JURNAL KHATULISTIWA INFORMATIKA VOL. IX, NO. I JUNI 2021
p-ISSN: 2339-1928 e-ISSN: 2579-633X Halaman : 17 - 22

SISTEM KEAMANAN OPERASI LINUX UBUNTU IPTABLES SEBAGAI FIREWALL DI DINAS PENDIDIKAN KABUPATEN SERANG

Desmira

Pendidikan Vokasional Teknik Elektro (PVTE)
Universitas Sultan Ageng Tirtayasa
Fakultas Keguruan dan Ilmu Pendidikan UNTIRTA (FKIP UNTIRTA)
desmira@untirta.ac.id

INFO ARTIKEL

Diajukan :
11 Januari 2021

Diterima :
17 Mei 2021

Diterbitkan :
14 Juni 2021

Kata Kunci :
Sistem Operasi Linux

INTISARI

Keamanan jaringan sangat dibutuhkan baik oleh individu maupun instansi. Ancaman dari penyusup yang bermaksud merusak atau mencuri informasi atau data penting melalui jaringan komputer. Beberapa jenis keamanan jaringan terdiri dari beberapa cara salah satunya adalah firewall, firewall banyak dipilih karena lebih efektif dan lebih mudah diimplementasikan. Implementasi sistem keamanan firewall menggunakan konfigurasi Iptables sebagai salah satu alternatif pengamanan data dari beberapa pihak yang tidak bertanggung jawab. Tujuan dari penelitian ini adalah membuat sebuah sistem operasi firewall dengan menggunakan iptables berbasis linux yang dapat memenuhi kebutuhan akan sebuah sistem jaringan komputer, manfaat dari penelitian ini adalah untuk mengurangi tingkat resiko kerusakan atau pencurian file atau informasi. Metode yang digunakan adalah dalam penelitian observasi, wawancara dan perancangan sistem keamanan operasi Linux Ubuntu iptables sebagai firewall di dinas pendidikan kabupaten Serang. Hasil yang diperoleh dari penelitian ini adalah penggunaan konfigurasi Iptables pada sistem operasi linux Ubuntu dapat dilakukan pada koneksi kabel LAN dan Wifi, selama semua klien berada pada kelas yang sama, konfigurasi Iptables dapat memblokir akses klien ke server dan dapat dilakukan sebaliknya, yaitu memblokir akses server . terhadap klien. Dari hasil penelitian yang dilakukan pada beberapa PC dengan beberapa konektor jaringan, konfigurasi Iptables dapat berjalan dan tidak mempengaruhi OS yang digunakan, karena konfigurasi Iptables

I. PENDAHULUAN

Perkembangan teknologi jaringan dari tahun ketahun semakin meningkat, dengan adanya internet komunikasi dapat dilakuakan dengan mudah. Seiring dengan perkembangan teknologi informasi maka dibutuhkan sutau sistem keamanan yang baik (Aini & Amrizal, 2010). Keamanan jaringan sangat dibutuhkan baik perorangan maupun instansi("ANALISA DAN KONFIGURASI NETWORK INTRUSION PREVENTION SYSTEM (NIPS) PADA LINUX UBUNTU 10 . 04 LTS ANALISA DAN KONFIGURASI NETWORK INTRUSION PREVENTION SYSTEM (NIPS)," 2011)(Sondakh, Najoan, & Lumenta, 2014)(Lyu & Lau, 2000). Beberapa jenis keamanan jaringan terdiri dari beberapa , salah satunya adalah firewall, firewall banyak dipilih karena lebih efektif dan mudah untuk diterapkan. masalah keamanan Internet menjadi topik hangat. Perusahaan yang mengakses Internet sedang mencari metode melindungi situs jaringan mereka dari serangan eksternal dan intrusi (Lyu & Lau, 2000)(Tran, Al-shaer, & Boutaba, n.d.)(Al-haj & Al-shaer, n.d.). Firewall adalah salah satu solusi terbaik. Implementasi sistem keamanan firewall dengan menggunakan konfigurasi Iptables ini sebagai alternatif cara untuk mengamankan data dari oknum atau pihak yang tidak bertanggungjawab. Adapun beberapa kelebihan antara konfigurasi Iptables dengan cara lain untuk mengamankan data, yaitu konfigurasi Iptables sangat efektif untuk mengamankan data, karena konfigurasi Iptables dapat memblock ip secara langsung atau keseluruhan(Diekmann, Michaelis, Haslbeck, & Carle, 2016)(Huraj, 2015)(Diekmann, Hupel, Michaelis, Haslbeck, & Carle, 2018). Penggunaan sistem operasi linux Ubuntu digunakan untuk mendukung konfigurasi Iptables sebagai firewall(Amien, Komputer, & Riau, 2020).

