**ISSN 2549-4805**

# PENYARINGAN WEBSITE MENGGUNAKAN IPTABLES PADA ROUTER BERBASIS LINUX

# FILTERING WEBSITE USING IPTABLES IN ROUTER BASED ON LINUX

**Dian Novianto[1], Laurentinus[2]**
**[1,2]Jurusan Teknik Informatika, STMIK Atma Luhur, Pangkalpinang**
**Jalan Jend. Sudirman – Selindung, Telp. (0717) 433506, Fax: (0717) 4255100, 433506**
**E-Mail: diannovianto@atmaluhur.ac.id[1], laurentinus@atmaluhur.ac.id[2]**

**Abstrak**

*Salah satu cara mengamankan jaringan adalah dengan cara melakukan filtering terhadap akses internet pengguna, oleh karena itu diperlukan kebijakan administrator mengenai informasi apa saja yang boleh diakses dan tidak boleh diakses, dimana kebijakan tersebut untuk melindungi privasi pengguna maupun keamanan sistem yang biasa disebut dengan internet sehat,, banyak kejahatan cyber terjadi akibat kelalaian pengguna dalam berselancar di dunia maya, terjebak dengan website phising, dan mendownload malware atau spyware secara tidak disengaja, salah satu cara untuk mencegah hal itu dengan melakukan filtering domain website pada proxy server, dimana seluruh pengguna akan diarahkan ke proxy server sebelum mendapatkan konten yang diinginkan, akan tetapi filtering menggunakan proxy server hanya dapat dilakukan untuk koneksi yang menggunakan protocol http, sedangkan pada protocol https, filtering domain website tidak dapat dilakukan karena sifat protocol https yang mengenkripsi komunikasi antara browser pengguna dan server tujuan. Oleh karena itu perlu dilakukan filtering dengan cara lain agar kebijakan penggunaan internet yang telah ditetapkan tidak dilanggar oleh pengguna, pada penelitian ini peneliti menggunakan metode network development live cycle untuk melakukan uji coba filtering melalui layer 7 menggunakan IPTABLES pada router dengan sistem operasi linux.*

**Kata Kunci** : *filtering web, iptables, ndlc, linux*

***Abstract***

*One way to secure networks is to perform filtering on a user's internet access, therefore it is necessary administrator policies about what information can be accessed and should not be accessed, where that policy to protect users' privacy and the security of the system is commonly referred to as a healthy internet, many cyber crimes happen caused by negligence users surf the internet, stuck with phishing website, and download malware or spyware unintentionally, one way to prevent it by doing the filtering domain websites on the proxy server, where all users will be redirected to the proxy server before getting the desired content, but filtering using a proxy server can only be performed for connections that use the http protocol, while the protocol https , the website domain filtering can not be performed due to the nature of https protocol that encrypts communication between the user's browser and the destination server. Therefore, it needs to be done other ways filtering internet use policy that has been set is not violated by the user, in this study researchers used a method live network development cycle to test filtering through layer 7 using IPTABLES on the router with Linux operating system.*

