Volume II Nomor 2, Februari 2007 ISSN 1858 - 2109

e-link

Jurnal Teknik Elektro dan Informatika

Diterbitkan Oleh :
Program Studi Teknik Elektro dan Teknik Informatika
Universitas Muhammadiyah Gresik

ISSN 1858 - 2109

e– link

Jurnal Teknik Elektro & Informatika

Diterbitkan Oleh : Program Studi Teknik Elektro dan Teknik Informatika
Universitas Muhammadiyah Gresik

Alamat Redaksi :

e– link Jurnal Teknik Elektro & Informatika
Program Studi Teknik Elektro dan Teknik Informatika
Universitas Muhammadiyah Gresik
Jl. Sumatra 101 GKB Gresik 61121 – Indonesia
Tel. 6231 3951414 ; Fax. 6231 3952585
E-mail : e-link@umg.ac.id
Website : www.umg.ac.id

diterbitkan tiap enam bulan sekali (Februari – Agustus)

Vol. II Nomor 2, Februari 2007 ISSN 1858 - 2109

e-link

Jurnal Teknik Elektro & Informatika

DAFTAR ISI **Hal.**

e – link
Jurnal Teknik Elektro & Informatika

ISSN 1858 - 2109

PENGAMANAN SISTEM JARINGAN KOMPUTER PADA ROUTER CISCO 2611 DENGAN MENGGUNAKAN ACCESS-LIST

Harunur Rosyid
Yogi Sucahyo

Program Studi Teknik Informatika-Univ. Muhammadiyah Gresik
PT. Cipta Nirmala Gresik

Abstrak

Sistem jaringan computer berfungsi untuk mengintegrasikan dan mengorganisasi data dari cabang sampai ke server pusat menjadi suatu keharusan, tetapi keamanan jaringan kurang optimal sehingga sangat rawan terhadap akses data dari orang yang tidak berhak dan rawan terhadap serangan virus.Untuk mengoptimalkan keamanan jaringan komputer maka perlu dilakukan seting konfigurasi router sesuai dengan daftar akses.

Salah satu fitur Router Cisco adalah kemampuannya dalam meneruskan atau menolak suatu paket yang melewati router. Sehingga dengan fitur tersebut router tidak hanya berfungsi sebagai penghubung antar jaringan, tetapi dapat berfungsi sebagai pengaman atau pagar dari jaringan. Dapat dibuat skenario alternatif pengamanan sistem jaringan komputer dengan menerapkan hak akses bagi komputer dengan menggunakan Daftar akses IP Standar (Standar IP Access List) dan menerapkan hak akses bagi komputer dengan menggunakan Daftar akses IP Extended (Extended IP Access List).

Kondisi riil jaringan komputer sangat rawan, yaitu daftar akses pada router belum dikonfigurasi, sehingga seluruh IP bisa mengakses ke jaringan. Hal ini sangat berbahaya karena orang yang tidak berhak bisa masuk ke jaringan.Dengan mengimplementasikan daftar akses pada router, maka hanya IP yang diinginkan saja yang bisa mengakses ke jaringan sesuai dengan hak nya.

Kata Kunci : access-list, IP Address, Router Cisco.

A. PENDAHULUAN

Penggunaan alat bantu komputer (*computerized*) sebagai pendukung dalam sistem informasi sudah merupakan kebutuhan mutlak. Banyak manfaat yang dapat dirasakan, antara lain pengorganisasian data, kecepatan dalam pembuatan laporan, dan lain lain yang akan berdampak pada efisiensi dan efektifitas perusahaan.

Jaringan komputer merupakan komponen utama dalam sistem komputerisasi. Salah satu fungsi jaringan komputer adalah menyampaikan informasi atau data antar komputer. Jaringan komputer dapatlah diibaratkan sebuah rumah dengan pintunya, apabila pintu tidak dikunci maka orang âkan bebas keluar masuk ke rumah tersebut. Apa yang akan terjadi jika data yang bersifat rahasia akan dibaca oleh orang yang tidak berhak.

Untuk menghindari penggunaan jaringan oleh orang yang tidak berhak, maka harus ada upaya pengamanan jaringan. Pengamanan jaringan dapat berupa daftar akses, yaitu hanya ketentuan yang ada pada tabel akses yang berlaku yaitu mengijinkan (*permit*) atau menolak (*deny*) terhadap akses ke suatu *port* dan *interface* tertentu pada router.

