BAB IV

PENGUJIAN SISTEM

Pengujian sistem yang dilakukan merupakan pengujian terhadap aplikasi pada PC *Router* yang telah selesai dibuat. Dimulai dari Pengujian terhadap authentifikasi, pengujian terhadap pengaturan iptables, pengujian terhadap pembuatan VLAN, pengujian terhadap pembuatan monitoring *bandwith* dan koneksi PC dalam jaringan dan pengujian terhadap pembuatan penjadwalan pada Ip tables.

4.1 Pengujian Terhadap proses authentifikasi

Pengujian terhadap proses authentifikasi dilakukan dengan memasukan *user*name dan password pada saat aplikasi akan dijalankan. Bila *user*name dan password tertentu saja yang dapat mengakses aplikasi, maka proses authentifikasi sudah berjalan.

4.1.1 Tujuan

Tujuan dari pengujian ini yaitu mengetahui apakah proses authentifikasi sudah berjalan dengan baik, sehingga orang yang mempunyai wewenang saja yang dapat mengakses aplikasi ini.

4.1.2 Alat yang Digunakan

1. PC yang ditempatkan sebagai PC *Router*
2. PC *client* yang mengakses PC *Router*.

3. switch.

4. kabel UTP (Unshielded Twisted Pair).

4.1.3 Prosedur Pengujian

1. Menyalakan PC *client* dan PC *Router*

2. Hubungkan PC *client* dengan PC *Router* sesuai dengan topologi.

3. buat database pada PC *Router* dengan menggunakan mysql.

4. login dengan menggunakan *user* dan password yang telah terdaftar pada mysql server.

4.1.4 Hasil pengujian Authentifikasi

Pengujian terhadap authentifikasi dilakukan dengan mengikuti prosedur diatas. PC *client* digunakan untuk mengakses aplikasi pada PC *Router*, dengan menulis alamat gateway pada *web* browser. Berikut ini adalah database sementara yang dibuat pada PC *Router*.

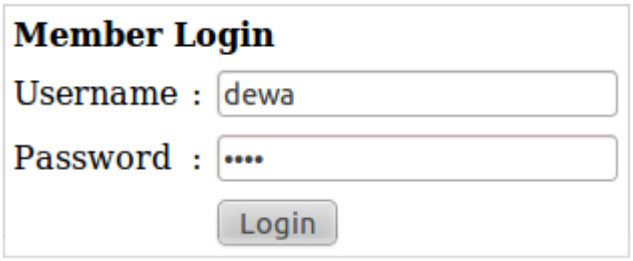
```
mysql> show tables;
+----------------+
| Tables_in_login |
+----------------+
| members        |
+----------------+
1 row in set (0.00 sec)

mysql> select * from members;
+----+----------+----------+
| id | username | password |
+----+----------+----------+
|  1 | dewa     | 1234     |
+----+----------+----------+
1 row in set (0.00 sec)

mysql>
```

Gambar 4.1 database yang dibuat

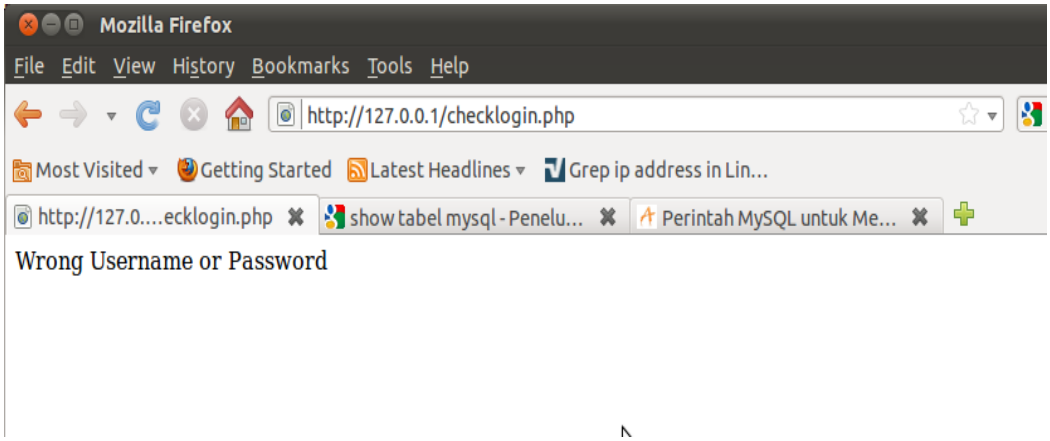
Proses authentifikasi dikatakan benar bila *user*name dan password yang dimasukan sesuai dengan *user*name dan password pada mysql (Gambar 4.1). Bila benar, aplikasi akan me-redirect page ke halaman aplikasi. Bila salah (tidak sesuai dengan database mysql), maka PC akan menolak untuk memasuki aplikasi. Berikut gambar hasil percobaaan:



Gambar 4.2 Login Sesuai Database

Gambar 4.3 Redirect Halaman Aplikasi

Gambar 4.4 Login Salah



Gambar 4.5 *User*name Salah

Uji coba dilakukan dengan menginputkan *user*name dan password. Ujicoba pertama dilakukan dengan memasukan *user*name dan password yang terdaftar pada database mysql (gambar 4.2). jika disubmit makan *user* dapat masuk ke sistem (gambar 4.3). sebaliknya jika *user*name memasukan *user*name dan password yang tidak terdaftar (Gambar 4.4). jika di submit makan aplikasi akan menolak untuk masuk kesistem (Gambar 4.5)

Dari gambar diatas dapat disimpulkan bahwa proses authentifikasi telah berjalan dengan baik. bila ada *user* yang tidak sesuai dengan database maka *user* tersebut tidak bisa mengakses aplikasi.

