Extended Access List untuk Mengendalikan Trafik Jaringan

Hari Antoni Musril[#1]

[#]*Jurusan Pendidikan Teknik Informatika dan Komputer Fakultas Tarbiyah dan Ilmu Keguruan IAIN Bukittinggi*
[1]*kum_ayik@yahoo.co.id*

Abstrak— **Keamana jaringan komputer saat ini menjadi hal penting untuk diterapkan. Banyak organisasi yang telah menjadikan teknologi informasi sebagai bahagian penting dalam menunjang aktivitasnya. Akses pengguna yang tidak dibatasi menjadi ancaman bagi sebuah organisasi, karena banyak data dan informasi penting yang tersebar dalam perangkat jaringan komputer di organisasi tersebut dapat disusupi oleh pihak yang tidak berwenang. Salah satu usaha yang dapat dilakukan adalah dengan menerapkan *extended access list* yang merupakan salah satu bagian dari metode *access control list*. *Extended access list* dapat menyaring lalu lintas data suatu jaringan dengan mengontrol apakah paket-paket tersebut dilewatkan atau dihentikan. *Extended access list* juga dapat menjamin keamanan untuk setiap komputer sehingga jalur komunikasi serta hak akses setiap komputer dapat berjalan dengan baik. *Extended access list* memungkinkan penyaringan berdasarkan sumber atau alamat tujuan, protokol yang dipilih, port yang digunakan, dan apakah koneksi sudah ditetapkan. Tulisan ini membahas penerapan *extended access list* dalam jaringan supaya dapat melakukan filter terhadap paket data yang melewati jaringan. Penerapannya menggunakan software Packet Tracer 6.1.1 untuk membuat prototipe jaringan dan mensimulasikannya. Sehingga nanti dapat diterapkan pada jaringan yang sebenarnya. List yang dibangun pada penelitian ini diterapkan untuk protokol antara lain : TCP (WWW, FTP, Telnet, SMTP, POP3), UDP (DNS), dan ICMP (Ping). Hasilnya didapatkan *extended access list* yang dikonfigurasi pada *router* dalam topologi penelitian ini mampu melakukan filter terhadap paket yang melewati jaringan. Hasil konfigurasinya sangat spesifik, sehingga penerapan hak akses *permit* dan *deny* dapat dilakukan sesuai dengan aturan dan skenario yang dirancang.**

***Kata kunci*— *access control list, extended access list, router, protocol, network,* paket data, filter.**

I. PENDAHULUAN

Perkembangan teknologi informasi yang cukup pesat dewasa ini berimplikasi terhadap ancaman keamanan jaringan komputer. Hal tersebut dapat terjadi karena akses teknologi informasi sangat mudah dilakukan. Mudahnya akses ini seiring dengan berkembangnya teknologi internet. Hal tersebut tentunya perlu menjadi perhatian bagi sebuah organisasi dan institusi baik nilik swasta maupun milik pemerintah. Perlu diterapkan berbagai strategi untuk bisa menjamin keamanan data dan informasi dari pihak-pihak yang tidak berkepentingan. Akses dalam sebuah jaringan komputer harus diawasi dan dibatasi.

Salah satu upaya yang dapat dilakukan adalah dengan menerapkan *access control list* pada jaringan komputer. *Access control list* merupakan sebuah metode yang digunakan untuk menyeleksi paket-paket yang keluar masuk *network* [1]. *Access control list* adalah daftar aturan untuk mengizinkan atau menolak akses jaringan ke sebuah *endpoint* [2]. Penggunaan *access list* yang paling umum digunakan adalah penyaringan paket yang tidak diinginkan ketika mengimplementasikan kebijakan keamanan [3]. *Access list* bekerja menyaring lalu-lintas data suatu *network* dengan mengontrol apakah paket-paket tersebut dilewatkan atau dihentikan pada alat penghubung (*interface*) *router* [4].

Extended access list merupakan salah satu jenis *access control list* yang sering dan banyak digunakan untuk mengatur keamana jaringan. Pengaturan menggunakan *extended access list* sangat spesifik, sehingga memudahkan *administrator* jaringan dalam mengatur trafik data di dalam jaringan.