B. MAKSUD DAN TUJUAN PENELITIAN

Adapun maksud dan tujuan pada penelitian ini adalah :

1. Merancang dan menerapkan fitur daftar akses *(access-list)* pada Router Cisco 2611 untuk memberikan hak akses bagi komputer dari luar jaringan mengakses kedalam jaringan lokal (LAN) kantor pusat.
2. Merancang dan menerapkan fitur daftar akses *(access-list)* pada Router Cisco 2611 untuk memberikan hak akses bagi komputer dari jaringan kantor pusat yang mengakses keluar jaringan lokal (LAN) kantor pusat.
3. Menerapkan sistem keamanan jaringan pada Router Cisco 2611

C. RUANG LINGKUP MASALAH

Adapun ruang lingkup masalah pada penelitian dibatasi pada Penerapan pengamanan jaringan dengan menggunakan daftar akses *(access-list)* ini, menggunakan Router Cisco 2611 dan *IP Address* dalam penulisan ini dalam bentuk fiktif, serta tidak membahas aspek pemilihan jenis *software* maupun *hardware*. Penelitihan dilakukan di PT. Cipta Nirmala Gresik.

D. METODE PENELITIAN

Metode penelitian yang dilakukan agar dapat lebih terarah dan mendapatkan hasil yang diinginkan, adalah sebagai berikut :

1. Asumsi-asumsi, ada beberapa asumsi yang digunakan untuk membantu memecahkan masalah yang berkaitan dengan pengumpulan data yaitu :

   Jaringan dalam kondisi baik, tidak ada kerusakan dari sisi *hardware* maupun *software*. Gangguan dari petir dapat ditanggulangi dengan memasang peralatan anti petir, Gangguan dari virus dapat ditanggulangi dengan memasang *software* antivirus, *Password* untuk dial dilakukan penggantian setiap bulan, dan Seluruh perangkat jaringan menggunakan tegangan yang berasal dari UPS dan sudah menggunakan *grounding*.
2. Secara operasional, dilakukan pengolahan data yang diperoleh dari hasil studi sebagai dasar penerapan keamanan jaringan yang sesuai, dengan langkah-langkah sebagai berikut:
   a. Memetakan IP Address mana yang dimasukkan dalam daftar akses *(access-list)*.
   b. Melakukan konfigurasi *access-list* sesuai dengan data pada pemetaan IP address.
   c. Melakukan pengujian dari hasil konfigurasi

E. TINJAUAN PUSTAKA

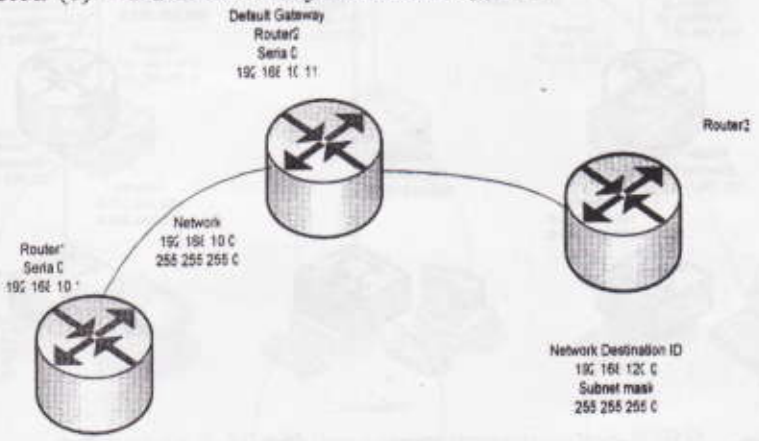
Protokol Routing Pada Router Cisco

A. *Static routing*

Berguna untuk jaringan sederhana yang hanya menggunakan beberapa router dan juga untuk menghemat penggunaan bandwitdth. *Static routing* dibuat dengan cara manual, dengan cara mengetik perintah-perintah tertentu untuk membuat tabel routing. *IP Routing* selalu ditetapkan (enable) untuk Cisco Router, sehingga untuk membuat IP static routing cukup dengan mengetik perintah [Wijaya, 2004]:

```
Router(config)# ip route <network destination id> <subnet mask>
<default gateway> <administrative distance>
```

1. *Network destination ID* adalah alamat jaringan yang dituju.
2. *Subnet Mask* adalah subnet mask dari jaringan yang dituju.
3. *Default Gateway* adalah IP Address gateway, biasanya IP Address Router yang berhubungan langsung.
4. *Administratif distance* adalah nilai 0 – 255 yang diberikan pada routing. Bertambah rendah nilai yang diberikan bertambah tinggi kegunaannya. Jika nilai tidak diberikan, nilai default akan dipakai. Nilai default untuk *directly connected* (c) = 0 dan *statically connected* (s) = 1.