4.2 Pengujian Terhadap Pengaturan VLAN

Pengujian terhadap pengaturan VLAN dilakukan dengan memasukan data pada VLAN yang akan dibuat.

4.2.1 Tujuan

Tujuan pengujian ini yaitu mengetahui apakah aplikasi pada halaman pengaturan VLAN sudah mampu merubah table VLAN pada PC *Router*.

4.2.2 Alat yang Digunakan

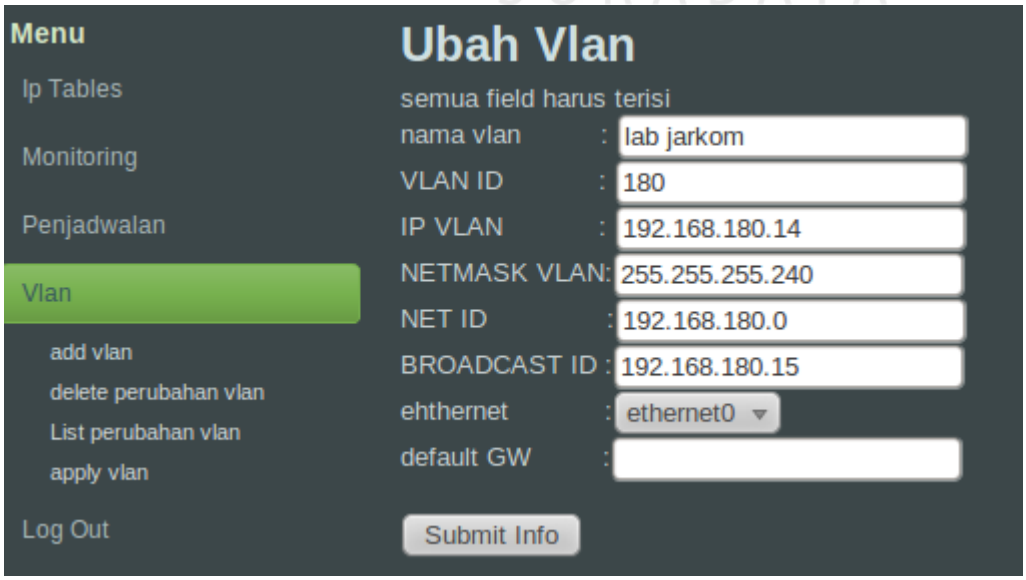
1. PC yang ditempatkan sebagai PC *Router*
2. aplikasi mengatur VLAN

4.2.3 Prosedur Pengujian

1. Menyalakan PC *Router*
2. masuk kedalam aplikasi penambahan VLAN
3. masukan data VLAN secara benar
4. pilih halaman apply VLAN untuk mengimplementasikan perubahan VLAN

4.2.4 Hasil Pengujian Pengaturan VLAN

Pengujian dilakukan dengan memasukan data VLAN pada aplikasi. Untuk pengujian, penulis memasukan VLAN sesuai dengan topologi pada laboratorium S1 Sistem Komputer Stikom Surabaya (Gambar 4.6).

