ISSN 1979-8555

JURNAL
TELEMATIK
VOLUME 2 NOMOR 3 JULI 2010

Kata Pengantar

Assalamu'alaikum Warahmatullahi Wabarakatuh

Puji dan syukur atas kehadirat Allah SWT, karena atas Rahmat dan HidayahNya, Jurnal Ilmiah Volume 2 Nomor 3 Bulan Juli Tahun 2010 ini dapat diterbitkan. Jurnal Ilmiah ini bernama Telematik yang berarti ***T***eknik ***ELE***ktro, teknik infor***MA***Tika, s***I***stem informasi dan ***K***omputer akuntansi yang diterbitkan oleh Fakultas Teknik Universitas Muhammadiyah Bengkulu.

Dengan diterbitkannya Jurnal Ilmiah Telematik ini diharapkan dapat bermanfaat dalam perkembangan Ilmu Pengetahuan dan Teknologi. Berkenaan dengan harapan tersebut kepada para peneliti produktif dan staf pengajar yang memiliki hasil-hasil penelitian untuk dapat kiranya mengirimkan naskah ringkasannya untuk dimuat pada Jurnal Ilmiah Telematik ini dengan mengikuti ketentuan sebagaimana yang telah ditetapkan oleh pihak dewan redaksi.

Akhirnya tak lupa kami mengucapkan banyak terima kasih kepada semua pihak yang telah membantu penerbitan Jurnal Ilmiah Telematik ini.

Wasalamu'alaikum Warahmatullahi Wabarakatuh

Bengkulu, Juli 2010

Dewan Redaksi

ISSN 1979-8555

JURNAL
TELEMATIK
VOLUME 2 NOMOR 3 JULI 2010

Visi
Sebagai media yang dapat memberikan
Sumbangan terhadap perkembangan Ilmu Pengetahuan dan Teknologi

Misi
Dapat menyumbangkan dan menyebarkan berupa Hasil penelitian (*research*) Maupun hasil kajian, Pendapat dan pemikiran dalam bidang Ilmu Pengetahuan dan Teknologi

Penerbit
Fakultas Teknik
Universitas Muhammadiyah Bengkulu

Alamat Redaksi
Fakultas Teknik
Universitas Muhammadiyah Bengkulu
Jl. Bali Po. Box 118 Bengkulu
Telp. 0736-22765, Fax. 0736-26161

Frekuensi Terbit
4(Empat) kali setahun

ISSN 1979-8555

JURNAL
TELEMATIK
VOLUME 2 NOMOR 3 JULI 2010

DAFTAR ISI

FIREWALL DAN TRAFFIC FILTERING MENGGUNAKAN CISCO ROUTER

Oleh : Mustaziri

ABSTRAK

Jurnal ini berjudul "Firewall Dan Traffic Filtering Menggunakan Cisco Router". Tujuan dari konfigurasi firewall untuk meningkatkan keamanan komputer dengan mengendalikan trafik-trafik yang keluar masuk ke web server. Penulis mendapatkan masalah yang ada pada jaringan komputer yaitu kurang amannya jaringan komputer yang terhubung ke internet. Penulis ingin mengkonfigurasi firewall berbasis cisco yakni cisco router yang merupakan pionir terdepan dalam memfilter paket yang keluar masuk ke web server. Analisa menggunakan dasar teori Rakhmat Rafiudin (2006) dan Syamsudin (2005). Cisco router menerapkan firewall menggunakan access-list dengan statement PERMIT jika paket atau host diizinkan masuk dan DENY jika paket atau host ditolak untuk masuk ke web server. Penulis menyimpulkan bahwa Firewall berbasis cisco dapat melindungi jaringan terutama web server dari tangan orang-orang jahil (hackers). Untuk tingkat keamanan yang lebih, Penulis menyarankan agar ditambahkannya Firewall IP tables atau Shorewall pada web server.

Kata Kunci : Router,Jaringan,Firewall, Filtering, Paket Data

PENDAHULUAN

Latar Belakang

Dengan *adanya internet*, seseorang dapat dengan mudah mengetahui dan mendapatkan informasi, mudah berkomunikasi tanpa memandang jarak dan waktu, mudah melakukan transaksi dimanapun dan kapanpun seakan dunia itu seperti tanpa batas karena dibelahan dunia manapun saat ini sudah dapat dihubungkan dengan *internet*.