**Keywords** : *filtering web, iptables, ndlc, linux*

ISSN 2549-4805

## 1. PENDAHULUAN

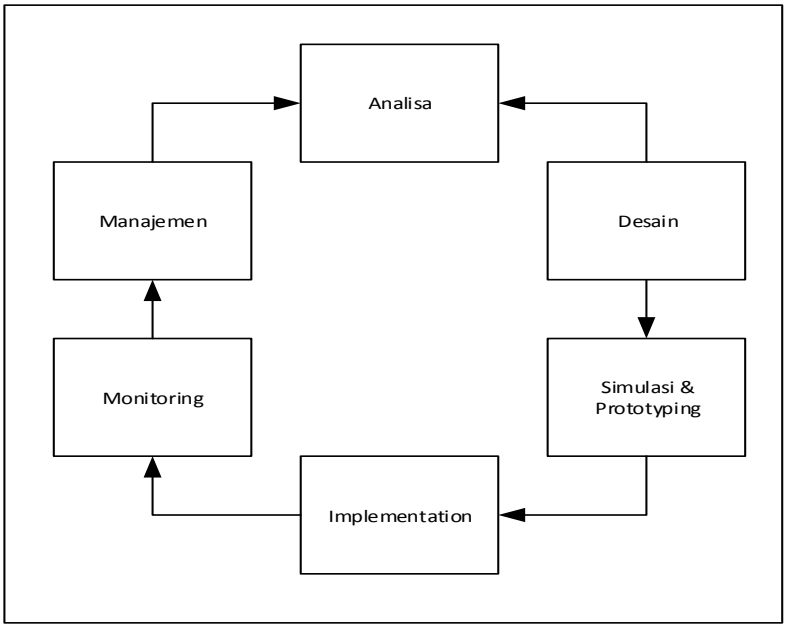
Dengan perkembangan internet yang semakin baik, dari sisi kecepatan maupun penyebarannya, memudahkan para pengguna dalam mengakses informasi, ditunjang teknologi perangkat mobile yang bisa dibawa kemana saja memungkinkan para pengguna mengakses tidak hanya melalui komputer, tetapi dapat menggunakan smartphone, dan notebook. Pada layanan internet ada satu hal yang perlu di ingat bahwa tidak ada jaringan komputer yang benar-benar aman. Sifat dari jaringan adalah melakukan komunikasi, dan setiap komunikasi dapat jatuh ke tangan orang lain serta disalahgunakan. Sistem keamanan membantu mengamankan jaringan tanpa menghalangi penggunaannya untuk berkomunikasi dan menempatkan antisipasi ketika jaringan bermasalah dari sisi keamanan. Tujuan keamanan jaringan komputer adalah *Availability*/Ketersediaan, *Reliability*/ Kehandalan, *Confidentiality*/Kerahasiaan. Banyak cara untuk mengamankan jaringan, salah satunya melalui media router, router adalah sebuah alat jaringan komputer yang mengirimkan paket data melalui sebuah jaringan atau internet menuju tujuannya, melalui sebuah proses yang dikenal sebagai routing. Router berfungsi sebagai penghubung antar dua atau lebih jaringan untuk meneruskan data dari satu jaringan ke jaringan lainnya. Salah satu kerja router adalah sebagai *packet inspector* yaitu memeriksa paket yang masuk kedalam jaringan internal maupun yang akan keluar jaringan internal. Ada banyak konfigurasi untuk mengamankan jaringan melalui router, antara lain, membatasi akses koneksi dengan cara memblok ip, memilih ip mana saja yang bisa saling terkoneksi, memblokir servis internet protokol, memblok domain website dan lain-lain. Masalah yang sering terjadi saat ini pada STMIK Atma Luhur Pangkalpinang adalah filtering yang dilakukan hanya mampu melakukan fungsinya pada website yang menggunakan protokol http, sedangkan pada protokol https *filtering* belum bisa dilakukan, Protokol HTTPS dirancang untuk menyediakan sarana komunikasi yang aman antara internet browser dan web server. Untuk mencapai tujuan ini protokol HTTPS mengenkripsi data melalui koneksi yang disediakan sehingga tidak dapat didekripsi dalam jumlah waktu yang wajar sehingga mencegah orang lain yang berniat mengambil data melalui koneksi ini. Protokol ini awalnya diciptakan terutama untuk komunikasi website lembaga keuangan atau lembaga pemerintah melalui media yang tidak aman seperti internet. Namum saat ini banyak website yang telah menyediakan akses dengan HTTPS untuk meningkatkan privasi pengunjung mereka. Masalah utama di sini adalah inti dari protokol HTTPS sendiri tidak ada seorang pun kecuali browser dan web server mampu melihat dan mentransfer data. Hal ini mungkin tidak selalu diinginkan oleh administrator jaringan. Isi yang biasanya diblokir tiba-tiba menjadi segera dapat diakses oleh siapa saja. Sedangkan banyak kejahatan *cyber* seperti penipuan melalui website *phising*, ataupun website yang memiliki *spyware* maupun virus, sehingga apabila pengunjung web tersebut mengunjungi tautan yang diberikan serta dengan tidak sengaja mengunduh kontent yang tidak dikenal dan ternyata konten tersebut adalah *spyware*, maka informasi pribadi yang bersifat rahasia bisa diketahui pihak lain, oleh karena itu perlunya penyaringan website apa saja yang bisa diakses dan yang tidak bisa diakses untuk keamanan jaringan maupun pengguna itu sendiri, baik ketika menggunakan protokol HTTP maupun HTTPS. Pada penelitian terdahulu pernah dilakukan penelitian oleh penulis sendiri dengan judul "Pemfilteran *Hypertext Transfer Protocol Secure* Untuk Penggunaan Internet Yang Aman" dan telah dipublikasikan pada jurnal informatika IBI Darmajaya No. ISSN : 1693-3877 dan No. e-ISSN : 2407-1544[1], yaitu memanfaatkan SSL Bump pada squid 3.x menggunakan aplikasi tambahan yaitu *diladele web safety*, kendala yang dihadapi adalah setiap internet browser klien harus mempunyai sertifikat

ISSN 2549-4805

diladele web safety supaya filtering bisa berhasil diterapkan, hal ini dirasa kurang praktis karena apabila pengguna tidak mengunduh website maka pengguna tidak dapat mengakses semua web dengan protokol https. Oleh karena itu penulis mencoba cara lain yang memungkinkan sebuah website dapat difilter sesuai kebijakan internet sehat melalui sistem tanpa melibatkan perangkat pengguna.