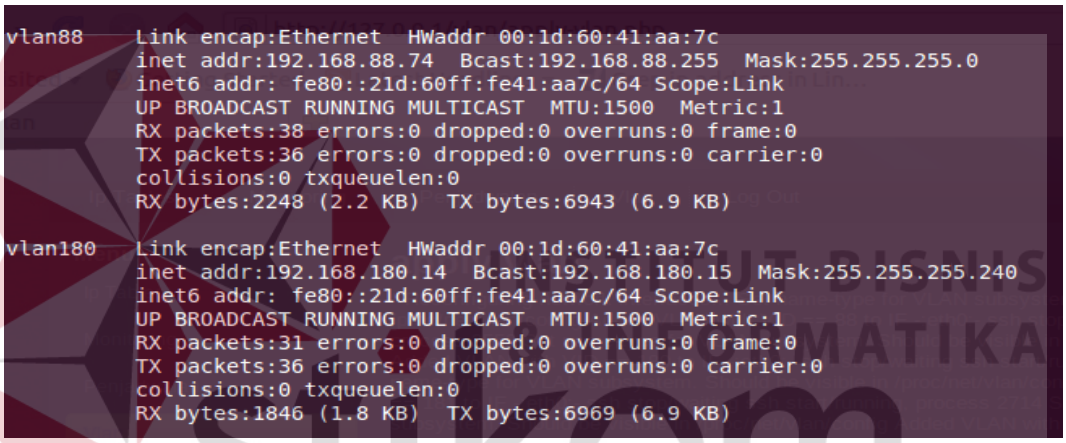


Gambar 4.6 Pengisian Form VLAN

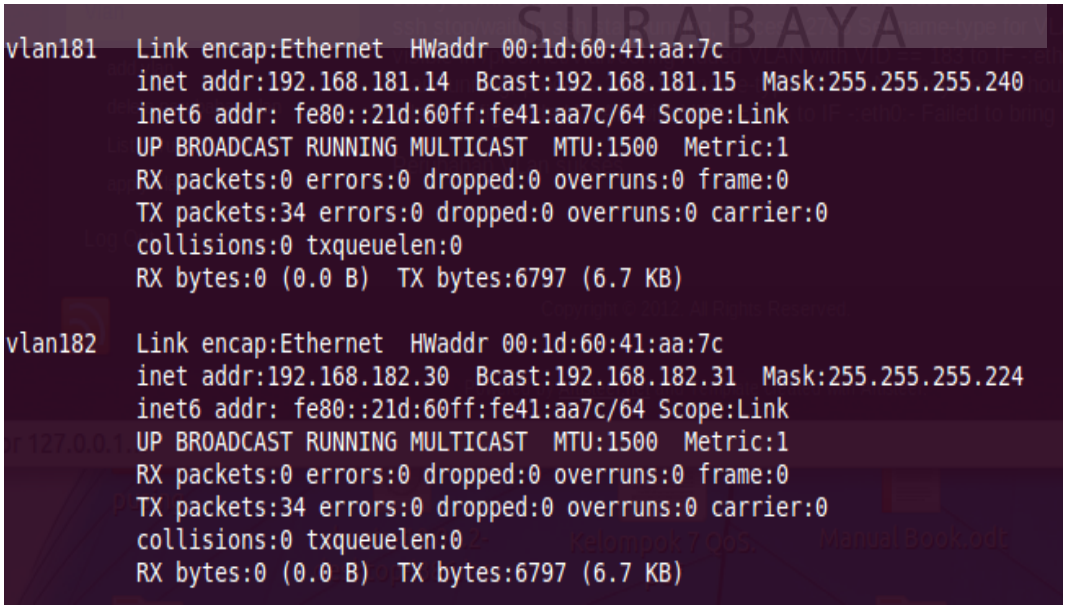
Langkah berikutnya setelah memasukan data tiap VLAN adalah proses apply. Dimana proses ini adalah proses memindahkan file interfaces yang dibuat pada penambahan VLAN ke /etc/*network*/interfaces. Selanjutnya mengulang layanan /etc/init.d/*network*ing. Penambahan VLAN dikatakan berhasil bila:

1. pada command ifconfig terlihat penambahan interface VLAN.
2. *client* berhasil melakukan ping terhadap gateway.

Berikut ini pengujian terhadap penambahan VLAN:



Gambar 4.7 VLAN 180 dan VLAN 88 berhasil dibuat



Gambar 4.8 VLAN 181 dan VLAN 82 berhasil dibuat

Gambar 4.8 dan 4.9 merupakan hasil ifconfig pada terminal setelah proses pembuatan VLAN dijalankan pada aplikasi. Kita lihat pada kolom pertama terbentuk VLAN-VLAN baru yaitu VLAN 88,180,181,182 dengan ip address, *broadcast* dan netmask yang telah dimasukkan pada aplikasi pembuatan VLAN.

Kesimpulannya penambahan VLAN pada aplikasi PC *Router* dapat berjalan semestinya, ditandai dengan adanya penambahan VLAN pada interface PC *Router*, dan juga PC *client* dapat melakukan akses ke internet.

4.3 Pengujian terhadap IP tables

Pengujian terhadap iptables dilakukan dengan memasukan aturan iptables yang akan dibuat.

4.3.1 Tujuan

Tujuan pengujian ini yaitu mengetahui apakah fungsi penambahan aturan iptables dan penghapusan aturan iptables sudah mampu merubah aturan iptable pada PC *Router*.

4.3.2 Alat yang digunakan

1. PC yang ditempatkan sebagai PC *Router*
2. aplikasi untuk mengatur iptables

4.3.3 Prosedur pengujian

1. Menyalakan PC *Router*

2. masuk kedalam aplikasi penambahan iptables

3. masukan aturan iptables

4. pilih submit

4.3.4 Hasil Pengujian IP Tables

Pengujian dilakukan yang dilakukan meliputi pengujian menambah aturan iptables, pengujian menghapus aturan iptables.

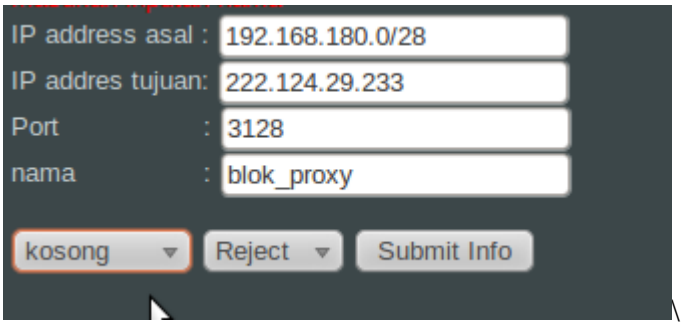
Pengujian terhadap penambahan aturan iptables dilakukan dengan memasukan data iptables kedalam halaman add VLAN. Sebagai percobaan penulis memasukan *rules* untuk menolak paket keluar dari laboratorium jaringan komputer. Maka aturan yang dibuat adalah laboratorium komputer dilarang untuk mengakses *proxy* dengan *port* 3128.