Adapun sistem operasi lain yang dapat digunakan untuk membuat firewall tapi tidak dapat menggunakan konfigurasi Iptables itu sendiri. Dalam sebuah intansi diperlukan perawatan jaringan yang dilakukan teknisi perusahaan atau instansi untuk mendukung kerja jaringan. Dari latar belakang masalah diatas maka dapat identifikasi masalah yang ada di dinas pendidikan serang. Adanya kemungkinan ancaman dari penyusup yang bermaksud merusak ataupun mencuri informasi atau data penting yang melalui jaringan komputer. Belum dioptimalkannya firewall yang fungsinya untuk mengantisipasi atau sebagai sistem keamanan data. Penggunaan konfigurasi Iptables sebagai salah satu cara untuk mengaktifkan firewall.

Adapun batasan dalam penelitian ini adalah mengimplementasikan sebuah sistem operasi firewall untuk mengawasi port-port yang tidak memiliki ijin untuk masuk. Sistem ini digunakan

agar bisa membantu user agar lebih mudah memantau PC yang berada di log-log tertentu dengan cara menjalankan dahulu sistem di PC user.

Penggunaan sistem operasi linux ubuntu sebagai pendukung sistem keamanan jaringan firewall. Penggunaan VirtualBox untuk dualboot sebagai media penginstalan sistem operasi linux Ubuntu. Konfigurasi Iptables pada sistem operasi linux Ubuntu sebagai firewall. Adapun tujuan dari penelitian adalah membuat sistem operasi firewall menggunakan Iptables berbasis linux yang dapat memenuhi kebutuhan akan sebuah sistem jaringan komputer. Menambahkan varian baru dalam lingkup jaringan komputer yaitu sebuah konfigurasi Iptables dalam sebuah sistem operasi linux Ubuntu. Mempermudah user untuk memfilter port-port. Manfaat dari penelitian ini adalah Mengurangi tingkat resiko perusakan atau pencurian file atau informasi dan melindungi aplikasi computer yang digunakan

II. METODOLOGI PENELITIAN

Terdapat tiga prosedur yang dilakukan dalam pembuatan aplikasi ini yang akan diuraikan. Studi literatur merupakan prosedur untuk mendapatkan literatur atau artikel tentang *filtering firewall* dengan Iptables, kemudian Mempelajari Sistem jaringan yang berjalan di Dinas Pendidikan dan memahami pemahaman dari jaringan yang terpasang, setelah itu melakukan Evaluasi Data untuk mendapatkan data-data penggunaan jaringan atau konten-konten yang di akses oleh pengguna internet dan memisahkan konten yang bisa di akses dengan yang tidak perlu. Perancangan Sistem, dalam hal ini membuat mekanisme filtering dan titik-titk yang akan ditempati firewall Implementasi Sistem, Instalasi Perangkat Keras dan Perangkat Lunak dari sistem yang dirancang. Melakukan monitoring jaringan untuk melihat bahwa filtering sudah berjalan dengan baik.