Gambar 1. IP routing

Cara membuat *static routing* untuk *router1* dengan *network destination* ID 192.168.120.0 dan subnet mask 255.255.255.0 adalah dengan mengetik perintah :

```
Router1(config)#ip route 192.168.120.0  255.255.255.0  192.168.10.11
```

Default Routing dan IP Classless

Default Routing dibuat agar ketika router menerima paket yang mempunyai alamat tujuan yang tidak dikenalnya, maka paket tersebut disalurkan lewat *default routing*. Cara membuat default routing adalah mirip dengan membuat static routing hanya destination network ID dan subnet mask nya diberi nilai 0.0.0.0 dan 0.0.0.0 [Sarjono, 2003] seperti dibawah ini: `Router1(config)#ip route 0.0.0.0  0.0.0.0 <default gateway>`

Setelah itu, konfigurasi dari default routing dapat diperiksa dengan perintah show ip route sebagai berikut : `Router1#show ip route`

Cisco Router dapat memilihkan jalur untuk paket yang tak dikenal tujuannya secara otomatis yaitu dengan syntax sebagai berikut : `Router1(config)#ip classless`

B. ***Dinamic routing*** adalah membuat suatu tabel *routing* secara dinamis berubah-ubah secara otomatis jika topologi jaringan berubah. Dinamic routing menggunakan protokol routing di dalam pembuatan tabel routing. [Wijaya, 2004]

Routing Information Protocol (RIP)

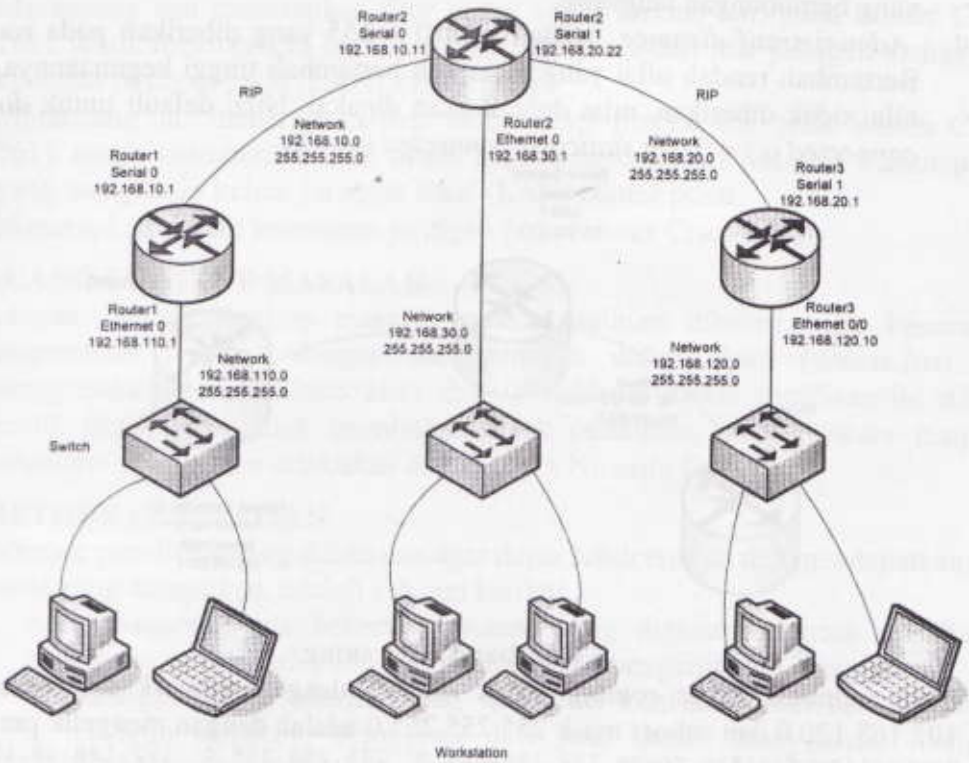
Routing Information Protocol (RIP) adalah routing protokol yang paling sederhana yang termasuk jenis *distance vector*. RIP menggunakan jumlah lompatan (*hop count*) sebagai *metric* dengan 15 hop maksimum. Jadi, *hop count* yang ke -16 tidak dapat tercapai dan router akan memberikan *error message* "*destination is unreachable* (tujuan tidak tercapai)". Daftar tabel routing protocol RIP di update setiap 30 detik sedangkan default *administrative distance* untuk RIP adalah 120. [Sarjono, 2003]

Untuk menerapkan RIP ke suatu router, ketik :

```
Router1(config)#router rip
```

Untuk menerapkan RIP tersebut kesuatu *network address*, ketik :

```
Router1(config-router)#network <network ID>
```



Gambar 2. WAN dengan mempergunakan RIP

Interior Gateway Routing Protocol (IGRP)

Interior Gateway Routing Protocol (IGRP) adalah jenis protocol distance vector yang diciptakan oleh perusahaan Cisco untuk mengatasi kekurangan-kekurangan protocol RIP. Jumlah hop maksimum menjadi 255 dan sebagai metric IGRP menggunakan bandwidth, MTU, Delay and Load. IGRP adalah protocol routing yang menggunakan autonomous system (AS). Dan dapat menentukan *routing* berdasarkan system, *interior* dan *exterior*. Sedangkan default *administrative distance* untuk IGRP adalah 100.