Penambahan aturan iptables dikatakan berhasil bila:

1. adanya penambahan aturan baru pada perintah *list* iptables.

2. tiap PC pada laboratorium jaringan komputer tidak dapat melakukan koneksi internet.

Berikut ini gambar pada pengujian penambahan aturan iptables:



Gambar 4.10 uji coba blok lab jarkom

Gambar 4.11 aturan berhasil ditambahkan

Gambar 4.10 merupakan aturan yang dibuat pada aplikasi untuk menola paket yang keluar dari laboratorium jaringan komputer dengan nama aturan adalah blok_proxy. Gambar 4.11 merupakan hasil melihat isi iptables yang dibuat, terlihat bahwa aturan yang dibuat telah masuk kedalam iptables.

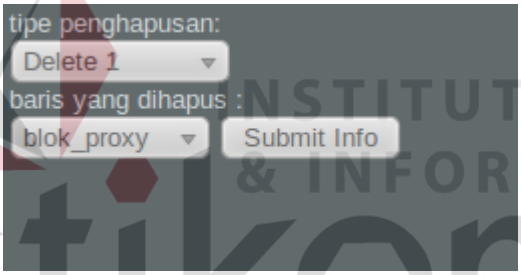
Pengujian terhadap penghapusan VLAN dilakukan dengan memasukan data pada halaman hapus VLAN. Terdapat 2 macam penghapusan, menghapus semua aturan dan menghapus aturan pada baris tertentu. Sebagai uji coba, penulis membuat 2 aturan, aturan pertama seperti gambar 4.10 dan aturan ke 2 adalah aturan untuk menolak paket ke proxy dengan ip 222.124.29.232 dengan nama blok_proxy2. Penghapusan dikatakan berhasil bila:

1. Aturan yang dihapus terhapus pada iptables *list*
2. Laboratorium jaringan komputer dapat melakukan koneksi kembali dengan internet

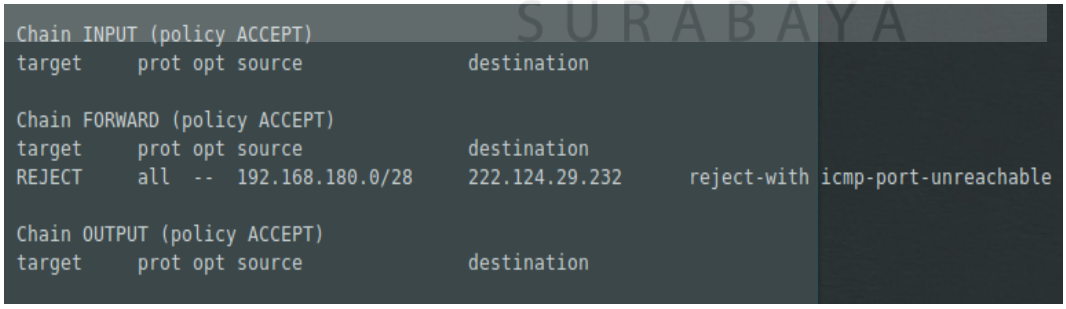
Berikut merupakan gambar hasil percobaan pada penghapusan iptables:

Gambar 4.12 Aturan uji coba sebelum dihapus

Gambar 4.12 terlihat bahwa isi dari iptables dimana ada 2 aturan yang baru dibuat untuk uji coba penghapusan iptables. Aturan yang dibuat adalah aturan untuk menolak paket laboratorium jaringan komputer untuk koneksi dengan proxy pegawai dan proxy mahasiswa.

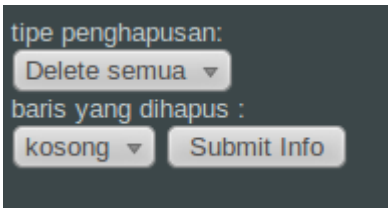


Gambar 4.13 menghapus aturan dengan nama blok_proxy

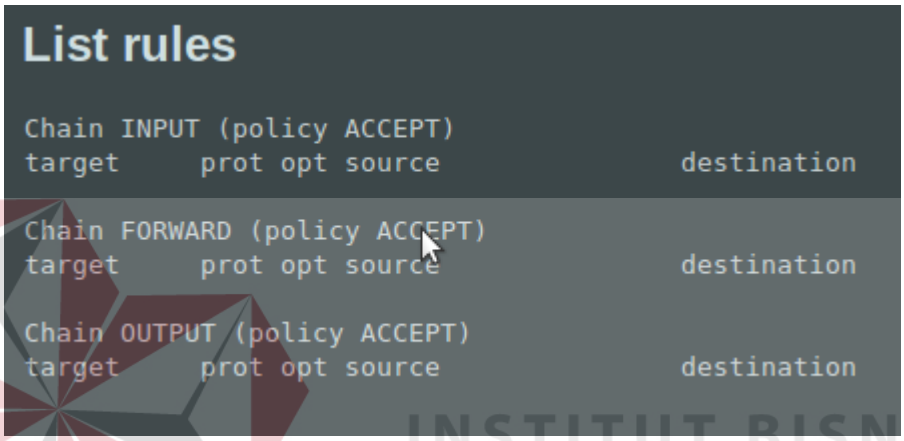


Gambar 4.14 aturan blok_proxy terhapus

Gambar 4.13 merupakan gambar inputan *user* pada form aplikasi, dimana *user* akan menghapus 1 aturan pada dengan nama blok_proxy. kita lihat bahwa aturan dengan nama blok_proxy terhapus. (gambar 4.14).



