ANALISIS DAN PERANCANGAN KEAMANAN JARINGAN DENGAN METODE STATEFUL MULTILAYER INSPECTION FIREWALL MENGGUNAKAN ROUTER MIKROTIK DALAM PENGAMANAN SERVER

(Analysis And Design Of Network Security With Stateful Multilayer Inspection Firewall Method Using Mikrotik Router In Server Security)

Abd.Haris Kusnadi[1], Ariyan Zubaidi[2], Ahmad Zafrullah[3]
[1]Dept Informatics Engineering, Mataram University)
Jl. Majapahit 62, Mataram, Lombok NTB, INDONESIA
Email: abdhariskusnadi@gmail.com, [zubaidi13, zaf]@unram.ac.id

Abstract

Routers are the main gateway in accessing networks connected to servers and are often used as the main access in attacks on a computer network. One way to minimize attacks on a network. namely by securing the router, but the built-in security system on the router can often be penetrated by attackers using attack techniques such as Distributed Denial of Service (DDoS) and Synchronize (SYN) Flooding. So, a security method is needed on the router to overcome this.

This research aims to secure the server from DDoS attacks by using the Mikrotik router firewall with the statefull multilayer inspection firewall method to find out the performance of the router when an attack with DDoS is carried out on the server. From the tests conducted, the results of router performance when using packet filtering firewall to overcome UDP / TCP flooding attacks were obtained by (96%) CPU and SYN flooding attacks by (69%) CPUs used for monitoring using the statefull multilayer inspection firewall method, CPU performance results from routers that did not increase too much, namely for TCP / UDP flooding attacks of (10%) CPU used and for SYN flooding attacks of (7%) CPU used, The use of the statefull multilayer inspection firewall method can reduce the performance of the CPU on the router compared to using packet filtering firewall.

Keywords: *Router,Server Distributed Denial of Service, Synchronize flooding, Packet filtering Firewall, Stateful multilayer inspection firewall.*

1. PENDAHULUAN

Keamanan teknologi informasi menjadi suatu hal yang sangat penting saat ini. Hal ini dimaksudkan untuk menjamin keamanan terhadap seluruh informasi yang dikirim ataupun disimpan melalui internet yang tidak bisa diakses sembarangan oleh pihak yang tidak bertanggung jawab[1]. Internet merupakan media yang dijadikan sebagai akses oleh banyak pihak tanpa terkecuali hacker dan cracker. Dengan alasan tertentu mereka melakukan penyusupan yang dapat merugikan para pemilik server dan jaringan komputer[2]. Perusahaan keamanan siber Kaspersky mencatat Indonesia menghadapi lebih dari 11 juta serangan siber pada kuartal pertama 2022. "Tren itu juga harus disambut dengan kewaspadaan dari semua pihak yang terlibat, karena para pelaku kejahatan siber selalu menunggu tren berikutnya untuk dieksploitasi," kata Manajer Umum Kaspersky Asia Tenggara, Yeo Siang Tiong, dikutip dari siran pers.

jenis serangan yang sering dilakukan pada router mikroTik diantaranya seperti bruteforce, Winbox exploitation Distributed Denial of Services (DDoS). Serangan DDoS terus menjadi salah satu ancaman paling menantang di dunia internet. Intensitas dan frekuensi serangan ini meningkat dengan kecepatan yang mengkhawatirkan[6]. Peningkatan level serangan DDoS dilakukan dengan pengubahan ukuran data yang dikirimkan ke target, dampak dari serangan DDoS menyebabkan router yang di lewatinya mengalami peningkatan konsumsi daya listrik dan beban kerja router yang berlebihan. Terdapat cara untuk melakukan pengamanan dari serangan DDoS pada router mikroTik untuk melindungi server pada suatu jaringan salah satunya yaitu dengan menggunakan firewall [4].

metode firewall yang sering digunakan untuk melakukan pengamanan dari serangan DDoS pada jaringan yaitu Stateful Multilayer Inspection Firewall (SMIF). Metode SMIF merupakan penggabungan dari

tiga jenis firewall yaitu paket filtering firewall,application firewall dan circuit level gateway firewall.