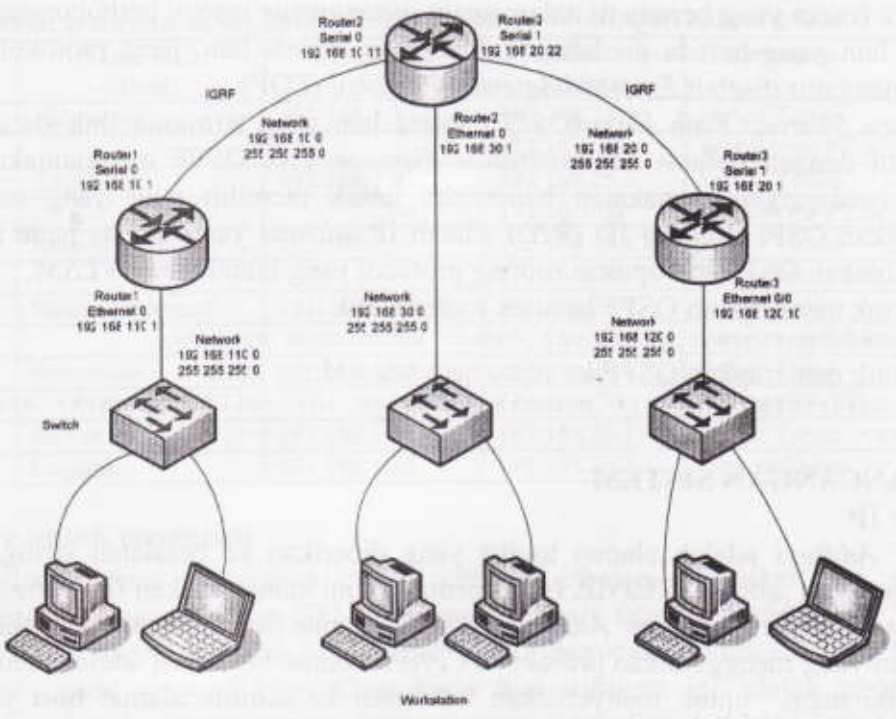
Autonomous System (AS) adalah koleksi sejumlah router yang berada dibawah satu naungan manajemen bersama yang dapat saling menukar informasi. [Sarjono, 2003]

Untuk menerapkan *IGRP* ke suatu *ROUTER*, ketik :

```
Router1(config)#router igrp <nomor autonomous system>
```

Untuk menentukan IGRP tersebut sesuatu *network address*, ketik :

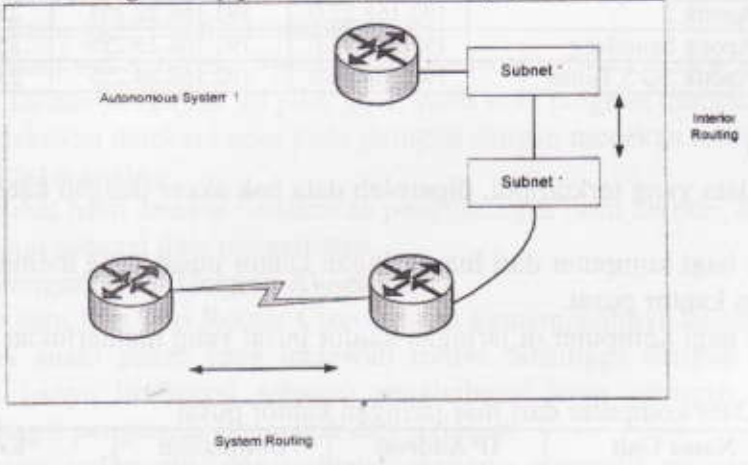
```
Router1(config-router)#network <network ID>
```



Gambar 3. WAN dengan mempergunakan IGRP

Protokol-protokol routing lanjutan

EIGRP (Enhanced Interior Gateway Protocol) adalah protokol lain yang juga diciptakan oleh perusahaan Cisco. Protokol ini mempunyai keunggulan, karena hanya mengirim update jika ada perubahan, sedangkan default *administrative distance* nya adalah 90. Router-router yang berada di dalam suatu *autonomous system* disebut *interior gateway protocol* (IGP) [Wijaya, 2004]



Gambar 4. System dan Interior Routing

Routing didalam 1 subnet dengan *autonomous* system yang sama disebut system routing. Sedangkan routing diantara 2 subnet yang berlainan dengan autonomous system yang sama disebut *interior routing*.