1. Evaluasi Data
   Untuk mendapatkan informasi dari pengguna internet berupa konten yang diakses, diperoleh dengan cara klarifikasi dengan administrator jaringan Dinas Pendidikan tentang konten-konten yang sering di akses oleh pengguna internet Dinas Pendidikan, kemudian menyesuaikan dengan aturan-aturan yang diberlakukan di Dinas Pendidikan tentang konten-konten apa saja yang bisa di akses.
2. Manajemen Jaringan
   Dalam penelitian ini penulis merancang sebuah komputer menjadi firewall dengan menggunakkan Iptables yang merupakan perangkat bawaan sistem operasi linux Ubuntu. pertama yang dilakukan adalah dengan menginstal sistem operasi linux Ubuntu di sebuah pc, kemudian aktifkan Iptables.
3. Model Perancangan

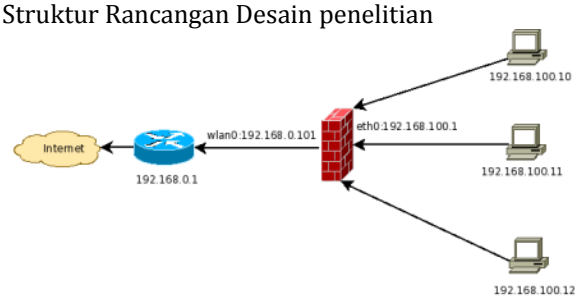
Dalam menyusun penelitian ini ada beberapa metode penilitian yang dilakukan untuk memperoleh data dan informasi yang diperlukan secara lengkap, guna mendukung kebenaran materi uraian dan pembahasan. Adapun metode yang dilakukan, ialah sebagai berikut :

Ada 3 tahap pengambilan data dalam penilitian ini adalah

a. Observasi
   Observasi dilakukan dengan mengamati secara langsung kondisi jaringan yang ada pada dinas pendidikan kabupaten serang("A Method for Observing and Evaluating Writing Lab Tutorials on JSTOR," n.d.)(Papini, Studies, & Building, 1988).
b. Wawancara
   Untuk mendapatkan data dalam penelitian ini penulis melakukan wawancara secara langsung dengan pihak yang terkait yang ada di dinas pendidikan kabupaten serang. Seperti teknisi yang melakukan perbaikan dan perawatan ketika ada kendala dengan jaringan.
c. Studi literature
   Setelah melakukan observasi dan wawancara dalam penelitian ini,selanjutnya peneliti mencari informasi dengan data yang terkait dari jurnal- jurnal dan buku yang berkaitan dengan penelitian
d. Kebutuhan perangkat yang akan digunakan
   Menentukan kebutuhan software dan hardware apa saja yang dibutuhkan untuk penulisan ilmiah ini.
e. Perancangan konfigurasi
   Merancang desain topologi dan konfigurasi settingan Iptables sebagai firewall.
f. Perancangan jaringan
   Melakukan perancangan dan konfiguras sistem keamanan firewall.
g. Pengujian
   Menguji dan mengetahui masing-masing jalan kerja dari suatu program sistem keamanan jaringan internet yang digunakan agar tidak terjadi kesalahan.

III. HASIL DAN PEMBAHASAN

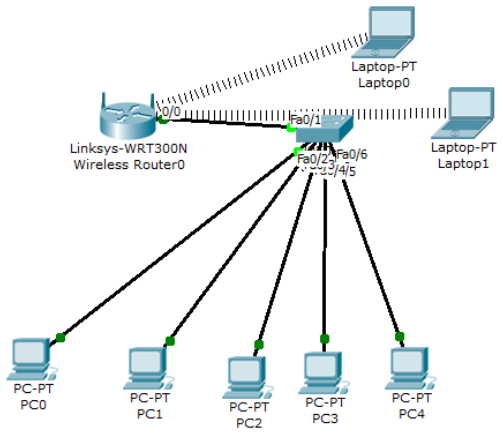
Merancang sebuah komputer menjadi firewall dengan menggunakkan Iptables yang merupakan perangkat bawaan sistem operasi linux Ubuntu. pertama yang dilakukan adalah dengan menginstal sistem operasi linux Ubuntu di sebuah pc, kemudian aktifkan Iptables.
Struktur Rancangan Desain penelitian