Stateful multilayer inspection protocol bekerja pada tiga lapisan OSI yaitu lapisan aplikasi, Transport dan internet [1]. Metode ini banyak digunakan untuk mendeteksi serangan DDoS yang digunakan sebagai filtrasi dari data yang berlebihan yang dikirim oleh penyerang ke server [7][8][9]. berbedanya gaya tulisan tangan dan karakter tulisan setiap orang[4].

1.1. Rumusan Masalah

Berdasarkan latar belakang yang telah dipaparkan sebelumnya, rumusan masalah tugas akhir ini adalah bagaimana membangun keamanan pada suatu jaringan dengan metode Stateful Multilayer Inspection Firewall (SMIF) sebagai keamanan pada router dalam melindugi server?

1.2. Tujuan Penitian

Penelitian ini bertujuan untuk menganalisis dan implementasi keamanan jaringan menggunakan metode Stateful Multilayer Inspection Firewall (SMIF) pada router MikroTik dalam pengamanan server.

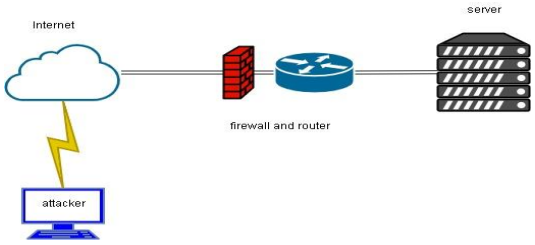
2. TINJAUAN PUSTAKA

Metode stateful multilayer inspection firewall juga telah digunakan untuk deteksi dari serangan Distributed Denial of Service (DDoS) untuk melakukan filtrasi dari data yang berlebihan yang dikirim oleh penyerang ke server Adapun penelitian yang berjudul "Effective Stateful firewall in software-Defined Networking" dalam penelitian tersebut membahas tentang keefektifan stateful firewall untuk mencegah terjadinya serangan DDos dan Syincronize Flooding (SYN flooding) dengan stateful firewall pada penelitian tersebut peneliti mendapatkan sebuah hasil yaitu stateful inspection firewall tidak hanya dapat melacak aliran TCP, tetapi juga mengurangi latensi dari jaringan dengan kelebihan lookup time up pada long-lived flow hingga 16% dan pada short-lived flow hingga 50%. Selain itu, menurut perspektif keamanan, akurasi untuk deteksi dan mitigasi DDoS dari aplikasi firewall stateful adalah 98,93 % dari serangan SYN flooding dan 92,09% untuk serangan UDP flooding [7].

Perkembangan firewall dengan metode stateful juga memiliki beberapa versi yaitu deep packet inspection firewall, high speed stateful packet inspection firewall dan stateful multilayer firewall. Dari beberapa versi terbaru stateful firewall, terdapat penelitian yang membahas tentang High Speed Stateful Packet Inspection (HSSPI) in Embedded Data-Driven Firewall dimana penelitian tersebut membahas tentang seberapa cepat data dapat diinspeksi pada embedded personal firewall prosesor yang diimplementasikan berdasarkan self-timed dan super-pipelined. Pada penelitian tersebut didapatkan hasil bahwa pada sistem tertanam yang dibuat, kinerja yang dihasilkan berdasarkan evaluasi field Programable Gateway Array (FPGA) dengan High Speed SPI dapat melebihi 3GB/s dari data yang diproses [10].