Untuk menerapkan EIGRP ke suatu router, ketik :

```
Router(config)#router eigrp <nomor autonomous system>
```

Untuk menerapkan EIGRP tersebut ke suatu network address, ketik :

```
Router(config-router)#network <network id>
```

Jika router yang berada di dalam suatu *autonomous system* berhubungan dengan router lain yang berada di dalam *autonomous system* lain, jenis protokol *routing* yang mengatur disebut *Exterior Gateway Protokol* (EGP)

Open Shortest Path First (OSPF) antara lain yang termasuk link state routing protokol dengan default *administrative distance* 110. OSPF menggunakan biaya (cost) berdasarkan pemakaian bandwidth untuk memilih jalur yang tersingkat. Sedangkan OSPF *routing* ID (RID) adalah IP *address* yang teratas pada interface yang dipakai. OSPF merupakan routing protocol yang mendukung VLSM.

Untuk menerapkan OSPF kesuatu router, ketik :

```
Router(config)# router ospf <nomor autonomous system>
```

Untuk menerapkan OSPF ke suatu network address ketik :

```
Router(config-router)# network <network id> <wildcard mask> area <no area>
```

F. RANCANGAN SISTEM

Daftar IP

IP Address adalah alamat logika yang diberikan ke peralatan jaringan yang menggunakan protokol TCP/IP. (pada penulisan ini kami gunakan *IP Address* fiktif) Alamat jaringan (*Network Address*) adalah alamat logika yang mewakili suatu jaringan yang menggunakan protokol TCP/IP. Alamat broadcast adalah alamat yang memiliki tugas untuk menyebarkan informasi ke seluruh alamat host yang ada dijaringan tersebut (*broadcasting*). Jika ada data yang ditujukan ke alamat broadcast ini, maka semua host yang ada di jaringan akan mendapatkannya juga, seperti pada Table 4.

Tabel 4. Data alamat jaringan dan broadcast

No	LAN	Network Address	Broadcast Address	Subnet Mask
1	LAN Kantor Pusat	192.168.1.0	192.168.1.255	255.255.255.0
2	LAN Apotik 1	192.168.21.0	192.168.21.255	255.255.255.0
3	LAN Apotik 2	192.168.22.0	192.168.22.255	255.255.255.0
4	LAN Apotik Sentolang	192.168.23.0	192.168.23.255	255.255.255.0
5	LAN Apotik SG 3 Tuban	192.168.24.0	192.168.24.255	255.255.255.0

Daftar Akses

Berdasarkan data yang terkumpul, diperoleh data hak akses dengan kategori sebagai berikut :

1. Hak akses bagi komputer dari luar jaringan kantor pusat yang memerlukan akses ke jaringan kantor pusat.
2. Hak akses bagi komputer di jaringan kantor pusat yang memerlukan akses keluar jaringan.

Tabel 5. Data komputer dari luar jaringan kantor pusat

No	Nama Unit	IP Address	Destination Address	Keterangan
1	WebServer intranet PT. SG (lalu lintas www, ftp)	172.16.1.20	192.168.1.3	Akuntansi
			192.168.1.9	Keuangan
			192.168.1.17	Rekam Medik
			192.168.1.55	Sarana Informasi
			192.168.1.67	Personalia

Tabel 6. Data hak akses keluar bagi komputer di jaringan kantor pusat

No	Nama Unit (client)	IP Address	Destination Address	Keterangan
1	Akuntansi	192.168.1.3	192.168.25.1	Server Tuban
			172.16.1.20	WebServer PT.SG
2	Keuangan	192.168.1.9	192.168.25.1	Server Tuban
			172.16.1.20	WebServer PT.SG
3	Rekam Medik	192.168.1.17	192.168.25.1	Server Tuban
			172.16.1.20	WebServer PT.SG
4	Sarana Informasi	192.168.1.55	192.168.25.1	Server Tuban
			172.16.1.20	WebServer PT.SG
5	Personalia	192.168.1.67	192.168.25.1,	Server Tuban
			172.16.1.20	Intranet PT. SG
6	Server Pusat	192.168.1.1	192.168.25.1,	Server Tuban
7	Logistik	192.168.1.45	192.168.25.1,	Server Tuban

Software untuk pengujian

Software yang digunakan untuk menguji sebelum perbaikan dan setelah perbaikan pengamanan adalah GFI LANguard Network Scanner Versi 2.0.

GFI LANguard Network Scanner Versi 2.0. merupakan software yang bisa di download pada www.gfi.com. Cara kerja dari software ini adalah melakukan deteksi (scan) pada network sesuai dengan range , kemudian dari hasil scan tersebut akan menghasilkan laporan / report detail dari komputer yang terdeteksi.