Sejalan dengan pesatnya perkembangan *internet*, selain memberikan dampak positif sebagai penyedia layanan informasi dan komunikasi, *internet* juga dapat memberikan dampak negatif sekaligus ancaman bagi penggunanya, Pada perusahaan atau dunia pendidikan telah terintegrasi dengan jaringannya secara terpusat dengan menggunakan komunikasi data *via* jaringan *private* atau bahkan menggunakan jaringan publik (*internet*), maka akan ada suatu permasalahan lain yang sangat krusial yaitu "Keamanan atau *Security*", pada jaringan .

Ancaman keamanan ini banyak sekali ditemui oleh *user* seperti, *Hacker, Cracker, Sniffing, Defaced, Buffer Overflow*, yang pasti akan menyusahkan *user* pada saat ancaman ini menyerang. Metode serangan saat ini sangat beragam, dari yang sederhana yang dilakukan para pemula atau *script kiddies* sampai dengan serangan dengan menggunakan metode-metode terbaru. Oleh karena itu semakin kompleksnya administrasi dari jaringan dengan skala luas seperti WAN maka diperlukan suatu mekanisme keamanan dan metode untuk dapat mengoptimalkan

FIREWALL DAN TRAFFIC FILTERING MENGGUNAKAN CISCO ROUTER

Oleh : Mustaziri

ABSTRAK

Jurnal ini berjudul "Firewall Dan Traffic Filtering Menggunakan Cisco Router". Tujuan dari konfigurasi firewall untuk meningkatkan keamanan komputer dengan mengendalikan trafik-trafik yang keluar masuk ke web server. Penulis mendapatkan masalah yang ada pada jaringan komputer yaitu kurang amannya jaringan komputer yang terhubung ke internet. Penulis ingin mengkonfigurasi firewall berbasis cisco yakni cisco router yang merupakan pionir terdepan dalam memfilter paket yang keluar masuk ke web server. Analisa menggunakan dasar teori Rakhmat Rafiudin (2006) dan Syamsudin (2005). Cisco router menerapkan firewall menggunakan access-list dengan statement PERMIT jika paket atau host diizinkan masuk dan DENY jika paket atau host ditolak untuk masuk ke web server. Penulis menyimpulkan bahwa Firewall berbasis cisco dapat melindungi jaringan terutama web server dari tangan orang-orang jahil (hackers). Untuk tingkat keamanan yang lebih, Penulis menyarankan agar ditambahkannya Firewall IP tables atau Shorewall pada web server.

Kata Kunci : Router,Jaringan,Firewall, Filtering, Paket Data

PENDAHULUAN

Latar Belakang

Dengan *adanya internet*, seseorang dapat dengan mudah mengetahui dan mendapatkan informasi, mudah berkomunikasi tanpa memandang jarak dan waktu, mudah melakukan transaksi dimanapun dan kapanpun seakan dunia itu seperti tanpa batas karena dibelahan dunia manapun saat ini sudah dapat dihubungkan dengan *internet*.

Sejalan dengan pesatnya perkembangan *internet*, selain memberikan dampak positif sebagai penyedia layanan informasi dan komunikasi, *internet* juga dapat memberikan dampak negatif sekaligus ancaman bagi penggunanya, Pada perusahaan atau dunia pendidikan telah terintegrasi dengan jaringannya secara terpusat dengan menggunakan komunikasi data *via* jaringan *private* atau bahkan menggunakan jaringan publik (*internet*), maka akan ada suatu permasalahan lain yang sangat krusial yaitu "Keamanan atau *Security*", pada jaringan .

Ancaman keamanan ini banyak sekali ditemui oleh *user* seperti, *Hacker, Cracker, Sniffing, Defaced, Buffer Overflow*, yang pasti akan menyusahkan *user* pada saat ancaman ini menyerang. Metode serangan saat ini sangat beragam, dari yang sederhana yang dilakukan para pemula atau *script kiddies* sampai dengan serangan dengan menggunakan metode-metode terbaru. Oleh karena itu semakin kompleksnya administrasi dari jaringan dengan skala luas seperti WAN maka diperlukan suatu mekanisme keamanan dan metode untuk dapat mengoptimalkan

sumber daya jaringan tersebut, karena semakin besar jaringan maka semakin rentan terhadap serangan dan semakin banyak *vulnerability* (celah) yang terbuka.