3. METODE PENELITIAN

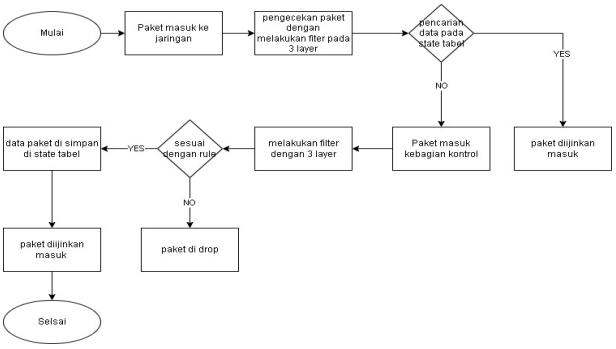
3.1. Perancangan Topologi



Gambar 1. Topologi Jaringan

Pada gambar 1 dapat dilihat topologi jaringan yang akan dirancang, dimana pada topologi jaringan di atas terdapat user, router dan server yang terhubung dengan internet, pada sisi user akan bertindak sebagai penyerangan untuk masuk ke jaringan server dimana pada user penyerang akan melakukan serangan DDoS dan SYN flood, pada sisi jaringan perangkat router akan dikonfigurasi stateful multilayer inspection firewall untuk menanggulangi serangan yang akan dilakukan user penyerang dimana firewall yang dibuat menjadi sebagai keamanan pada jaringan sedangkan pada sisi server terdapat server DNS, FTP, Proxy dan WEB server.

3.2. Metode Penelitian



Gambar 2. Diagram alir metode stateful multilayer inspection firewall

Pada diagram alur di atas dapat dilihat alur data yang masuk ke jaringan pada bagian pertama data masuk selanjutnya dilakukan pengecekan data dengan cara dilakukan filtrasi pada tiga lapisan yaitu jaringan, transport dan aplikasi pada setiap lapisan tersebut dilakukan penyaringan dengan kriteria protokol

jaringan pada setiap lapisannya, langkah selanjutnya dilakukan pengecekan koneksi dimana data koneksi diambil dari state table pada router jika koneksi dikenali maka paket diizinkan masuk ke server, apabila paket tidak dikenali maka akan dimasukkan pada paket kontrol dimana selanjutnya akan dilakukan filter pada setiap paket yang tidak dikenali dengan tiga lapisan OSI dengan kriteria protokol jaringan, paket yang belum dikenali akan di-drop jika tidak sesuai dengan aturan firewall pada setiap lapisan, jika sesuai dengan aturan firewall maka selanjutnya data dari paket akan diubah menjadi hash dan disimpan pada state table router agar data tersbut dikenal apabila nantinya akan melakukan permintaan kembali pada server setelah data paket disimpan, paket yang lolos akan diizinkan masuk ke server.

3.3. Skema Pengujian

Pada tahapan ini dilakuan pengujian terhadap konfigurasi yang telah dilakukan untuk mengetahui seberapa efektif metode yang digunakan dalam menanggulangi serangan yang akan dilakukan, pengujian keamanan dilakukan dengan dua tahap yaitu dengan menggunakan firewall filtering standar dan stateful multilayer inspection firewall dalam pengiriman paket ke server dengan DDoS menggunakan aplikasi LOIC dengan mengirimkan (jumlah paket yang dikirim dengan waktu yang sama).

3.3.1. Pengujian serangan dengan firewall packet filtering

Pada tahapan ini dilakukan proses pengujian serangan DDoS dan SYNflood kepada server yang telah menerapkan firewall standar. pengujian dilakukan menggunakn tools LOIC dari sisi client dengan spesifikasi konfigurasi jumlah thread yang dikirim sebesar 100 thread pada port 80 dah 53
Pada sisi server dilakukan analisa untuk mendaptkan presentase paket yang ditolak oleh firewall packet filtering.

3.3.2. Pengujian seranga dengan metode Stateful Multilayer Inspection Firewall

Pada tahapan ini dilakukan proses pengujian serangan DDoS dan SYNflood kepada server yang telah menerapkan firewall standar. pengujian dilakukan menggunakn tools LOIC dari sisi client dengan spesifikasi konfigurasi jumlah thread yang dikirim sebesar 100 thread pada port 80 dah 53
Pada sisi server dilakukan analisa untuk mendaptkan presentase paket yang ditolak oleh firewall packet filtering.