## 2. METODE PENELITIAN

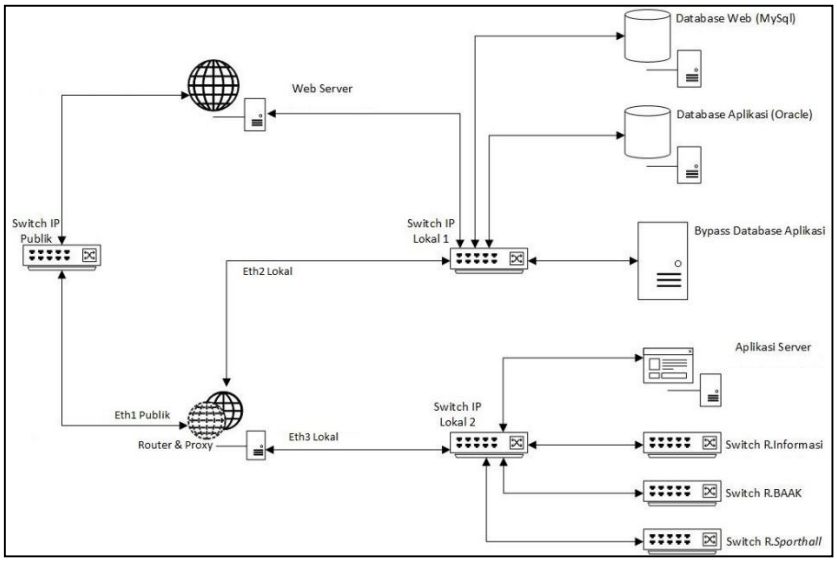
Metode penelitian yang digunakan pada penelitian ini adalah *network development life cycle* (NDLC), merupakan sebuah metode yang bergantung pada proses pembangunan sebelumnya seperti perencanaan, daur hidup pengembangan aplikasi, dan analisis pendistribusian data. Jika pengimplementasian teknologi jaringan dilaksanakan dengan efektif, maka akan memberikan sistem informasi yang akan memenuhi tujuan strategis bagi bisnis.




**Gambar 2.1** NDLC (*Network Development Life Cycle*)

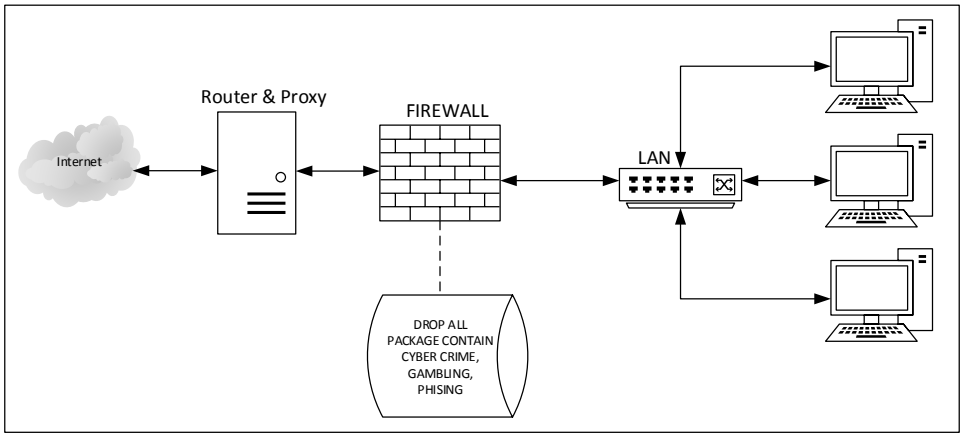
Analisa yang dilakukan adalah dengan melihat data – data berupa spesifikasi perangkat lunak dan perangkat keras yang digunakan, jumlah pengguna, topologi jaringan yang ada pada jaringan STMIK Atma Luhur Pangkalpinang saat ini, dimana router akan terhubung ke IP Publik melalui Ethernet 1, dan koneksi akan diteruskan ke jaringan lokal melalui Ethernet 2 dan Ethernet 3, dimana kelas ip lokal 1 dan ip lokal 2 tersebut berbeda yaitu 192.168.0.0/24 dan 192.168.1.0/24.

ISSN 2549-4805




**Gambar 2.2.** Topologi Jaringan Atma Luhur

Tahapan kedua berupa desain yaitu merencanakan bagaimana sistem ini akan berjalan ketika penerapan konfigurasi telah dilakukan, yaitu seluruh permintaan akses web pengguna dengan menggunakan protokol http maupun https dapat ter*filter* dengan baik menggunakan iptables, sehingga dapat terbentuk *firewall* seperti desain jaringan dibawah ini.




**Gambar 2.3.** Desain Sistem

Dimana firewall yang terbentuk akan membuang paket yang masuk kedalam kategori *blacklist*, Firewall sendiri merupakan perangkat jaringan yang berada pada Lapisan 3 (*Network layer*) dan Lapisan 4 (*Transport layer*) pada protokol OSI layer. Seperti diketahui, lapisan 3 adalah lapisan yang mengurus masalah pengalamatan IP, dan layer 4 adalah menangani permasalahan *port-port* komunikasi (TCP/UDP). Salah satu cara membangun sebuah *firewall* dalam sistem operasi linux adalah dengan memanfaatkan program iptables.