Ada beberapa cara yang dapat dilakukan untuk mengamankan jaringan komputer, tapi sistem yang biasa digunakan saat ini adalah *firewall*. *Firewall* merupakan salah satu metode untuk mengamankan atau membuat *secure* sistem pada jaringan. Ada banyak tipe *firewall* dan beragam cara untuk membangun *firewall*. Diantaranya, bisa menggunakan *tool-tool* atau *software-software traffic filtering*, menggunakan *device-device* (perangkat keras) yang dirancang khusus untuk membentuk fungsionalitas *filtering*, dan lainnya. Disini penulis hanya membahas *firewall* berbasis *cisco*.

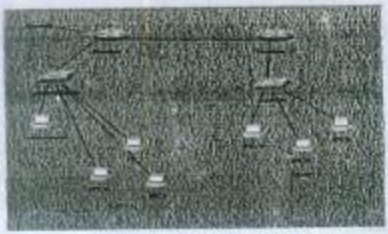
BAHAN DAN METODE

Untuk merancang suatu sistem *firewall* dan *traffic filtering* menggunakan cisco router, bahan dan metode yang diperlukan sebagai berikut :

A. Konfigurasi *Firewall* Melalui Router

Pengkabelan antar *router* menggunakan kabel DCE (*Data communication Equipment*) dan *DTE* (Data terminating Equipment) atau kabel *serial*, ruoter yang digunakan kali ini adalah seri router 2500 *series* mempunyai dua kabel *serial* dan satu kabel *Ethernet*. Pengkabelan tiap jaringan sama seperti cara membuat *LAN*, Perlengkapan yang diperlukan untuk membuat jaringan seperti, *switch*, *network LAN*, kabel UTP dan dan Konektor RJ-45. Komputer dan *switch* dihubungan dengan kabel UTP. Sebelumnya lakukan pemasangan konektor RJ-45 pada kabel UTP, dengan kabel *straight*.

Firewall, dalam hal ini dikonfigurasi lansung melalui *router* yang berfungsi sebagai pengontrol *traffic* jaringan antara jaringan A dan jaringan B, *Firewall* juga berfungsi mengatur *host* mana yang boleh akses maupun tidak, dengan sistem *permit or deny*.



Gambar 1. Topologi Firewall

Pada gambar diatas *Router1* merupakan jaringan A , dan *Router* 2 merupakan jaringan B yakni dengan *network* yang berbeda. Kedua *router* ini dihubungan satu sama lain. *Router*1 yakni jaringan A dihubungkan langsung ke *webserver* dan selanjutnya di arahkan ke *LAN* 1 melalui *switch/hub*.

B. Setting IP Router

Seperti yang telah dijelaskan sebelumnya, untuk menghubungkan *cisco router* ke suatu terminal atau komputer, diperlukan kabel *rollover* dan adaptor RJ-

45 ke DB-9 yang biasanya disertakan dengan peralatan router tersebut, kemudian Kabel rollover ini dihubungkan dari console port router ke serial port COM 1 atau COM 2 komputer.

Setelah memastikan konfigurasi kabel telah terpasang dengan benar, Setting ip dan konfigurasi lainnya pada *router* dapat menggunakan *hyper terminal* pada *windows xp*, pilih *start* > *all programs* > *accessories* > *communications* > *hyperterminal*. Maka akan keluar kotak dialog **Connect To** seperti yang terlihat pada gambar dibawah ini, di bagian **Connect Using** dengan pilihan *Direct to COM 1 atau COM 2* sesuai dengan *COM port* yang anda hubungkan dengan *router cisco*.

Gambar 2. Connect using

Selanjutnya pada bagian *Port Settings*, isilah *Bits per seconds* menjadi 9600 , data bit 8 parity pilih none , *stop bits* 1 dan *flow control hardware*, pada bagian ini sebenarnya hanya mengubah *bit persecond* saja, sedangkan setting yang lain sudah otomatis terbentuk.

Gambar .3 Setting bit persecond

Apabila *hyperterminal* sudah terkoneksi, maka tekan tombol Enter dua kali, dan akan muncul layar terminal kotak dialog *logon* ke *Cisco router*. Seperti pada gambar dibawah ini

Gambar 4. Tampilan awal router

Langkah selanjutnya ialah konfigurasi *cisco router*, router mempunyai dua interface, yakni *interface Ethernet* dan Serial. Misalkan, jaringan A ingin diberi IP

seperti, *Ethernet Interface* Router1 192.168.0.1 dan serial router1 192.168.3.1/24 dimana host masing-masing diawali dengan 192.168.0.2 – 192.168.0.254

Setting awal pada *user exec mode*, pilih *enable*, pada *privileged xec mode* ketik *configure terminal* untuk memasuki konfigurasi *global mode*, pada interface configuration mode ketik interface Ethernet0 dan interface serial0, untuk membuat ip pada *Ethernet* dan *serial router*.