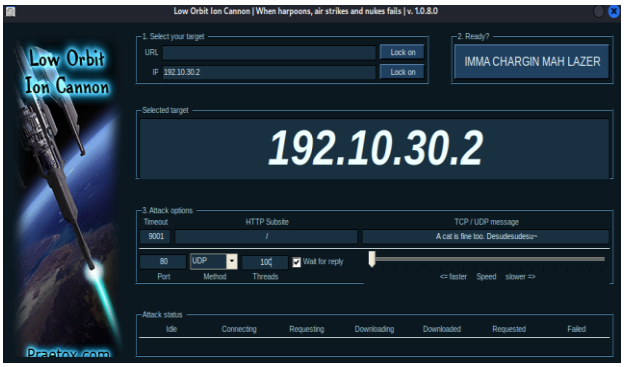
4. HASIL DAN PEMBAHASAN

4.1. Pengujian Sistem Keamnana Jaringan.

Pengujian dengan DDoS dilakukan dengan dua cara yaitu dengan User Datagram Protocol (UDP) flooding dan synchronize (SYN) flooding berikut tahap yang dilakukan untuk melakukan serangan terhadap server yang akan menjadi korban untuk melihat performa dari kinerja router Mikrotik sebagai keamanan dari server.

4.1.1. Transmision Control Protocol/User Datagram Protocol (TCP/UDP) Flooding.

Pengujian serangan dilakukan menggunakan tools Low Orbit Ion Cannon (LOIC). Pengujian serangan dengan LOIC digunakan untuk melakukan peneyerangan DDoS, Dengan LOIC dapat dilakukan penyerangan dengan menggunakan alamat URL ataupun alamat IP address dari taget dan dapat mementukan jumlah thread, port, dan metode yang digunakan untuk penyerangan.



Gambar 3. Tools DDoS low cannon ion orbit(LOIC).

Pada gambar 3 di atas merupakan model serangan yang akan dilakukan menuju IP address 192.10.30.2 (IP server) dengan port tujuan 80 atau http dengan protocol UDP dan jumlah serangan 100 Thread saat serangan dilakukan dengan UDP flood penyeranga hanya akan meminta paket sebanyak 100 thread kepada server target.

4.1.2. Syncronize(SYN) flooding

Pengujian SYN flooding dilakukan menggunakan tools hping3 dari kali linux dengan contoh penyerangan hping3 192.10.30.2 -q -n -d 120 -S -p 80/53 –flood –rand-source. dimana alamat ip 192.10.30.2 akan menjadi target tujuan korban, -q sebagai berief output , -n memperlihatkan ip target dari host -d 120 merupakan ukuran paket yang akan dikrimkan ke korban, -S merupakan jenis paket SYN yang akan dikirim ke korban, -p 53 merupaka port tujuan dari target, --flood data yang dikirim akan terus menerus,

dan –rand-source menyembunyikan alamat ip dari pelaku penyerangan.

```
┌──(haris㉿attacker)-[~]
└─$ hping3 192.10.30.2 -q -n -d 1200 -S -p 53 --flood --rand-source
```

Gambar 4. Skrip metode penyerangan SYN flood dengan haping3

4.2. Konfigurasi Keamanan Jaringan

4.2.1. Packet filtering Firewall

Packet filtering firewall berfungsi untuk menyaring mengontrol aliran data yang masuk ke dalam suatu jaringan dan yang berasal dari jaringan itu sendiri. Firewall filtering memberikan akses ataupun membelokir pengiriman data yang berasal dari alamat sumber paket yang dikirim oleh klien dan alamat tujuan paket.

```
[admin@MikroTik] /ip firewall> filter print
Flags: X - disabled, I - invalid, D - dynamic
[admin@MikroTik] /ip firewall> filter add chain=input in-interface=LAN action=ac
cept
[admin@MikroTik] /ip firewall> filter add chain=output out-interface=LAN action=
accept
[admin@MikroTik] /ip firewall> filter add chain=input in-interface=WAN action=dr
op
[admin@MikroTik] /ip firewall> filter add chain=output out-interface=WAN action=
drop
```