Iptables adalah program baris perintah yang digunakan untuk mengkonfigurasi paket *filtering ruleset* pada kernel linux 2.4.x. Dan ditargetkan untuk administrator sistem[2].

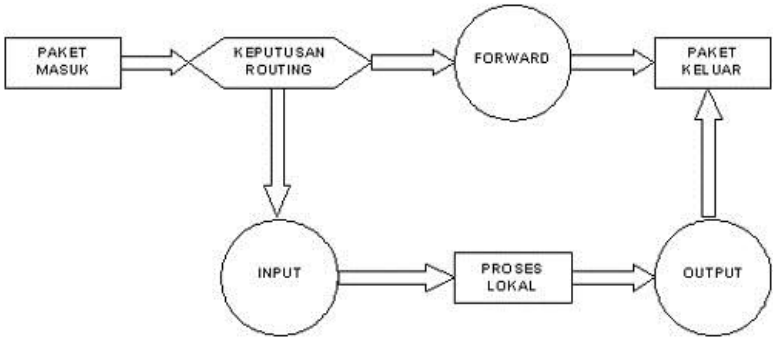
Fitur yang dimiliki IPTables:

1. *Connection Tracking Capability* yaitu kemampuan unutk inspeksi paket serta bekerja dengan icmp dan udp sebagaimana koneksi TCP.
2. Menyederhanakan perilaku paket-paket dalam melakukan negosiasi built in chain (*input*, *output*, dan *forward*).

ISSN 2549-4805

3. *Rate-Limited connection* dan *logging capability*. Kita dapat membatasi usaha-usaha koneksi sebagai tindakan preventif dari serangan *Syn flooding* yang dapat berakibat *denial of services* (DOS) pada sistem.
4. Kemampuan untuk memfilter flag-flag dan opsi tcp dan address dari MAC[3].

Iptables mengizinkan user untuk mengontrol sepenuhnya jaringan melalui paket IP dengan system LINUX yang diimplementasikan pada kernel Linux. Sebuah kebijakan atau Policy dapat dibuat dengan iptables sebagai polisi lalulintas jaringan. Sebuah policy pada iptables dibuat berdasarkan sekumpulan peraturan yang diberikan pada kernel untuk mengatur setiap paket yang datang. Pada iptable ada istilah yang disebut dengan Ipchain yang merupakan daftar aturan bawaan dalam Iptables. Ketiga chain tersebut adalah INPUT, OUTPUT dan FORWARD. Sebuah rantai adalah aturan-aturan yang telah ditentukan. Setiap aturan menyatakan "jika paket memiliki informasi awal (header) seperti ini, maka inilah yang harus dilakukan terhadap paket". Jika aturan tersebut tidak sesuai dengan paket, maka aturan berikutnya akan memproses paket tersebut. Apabila sampai aturan terakhir yang ada, paket tersebut belum memenuhi salah satu aturan, maka kernel akan melihat kebijakan bawaan (*default*) untuk memutuskan apa yang harus dilakukan kepada paket tersebut. Ada dua kebijakan bawaan yaitu default DROP dan default ACCEPT [4].




**Gambar 2.4. A**lur kerja *Iptables*

Pada pemfilteran ini dilakukan menggunakan chain *forward,* dimana cara kerja dari chain forward pada iptables itu sendiri antara lain :

1. Dimulai dengan paket data berada pada jaringan fisik.
2. Paket masuk ke *interface* jaringan.
3. Paket masuk ke chain PREROUTING pada table Mangle. Chain ini berfungsi untuk me-mangle (menghaluskan) paket, seperti merubah TOS, TTL dan lain-lain.
4. Paket masuk ke chain PREROUTING pada tabel NAT. Chain ini fungsi utamanya untuk melakukan DNAT (*Destination Network Address Translation*).
5. Paket mengalami keputusan routing, apakah akan diproses oleh host lokal atau diteruskan ke host lain.
6. Paket masuk ke chain FORWARD pada tabel filter. Disinlah proses pemfilteran yang utama terjadi.
7. Paket masuk ke chain POSTROUTING pada tabel NAT. Chain ini berfungsi utamanya untuk melakukan SNAT (*Source Network Address Translation*).
8. Paket keluar menuju interface jaringan.
9. Paket kembali berada pada jaringan fisik[3].