Cisco Router mempunyai dua kabel *serial* yakni serial 0 dan serial 1 , kabel *serial* digunakan untuk menghubungkan antar *router* , *Cisco Router* 2500 *series* mempunyai satu interface Ethernet yakni ethernet0, disini akan digunakan serial1 untuk menghubungkan antar *router* dan *Ethernet* 0 untuk konfigurasi ip Router. seperti pada gambar berikut ini

```
Router>enable
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname router1
router1(config)#interface ethernet0
router1(config-if)#ip address 192.168.0.1 255.255.255.0
router1(config-if)#no shut
router1(config-if)#
```

Gambar 5. Setting ip interface ethernet pada router

```
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface serial0
Router(config-if)#ip address 192.168.3.1 255.255.255.0
Router(config-if)#clock rate 64000
Router(config-if)#bandwidth 64
Router(config-if)#ip route 192.168.1.0 255.255.255.0 192.168.3.2
Router(config)#
```

Gambar 6. Setting IP interface serial pada router1

C. Filtering Webserver Dengan Standard Access List

*Ethernet Interface router*1 sekarang mempunyai ip yakni 192.168.0.1 , dan *web server* dengan *ip* 192.168.0.2 , *access list* akan memfilter *web server* terhadap dunia luar. Dimisalkan blok *host* dengan *IP* 192.168.1.2 untuk masuk ke *webserver*.

Untuk menggunakan access list terlebih dahulu aplikasikan access list tersebut ke router interface Ethernet , jika ingin mengaplikasikannya ke port serial Maka perintah *standard access list* diketik di *interface serial*. Dalam hal ini, akan digunakan *interface Ethernet0* untuk mengaplikasikan *access list*.

```
router1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
router1(config)#int e0
router1(config-if)#ip acc
router1(config-if)#ip acces
router1(config-if)#ip access-group 10 out
router1(config-if)#exit
router1(config)#
```

Gambar 7. mengaplikasi access list ke router pada interface ethernet0

Access list number telah diaplikasikan ke *interface Ethernet router*, langkah selanjutnya ialah membuat sintaks *access list* dengan sistem *permit or deny*. Dalam hal ini kita akan blok host sumber yang datang dari 192.168.1.2, dengan list number 10.

Firewall dengan sintaks ACL akan memblok *traffic* yang datang dari ip 192.168.1.2, 0.0.0.0 berarti bahwa nilai-nilai tersebut harus tepat terpenuhi, keyword permit any menyatakan bahwa selain traffic yang datang dari 192.168.1.2, semuanya akan diijinkan atau terpenuhi, seperti pada gambar berikut ini

```
router1>en
router1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
router1(config)#int e0
router1(config-if)#ip access-group 10 out
router1(config-if)#exit
router1(config)#acc
router1(config)#access-list 10 deny 192.168.1.2 0.0.0.0
router1(config)#access-list 10 permit any
router1(config)#
```

Gambar 8. sintaks deny ip yang datang dari 192.168.1.2

D. Filtering Webserver Dengan Extended Access List

Sebelum merancang konfigurasi-konfigurasi *access-list* yang dibutuhkan, pada kasus ini , *Line serial router* menggunakan serial1, *web server* tinggal dalam segmen 192.168.0.1 dengan IP Address 192.168.0.2 dan menggunakan *port* standar HTTP 80, serta menggunakan *interface Ethernet0*.

Filtering IP Address untuk Akses *ke web server* sama halnya seperti menggunakan *Standard Access List* akan tetapi *Extended Access-list* menerapkan *source IP* (alamat sumber) dan *destination IP* (IP tujuan).

```
Router1>en
Router1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router1(config)#int e0
Router1(config-if)#ip access-
Router1(config-if)#ip access-group 100 out
Router1(config-if)#exit
Router1(config)#acc
Router1(config)#access-list 100 deny ip host 192.168.1.2 host 192.168.0.2
Router1(config)#access-list 100 permit ip any any
Router1(config)#
```