Gambar 5. Rule packet filtering firewall

Gambar di atas merupkan aturan yang dibuat untuk mengelola keluar atau masuknya *traffic* jaringan pada ethernet yang diberikan nama LAN dan WAN dimana untuk melindungi jaringan lokal setiap traffic yang masuk ke router melalui port WAN akan di-drop sedangakn traffic yang keluar melalu port WAN akan diberikan akses yaitu pada penyerangan menggunakan Denial of Service dan SYN flooding menuju port 53 dan 80 menyebabkan peningkatan performa CPU dan Memori pada server serta penyerangan terhadap port 53 dan 80 berhasil dilakukan oleh penyerang.

4.2.2. Stateful multilayer inspection firewall

Stateful multilayer inspection firewall merupakan penggabungan dari tiga layer keamanan yang ada pada OSI layer yaitu pada layer Network, Transport, Dan Application berikut konfigurasi pada setiap layer keamanan

```
Flags: X - disabled, I - invalid, D - dynamic
0    ;;; Trasnsport
     chain=forward action=drop connection-state=new src-address-list=asal
     dst-address-list=tujuan log=no log-prefix=""

1    chain=forward action=jump jump-target=deteksi-paket connection-state=new

2    chain=deteksi-paket action=return
     dst-limit=32,32,src-and-dst-addresses/1s

3    chain=deteksi-paket action=return src-address=192.10.30.2

4    chain=deteksi-paket action=add-dst-to-address-list address-list=asal
     address-list-timeout=5m

5    chain=deteksi-paket action=add-dst-to-address-list address-list=tujuan
     address-list-timeout=5m

6    ;;; Network
     chain=input action=accept connection-state="" src-address=192.10.30.2
     in-interface=LAN log=no log-prefix=""

7    chain=input action=drop in-interface=WAN log=no log-prefix=""
```

Gambar 6. Rule SMIF

Pada gambar diatas merupkan aturan yang dibuat untuk menginspeksi paket yang masuk dari WAN yang masuk meuju server yaitu pada jaringan LAN pada ada pun beberapa rule yang dibuat pada gambar di atas pada rule 0 chain=forward connection-state=new src-address-list=asal dst-address-list=tujuan action=drop pada rule ini berfungsi untuk memfilter dengan action=drop dengan alamat IP asal dengan alamat tujuan, Rule 1 chain=forward connection-state=new action=jump jump-target=deteksi-paket digunakan untuk membuat chain baru bernama deteksi paket, Rule no 2-5 dengan berfungi ketika ada paket abnormal baru, misalnya lebih dari 32 paket per detik, firewall akan sekaligus menandai alamat sumber dan alamat tujuan. Misalnya alamat IP penyerang akan dikelompokkan dengan nama “asal”, kemudian untuk alamat IP target akan dikelompokkan dengan nama “tujuan”.

4.3. Hasil pengujian Keamanan Jaringan

4.3.1. Pengujian keamanan metode filtering firewall pada router.

dari hasil penyerangan berikut dari penyerangan TCP/UDP flooding dan SYN flooding dapat dilihat pada tabel 1

Tabel 1. Hasil performa router dengan pengamanan Packet filtering firewall dari serangan DDos

Serangan	*Port*	CPU	Free Memory	Penyerangan	
				Berhasil	Gagal
TCP/UDP *flooding*	53	95%	19916KiB	✓	
	80	96%	16942KiB	✓	
SYN *flooding*	53	69%	11164KiB	✓	
	80	61%	11664KiB	✓	

Berdasakan hasil pengujian menggunakan metode packet filtering firewall pada Tabel 4.1, didapatkan hasil yaitu pada penyerangan menggunakan Denial of Service dan SYN flooding menuju port 53 dan 80 menyebabkan peningkatan performa CPU dan memori pada router serta penyerangan terhadap port 53 dan 80 berhasil dilakukan oleh penyerang.