II. LANDASAN TEORI

A. Access Control List

Access control list (ACL) berfungsi untuk mengizinkan atau membatasi paket data yang melintas pada sebuah jaringan. *Access control list* merupakan suatu metode yang mengatur lalu lintas IP pada pintu masuk jaringan dan memfilter paket data pada saat akan melewati *router* apakah akan diizinkan melalui *router* atau ditolak [4]. Jadi pengaturan ACL ini dilakukan di dalam *router* yang terdapat pada sebuah jaringan. *Router* menguji semua paket data untuk menentukan apakah paket tersebut diijinkan untuk lewat atau tidak berdasarkan kriteria yang ditentukan di dalam *access list* [4]. *Router* ACL membuat keputusan berdasarkan

ISSN 2460-0741

alamat asal, alamat tujuan, protokol, dan nomor *port* [5]

Access list dibagi atas dua kelompok, yaitu *standard access list* (1-99) dan *extended access list* (100-199) [6]. *Standar access list* dalam melakukan penyaringan paket data hanya memperhatikan alamat sumber (alamat asal) dari paket yang dikirimkan. Sedangkan *extended access list* mempertimbangkan antara lain adalah alamat sumber (pengirim) dan alamat tujuan (penerima) paket data, protokol dan jenis yang digunakan. Sehingga *extended access list* lebih spesifik dalam melakukan penyaringan paket data.

Mekanisme dasar ACL yakni menyaring paket yang tidak diinginkan ketika komunikasi data berlangsung sehingga menghindari permintaan akses maupun paket data yang mencurigakan dalam akses keamanan sebuah jaringan [7]. Apabila ditemukan akses yang tidak diizinkan maka *router* akan langsung memblok alamat perangkat jaringan tersebut. Saat router memutuskan apakah perlu mem-*forward* atau memblok sebuah paket, *software* cisco IOS mengetes paket tersebut untuk setiap statemen kriteria dalam urutan yang sesuai saat mereka dibuat [3].

B. Extended Access List

Extended access list memungkinkan penyaringan berdasarkan sumber atau alamat tujuan, protokol yang dipilih, *port* yang digunakan, dan apakah koneksi sudah ditetapkan [8]. Dengan menggunakan *extended access list*, kita dapat secara efektif mengizinkan akses pengguna ke LAN fisik dan menghentikan mereka dari mengakses *host* tertentu atau hanya layanan tertentu saja dari *host* tersebut [9].

Terdapat dua keadaan yang didefinisikan pada pengaturan list tersebut, yaitu *permit* dan *deny*. Perintah untuk mengkonfigurasi *extended access list* secara umum dapat digambarkan seperti gambar 1 berikut ini [10] :

```
Router(config)#access-list [nomor daftar akses IP extended] [permit atau deny]
[protokol] [source address] [wildcard mask] [destination address] [wildcard mas
k] [operator] [informasi port]
```

Gambar 1. Sintak konfigurasi *extended access list*

Nomor daftar akses IP *extended* adalah 100 hingga 199 [11]. Untuk protokol yang digunakan antara lain terdapat pada tabel I.

TABEL I

NAMA DAN NOMOR *PORT* PROTOKOL [12]

Jenis Protokol	**Nama Port**	**Informasi Port**	**Nomor Port**
TCP	FTP Data	ftp-data	20
	FTP Control	ftp	21
	Telnet	telnet	23
	SMTP	smtp	25
	WWW	www	80
UDP	DNS Query	dns	53
	TFTP	tftp	69
	SNMP	snmp	161
	IP RIP	rip	520

Kesalahan pada saat pengaturan list dapat membuat jaringan menjadi *down*. Untuk itu diperlukan kecermatan administrator jaringan dalam melakukan analisis sebelum membuatkan list di *router*. Pengaturan dapat dilakukan untuk tiga keadaan, yaitu *network* ke *network*, *host* ke *network*, dan *host* ke *host*.

III. METODE PENELITIAN

Pada tulisan ini metode penelitian yang digunakan adalah :

1. Analisis (*Analysis*). Pada tahapan ini dilakukan analisis literatur yang relevan. Literatur bersumber dari buku, jurnal ilmiah, dan penelitian yang membahas mengenai *extended access list*.
2. Desain (*Desaign*). Tahapan desain berisikan bentuk prototipe topologi jaringan yang dikembangkan. Desain ini meliputi skenario jaringan secara fisik dan juga logika. Perancangan prototipe jaringan memanfaatkan *software* simulasi jaringan komputer Cisco Packet Tracer 6.1.1.
3. Pengembangan *(Developmen*t). Tahapan ini dilakukan untuk mengkonfigurasi prototipe jaringan yang telah didesain sebelumnya. Konfigurasi dilakukan pada setiap device yang ada di dalam prototipe jaringan, antara lain adalah PC, laptop, server, dan *router*. Konfigurasi *extended access list* dilakukan di *router* dengan mengetikkan kode program pada jendela CLI *router* tersebut. Pengaturan *router* dilakukan untuk pengendalian trafik jaringan sehingga bisa melakukan penyaringan paket data dalam jaringan.