Gambar 1. Implementasi Topologi Jaringan

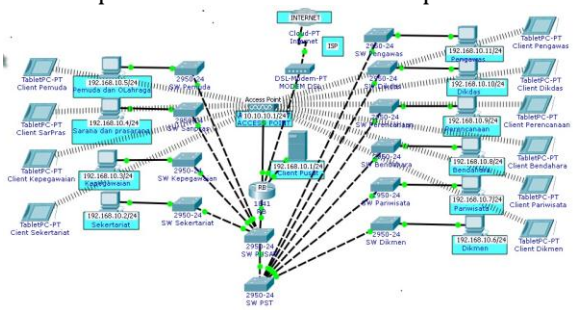
Memahami bagaimana cara kerja Iptables serta memahami cara hacker masuk dan mengakses jaringan tanpa melalui log in terlebih dahulu, menentukan policy atau kebijakan, mengidentifikasi. Memahami teknik yang biasa dilakukan dan di gunakan seorang hacker, mempelajari konfigurasi sebuah firewall, mencoba instalasi-instalasi dan mencoba memeperaktikannya. Implementasi sistem di dalam *filtering firewall* yaitu instalasi hardware dan instalasi software. Komputer akan berfungsi sebagai router dan Pc terpasang 2 buah ethernet card yang merupakan media untuk menghubungkan dua jaringan yang berbeda. Untuk Instalasi software menggunakkan sistem operasi Linux Ubuntu, OS (Operating System) ini. traffic yang sekedar melewati komputer kita. untuk Konfigurasi filtering, ada dua konfigurasi yaitu positive list dan negative list. untuk Positive list merupakan proses filtering dimana semua paket yang masuk akang di Drop dan hanya jalur-jalur atau port-port tertentu saja yang dibuka untuk bisa di akses. Untuk Negative list merupakan proses filtering dimana semua jalur-jalur atau port kita buka, kemudian menutup satu persatu port-port yang penting dalam server kita seperti DNS, WEB, FTP, SMTP.
Topologi jaringan terdapat beberapa macam, tetapi pada Dinas Pendidikan Kabupaten Serang menggunakan topologi star sebagai jalur internet dan sambungan datanya.

Topologi star dipilih karena lebih mudah dan sederhana, dan untuk tampilan tologi pada Dinas Pendidikan Kabupaten Serang adalah sebagai berikut :



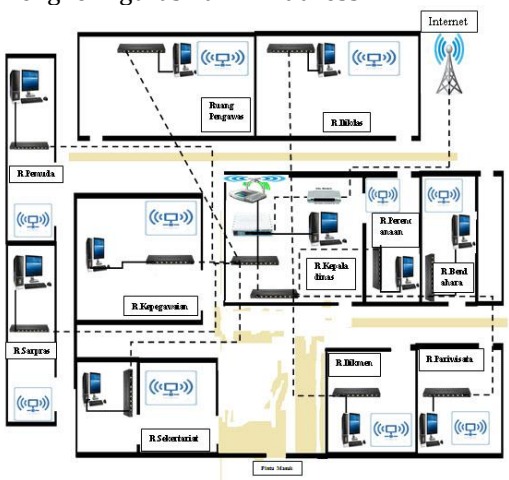
Gambar 2. Topologi Jaringan pada Dinas Pendidikan Kabupaten Serang

Topogi jaringan yang digunakan Dinas Pendidikan Kabupaten Serang adalah topologi Star yang mana setiap client telah terinstal sistem oprasi windows 7 tersusun rapih



Gambar 4. Topologi Jaringan Dinas Pendidikan Kabupaten Serang

Jika semua peralatan dan perlengkapan telah siap dan komputer telah di Instal maka langkah yang akan dilakukan selanjutnya adalah mengkoneksikan komputer satu dengan komputer lainnya namun hal tersebut tidak dapat dilakukan apabila kita belum mengkonfigurasikan IP Address.