Perjalanan paket yang ditujukan bagi host lokal

ISSN 2549-4805

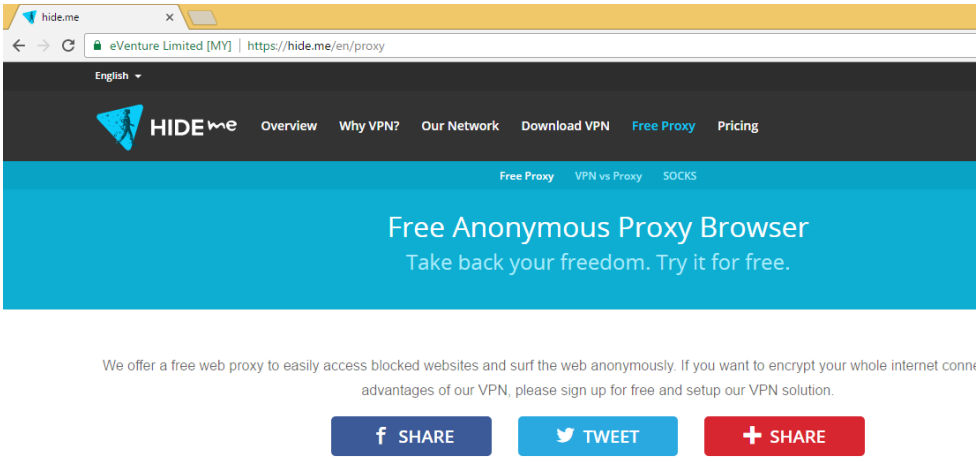
1. Paket beradadalam jaringan fisik.
2. Paket masuk ke interface jaringan.
3. Paket masuk ke chain PREROUTING pada tabel mangle.
4. Paket masuk ke chain PREROUTING pada tabel NAT.
5. Paket mengalami keputusan routing.
6. Paket masuk ke chain INPUT pada tabel filter untuk mengalami proses penyaringan.
7. Paket akan diterima oleh aplikasi lokal [3].

Perjalanan paket yang berasal dari host lokal

1. Aplikasi lokal menghasilkan paket data yang akan dikirimkan melalui jaringan.
2. Paket memasuki chain OUTPUT pada tabel mangle.
3. Paket memasuki chain OUTPUT pada tabel NAT.
4. Paket memasuki chain OUTPUT pada tabel filter.
5. Paket mengalami keputusan routing, seperti ke mana paket harus pergi dan melalui interface mana.
6. Paket masuk ke chain POSTROUTING pada tabel NAT.
7. Paket masuk ke interface jaringan
8. Paket berada pada jaringan fisik[3].

## 3. HASIL DAN PEMBAHASAN

Sebelum dilakukan konfigurasi pada router, pengguna masih dapat mengakses website yang menjadi contoh ujicoba, itu https://hide.me melalui media browser, dimana website ini menyediakan akses proxy gratis dan vpn gratis.




**Gambar 3.1.** Akses Website

Pada media lain menggunakan command prompt dengan mengetikan perintah ping, terlihat server tujuan memberikan balasan berupa ukuran paket yang dikirim dalam satuan byte, waktu untuk mencapai tujuan, TTL (time to live) dari server tujuan.

ISSN 2549-4805

```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\vian>ping hide.me

Pinging hide.me [128.199.189.242] with 32 bytes of data:
Reply from 128.199.189.242: bytes=32 time=77ms TTL=52
Reply from 128.199.189.242: bytes=32 time=82ms TTL=52
Reply from 128.199.189.242: bytes=32 time=81ms TTL=52
Reply from 128.199.189.242: bytes=32 time=81ms TTL=52

Ping statistics for 128.199.189.242:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 77ms, Maximum = 82ms, Average = 80ms

C:\Users\vian>_
```

**Gambar 3.2.** Ping website

Selain menggunakan perintah ping, digunakan perintah lain yaitu tracert, fungsi tracert hamper sama dengan mengirimkan pesan ICMP untuk mengetahui apakah website tujuan bisa diakses beserta jalur yang dilaluinya.

```
C:\Users\vian>tracert hide.me

Tracing route to hide.me [128.199.189.242]
over a maximum of 30 hops:

  1     1 ms    <1 ms     1 ms  192.168.1.1
  2    11 ms    20 ms    10 ms  ip-182-113.moratelindo.co.id [202.43.182.113]
  3     7 ms     7 ms     7 ms  ip-203-176-181-229.moratelindo.co.id [203.176.18
1.229]
  4    20 ms    20 ms    20 ms  103.56.234.65
  5    26 ms    42 ms    21 ms  133165.sgw.equinix.com [27.111.228.201]
  6    26 ms    21 ms    20 ms  138.197.250.227
  7    21 ms    24 ms    21 ms  hide.me [128.199.189.242]

Trace complete.

C:\Users\vian>
```

**Gambar 3.3.** *Tracert* website

Pada tahapan simulasi dan implementasi yang dilakukan adalah melakukan konfigurasi pada router, agar dapat meneruskan paket data, kepada para pengguna karena pada topologi diatas telihat bahwa jaringan di atmaluhur memiliki 2 kelas ip lokal yang berbeda, dan agar tetap dapat terhubung digunakan perintah route add, sedangkan /etc/network/filter.rule merupakan lokasi baris perintah untuk melakukan filtering terhadap mac address dari pengguna, hanya pengguna yang terdaftar di bagian sistem informasi yang bisa mendapatkan hak akses di jaringan lan melalui media kabel di STMIK Atma Luhur, selain filtering mac address, filter.rule juga berisi baris perintah prerouting, dimana seluruh koneksi akan diarahkan menuju port 3128 terlebih dahulu yang dimiliki oleh proxy.