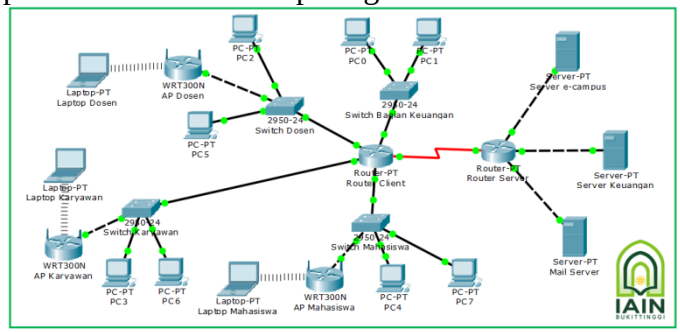
ISSN 2460-0741

4. Pengujian (*Test*). Setelah prototipe jaringan selesai dikembangkan, setiap *device* dilakukan pengujian konektivitasnya. *Extended access list* yang telah dibuat harus dapat berjalan di dalam prototipe jaringan ini. Apabila tidak berhasil, maka kembali dilakukan tahapan konfigurasi (pengembangan) sampai pengujian sukses dilakukan.

IV. PEMBAHASAN

A. *Topologi Jaringan untuk Penelitian*

Topologi jaringan yang digunakan dalam penelitian ini adalah seperti gambar 2 berikut ini.



Gambar 2. Topologi jaringan yang digunakan dalam penelitian

Berdasarkan topologi di atas, dapat diatur pengalamatan setiap *device* seperti pada Tabel II.

Setiap *device* dikonfigurasi sesuai dengan alamat yang ada pada tabel di atas. Kemudian dilakukan pemeriksaan apakah setiap komponen jaringan telah terhubung atau belum.

B. *Pengaturan Alamat Router*

Langkah selanjutnya adalah melakukan proses *routing* pada *router server* dan *router client* sehingga kedua *router* dapat saling berkomunikasi. *Routing protocol* yang digunakan adalah RIPv2. Berikut ini adalah pengaturannya pada jendela CLI masing-masing *router*.

Konfigurasi di *router server* :

```
Router>enable
Router#configure terminal
Router(config)#hostname Router_Server
Router_Server(config)#router rip
Router_Server(config-router)#version 2
Router_Server(config-router)#network 192.168.0.0
Router_Server(config-router)#network 118.97.170.0
Router_Server(config-router)#network 10.121.45.0
Router_Server(config-router)#network 188.125.173.0
Router_Server(config-router)#no auto-summary
Router_Server(config-router)#exit
```

TABEL II

PENGATURAN ALAMAT *DEVICE* JARINGAN

Nama Perangkat	**IP Address /Prefix**	**Default Gateway**
Router Server	Fa0/0 : 118.97.170.100 /24 Fa1/0 : 10.121.45.100 /24 Fa8/0 : 188.125.173.100 /24 Serial2/0 : 192.168.0.1 /24	-
Router Client	Fa0/0 : 193.169.10.100 /24 Fa1/0 : 195.171.10.100 /24 Fa6/0 : 197.173.10.100 /24 Fa7/0: 199.175.10.100 /24 Serial2/0 : 192.168.0.2 /24	-
Server e-campus	118.97.170.198 /24	118.97.170.100 /24
Server Keuangan	10.121.45.152 /24	10.121.45.100 /24
Mail Server	188.125.173.108 /24	188.125.173.100 /24
PC Keuangan	193.169.10.1 /24 193.169.10.2 /24	193.169.10.100 /24
PC Dosen	195.171.10.1 /24 195.171.10.2 /24	195.171.10.100 /24
Laptop Dosen	DHCP	195.171.10.3 /24
PC Karyawan	197.173.10.1 /24 197.173.10.2 /24	197.173.10.100 /24
Laptop Karyawan	DHCP	197.173.10.3 /24
PC Mahasiswa	199.175.10.1 /24 199.175.10.2 /24	199.175.10.100 /24
Laptop Mahasiswa	DHCP	199.175.10.3 /24

Konfigurasi di *router client* :

```
Router>enable
Router#configure terminal
Router(config)#hostname Router_Client
Router_Client(config)#router rip
Router_Client(config-router)#version 2
Router_Client(config-router)#network 192.168.0.0
Router_Client(config-router)#network 193.169.10.0
Router_Client(config-router)#network 195.171.10.0
Router_Client(config-router)#network 197.173.10.0
Router_Client(config-router)#network 199.175.10.0
Router_Client(config-router)#no auto-summary
Router_Client(config-router)#exit
```

C. *Konfigurasi Extendeed Access List*

Berikut adalah pengaturan dan skenario *extended access list* yang diterapkan pada topologi pada penelitian ini.