4.3.2. Pengujian keamanan metode stateful multilayer inspection firewall pada router.

Dalam pengujian ini dilakukan penyerangan TCP/UDP flooding dan SYN flooding unutuk mengetahu performa dari router pada saat dilakukan penyerangan yang di amankan dengan metode statefull multilayer inspection firewall (SMIF), Untuk mengetahu performa dari router dilakukan dua seragan DDoS seperti berikut. hasil penyerangan berikut dari penyerangan TCP/UDP flooding dan SYN flooding dapat dilihat pada tabel 2

Tabel 2. Hasil performa router dengan pengamanan Stateful multilayer inspection firewall dari serangan DDos

Serangan	*Port*	CPU	Free Memory	Penyerangan	
				Berhasil	Gagal
TCP/UDP flooding(DDOS)	53	1%	13652KiB		✓
	80	1%	13784KiB		✓
SYN flooding	53	10%	15116KiB		✓
	80	7%	14726KiB		✓

Berdasakan hasil pengujian menggunakan metode packet filtering firewall pada tabel 4.2, didapatkan hasil yaitu pada penyerangan menggunakan Denial of Service pada port 53 dan 80 dapat diakatakan berhasil karena kinerja dari CPU normal pada saat diserang sedangkan dengan serangan SYN flooding menuju port 53 dan 80 membuat kinerja dari CPU menigkat 10% dan 12% dan jumlah memori terpakai sekitar 1,5 MB dari kedua serangan dengan total memory sebesar 16 MB.

5. KESIMPULAN DAN SARAN

5.1. Kesimpulan

Berdasarkakan hasil dari penyerangan TCP/UDP flooding dan SYN flooding dengan pengamana packet filtering firewall dan statefull multilayer inspection firewall di dapatkan hasil sebagai berikut:

1. Dengan penegamanan Packet filtering firewall performa dari serangan TCP/UDP flooding sebesar (96%) pada port 53 dan (95%) untuk port 80 sedangkan untuk serangan SYN flooding sebesar (69%) pada port 53 dan (61%) untuk port 80.
2. Pengamanan dengan stateful multilayer inspection firewall performa router saat dilakukan penyerangan dengan TCP/UDP flooding pada port 53 sebesar (1%) dan (1%) pada port 80, Sedangkan untuk serangan SYN flooding sebesar (10%) pada port 53 dan (7%) pada port 80.
3. Pengguaan statefull multilayer inspection firewall lebih efisien dibandingkan dengan packet filtering firewall dikarenkan performa dari dari router pada saat dilakukan serangan.

5.2. Saran

Saran dari penelitian ini adalah sebagai berikut:

1. Penggunaan stateful multilayer inspection firewall cukup baik untuk menggulangi TCP/UDP floding namun masih kurang dalam SYN flooding karena performa CPU dapat mengikat pada saat penyerangan
2. Penelitian ini dapat di jadikan acuan untuk pengembangan keamana jaringan computer untuk kedepannya.

DAFTAR PUSTAKA

[1] Z. A. Pribadi, "Analisis dan Implementasi Firewall dengan Metode Stateful Multilayer Inspection Pada Mikrotik Router OS," no. 1, pp. 1–9, 2013.

[2] R. Sharma and P. Chandresh, "Firewalls : A Study and Its Classification," Int. J. Adv. Res. Comput. Sci., vol. 8, no. 4, pp. 1979–1983, 2017, [Online]. Available: www.ijarcs.info.