Gambar 4.15 menghapus semua aturan



Gambar 4.16 Semua Aturan Terhapus

Gambar 4.15 merupakan percobaan untuk menghapus semua aturan pada iptables. Setelah input dari form penghapusan dijalankan, terlihat bahwa isi dari iptables terhapus semua (Gambar 4.16) .

Dari hasil percobaan diatas dapat disimpulkan bahwa fungsi untuk pengaturan iptables, baik penambahan dan penghapusan iptables dapat berjalan dengan baik.

4.4 Pengujian Terhadap penjadwalan

Pengujian terhadap penjadwalan dilakukan dengan memasukan jadwal untuk menghapus aturan ataupun menambah aturan iptables.

4.4.1 Tujuan

Tujuan pengujian ini yaitu mengetahui apakah Penjadwalan iptables telah berjalan dengan baik atau tidak.

4.4.2 Alat yang Digunakan

1. PC yang ditempatkan sebagai PC *Router*
2. aplikasi untuk mengatur penjadwalan iptables

4.4.3 Prosedur pengujian

1. Menyalakan PC *Router*
2. masuk kedalam aplikasi penjadwalan iptables
3. masukan jadwal dan aturan iptables
4. pilih submit

4.4.4 Hasil Pengujian Penjadwalan

Pengujian dilakukan yang dilakukan meliputi pengujian penjadwalan untuk menambah aturan iptables, pengujian penjadwalan untuk menghapus aturan iptables.

Pengujian terhadap penjadwalan penambahan aturan iptables dilakukan dengan memasukan data iptables dan waktu penambahan iptables kedalam halaman penjadwalan penambahan iptables. Sebagai percobaan penulis memasukan *rules* untuk menolak paket keluar dari laboratorium jaringan komputer pada jam 13.42 tanggal 12 Februari. Maka aturan yang dibuat adalah

laboratorium komputer dilarang untuk mengakses *proxy* dengan *port* 3128 pada waktu yang ditentukan.

Penjadwalan Penambahan aturan iptables dikatakan berhasil bila:

1. terdapat aturan baru blok laboratorium pada waktu yang ditentukan.
2. laboratorium tidak dapat terkoneksi dengan internet.

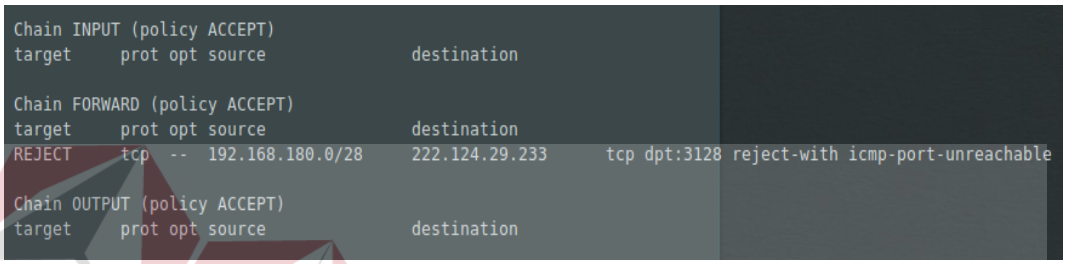
Berikut merupakan gambar hasil percobaan pada penjadwalan penambahan iptables:

Gambar 4.17 penambahan aturan penjadwalan lab jarkom

```
40 8 * * * echo sapi~   >> /home/sendy/vlan/nama
40 8 * * * sudo iptables -A FORWARD -s 192.168.180.0/28 -p tcp --dport 3128 -d 222.124.29.233 -j REJECT
```

Gambar 4.18 penambahan jadwal masuk kedalam file jadwal

Gambar 4.17 merupakan isi dari form penambahan jadwal iptables. Dimana terisi penambahan aturan untuk menolak paket lab jarkom ke proxy dengan *port number* 3128 pada jam 8.40 setiap hari dengan nama aturan adalah sapi. Ketika di submit, halaman melihat jadwal terbentuk 2 perintah baru perintah pertama berfungsi untuk menambah nama aturan kedalam file nama, sedangkan aturan kedua berfungsi menolak paket dari lab jarkom ke *proxy* (gambar 4.18).



Gambar 4.19 penambahan jadwal berhasil

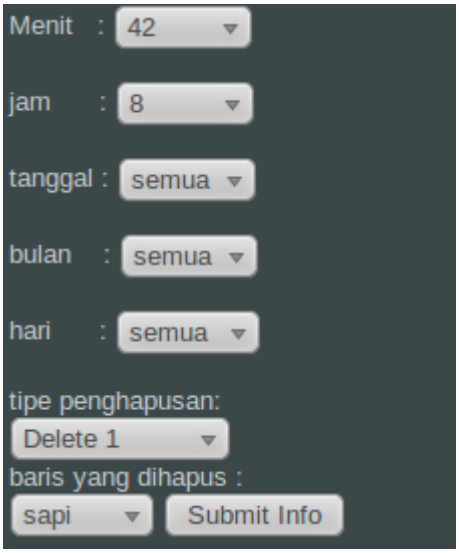
Gambar 4.19 merupakan isi iptables pada jam 8.40, dimana terbentuk suatu aturan baru yang menolak laboratorium jarkom untuk mengakses *proxy*.