1. Server e-campus bisa diakses oleh dosen, bagian keuangan, karyawan, dan mahasiswa. Dengan demikian pada skenario ini tidak dibutuhkan pengaturan *extended access list*.
2. Server Keuangan hanya bisa diakses oleh bagian keuangan. Dosen, karyawan, dan mahasiswa

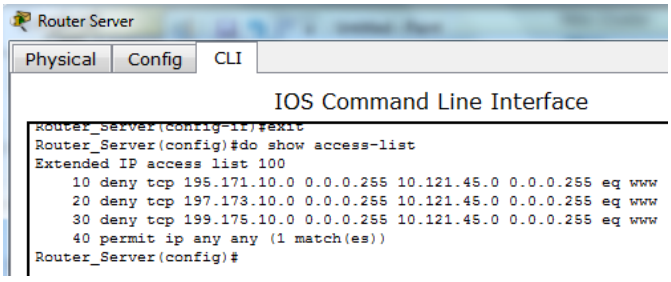
ISSN 2460-0741

masih tidak bisa mengakses server keuangan. *Protocol* pada server keuangan yang dikonfigurasi adalah HTTP, ICMP (*ping*), dan FTP. Pengaturan list *extended* dilakukan di *router server*. Berikut konfigurasi *extended access list* untuk memblok akses ke server keuangan :

a) Hanya komputer bagian keuangan yang bisa mengakses HTTP pada server keuangan. Konfigurasi pada bagian CLI di *router server* adalah seperti berikut ini.

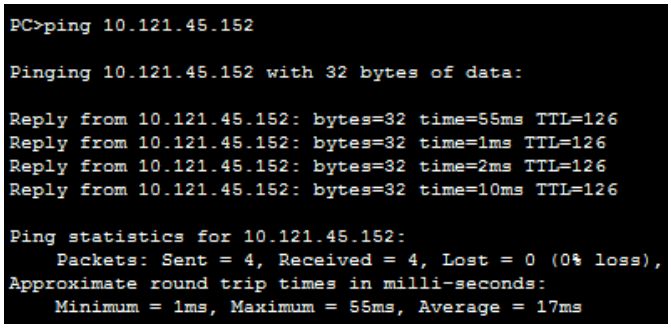
```
Router_Server>enable
Router_Server#configure terminal
Router_Server(config)#access-list 100 deny
tcp 195.171.10.0 0.0.0.255 10.121.45.0
0.0.0.255 eq www
Router_Server(config)#access-list 100 deny
tcp 197.173.10.0 0.0.0.255 10.121.45.0
0.0.0.255 eq www
Router_Server(config)#access-list 100 deny
tcp 199.175.10.0 0.0.0.255 10.121.45.0
0.0.0.255 eq www
Router_Server(config)#access-list 100 permit
ip any any
Router_Server(config)#int fa1/0
Router_Server(config-if)#ip access-group 100
out
Router_Server(config-if)#exit
```

Daftar list *extended* yang dihasilkan adalah seperti gambar 3 di bawah ini.



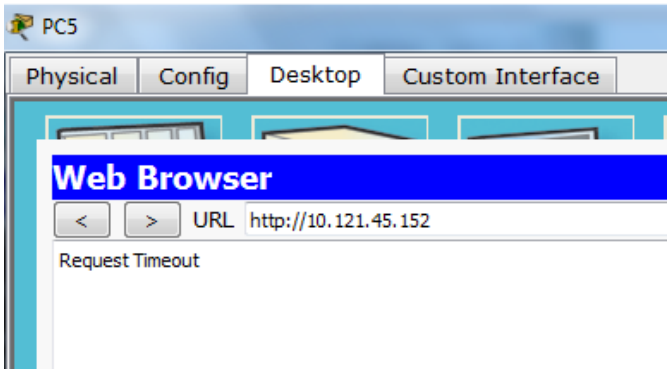
Gambar 3. Daftar list *extended*

Hasil yang didapatkan adalah komputer dan laptop yang ada pada bagian dosen, keuangan, karyawan, dan mahasiswa dapat merespon pesan *ping*, seperti gambar 4 berikut ini.