Langkah-langkah pengujian dengan menggunakan GFI LANguard Network Scanner adalah :

1. Pilih File > New scan
2. Isikan range IP address yang akan di deteksi, ada tiga pilihan yaitu :
   1.*Scan one computer* : Melakukan deteksi untuk satu buah komputer
   2.*Scan range of computer* : Melakukan deteksi komputer sesuai dengan batas yang telah ditentukan
   3.*Scan local network* : Melakukan scan local network atau scan per kelas.
   Dalam pengujian ini pilih no 2, yaitu scan range of computer.
3. Melakukan deteksi / scan pada jaringan dengan menekan tombol / toolbar > Start scanning
4. Melihat hasil deteksi : dilakukan penghitungan hasil deteksi, kemudian dicatat sebagai data pengamatan.

Perbaikan Pengamanan Dengan Akses List

Salah satu fitur dari Router Cisco adalah kemampuannya dalam meneruskan atau menolak suatu paket yang melewati router. Sehingga dengan fitur tersebut router tidak hanya berfungsi sebagai penghubung antar jaringan, tetapi dapat berfungsi sebagai pengaman atau pagar dari jaringan.

Dari data yang terkumpul, dapat dibuat skenario alternatif pengamanan sistem jaringan komputer yaitu :

1. Skenario 1 : Menerapkan hak akses bagi komputer dengan menggunakan Daftar akses IP Standar (*Standar IP Access List*)
2. Skenario 2 : Menerapkan hak akses bagi komputer dengan menggunakan Daftar akses IP Extended (*Extended IP Access List*)

Sebelum melakukan konfigurasi terlebih dahulu harus melakukan telnet ke router sampai dengan router dalam keadaan prompt seperti dibawah ini :

Router1#

Menerapkan hak akses bagi komputer dengan menggunakan Daftar Akses IP Standar (Standar IP Access List)

A. Memberikan ijin bagi komputer dari luar jaringan untuk mengakses ke dalam jaringan kantor pusat.

1. Memberikan ijin akses bagi client dari web server Penerapan :

```
Router1(config)#access-list 1 permit host 172.16.1.20
Router1(config)#access-list 1 permit host 192.168.25.1
Router1(config)#access-list 1 permit host 192.168.25.2
Router1(config)#^Z
```

2. Menerapkan daftar akses list 1 ke interface Serial0/0 in

```
Router1(config)#int Serial0/0
Router1(config-if)#ip access-group 1 in
Router1(config-if)#^Z
```

A. Memberikan ijin bagi komputer dari jaringan kantor pusat untuk mengakses ke luar jaringan, Penerapan :

1. Memberikan ijin akses bagi client Penerapan :

```
Router1(config)#access-list 2 permit host 192.168.1.3
Router1(config)#access-list 2 permit host 192.168.1.9
Router1(config)#access-list 2 permit host 192.168.1.17
Router1(config)#access-list 2 permit host 192.168.1.55
Router1(config)#access-list 2 permit host 192.168.1.67
Router1(config)#access-list 2 permit host 192.168.1.1
Router1(config)#access-list 2 permit host 192.168.1.45
```

2. Menerapkan daftar akses list 2 ke interface Serial0/0 out

```
Router1(config)#int Serial0/0
Router1(config-if)#ip access-group 2 out
Router1(config-if)#^Z
```

G. PENGUJIAN SISTEM

A. Pengujian terhadap pendeteksian : yaitu untuk melihat apakah komputer dapat digunakan sesuai dengan yang diharapkan.

Tabel 7. Hasil pengujian pendeteksian jika menggunakan akses list ip extended

No	Lokasi Pengujian	Hasil deteksi	Keterangan
1	192.168.1.3, 192.168.1.9, 192.168.1.17, 192.168.1.55, 192.168.1.67, 192.168.1.1,	-	Tidak bisa mendeteksi komputer dari luar jaringan
2	Komputer Diluar *access-list 2* 192.168.1.23 192.168.1.24 192.168.1.25 192.168.1.18 192.168.1.10	-	Tidak bisa mendeteksi komputer dari luar jaringan

B. Pengujian dengan pendeteksian : Melakukan pendeteksian dengan software GFI LANguard Network Scanning V.2.0.

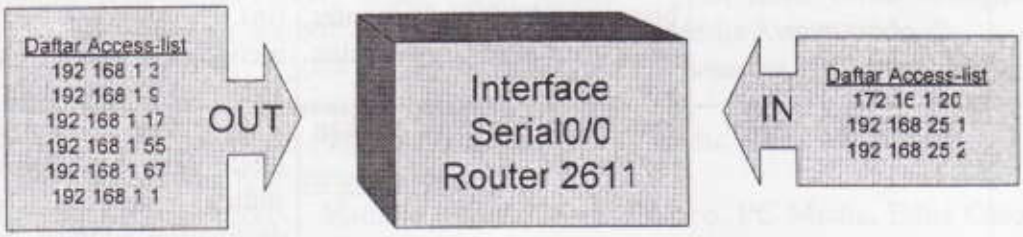
Tabel 8. Hasil pengujian pendeteksian jika menggunakan akses list ip standar