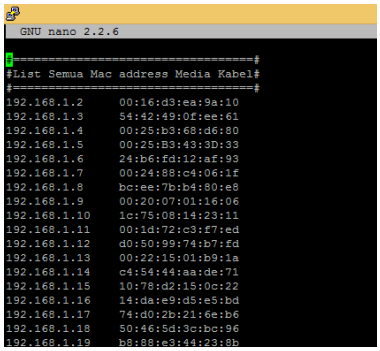
```
#!/bin/sh -e
#
# rc.local
#
# This script is executed at the end of each multiuser runlevel.
# Make sure that the script will "exit 0" on success or any other
# value on error.
#
# In order to enable or disable this script just change the execution
# bits.
#
# By default this script does nothing.

#Limiting the incoming icmp ping request:
iptables -F
iptables -t nat -F
iptables -t mangle -F
iptables -t nat -A POSTROUTING -j MASQUERADE
iptables -t nat -A POSTROUTING -o eth3 -j MASQUERADE
iptables -t nat -A POSTROUTING -o eth2 -j MASQUERADE
route add -host 192.168.0.12 gw 192.168.0.1
route add -host 192.168.0.229 gw 192.168.0.1
route add -host 192.168.0.249 gw 192.168.0.1
route add -host 192.168.0.251 gw 192.168.0.1
route add -host 192.168.0.250 gw 192.168.0.1
route add -host 192.168.0.252 gw 192.168.0.1
route add -host 192.168.0.253 gw 192.168.0.1

/etc/network/filter.rule
iptables -A FORWARD ! -s 192.168.1.0/24 -m string --string "hide" --algo bm --to 65535 -j DROP
```

**Gambar 3.3.** Konfigurasi

ISSN 2549-4805


**Gambar 3.4.** Konfigurasi *direct proxy*

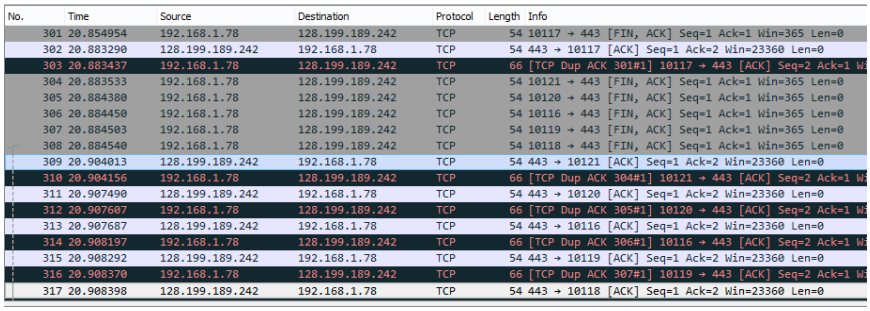
Sedangkan letak daftar mac address berada pada direktori /etc/network/filter.list, cara kerja perintah diatas adalah dengan memastikan bahwa para pengguna dengan mac address yang telah terdaftar hanya menggunakan ip address yang diberikan, tanpa bisa merubah sendiri, apabila pengguna memakai ip address yang berbeda dari yang diberikan oleh bagian sistem informasi, maka pengguna tidak akan bisa mengakses internet maupun sistem.




**Gambar 3.5.** *List mac address*

Pada konfigurasi penelitian ini, ditambahkan *rule Drop* pada *chain forward* menggunakan iptables dengan Opsi perintah -A, atau append, perintah ini berguna untuk menambahkan satu aturan baru yang akan ditempatkan pada aturan paling bawah, lalu –s adalah *source* berupa alamat *ip* jaringan lokal pada eth3, dan paket yang di drop menggandung karakter string pada domain yaitu *hide.*, dan sample website yang digunakan adalah https://hide.me dengan ip 128.199.189.242.

Pada tahapan monitoring, yang dilakukan adalah mengamati kondisi jalannya paket di jaringan setelah implementasi dilakukan dapat berupa pewaktuan, latency, troughput, dan lain-lain, menggunakan *tools* tambahan yaitu wireshark.



| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 301 | 20.854954 | 192.168.1.78 | 128.199.189.242 | TCP | 54 | 10117 → 443 [FIN, ACK] Seq=1 Ack=1 Win=365 Len=0 |
| 302 | 20.883290 | 128.199.189.242 | 192.168.1.78 | TCP | 54 | 443 → 10117 [ACK] Seq=1 Ack=2 Win=23360 Len=0 |
| 303 | 20.883437 | 192.168.1.78 | 128.199.189.242 | TCP | 66 | [TCP Dup ACK 301#1] 10117 → 443 [ACK] Seq=2 Ack=1 W |
| 304 | 20.883533 | 192.168.1.78 | 128.199.189.242 | TCP | 54 | 10121 → 443 [FIN, ACK] Seq=1 Ack=1 Win=365 Len=0 |
| 305 | 20.884380 | 192.168.1.78 | 128.199.189.242 | TCP | 54 | 10120 → 443 [FIN, ACK] Seq=1 Ack=1 Win=365 Len=0 |
| 306 | 20.884450 | 192.168.1.78 | 128.199.189.242 | TCP | 54 | 10116 → 443 [FIN, ACK] Seq=1 Ack=1 Win=365 Len=0 |
| 307 | 20.884503 | 192.168.1.78 | 128.199.189.242 | TCP | 54 | 10119 → 443 [FIN, ACK] Seq=1 Ack=1 Win=365 Len=0 |
| 308 | 20.884540 | 192.168.1.78 | 128.199.189.242 | TCP | 54 | 10118 → 443 [FIN, ACK] Seq=1 Ack=1 Win=365 Len=0 |
| 309 | 20.904013 | 128.199.189.242 | 192.168.1.78 | TCP | 54 | 443 → 10121 [ACK] Seq=1 Ack=2 Win=23360 Len=0 |
| 310 | 20.904156 | 192.168.1.78 | 128.199.189.242 | TCP | 66 | [TCP Dup ACK 304#1] 10121 → 443 [ACK] Seq=2 Ack=1 W |
| 311 | 20.907490 | 128.199.189.242 | 192.168.1.78 | TCP | 54 | 443 → 10120 [ACK] Seq=1 Ack=2 Win=23360 Len=0 |
| 312 | 20.907607 | 192.168.1.78 | 128.199.189.242 | TCP | 66 | [TCP Dup ACK 305#1] 10120 → 443 [ACK] Seq=2 Ack=1 W |
| 313 | 20.907687 | 128.199.189.242 | 192.168.1.78 | TCP | 54 | 443 → 10116 [ACK] Seq=1 Ack=2 Win=23360 Len=0 |
| 314 | 20.908197 | 192.168.1.78 | 128.199.189.242 | TCP | 66 | [TCP Dup ACK 306#1] 10116 → 443 [ACK] Seq=2 Ack=1 W |
| 315 | 20.908292 | 128.199.189.242 | 192.168.1.78 | TCP | 54 | 443 → 10119 [ACK] Seq=1 Ack=2 Win=23360 Len=0 |
| 316 | 20.908370 | 192.168.1.78 | 128.199.189.242 | TCP | 66 | [TCP Dup ACK 307#1] 10119 → 443 [ACK] Seq=2 Ack=1 W |
| 317 | 20.908398 | 128.199.189.242 | 192.168.1.78 | TCP | 54 | 443 → 10118 [ACK] Seq=1 Ack=2 Win=23360 Len=0 |

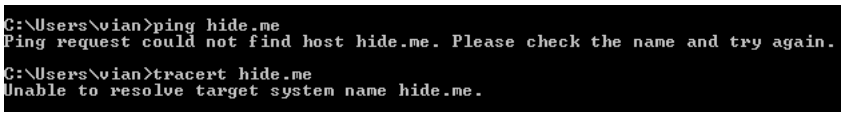
**Gambar 3.4.** *wireshark*

ISSN 2549-4805

Dari wireshark dapat diketahui bagaimana komputer klien dengan ip 192.168.1.78 melakukan hubungan dengan server tujuan dengan melakukan three way handshake, sebelum komunikasi dapat terjalin, informasi waktu antar paket juga dapat dilihat dalam hitungan *millisecond*, terlihat bahwa port yang dituju adalah 443, dimana port ini digunakan oleh protokol secure untuk halaman website.

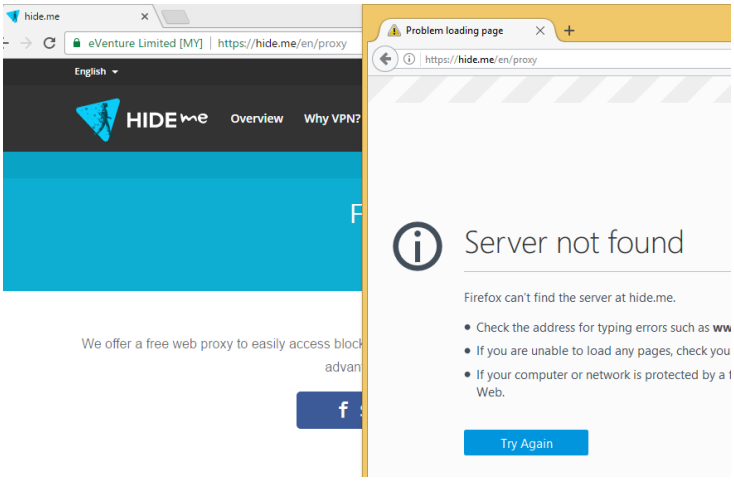
Setelah monitoring dilakukan menggunakan wireshark, dilakukan kembali dengan *tools command prompt* yang dimiliki oleh sistem operasi pengguna, dengan mengetikkan perintah ping dan tracert, perintah ping berfungsi sebagai sebuah tool yg digunakan untuk mengecek konektivitas antar satu komputer dengan lainnya, Hal ini dilakukan dengan mengirim sebuah pesan *Internet Control Message Protocol* (ICMP) kepada IP Address yang hendak diujicoba konektivitasnya dan menunggu respon darinya [5].