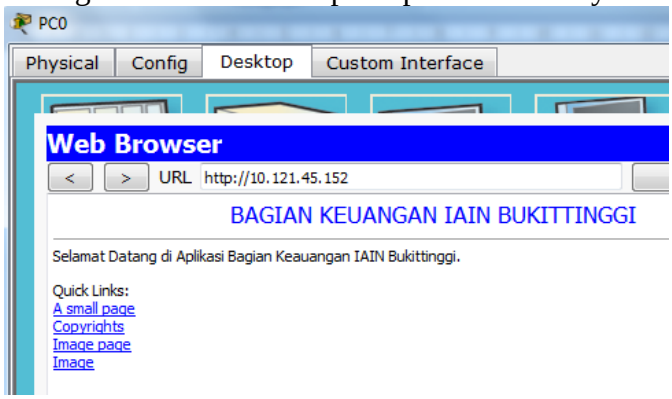
Gambar 4. Hasil uji *ping* ke *server* keuangan

Sedangakan untuk akses protokol http didapatkan hasil bahwa perangkat yang berada di daerah dosen, karyawan, dan mahasiswa tidak dapat mengakses web (www) yang ada pada server keuangan. Berikut ini tampilan pada browser komputer dosen, karyawan, dan mahasiswa.



Gambar 5. Halaman web tidak bisa diakses

Komputer yang berada pada bagian keuangan dapat mengakses protokol http yang berada di server keuangan. Berikut ini tampilan pada browsernya.



Gambar 6. Halaman web bisa diakses

ISSN 2460-0741

b) Melakukan blok terhadap protokol ICMP sehingga tidak dapat melakukan *ping*. Pengaturannya seperti berikut ini.

```
Router_Server(config)#access-list 101 deny
icmp 195.171.10.0 0.0.0.255 10.121.45.0
0.0.0.255 echo
Router_Server(config)#access-list 101 deny
icmp 195.171.10.0 0.0.0.255 10.121.45.0
0.0.0.255 echo-reply
Router_Server(config)#access-list 101 deny
icmp 197.173.10.0 0.0.0.255 10.121.45.0
0.0.0.255 echo
Router_Server(config)#access-list 101 deny
icmp 197.173.10.0 0.0.0.255 10.121.45.0
0.0.0.255 echo-reply
Router_Server(config)#access-list 101 deny
icmp 199.175.10.0 0.0.0.255 10.121.45.0
0.0.0.255 echo
Router_Server(config)#access-list 101 deny
icmp 199.175.10.0 0.0.0.255 10.121.45.0
0.0.0.255 echo-reply
Router_Server(config)#access-list 101 permit
ip any any
Router_Server(config)#int fa1/0
Router_Server(config-if)#ip access-group 101
out
Router_Server(config-if)#exit
```

Hasilnya didapatkan semua komputer dosen, karyawan, dan mahasiswa tidak sukses melakukan pesan *ping*. Sedangkan komputer bagian keuangan dapat melakukan pesan *ping*. Perhatikan gambar 7 berikut ini.

```
Packet Tracer PC Command Line 1.0
PC>ping 10.121.45.152

Pinging 10.121.45.152 with 32 bytes of data:

Reply from 192.168.0.1: Destination host unreachable.
Reply from 192.168.0.1: Destination host unreachable.
Reply from 192.168.0.1: Destination host unreachable.
Reply from 192.168.0.1: Destination host unreachable.

Ping statistics for 10.121.45.152:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Gambar 7. Pesan *ping* gagal dilakukan ke server keuangan

c) Melakukan pembatasan terhadap protokol FTP. Konfigurasinya adalah seperti berikut ini.

```
Router_Server(config)#access-list 102 deny
tcp 195.171.10.0 0.0.0.255 10.121.45.0
0.0.0.255 eq ftp
Router_Server(config)#access-list 102 deny
tcp 197.173.10.0 0.0.0.255 10.121.45.0
0.0.0.255 eq ftp
Router_Server(config)#access-list 102 deny
tcp 199.175.10.0 0.0.0.255 10.121.45.0
0.0.0.255 eq ftp
Router_Server(config)#access-list 102 permit
ip any any
Router_Server(config)#int fa1/0
Router_Server(config-if)#ip access-group 102
out
Router_Server(config-if)#exit
Router_Server(config)#
```

Hasil yang didapatkan untuk bagian kepegawaian adalah seperti gambar 8 berikut ini.

