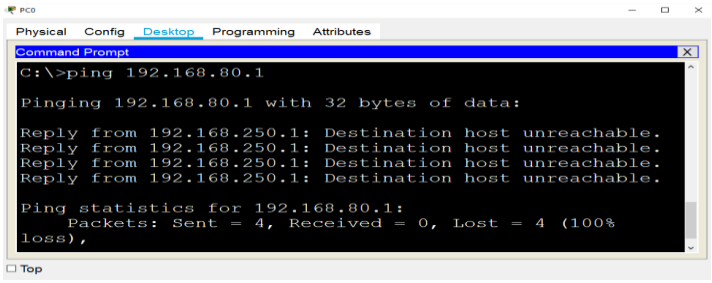
   Extended IP access list 101

   deny ip any host 192.168.80.1

   deny tcp 192.168.32.0 0.0.1.255 host 192.168.80.2 eq ftp

   permit ip any any

Implementasi firewall yang menggunakan feature *Access Control List* (ACL) pada skema jaringan pada penulisan ini berupa pemblokkan salah satu situs yang berada diseberang Router. Router dan jaringan LAN yang berada pada seberang Router PT Indoraya Makmur Abadi dianggap sebagai koneksi internet. Salah server yang berada pada jaringan LAN pada Router seberang merupakan sebuah web server dengan domain www.asusila.com dengan IP Address 192.168.80.1. Server ini yang akan diblok, sehingga semua perangkat jaringan yang ada pada PT Indoraya Makmur Abadi tidak dapat mengakses ke web server www.asusila.com. Pada pengujian ini penulis lakukan pada salah satu client yang berada pada tiap lantai PT Indoraya Makmur Abadi, lantai 25 sampai dengan lantai 27.



Gambar 3. Hasil Pengujian Client Lantai 25 Koneksi ke Web Server

Gambar 4. Hasil Pengujian Client Lantai 25 Koneksi ke Web Server

Dapat disimpulkan bahwa dengan membangun firewall menggunakan ACL pembatasan / memblok sebuah situs dapat dilakan. Pada kasus ini Web server www.asusila.com diblok semua paket data yang ada, sehingga client-client yang ada pada PT Indoraya Makmur Abadi dalam melakukan pengujian koneksi dengan menggunakan perintah ping pada command prompt hasilnya akan diblok oleh router. Begitu pula saat client-client pada PT Indoraya Makmur Abadi memanggil domain www.asusila.com dengan menggunakan aplikasi browser maka web browser tersebut akan menampilkan Request Time Out, yang berarti permintaan client-client yang berada pada lantai 25 sampai dengan lantai 27 tidak diteruskan oleh Router PT Indoraya Makmur Abadi ke Router seberang.

Di dalam PT Indoraya Makmur Abadi terdiri dari beberapa bagian atau divisi, dari bagian atau divisi kebutuhan akan adanya koneksi ke sebuah sistem berbeda-berbeda sesuai dengan kebutuhan berdasarkan tanggung jawab dari divisi atau bagian dalam perusahaan tersebut. Didalam penulisan ini penulis mengangkat akan adanya authotisasi akses sebuah sistem berkas yang berada pada koneksi internet berupa FTP server terhadap divisi atau bagian marketing. Penulis menganggap divisi atau bagian marketing ini sebaiknya tidak memerlukan akses koneksi ke FTP server, karna FTP server disediakan akan adanya kebutuhan dokumen-dokumen lapangan dalam pemasangan, pengorganisasian, perbaikan BTS (*Base Transceiver Station*). Pada skema jaringan client-client yang digunakan oleh divisi atau bagian marketing terdapat pada lantau 26 dengan segment IP address 192.168.32.0/22. Sedangkan FTP server berada pada jaringan LAN Router seberang dengan IP address 192.168.80.2/24. Disini penulis hanya memfilter paket data FTP (*File Transfer Protocol*) saja, sedangkan paket-paket data lainnya pada FTP server tidak difilter.

Didalam pengujian ini penulis akan melakukan pengujian koneksi dan memanggil ftp server pada client-client setiap lantai 25 sampai dengan lantai 27 pada PT Indoraya Makmur Abadi.