Gambar 9. Blok IP yang datang dari 192.168.1.2 ke dalam 192.168.0.2

Merestriksi akses-akses *Web* dapat diterapkan melalui *Extended Access-list*, apakah *Host* di beri akses *permit* (diizinkan) atau *deny* (ditolak) untuk membuka file *www / http* dalam *web server*.

```
Router1(config-if)#$ 100 deny tcp host 192.168.1.2 host 192.168.0.2 eq www
Router1(config)#$ 100 permit tcp any any
Router1(config)#
```

Gambar 10. Deny / Permit HTTP Web server

Web server juga mempunyai aplikasi pendukung untuk melakukan proses *transfer file* yakni *FTP* (*file transfer protocol*) yang menggunakan *port* 21 sebagai sumber, Disini dapat di implementasikan bagaimana menset-up *rule* yang mengizinkan atau menolak akses *FTP* dari *host* ke *web server*.

```
Router#show access-list
Extended IP access list 100
    deny tcp 0.0.0.0 192.168.1.2 0.0.0.0 192.168.0.2 eq ftp (12 matches)
    permit tcp any any
Router#
```

Gambar 11. Deny / Permit FTP Web Server

Kebanyakan user merasa tidak bebas karena tidak bisa melakukan ping ke web server, jika ingin memberi hak ping bagi user, konfigurasi access-list menggunakan perintah ICMP.

```
Router#show access-list
Extended IP access list 100
    deny tcp 0.0.0.0 192.168.1.2 0.0.0.0 192.168.0.2 eq ftp (13 matches)
    permit tcp any any (36 matches)
    permit icmp any any
Router#
```

Gambar 12. Memberi Hak ping ke User

E. Access List

Ada 2 tipe *access list* pada *cisco router* yakni *standard access list* dan *extended access list*.

1. *Standard access list* hanya digunakan untuk *filtering address* sumber IP/IPX.
2. *Extended Acess list*
   Digunakan untuk filtering lebih kompleks , seperti filtering berdasarkan jenis protokol , address sumber dan tujuan , port-port sumber dan tujuan dan tipe pesan-pesan (ICMP/IGMP), dan lain-lain.

Tabel dibawah ini merangkum daftar tipe access list beserta nomor-nomornya.

Tabel 3.1 Range Access List

Tipe Access list	*Range* Nomor
Standard IP Access List	1-99
Extended IP Access List	100-199

F. Blok Host / Permit Ip Untuk Akses Ke Web Server

Filtering IP Address untuk Akses *ke web server* sama halnya seperti menggunakan *Standard Access List* akan tetapi *Extended Access-list* menerapkan *source IP* (alamat sumber) dan *destination IP* (IP tujuan).

```
Router#en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#int e0
Router(config-if)#ip access-
Router(config-if)#ip access-group 100 out
Router(config-if)#exit
Router(config)#exc
Router(config)#access-list 100 deny ip host 192.168.1.2 host 192.168.0.2
Router(config)#access-list 100 permit ip any any
Router(config)#
```

Gambar 13. Blok IP yang datang dari 192.168.1.2 ke dalam 192.168.0.2

Merestriksi akses-akses *Web* dapat diterapkan melalui *Extended Access-list*, apakah *Host* di beri akses *permit* (diizinkan) atau *deny* (ditolak) untuk membuka file *www / http* dalam *web server.*

```
Router1(config-if)# 100 deny tcp host 192.168.1.2 host 192.168.0.2 eq www
Router1(config)# 100 permit tcp any any
Router1(config)#
```

Gambar 14. Deny / Permit HTTP Web server

Web server juga mempunyai aplikasi pendukung untuk melakukan proses *transfer file* yakni *FTP (file transfer protocol)* yang menggunakan *port* 21 sebagai sumber, Disini dapat di implementasikan bagaimana menset-up *rule* yang mengizinkan atau menolak akses *FTP* dari *host* ke *web server.*

```
Router1#show access-list
Extended IP access list 100
    deny tcp 0.0.0.0 192.168.1.2 0.0.0.0 192.168.0.2 eq ftp (12 matches)
    permit tcp any any
Router1#
```

Gambar 15. Deny / Permit FTP Web Server

Kebanyakan user merasa tidak bebas karena tidak bisa melakukan ping ke web server, jika ingin memberi hak ping bagi user, konfigurasi access-list menggunakan perintah ICMP.

```
Router1#show access-list
Extended IP access list 100
    deny tcp 0.0.0.0 192.168.1.2 0.0.0.0 192.168.0.2 eq ftp (33 matches)
    permit tcp any any (36 matches)
    permit icmp any any
Router1#
```