```
Packet Tracer PC Command Line 1.0
PC>ftp 10.121.45.152
Trying to connect...10.121.45.152
Connected to 10.121.45.152
220- Welcome to PT Ftp server
Username:cisco
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>
```

Gambar 8. Koneksi FTP berhasil

Sedangkan pada komputer dosen, karyawan, dan mahasiswa tidak dapat mengakses ftp. Perhatikan gambar 9 berikut ini.

```
PC>ftp 10.121.45.152
Trying to connect...10.121.45.152

%Error opening ftp://10.121.45.152/ (Timed out)
.



Packet Tracer PC Command Line 1.0
PC>(Disconnecting from ftp server)



Packet Tracer PC Command Line 1.0
PC>
```

Gambar 9. Koneksi FTP tidak berhasil

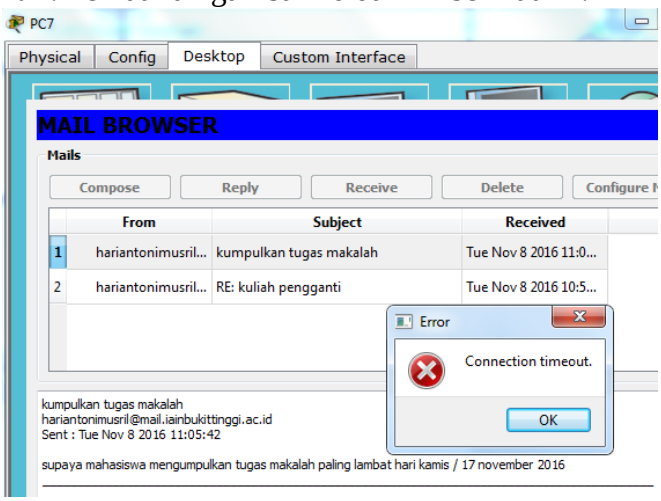
3. Mail Server bisa diakses oleh dosen, bagian keuangan, dan karyawan. Sedangkan mahasiswa tidak dapat mengaksesnya. Pada bagian ini protokol yang dikonfigurasi adalah SMTP, POP3, dan DNS. Berikut pengaturannya :
   a) Konfigurasi *protocol* SMTP dilakukan pada jendela IOS *router* server sebagai berikut.

```
Router_Server(config)#access-list
103 deny tcp 199.175.10.0 0.0.0.255
188.125.173.0 0.0.0.255 eq smtp
Router_Server(config)#access-list
103 permit ip any any
Router_Server(config)#int fa8/0
Router_Server(config-if)#ip access-
group 103 out
Router_Server(config-if)#exit
Router_Server(config)#
```

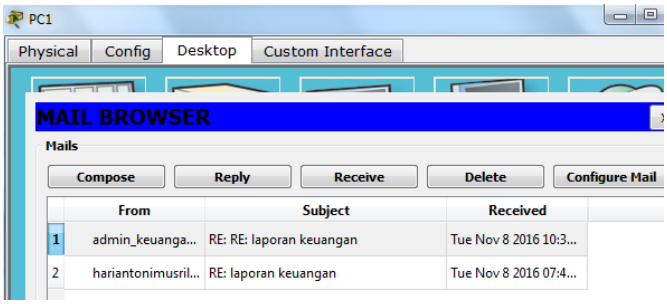
Setelah dilakukan konfigurasi didapatkan hasil komputer mahasiswa tidak dapat mengirimkan

ISSN 2460-0741

pesan (*mail*) karena tidak diizinkan mengakses *mail* server, namun komputer mahasiswa ini masih bisa menerima *mail* dari user lainnya karena protokol POP3 belum diblokir. Sedangkan komputer dosen, bagian keuangan, dan karyawan dapat terhubung ke *mail* server sehingga bisa mengirim dan membalas *mail*. Perhatikan gambar 10 dan 11 berikut ini.



Gambar 10. Komputer mahasiswa tidak dapat mengirim *mail*, namun masih bisa menerima *mail* dari user lain

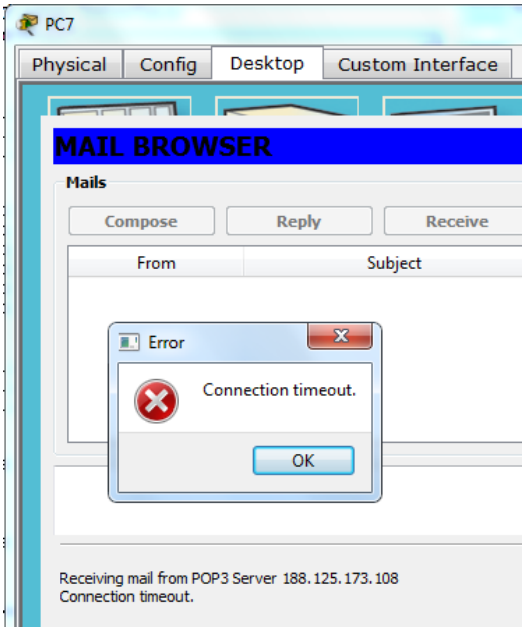


Gambar 11. Komputer dosen, bagian keuangan, dan karyawan bisa mengirim dan membalas *mail*

b) Pengaturan protokol POP3 dilakukan dengan perintah berikut ini.