No	Lokasi Pengujian	Hasil deteksi	Keterangan
1	192.168.1.3, 192.168.1.9, 192.168.1.17, 192.168.1.55, 192.168.1.67, 192.168.1.1,	172.16.1.20, 192.168.25.1, 192.168.25.2	Bisa mendeteksi adanya IP address sesuai dengan *access-list 1*
2	Komputer Diluar *access-list 2* 192.168.1.23 192.168.1.24 192.168.1.25 192.168.1.18 192.168.1.10		Tidak bisa mendeteksi komputer dari luar jaringan

Kondisi Penerapan Skenario 1 Pengamanan dengan menggunakan Daftar Akses IP Standar (Standar IP Access-list)

Dengan menerapkan Daftar Akses IP Standar, akses keluar dan akses ke dalam LAN Kantor Pusat dapat dibatasi. Setiap interface hanya bisa berisi 2 (dua) grup akses list yaitu in dan out. Penerapan daftar akses IP Standar ini terdiri dari 2 grup yaitu grup1 dan grup 2 yang terletak pada interface serial0/0.

- Grup Akses 1 (in) terdiri dari : Web server PT. Semen Gresik (172.16.1.20) dan Server BP/RB Bogorejo Tuban (192.168.25.1)
- Grup akses 2 (out) terdiri dari : Akuntansi (192.168.1.3), Keuangan (192.168.1.9), Rekam Medik (192.168.1.17), Sarana Informasi (192.168.1.55), Personalia (192.168.1.67), Server Pusat (192.168.1.1) dan Logistik (192.168.1.45)



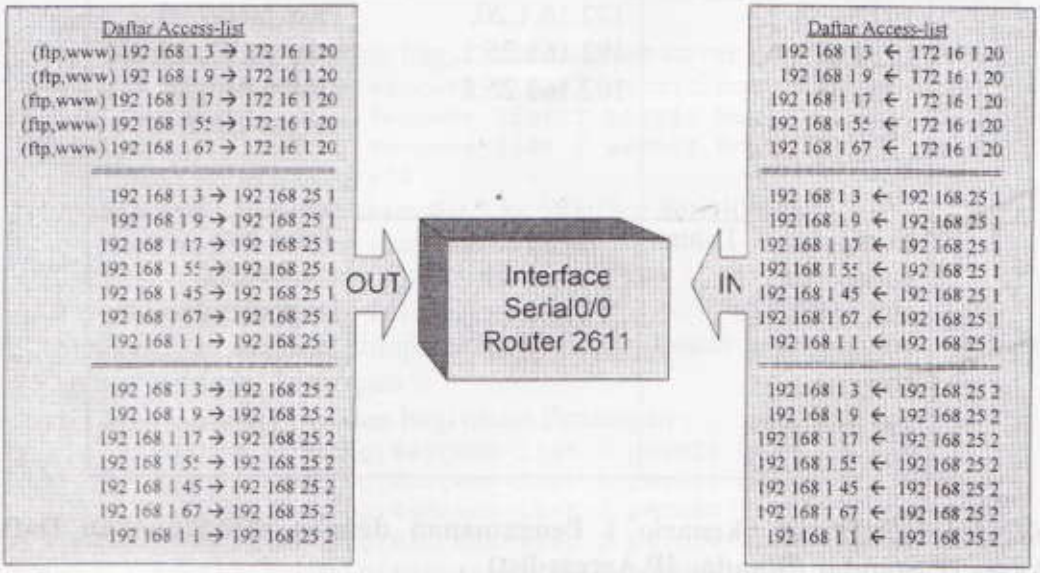
Gambar 5. Skenario 1 Daftar Akses List dengan menggunakan IP Akses

Kondisi Penerapan Skenario 2 Pengamanan dengan menggunakan Daftar Akses IP Extended (Extended IP Access-list)

Dengan menerapkan Daftar Akses IP Extended, akses keluar dan akses ke dalam LAN Kantor Pusat dapat dibatasi. Daftar Akses IP Extended memiliki lebih banyak parameter yang dapat diatur. Penerapan daftar akses IP Standar ini terdiri dari 2 grup yaitu grup100 (in) dan grup 101 (out) yang terletak pada interface serial0/0.

Berbeda dengan Daftar Akses IP Standar, pada Daftar Akses IP Extended ini terdapat parameter protokol (TCP, UDP, ICMP), Source Address, Destination Address, Operator(eq,lt, gt), dan port (nomor port, dns, ftp, www, telnet, smtp, dll).