Gambar 5. Skema jaringan dinas pendidikan kota serang

Aspek yang meliputi kebutuhan hardware atau perangkat keras. Berikut kebutuhan hardware yang diperlukan seperangkat komputer dengan spesifikasi seperti pada tabel berikut ini:

Tabel 2 Spesifikasi Perangkat Komputer

Perangkat keras dan *software*	**Keterangan**
Prosesor	*Dual core*
Memori	Ram DDR III 2 Gb
Harddisk	256 Gb

Aspek menyangkut tentang kebutuhan software atau perangkat lunak

1. Os windows 7 untuk PC client
2. Os Linux Ubuntu untuk PC Server

Sebelum mengkonfigurasi pengaturan tertentu, pertama harus menentukan apakah default behavior dari ketiga chain tersebut. Dengan kata lain, harus menentukan apakah yang harus dilakukan iptables jika sebuah sambungan tidak cocok dengan aturan yang ada Untuk mengetahui apakah pengaturan yang sedang digunakan, jalankan perintah iptables –L

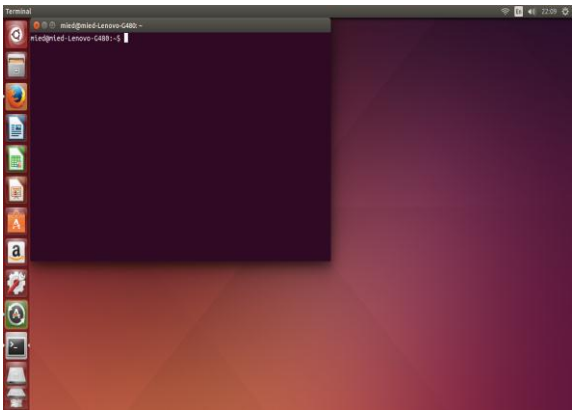
```
geek@ubuntu:~$ sudo iptables -L | grep policy
Chain INPUT (policy ACCEPT)
Chain FORWARD (policy ACCEPT)
Chain OUTPUT (policy ACCEPT)
geek@ubuntu:~$
```

Gambar 6. Chain digunakan untuk menerima sambungan

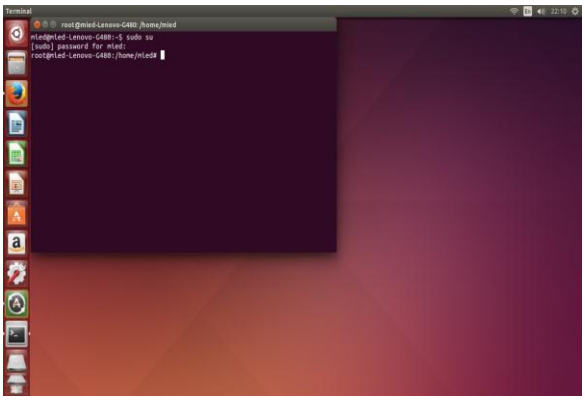
Kemudian agar menerima sambungan secara default, maka menggunakan perintah dibawah ini:
“iptables –policy INPUT ACCEPT
iptables –policy OUTPUT ACCEPT
iptables –policy FORWARD ACCEPT”
Dengan menggunakan pengaturan accept, maka dapat menggunakan Firewall Linux ini untuk menolak alamat IP atau port tertentu, disamping menerima sambungan lainnya. Jika ingin menolak semua sambungan dan ingin menentukan sambungan apa saja yang ingin dilakukan secara manual, maka harus merubah pengaturan default dari chain menjadi drop. Cara ini hanya dapat berguna untuk server yang memiliki informasi sensitif, dan hanya digunakan alamat IP yang sama untuk terhubung kepada server tersebut.
“iptables –policy INPUT DROP
iptables –policy OUTPUT DROP
iptables –policy FORWARD DROP”