Pengujian terhadap penjadwalan penghapusan aturan iptables dilakukan dengan memasukan data penghapusan iptables dan waktu penghapusan aturan iptables kedalam halaman penjadwalan penghapusan aturan iptables. Sebagai percobaan penulis memasukan *rules* menghapus aturan dengan nama sapi yaitu aturan menolak laboratorium jarkom keluar jaringan pada jam 8.42.

Penjadwalan Penambahan aturan iptables dikatakan berhasil bila:

1. aturan iptables dengan nama sapi hilang dari *list* iptables.
2. laboratorium dapat melakukan koneksi dengan internet.

Berikut merupakan gambar hasil percobaan pada penjadwalan penghapusan iptables:



Gambar 4.20 memasukan jadwal untuk menghapus aturan iptables

```
40 8 * * * echo sapi~   >> /home/sendy/vlan/nama
40 8 * * * sudo iptables -A FORWARD -s 192.168.180.0/28 -p tcp --dport 3128 -d 222.124.29.233 -j REJECT
42 8 * * * sudo iptables -D FORWARD 1
42 8 * * * sudo sh /home/sendy/vlan/coba.sh sapi
```

Gambar 4.21 hasil file jadwal

Gambar 4.20 merupakan form pengisian untuk penjadwalan penghapusan iptables, dengan perintah untuk menghapus aturan baris dengan nama sapi pada jam 8.42. Ketika di submit, terlihat pada *list* jadwal terbentuk penjadwalan yang baru (gambar 4.21). baris ke 3 adalah penjadwalan untuk menghapus baris 1 yaitu baris dengan nama aturan sapi, dan baris ke 4 adalah penjadwalan untuk memanggil *script* coba.sh. *script* coba.sh adalah *script* untuk menghapus nama dari aturan.

```
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
```

Gambar 4.22 aturan iptables berhasil dihapus

Gambar 4.22 merupakan isi dari iptables pada saat jadwal terpenuhi, terlihat bahwa iptables menghapus aturan sapi yaitu aturan untuk menolak paket keluar dari laboratorium mikro ke *proxy*. Sehingga komputer dari laboratorium jarkom dapat melakukan akses ke internet.

Dari gambar diatas disimpulkan bahwa penjadwalan iptables baik penghapusan dan penambahan aturan dapat berjalan dengan baik sesuai dengan harapan.

4.5 Pengujian terhadap Monitoring *Bandwith*

Pengujian terhadap monitoring *bandwith* dilakukan dengan memasukan laboratorium yang akan dipantau.

4.5.1 Tujuan

Tujuan pengujian ini yaitu mengetahui apakah fungsi monitoring *bandwith*, mampu menunjukan hasil yang akurat.

4.5.2 Alat yang Digunakan

1. PC yang ditempatkan sebagai PC *Router*
2. aplikasi untuk memonitoring *bandwith*.
3. *client* untuk ujicoba *bandwith* yang dipantau.

4.5.3 Prosedur Pengujian

1. Menyalakan PC *Router*
2. masuk kedalam aplikasi monitoring *bandwith*

3. masukan laboratorium yang dipantau dan submit

4. buka PC clien dan koneksikan dengan internet.

4.5.4 Hasil Pengujian *Bandwith*

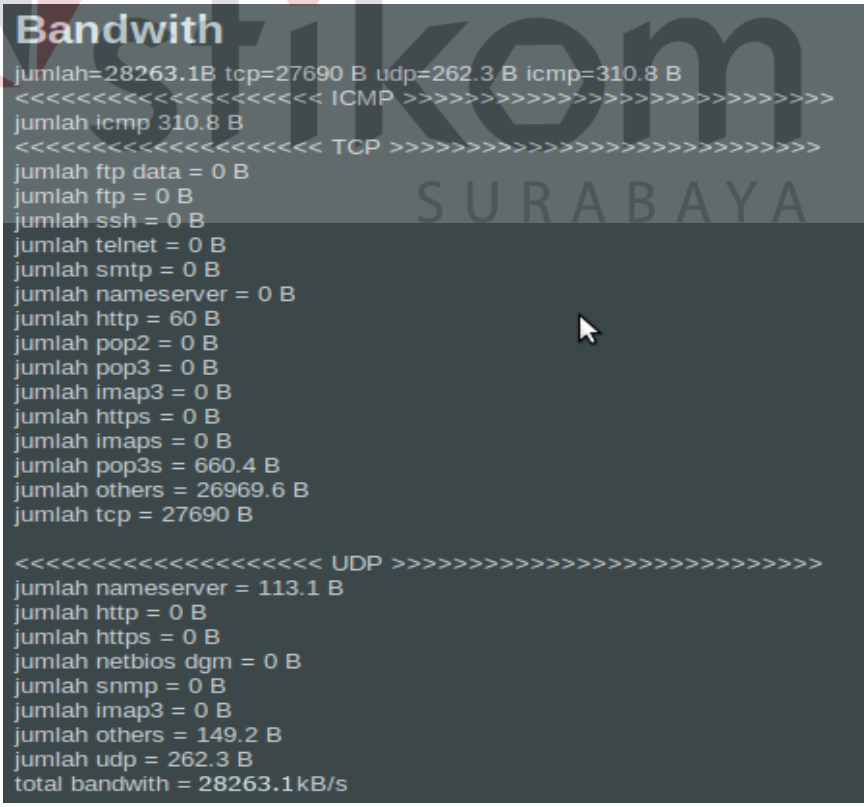
Pengujian dilakukan dengan pemantauan *bandwith* terhadap laboratorium tertentu. Sebagai uji coba penulis memantau *bandwith* untuk laboratorium jaringan komputer.