Penggunaan Daftar Akses IP Extended untuk jaringan yang memerlukan pengamanan yang kompleks sangat tepat, karena kemampuannya dalam membatasi komputer sampai dengan level protokol, dan port.



Gambar 6. Skenario 2 Daftar Akses List dengan menggunakan IP Akses Extended

Perbandingan antara skenario 1 dan skenario 2

Dari hasil pengujian, dapat dibuktikan bahwa penggunaan daftar akses (*access-list*) dapat membatasi akses lalu lintas data yang melewati router, sehingga pengamanan jaringan dari akses ilegal dapat di hindari.

Tabel 9. Rekap Perbandingan skenario 1 dan skenario 2

No	Keterangan	Skenario 1 (Standar IP Access-List)	Skenario 2 (Extended IP Access-List)
1	Pendeteksian	Anggota grup akses 1 (in) bisa mendeteksi komputer pada grup akses 2 (out) dan sebaliknya	Anggota grup akses 100 (in) tidak bisa mendeteksi grup akses 101 (out) dan sebaliknya.
2	Hak Akses Koneksi	Hak akses hanya di berikan per group	Hak akses mengatur lebih detil ke protokol, source address dan destination address, serta informasi port
3	Seting Konfigurasi	Seting konfigurasi sederhana	Seting konfigurasi yang lebih rumit / kompleks

Dari tabel tersebut diatas, dapat disimpulkan bahwa penerapan pengamanan dengan menggunakan skenario 2 lebih tepat dibandingkan skenario 1.

H. PENUTUP

1. Merancang keamanan jaringan berbasis komputer haruslah memperhatikan beberapa aspek dibawah ini :
   a. Konsep lapisan jaringan model OSI maupun DOD, memahami fungsi perangkat yang bisa memberikan kontribusi pengamanan terhadap jaringan pada level lapisan jaringan tertentu.
   b. Topologi Jaringan, yaitu denah dimana komputer dan perangkat jaringan dihubungkan.
   c. Penerapan hak akses dari luar maupun dari dalam jaringan
2. Router memiliki intelegensi untuk membuat keputusan dalam menentukan jalur yang terbaik untuk mengirim data. Dalam dunia jaringan, terdapat dua model pengalamatan, yaitu *MAC address* yang merupakan alamat *data link layer* (*Layer 2*) dan alamat *network layer (Layer 3*) model OSI. Contoh alamat *Layer 3* adalah alamat IP, *Router* merupakan perangkat *internetworking* yang meneruskan paket data antar jaringan, berdasarkan alamat *Layer 3*.
3. Router Cisco 2611, merupakan router yang diproduksi oleh Cisco Corporation yang mempunyai beragam fasilitas / fungsi, selain fungsi utamanya sebagai perangkat yang bertugas meneruskan paket data antar jaringan. Salah satu kelebihan dari Router Cisco 2611 adalah fitur akses list (*access-list*) yaitu menggunakan suatu metode yang disebut "*packet filter*" untuk mengatur ijin-ijin akses lalu lintas data lewat router.
4. Dari hasil pengujian, dapat dibuktikan bahwa penggunaan daftar akses (*access-list*) dapat membatasi akses lalu lintas data yang melewati router, sehingga pengamanan jaringan dari akses ilegal dapat di hindari.

I. DAFTAR PUSTAKA

Hendra Wijaya, Ir. (2004). *Buku Cisco Router – Edisi Baru Untuk Mengambil Sertifikat CCNA(640-801)*. Jakarta : PT. Elex Media Komputindo.

Vincent Bayu T.B. (2004). *Seri Jaringan dan Keamanan*. PC Plus Edisi 26 Oktober – 01 November, halaman 7.

Hayri. (2003). *IP Angka Penting Dunia Maya.* PC Media, Edisi Maret.

Cisco Corporation, http://www.cisco.com

Gunung Sarjono. (2003). *Melihat Model Jaringan Cisco.* PC Media, Edisi Oktober 2003, halaman 78 – 79.

Hayri. (2004). *Menjadi Penguasa Jaringan Rumah Anda.* PC Media, Edisi Oktober 2004, halaman 72 – 73.

Gunung Sarjono. (2003). *Memahami Konsep Jaringan.* PC Media, Edisi November 2003, halaman 80 – 82.

Gunung Sarjono. (2003). *Menangani Masalah Jaringan dengan Tool TCP/IP.* PC Media, Edisi Juni 2003, halaman 74 – 76

Gunung Sarjono. (2003). *Mengenal Switch LAN.* PC Media, Edisi April 2003.

Hayri. (2002). *Berkenalan dengan Jaringan Komputer.* PC Media, Edisi Desember 2002, halaman 96 – 99

Hayri. (2005). *Wide Area Network, Jalur Panjang Data Anda.* PC Media, Edisi Juli 2005, halaman 78 – 82