KESIMPULAN DAN REKOMENDASI

Berdasarkan Kesimpulan yang didapatkan pada penelitian ini adalah :

1. Dengan mengaktifkan firewall menggunakan feature Access Control List (ACL) dapat digunakan untuk memblok situs yang dianggap tidak ada relevansi dengan kebutuhan kerja dari perusahaan, dan pada pemblokan ini menggunakan ip address yang dimiliki oleh situs tersebut.
2. Dengan lebih mengoptimalkan ACL dapat membuat hak akses pada sebuah sistem yang terhubung pada internet sebagai pemfilter divisi-divisi dalam menentukan keabsahan client-client yang koneksi ke ftp server. Jadi sistem hanya dapat diakses pada client-client yang membutuhkan sistem tersebut.

REFERENSI

Andri, Gunawan I, Kirana IO. Optimasi Sistem Keamanan Jaringan Komputer Terhadap Serangan Malware Menggunakan Filtering Firewall dengan Metode Port Blocking. JOMLAI J Mach Learn Artif Intell [Internet]. 2022;1(2):2828–9099. Available from: https://journal.literasisains.id/index.php/jomlai/

Alfred, Chandra JC. (2018). Pemanfaatan Firewall pada Jaringan Komputer SMK Fadilah. JIDEALIS[Internet].;1(5):422–8. Available from: http://jom.fti.budiluhur.ac.id/index.php/IDEALIS/article/download/1037/263

Akbar, KN (2021). Implementasi Port Knocking, Firewall, dan Fail2ban Sebagai Keamanan Data pada FTP Server Berbasiskan Centos7., digilib.yarsi.ac.id, http://digilib.yarsi.ac.id/9474/

Bringhenti, D, Marchetto, G, Sisto, R, & ... (2022). Automated firewall configuration in virtual networks. *... on Dependable and ...*, ieeexplore.ieee.org, https://ieeexplore.ieee.org/abstract/document/9737389/

Cybellium. Mastering Firewall. Leicestershire: Cybellium Ltd; 2023. 1–186 p.

Evans, C (2021). Vsftpd: Probably the most secure and fastest ftp server for unix-like systems. *URL: http://vsftpd. beasts. org*

Gunda, LV, Poon, A, & Jayant, J (2020). Performing appID based firewall services on a host. *US Patent 10,812,451*, Google Patents,

https://patents.google.com/patent/US10812451B2/en

Hidayat A., S. (2017). Wildcard Mask Sebagai Filtering IP Address Menggunakan Metode Access List ControlpPada Router Cisco. J Tek Komput Amik BSI [Internet]; III(1):60–73. Available from: https://ejournal.bsi.ac.id/ejurnal/index.php/jtk/article/view/1344/1093

Hidayat AS, Nuryadi N, Handono FW. (2023). Pemanfaatan Router Modem Wireles Bekas Sebagai Jaringan Dalam Penyedian Backup Storage Smartphone Secara Offline. INTECOMS J Inf Technol Comput Sci.;6(1):470–8.

Iwan S. (2017). Jaringan Komputer Berbasis MikroTik. Jaringan Komputer. Bandung: Informatika Bandung; 2017. 1–405 p.

Jose S. (2015). Security Configuration Guide: Access Control Lists, Cisco IOS XE Release [Internet]. Release 3S. Cisco System I, editor. San Jose, California: Cisco System, Inc; 1–255 p. Available from: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_data_acl/configuration/xe-3s/sec-data-acl-xe-3s-book.pdf

Khadafi, S, Pratiwi, YD, & Alfianto, E (2021). Keamanan Ftp Server Berbasiskan Ids Dan Ips Menggunakan Sistem Operasi Linux Ubuntu. *Network Engineering Research …*, academia.edu, https://www.academia.edu/download/78082743/157.pdf

Pastima Simanjuntak, Cosmas Eko Suharyanto J. (2019). Analisis Penggunaan Access Control List (Acl) Dalam Jaringan Komputer di Kawasan Batamindo Industrial Park Batam; 2(2):122–8.

Sulistyo HW, Oktavianto H. (2020). Perancangan Dan Implementasi File Sharing. J Apl Sist Inf Dan Elektron;2(1):24–30.

Tudosi, AD, Graur, A, Balan, DG, & Potorac, AD (2023). Research on Security Weakness Using Penetration Testing in a Distributed Firewall. *Sensors*, mdpi.com, https://www.mdpi.com/1424-8220/23/5/2683