1. Hal yang pertama dilakukan adalah membuka terminal pada sistem operasi linux Ubuntu.
2. Setelah membuka terminal, maka masuk pada mode root dengan perintah sudo su.
3. Isikan password.
4. Scan ip yang terhubung dengan server.

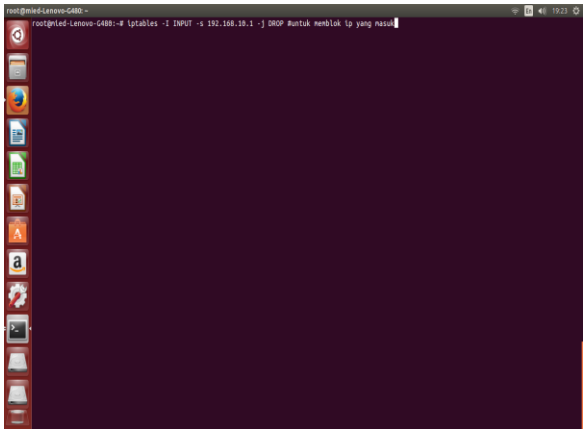
Kemudian konfigurasi mana saja ip yang akan di block dengan konfigurasi Iptables.
Hasil pengujian Tahapan ini adalah proses pengujian sistem dengan beberapa ip yang akan di block. Pada tahapan ini penulis mencoba untuk memblock semua komputer yang terdapat pada lokasi penelitian dengan sambungan LAN dan Wifi.



Gambar 7. Tampilan terminal pada Linux Ubuntu



Gambar 8. Tampilan mode root



Gambar 9.Konfigurasi Iptables untuk memblock ip

Pada gambar diatas terlihat konfigurasi Iptables untuk memblock ip komputer lain, jika hendak menghubungkan kembali maka ubah konfigurasinya dari DROP menjadi ACCEPT, maka komputer tersebut akan terhubung kembali.

Langkah-Langkah Pengujian Pada tahapan ini, penulis menjelaskan proses pengoperasian secara detail mengenai cara sistem ini, diantaranya :

Tabel 1. Hasil Penelitian

.No	Ruangan	Ip	Sambungan	Kondisi
1.	R. Kepala Dinas	192.168.10.2	LAN	BLOCK
2.	R. Pengawas	192.168.10.6	LAN	BLOCK
3.	R. Bendahara	192.168.10.3	LAN	BLOCK
4.	R. Perencanaan	192.168.10.5	LAN	BLOCK
5.	R. Dikdas	192.168.10.7	LAN	BLOCK
6.	R. Pemuda	192.168.10.10	Wifi	BLOCK
7.	R. Sarpas	192.168.10.11	Wifi	BLOCK
8.	R. Sekretariat	192.168.10.4	Wifi	BLOCK
9.	R. Dikmen	192.168.10.9	LAN	BLOCK
10.	R. Pariwisata	192.168.10.12	Wifi	BLOCK
11.	R. Kepegawaian	192.168.10.8	LAN	BLOCK

Pada tabel hasil penelitian diatas dimaksudkan untuk mencoba apakah konfigurasi Iptables dapat dilakukan pada beberapa PC yang menggunakan beberapa penghubung jaringan, penghubung yang dimaksud, yaitu LAN (Local Area Network) dan Wifi. Dan hasil penelitian menyimpulkan jika konfigurasi Iptables dan bekerja pada beberapa penghubung jaringan.