```
Router_Server(config)#access-list 104 deny
tcp 199.175.10.0 0.0.0.255 188.125.173.0
0.0.0.255 eq pop3
Router_Server(config)#access-list 104 permit
ip any any
Router_Server(config)#int fa8/0
Router_Server(config-if)#ip access-group 104
out
Router_Server(config-if)#exit
Router_Server(config)#
```

Hasilnya adalah komputer mahasiswa tidak dapat lagi menerima *mail* yang dikirimkan dari user lainnya. Tampilannya seperti gambar 12.

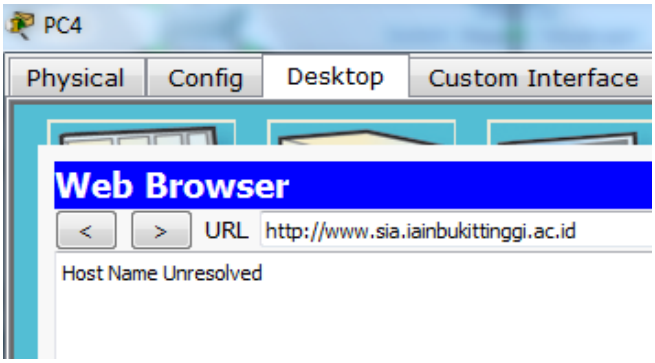


Gambar 12. Komputer mahasiswa tidak dapat menerima *mail*

c) Konfigurasi DNS dapat dilakukan dengan perintah berikut ini.

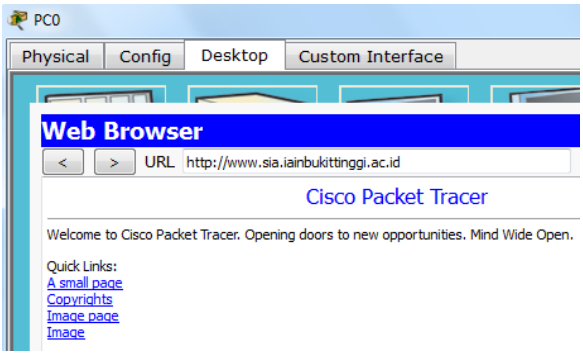
```
Router_Server(config)#access-list 105 deny
udp 199.175.10.0 0.0.0.255 188.125.173.0
0.0.0.255 eq domain
Router_Server(config)#access-list 105 permit
ip any any
Router_Server(config)#int fa8/0
Router_Server(config-if)#ip access-group 105
out
Router_Server(config-if)#exit
Router_Server(config)#
```

Hasil dari pengaturan ini adalah komputer mahasiswa tidak dapat membuka *domain name* yang ada di *mail server*. Sedangkan komputer dosen, bagian keuangan, dan karyawan dapat membuka *domain* tersebut. Perhatikan gambar 13 dan 14 berikut ini.



Gambar 13. Komputer mahasiswa tidak dapat membuka *domain name*

ISSN 2460-0741



Gambar 14. Komputer dosen, bagian keuangan, dan karyawan dapat membuka *domain name*

d) Konfigurasi telnet dilakukan seperti berikut.

Mengaktifkan telnet di router server dilakukan dengan mengetikkan perintah berikut di CLI *router server*.

```
Router_Server(config)#username hari password iain
Router_Server(config)#enable secret hari
Router_Server(config)#line vty 0 4
Router_Server(config-line)#login local
Router_Server(config-line)#exit
Router_Server(config)#
```

Berikutnya dilakukan skenario dimana komputer mahasiswa tidak bisa mengakses telnet di *router server*. Berikut ini adalah konfigurasinya.