Monitoring *bandwith* dikatakan berhasil bila:

1. paket yang keluar dari PC *client*, terbaca oleh monitoring pada PC *Router*.

2. jumlah *bandwith* yang terbaca sesuai dengan jumlah *bandwith* dikeluarkan tiap PC *client*

Berikut ini gambar pada pengujian monitoring laboratorium jaringan komputer:



Gambar 4.23 Monitoring laboratorium jaringan komputer

Gambar 4.24 *bandwith* yang terlihat laboratorium jaringan komputer

Dari gambar 4.23 terlihat bahwa, jumlah paket yang dari *port* other sebesar 26.969,6 B. jumlah ini didapat dari pengelompokan panjang paket berdasarkan *port* dan jenis *protocol*. Setiap panjang paket *protocol* TCP dengan *port* other ditangkap dalam suatu variabel. Variabel tersebut dibagi dengan 10 (karena proses penangkapan terjadi selama 10 detik). Begitu pula dengan *port* dan *protocol* yang lainya.

Dari gambar diatas keseluruhan *bandwith* didapat dari jumlah paket TCP ditambah jumlah paket UDP ditambah jumlah paket ICMP. Untuk jumlah TCP, TCP = 60 Byte (http) + 660.4 Byte (pop3s) + 26.969,6 Byte (others). Hasilnya total TCP adalah 27.690 B . Total UDP = 113,1 Byte (name server) + 149,2 Byte (others). Total UDP adalah 262,3 total ICMP adalah 310,8 B. maka total *bandwith* = (27.690 Byte + 113,1 Byte + 310,8 Byte) / 1 s. Total *bandwith* adalah 28.2631 B/s

Dari hasil diatas disimpulkan bahwa monitoring *bandwith* dapat berjalan dengan baik. Angka yang terdapat pada speedometer adalah angka pembulatan dari total *bandwith*.

4.5 Pengujian terhadap monitoring PC

Pengujian terhadap monitoring PC dilakukan dengan memasukan laboratorium yang akan dipantau.

4.5.1 Tujuan

Tujuan pengujian ini yaitu mengetahui apakah fungsi monitoring PC dapat berjalan dengan baik.

4.5.2 Alat yang digunakan

1. PC yang ditempatkan sebagai PC *Router*
2. aplikasi untuk memonitoring PC.
3. *client* untuk ujicoba PC yang dipantau.

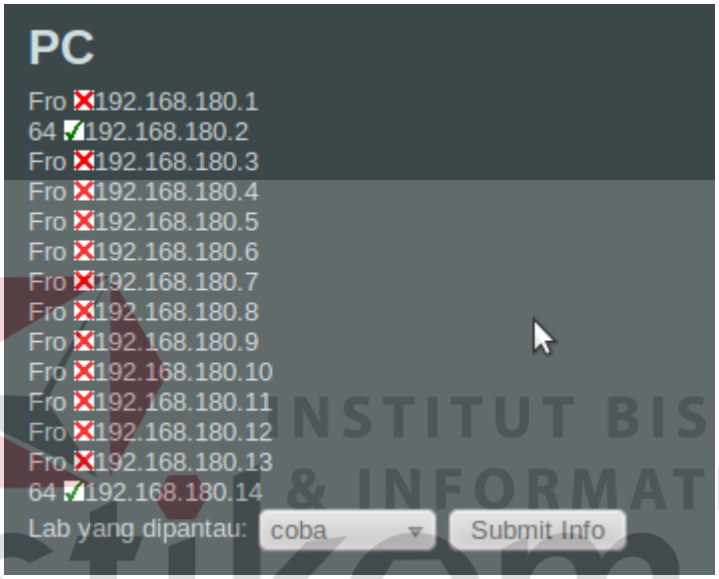
4.5.3 Prosedur pengujian

1. Menyalakan PC *Router*
2. masuk kedalam aplikasi monitoring PC
3. masukan laboratorium yang dipantau dan submit

4.5.4 Hasil Pengujian Monitoring PC

Pengujian dilakukan dengan pemantauan PC terhadap laboratorium tertentu. Sebagai uji coba penulis memantau *bandwith* untuk laboratorium

jaringan komputer. Monitoring *bandwith* dikatakan berhasil bila Data PC yang terhubung dengan jaringan sesuai dengan kondisi sesungguhnya. Uji coba dilakukan dengan 2 komputer, dimana komputer adalah PC *Router* (sebagai gateway) dengan ip 192.168.180.14 dan PC *client* dengan ip 192.168.180.2. berikut adalah gambar hasil uji coba.