[3] C. A. Pamungkas, "Manajemen Bandwith Menggunakan Mikrotik Routerboard di Politeknik Indonusa Surakarta," J. Inf. Politek. Indonusa Surakarta, vol. 1, pp. 17–22, 2016.

[4] I. G. Komang and O. Mardiyana, "Keamanan Jaringan Dengan Firewall Filter Berbasis Mikrotik Pada Laboratorium Komputer STIKOM Bali," Stmik Stikom, vol. 1, no. 86, pp. 9–10, 2015, doi: 10.1016/j.bbrc.2003.07.013.

[5] F. Ardianto, "Penggunaan mikrotik router sebagai jaringan server," Pengguna. Router Mikrotik, no. 1, pp. 26–31, 2020.

[6] F. Ridho, A. Yudhana, and I. Riadi, "Analisis Forensik Router Untuk Mendeteksi Serangan Distributed Danial of Service (DDoS) Secara Real Time," vol. 2, no. 1, pp. 111–116, 2016, [Online]. Available: http://ars.ilkom.unsri.ac.id.

[7] A. H. Maw, "Effective Stateful Firewall in Software-Defined Networking," Int. J. Comput. Sci. Eng., vol. 7, no. 8, pp. 269–274, 2019, doi: 10.26438/ijcse/v7i8.269274.

[8] P. Soepomo, "Analisis Perancangan Firewall Paket Filtering Dan Proxy Server Untuk Optimasi Bandwidth (Studi Kasus Di Laboratorium Riset Universitas Ahmad Dahlan Kampus 3), vol. 3, no. 1, pp. 89–97, 2015, doi: 10.12928/jstie.v3i1.2926.

[9] V. Vydia, S. Surono, and G. Setiarso, "Application Gateway Dan Stateful Inspection Method Pada Implementasi Firewall Untuk Optimasi Keamanan Jaringan Komputer," … Pengemb. Rekayasa dan …, vol. 16, no. 2, pp. 87–97, 2020, [Online]. Available: https://journals2.usm.ac.id/index.php/jprt/article/view/2624.

[10] R. Zhang, M. Iwata, Y. Shirane, and T. Asahiyama, "High Speed Stateful Packet Inspection in Embedded Data-Driven Firewall," no. January 2004, 2014.

[11] T. Booth and K. Andersson, "Network Security of Internet Services: Eliminate DDoS Reflection Amplification Attacks," J. Internet Serv. Inf. Secur., vol. 5, no. 3, pp. 58–79, 2015, doi: 10.22667/JISIS.2015.08.31.058.

[12] S. R. I. Mardiyati, "Mengoptimalkan Suatu Sistem Firewall Pada," vol. 7, no. 1, pp. 72–83, 2014.

[13] K. N. Siti, "KEAMANAN JARINGAN DENGAN PACKET FILTERING FIREWALL," Keamanan Jar. dengan paket Filter. firewall, vol. 9, no. 2, pp. 621–633, 2018, doi: 10.5151/cidi2017-060.

[14] N. Fahriani, P. A. R. Devi, and D. Aditama, “Alternatif Penanganan Jenis Serangan Pencurian Data Pada Jaringan Komputer,” Altern. Penanganan Jenis Serangan Pencurian Data Pada Jar. Komput., no. November, pp. 19–24, 2017.
[15] G. Sondakh, M. E. I. Najoan, and A. S. Lumenta, “Perancangan Filtering Firewall Menggunakan Iptables Di Jaringan Pusat Teknologi Informasi Unsrat,” J. Tek. Elektro dan Komput., vol. 3, no. 4, pp. 19–27, 2018.
[16] S. Jenkins, “OSI Defense in Depth to Increase Application Security,” SANS Inst., vol. v1.4b, no. Security 401, 2003.
[17] R. O. Nitra and M. Ryansyah, “Implementasi Sistem Keamanan Jaringan