Traceroute (Tracert) adalah perintah untuk menunjukkan rute yang dilewati paket untuk mencapai tujuan. Ini dilakukan dengan mengirim pesan Internet Control Message Protocol (ICMP) Echo Request Ke tujuan dengan nilai Time to Live yang semakin meningkat. Rute yang ditampilkan adalah daftar interface router (yang paling dekat dengan host) yang terdapat pada jalur antara host dan tujuan [6].




**Gambar 3.5** Hasil *Ping* dan *Tracert*

Terlihat dari gambar diatas bahwa klien tidak bisa menemukan website yang menjadi bahan ujicoba, dimana browser memberitahu bahwa sistem tidak bisa menemukan domain dengan nama hide.me, sesuai dengan cara kerja iptables, dimana pada layer aplikasi pada browser dihalangi untuk melakukan permintaan terhadap server tujuan.




**Gambar 3.6** Hasil *Browsing* 2

Setelah konfigurasi berhasil diterapkan langkah terakhir yang juga penting adalah melakukan tahapan manajemen, Pada level manajemen atau pengaturan, salah satu yang menjadi perhatian khusus adalah masalah kebijakan (*policy*). Kebijakan perlu dibuat untuk membuat/mengatur agar sistem yang telah dibangun dan berjalan dengan baik dapat berlangsung lama dan unsur *reliability* terjaga.

ISSN 2549-4805

## 4. KESIMPULAN

Kesimpulan dari penelitian ini bahwa dengan memanfaatkan fungsi dari forward iptables, paket – paket yang sesuai dengan rule DROP akan langsung di buang oleh router, sehingga pengguna tidak akan bisa mengakses website yang dituju, tetapi pengguna tidak akan langsung mengetahui bahwa website tersebut tidak bisa diakses karena browser akan mencoba menunggu balasan dari server yang dituju beberapa saat sebelum memberikan informasi kepada pengguna bahwa server tujuan tidak ditemukan. Berhasil atau tidaknya penggunaan filtering ini tergantung dari kata kunci yang dimasukkan, dan terkadang website yang tidak masuk dalam blacklist tetapi domainnya mengandung kata yang sesuai dengan kategori blacklist maka website tersebut akan ikut terfilter, karena filtering ini dilakukan pada layer 7, apabila browser cache dan cookies nya tidak dibersihkan, atau browser tidak dimuat ulang, maka filtering tidak akan langsung berdampak terhadap aktivitas browsing dari klien.

## 5. SARAN

Perlunya dicari konfigurasi tambahan agar filtering dapat tepat sasaran sesuai dengan domain yang dimaksud dan langsung berdampak terhadap aktivitas browsing yang dilakukan oleh klien, tanpa harus memuat ulang browser.

## UCAPAN TERIMA KASIH

1. Terima kasih kepada yayasan atma luhur yang telah memberikan bantuan dana sehingga penelitian ini dapat berjalan dengan baik.
2. Terima kasih kepada Kepala Bagian Sistem Informasi yang telah mengizinkan peneliti untuk menggunakan berbagai peralatan inventaris BSI yang dibutuhkan dalam penelitian ini.
3. Terima kasih kepada rekan-rekan dosen yang telah membantu peneliti dalam menyelesaikan penelitian ini.

## DAFTAR PUSTAKA

[1] Novianto Dian, 2015, pemfilteran hypertext transfer protocol secure untuk penggunaan internet yang aman, jurnal informatika IBI Darmajaya, ISSN : 1693-3877. e-ISSN : 2407-1544.

[2] https://www.netfilter.org/projects/iptables/index.html, diakses 02 februari 2017

[3] www.unsri.ac.id/upload/arsip/iptables.doc, diakses 02 februari 2017

[4] Glend Sondakh, Meicsy E. I. Najoan, (2),Arie S. Lumenta, 2014. Perancangan Filtering Firewall Menggunakan Iptables Di Jaringan Pusat Teknologi Informasi Unsrat. E-journal Teknik Elektro dan Komputer ISSN : 2301-8402

[5] https://lendcreative.com/fungsi-dan-perintah-dari-ping-tracert-dan-nslookup-di-cmd/, diakses 02 februari 2017

[6] https://www.rumahweb.com/journal/traceroute-tracert.htm, diakses 02 februari 2017