Gambar 4.25 PC yang terkoneksi dengan jaringan

```
sendy@sendy-laptop:~$ ping 192.168.180.2
PING 192.168.180.2 (192.168.180.2) 56(84) bytes of data.
64 bytes from 192.168.180.2: icmp_req=1 ttl=128 time=2.96 ms
64 bytes from 192.168.180.2: icmp_req=2 ttl=128 time=0.112 ms
64 bytes from 192.168.180.2: icmp_req=3 ttl=128 time=0.114 ms
64 bytes from 192.168.180.2: icmp_req=4 ttl=128 time=0.112 ms
64 bytes from 192.168.180.2: icmp_req=5 ttl=128 time=0.113 ms
64 bytes from 192.168.180.2: icmp_req=6 ttl=128 time=0.109 ms
64 bytes from 192.168.180.2: icmp_req=7 ttl=128 time=0.101 ms
```

Gambar 4.26 ping terhadap 192.168.180.2 sukses

```
sendy@sendy-laptop:~$ ping 192.168.180.3
PING 192.168.180.3 (192.168.180.3) 56(84) bytes of data.
From 192.168.180.14 icmp_seq=1 Destination Host Unreachable
From 192.168.180.14 icmp_seq=2 Destination Host Unreachable
From 192.168.180.14 icmp_seq=3 Destination Host Unreachable
```

Gambar 4.27 Ping terhadap 192.168.180.1 gagal

Terlihat pada gambar 4.25 bahwa PC yang terkoneksi pada aplikasi adalah ip 192.168.180.2 dan ip 192.168.180.14. ip 192.168.180.2 adalah ip *client* dan 192.168.180.14 adalah ip dari server.

Ip yang terlihat pada aplikasi sama dengan paket ICMP yang dilakukan oleh terminal pada keadaan sesungguhnya (gambar 4.26 dan gambar 4.27). Kesimpulanya adalah aplikasi untuk monitoring PC sudah berjalan dengan baik.

4.6 Pengujian terhadap Validasi IP

Pengujian terhadap Validasi IP dilakukan dengan memasukan laboratorium yang akan dipantau.

4.6.1 Tujuan

Tujuan pengujian ini yaitu mengetahui apakah fungsi Validasi IP dapat berjalan dengan baik.

4.6.2 Alat yang digunakan

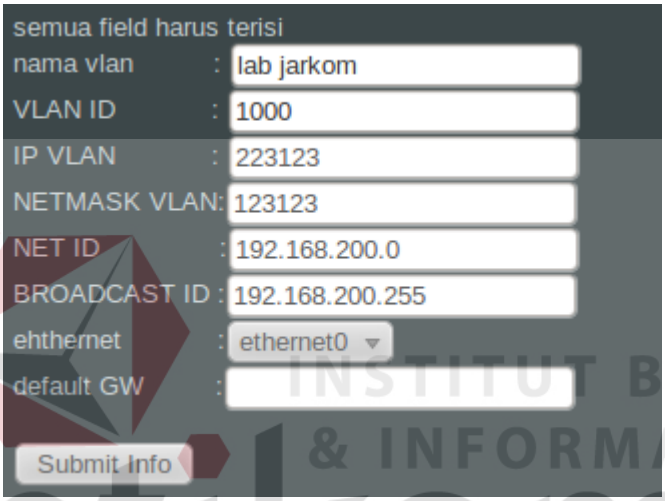
1. PC yang ditempatkan sebagai PC *Router*
2. aplikasi untuk valiadsi ip pada add vlan.

4.6.3 Prosedur pengujian

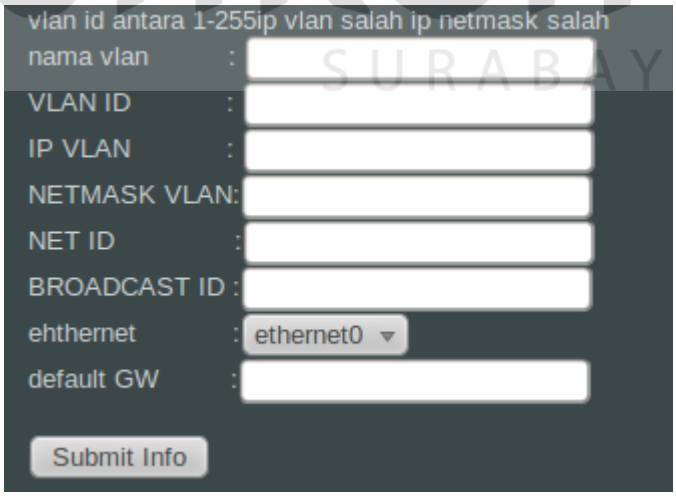
1. Menyalakan PC *Router*
2. masuk kedalam aplikasi Add vlan
3. masukan IP yang salah dan submit

4.6.4 Hasil Pengujian Validasi

Pengujian validasi dilakukan pada form penambahan VLAN, itput form yang dimasukan adalah ip yang salah seperti gambar 4.28. dimana ip vlan, vlan ID dan netmask vlan merupakan vlan yang tidak valid. Ip vlan harus mempunyai format x.x.x.x dimana tiap x mempunyai kisaran angka dari 0-255. Vlan id mempunyai kisaran angka dari 1-255.



Gambar 4.28 Percobaan validasi



Gambar 4.29 validasi berhasil

Setelah dilakukan form submit, maka akan terlihat hasil validasi pada gambar 4.29. dimana terdapat keterangan bahwa validasi yang dimasukan salah, sehingga *user* harus memasukkan ulang input ip, netmask dan juga vlan id.