```
Router_Server(config)#access-list 106 deny tcp
199.175.10.0 0.0.0.255 any eq telnet
Router_Server(config)#access-list 106 permit ip
any any
Router_Server(config)#int se2/0
Router_Server(config-if)#ip access-group 106 in
Router_Server(config-if)#exit
```

Didapatkan hasil bahwa komputer yang ada di bagian mahasiswa tidak dapat menjalankan telnet. Sedangkan komputer dosen, bagian keuangan, dan karyawan dapat melakukan telnet. Perhatikan gambar berikut ini.

```
PC>telnet 192.168.0.1
Trying 192.168.0.1 ...
% Connection timed out; remote host not responding
PC>
```

Gambar 15. Komputer mahasiswa tidak bisa mengakses telnet

```
PC>telnet  192.168.0.1
Trying 192.168.0.1 ...Open


User Access Verification

Username: hari
Password:
Router_Server>exit

[Connection to 192.168.0.1 closed by foreign host]
PC>
```

Gambar 16. Komputer dosen, bagian keuangan, dan karyawan dapat mengakses telnet

V. KESIMPULAN

Berdasarkan pada percobaan yang telah dilakukan, extended *access list* dapat melakukan pengendalian trafik jaringan dengan menyaringan paket data yang melewati *router*. *Router* akan melakukan pengecekan *access list* pada saat setiap paket data akan masuk pada *port* yang ada di *router* tersebut. *Extended access list* melakukan pengecekan terhadap beberapa atribut, yaitu alamat sumber, alamat tujuan, *protokol*, dan nama *port*. Pada penelitian ini protokol yang dikonfigurasi antaralain adalah TCP (*port* yang diatur adalah www/http, telnet, ftp, dan smtp), UDP (*port* yang diatur adalah dns), dan ICMP (*port* yang dikonfigurasi adalah *ping*). Hasil dari pengaturan terhadap semua *port* tersebut adalah sesuai dengan konsep dan skenario yang direncanakan dalam penelitin. Sehingga dapat disimpulkan bahwa *extended access list* melakukan filter terhadap trafik jaringan dengan sangat spesifik sehingga mampu memberikan jaminan terhadap keamana dalam sebuah jaringan.

REFERENSI

[1] Sofana, Iwan. 2012. *Cisco CCNA & Jaringan Komputer*. Bandung : Informatika.

[2] Washam, M., Rainey, R. 2015. *Exam Ref 70-533 Implementing Microsoft Azure Infrastructure Solutions*. Washington : Microsoft Press.

[3] Purwanto, Agus D., Badrul, Muhammad. 2016. Implementasi Access List Sebagai Filter Traffic Jaringan (Study Kasus PT. Usaha Entertainment Indonesia). Jakarta, Jurnal Teknik Komputer AMIK BSI Vol 2 No 1

[4] Rahmawati. 2015. *Konfigurasi Keamanan Jaringan Komputer Pada Router Dengan Metode ACL'S*. Jakarta, Jurnal Teknik Komputer AMIK BSI Vol 1 No 2.

[5] Dinata, Septian Krisna. 2013. *Monitoring Aktifitas Jaringan dan Simulasi Access Control List Pada STMIK PalComTech Berbasis Cisco Router*. Palembang, Jurnal Teknologi dan Informatika (TEKNOMATIKA) Vol 3 No 1.

[6] Saputro, Joko. 2010. *Praktikum CCNA di Komputer Sendiri Menggunakan GNS3*. Jakarta : MediaKita.

[7] Rafiudin, Rahmat. 2008. *SQUID*. Yogyakarta : Andi Offset.

[8] Mason, Andrew G., Newcomb, Mark J. 2001. *Cisco Secure Internet Security Solutions*. Indianapolis : Cisco Press.

[9] Lammle, Todd. 2005. *CCNA First Pass 2nd Edition*. New Jersey : Wiley Publishing, Inc.

[10] Lee, Donald C. 2002. *Enhanced IP Services for Cisco Networks*. Indianapolis : Cisco Press.

[11] Rafiudin, Rahmat. 2004. *Mengupas Tuntas Cisco Router*. Jakarta : Elex Media Komputindo.

[12] Suman, S., Agrawal, ER. Aditi. 2016. *IP Traffic Management With Access Control List Using Cisco Packet Tracer*. India, International Journal of Science, Engineering and Technology Research (IJSETR) Vol 5 No 5.

ISSN 2460-0741