Setelah melakukan beberapa tahapan dapat ditarik beberapa kelebihan dan kekurangan pada sistem, diantaranya :

Kelebihan

1. Konfigurasi Iptables mudah untuk dilakukan, karena konfigurasi yang pendek dan mudah untuk diingat.
2. Penggunaan linux Ubuntu yang sangat support untuk konfigurasi Iptables.

Kekurangan

1. Penggunaan linux Ubuntu yang belum begitu familiar dalam fungsi untuk mengamankan data.
2. Penggunaan VirtualBox yang membutuhkan konsumsi ram yang besar.

IV. KESIMPULAN

Setelah analisa dan implementasi yang ada dalam penelitian Penggunaan konfigurasi Iptables pada sistem operasi linux Ubuntu bisa dilakukan pada sambungan kabel LAN dan Wifi, asalkan semua client berada pada kelas yang sama.

1. Konfigurasi Iptables bisa memblock akses client terhadap server dan bisa dilakukan sebaliknya, yaitu memblock akses server terhadap client.
2. Dari hasil penelitian yang dilakukan pada beberapa PC dengan beberapa penghubung jaringan, konfigurasi Iptables bisa bekerja dan tidak berpengaruh OS yang digunakan, karena konfigurasi Iptables ini justru menggunakan OS Linux yang client nya menggunakan OS Windows.

Saran untuk pengembangan tentang sistem keamanan firewall dengan menggunakan konfigurasi Iptables adalah sebagai berikut :

1. Perlu adanya perawatan koneksi server dan client untuk mengetahui secara umum tentang jaringan koneksi internet.
2. Jangan lupa untuk mensetting komputer dengan static agar dalam konfigurasi tidak sulit.
3. Sebagai antisipasi jika OS Linux Ubuntu tidak tersedia, bisa menggunakan OS Linux lainnya.

REFERENSI

A Method for Observing and Evaluating Writing Lab Tutorials on JSTOR. (n.d.).

Aini, Q., & Amrizal, V. (2010). Implementasi IP-Tables Firewall pada Linux sebagai Sistem Keamanan Jaringan yang Handal, *3*(1), 1–10.

Al-haj, S., & Al-shaer, E. (n.d.). Measuring Firewall Security, 2–5.

Amien, J. Al, Komputer, F. I., & Riau, U. M. (2020). Implementasi keamanan jaringan dengan iptables sebagai firewall menggunakan metode port knocking 1, *10*(2), 159–165.

ANALISA DAN KONFIGURASI NETWORK INTRUSION PREVENTION SYSTEM (NIPS) PADA LINUX UBUNTU 10 . 04 LTS ANALISA DAN KONFIGURASI NETWORK INTRUSION PREVENTION SYSTEM (NIPS). (2011).

Diekmann, C., Hupel, L., Michaelis, J., Haslbeck, M., & Carle, G. (2018). Verified iptables Firewall Analysis and Verification. *Journal of Automated Reasoning*. https://doi.org/10.1007/s10817-017-9445-1

Diekmann, C., Michaelis, J., Haslbeck, M., & Carle, G. (2016). Verified iptables Firewall Analysis, 252–260.

Huraj, L. (2015). Performance Evaluations of IPTables Firewall Solutions under DDoS attacks, *11*(2), 35–45.

Lyu, M. R., & Lau, L. K. Y. (2000). Firewall Security : Policies , Testing and Performance Evtaluation, 116–121.

Papini, D. R., Studies, F., & Building, E. (1988). An Observational Study of Affective and Assertive Family Interactions During Adolescence, *17*(6), 477–492.

Sondakh, G., Najoan, M. E. I., & Lumenta, A. S. (2014). Perancangan *Filtering firewall* Menggunakan Iptables Di Jaringan Pusat Teknologi Informasi Unsrat, 19–27.

Tran, T., Al-shaer, E., & Boutaba, R. (n.d.). PolicyVis : Firewall Security Policy Visualization and Inspection, 1–16.