Gambar 16. Memberi Hak ping ke User

PEMBAHASAN

Masing-masing IP yakni *IP Ethernet0 router* 1 dan router2, IP *serial1 router1 dan router2* serta *host* pada masing-masing *router* pada jaringan yang berbeda. Seperti yang telah dijelaskan sebelumnya, *Router1* mempunyai IP *Ethernet0* 192.168.0.1, dengan *serial* 192.168.3.1 dan host 192.168.0.2 – 192.168.0.254 sedangkan *router2* mempunyai *IP Ethernet0* 192.168.1.1, dengan *serial*1 192.168.3.2 dan *host* diawali 192.168.1.2 - 192.168.1.254.

```
Router1>enable
Router1#ping 192.168.0.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.0.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/4 ms
Router1#
```

Gambar 17. Ping IP Ethernet router1

```
Router1>enable
Router1#ping 192.168.0.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.0.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
Router1#
```

Gambar 18. Ping pada IP Klient router1

```
Router1>enable
Router1#ping 192.168.3.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.3.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 56/56/60 ms
Router1#
```

Gambar 19. Ping pada IP serial router1

Pengujian *ping* ke *IP serial router2*

```
Router1>enable
Router1#ping 192.168.3.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.3.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 31/32/32 ms
Router1#
```

Gambar 20. Ping pada IP serial router2

Pengujian *ping* ke *IP Ethernet router2*

```
Router1>enable
Router1#ping 192.168.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 32/32/32 ms
Router1#
```

Gambar 21. Ping pada IP Ethernet Router2

Pengujian *ping* ke IP Klient *router2*

```
Router1>enable
Router1#ping 192.168.1.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/30/32 ms
Router1#
```

Gambar 22. Ping pada IP Klient router2

KESIMPULAN DAN SARAN

Kesimpulan

Dari hasil dan pembahasan serta perancangan yang telah dibuat maka dapat ditarik kesimpulan sebagai berikut :

1. Teknologi *Cisco* dapat di Implementasikan sebagai *firewall* dalam memfilter *traffic* yang keluar masuk jaringan dengan menggunakan perintah *access-list*.
2. *Access-list* pada *cisco router* menerapkan statement "*permit*" untuk mengizinkan paket dan " *deny*" untuk memblok paket.
3. Rule-rule *access-list firewall* memberikan perlindungan terhadap web server dalam hal serangan dari dunia luar.

Saran

Berikut saran yang dapat diambil untuk pengembangan lebih lanjut :

1. Sebaiknya menggunakan *web server* yang berbasis *linux* dibandingkan dengan *windows server* dikarenakan faktor keamanan pada Linux yang jauh lebih baik dan anti terhadap *virus* maupun spyware.
2. Gunakanlah *Proxy server* Linux , Untuk mengoptimalkan kinerja akses ke *web server*, karena *Proxy server* menyediakan sistem *Cache* yang dapat mempercepat kinerja *transfer* data selain itu, *Proxy server* juga menyediakan sistem ACL (*access-list*) sehingga tingkat keamanan lebih tinggi.

DAFTAR PUSTAKA

1. Faruddin , Rahmat. 2005. *Membangun Firewall Dengan IPTables di linux.* Jakarta : PT. Elexmedia Komputindo.
2. Raiding, Rahmat. 2006. membangun *firewall* dan *traffic filtering* berbasis *cisco* Yogyakarta : Penerbit andi
3. M, Syamsudin.2005. *60 Menit Belajar Linux dan Jaringan.* Yogyakarta : C.V.
4. Andi Offset.
5. Rafiudin, Rahmat. 2006. IP Routing dan firewall dalam *linux*. Yogyakarta : Penerbit : Andi
6. Wijaya, Hendra. 2001. Belajar sendiri *cisco router*. Jakarta: PT elex media Komputindo
7. Suhendro atmawijaya. Ilmu komputer dan Jaringan.
8. http://www.total.or.id/info.php?kk=jaringan
9. http://belajar-komputer-mu.com/pengertian-jaringan-komputer
10. http://mikrotik-id.blogspot.com/2007/07/spesifikasi-router-board-mikrotik-untuk.html
11. http://www.scribd.com/doc/3495063/cisco-Router-2500-series
12. http://d307244.files.wordpress.com/2008/04/access-list.doc