Jurnal Informatika Terpadu

https://journal.nurulfikri.ac.id/index.php/JIT
ISSN ONLINE : 2460-8998

PERANCANGAN KEAMANAN JARINGAN *NEXT-GENERATION FIREWALL* MENGGUNAKAN *ROUTER FORTINET* PADA PT. ALODOKTER TEKNOLOGI SOLUSI

Erwin Dwi Setiawan[1], Ridwansyah[2], Mugi Raharjo[3]

[1,2,3]Teknologi Informasi, Universitas Nusa Mandiri
Jakarta Selatan, DKI Jakarta, 12540
erwindwi0408@gmail.com, ridwansyah.rid@nusamandiri.ac.id, mugi.mou@nusamandiri.ac.id

Abstract

Attacks that occur on computer network systems can occur at any time. For that, it is important to implement network security through a firewall. Researchers carried out observation methods and several research stages such as needs analysis, design, testing, and implementation. Using the Next-Generation Firewall on Fortinet routers can make network security tighter because the Next-Generation Firewall has additional features such as the Intrusion Prevention System (IPS), Web Filtering, and Application Control so that they can maintain network security, prevent cyber-attacks from third parties, limit internal access that has the potential to cause attacks or things that harm internal users and can review traffic on various platforms on the network. The results of this study are that the Next-Generation Firewall on Fortinet routers can help maintain internet network security, ward off cyber-attacks from third parties, limit internal access that has the potential to cause attacks or things that harm internal users and can monitor traffic on various platforms within a network, the Intrusion Prevention System (IPS) feature can help actively blacklist suspicious traffic. With the Next-Generation Firewall, internal users cannot access things that are not permitted, monitor the traffic used, and ward off cyber-attacks from third parties. PT. ALODOKTER TECHNOLOGY SOLUTION can prevent attacks from happening and block suspicious traffic, and it becomes more secure.

Keywords: *Firewall, Fortinet, Network Security, Next-Generation Firewall, PT. ALODOKTER*

Abstrak

Serangan yang terjadi pada sistem jaringan komputer bisa terjadi kapan saja. Oleh karena itu, penting untuk mengimplementasikan ide keamanan jaringan berupa *firewall*. Peneliti melakukan metode observasi dan beberapa tahapan penelitian seperti Analisa kebutuhan, desain, testing dan implementasi. *Next-Generation Firewall* pada *router Fortinet* dapat membuat keamanan jaringan menjadi lebih ketat, karena dalam *Next-Generation Firewall* terdapat fitur tambahan seperti *Intrusion Prevention System (IPS), Web Filtering* dan *Application Control* sehingga dapat menjaga keamanan jaringan, menangkal serangan siber dari pihak ketiga, membatasi akses internal yang berpotensi menyebabkan serangan atau hal yang berdampak negatif bagi user internal dan dapat meninjau *traffic* di berbagai *platform* yang ada pada jaringan. Hasil dari penelitian ini adalah dengan *Next-Generation Firewall* pada *router Fortinet* dapat membantu menjaga keamanan jaringan internet, menangkal serangan siber dari pihak ketiga, membatasi akses internal yang berpotensi menyebabkan serangan atau hal yang berdampak negatif bagi *user* internal dan dapat memantau *traffic* di berbagai *platform* dalam jaringan, Fitur *Intrusion Prevention System (IPS)* dapat membantu secara aktif memasukkan *traffic* mencurigakan ke daftar hitam. Dengan adanya *Next-Generation Firewall, user* internal tidak dapat mengakses hal yang tidak diizinkan dan dapat memantau *traffic* yang digunakan serta menangkal serangan siber dari pihak ketiga. PT. ALODOKTER TEKNOLOGI SOLUSI dapat mencegah terjadinya serangan, memblokir *traffic* mencurigakan dan menjadi lebih aman.

Kata Kunci: *Firewall, Fortinet,* Keamanan Jaringan, *Next-Generation Firewall*, PT. ALODOKTER

1. PENDAHULUAN

Fasilitas jaringan internet selalu mendapatkan risiko adanya kerugian yang akan diterima oleh pengguna internet tersebut. Seperti serangan melalui internet dari pihak-pihak yang tidak bertanggung jawab atau sering disebut dengan *hacker*. Oleh karena itu seorang administrator jaringan harus memastikan bahwa sistem jaringan internet pada suatu perusahaan harus aman dari serangan *hacker* [1].

Diterima 12 Januari 2023, Direvisi 02 Maret 2023, Diterima untuk publikasi 16 Maret 2023

Semua jenis bahaya yang masuk baik secara langsung maupun tidak langsung akan mengganggu jalannya proses yang berkelanjutan dalam suatu organisasi komputer. Untuk mengamankan jaringan dari serangan yang potensial, penting untuk mengimplementasikan ide jaringan *firewall*. Dimana *firewall* diterapkan untuk mencegah akses yang tidak diizinkan yang datang baik dari dalam organisasi maupun dari luar organisasi. Penggunaan ide jaringan *firewall* sangat mendasar jika ada lalu lintas yang masuk atau keluar ke jaringan, *firewall* kemudian akan memeriksa dan mengatur *traffic* tersebut, yang kemudian akan mengirimkannya ke tujuan [2].

Keamanan jaringan komputer yang berada pada PT. Alodokter Teknologi Solusi sudah diterapkan dengan baik. Namun setelah melakukan riset, ditemukan permasalahan pada keamanan jaringan PT. Alodokter Teknologi Solusi yakni adanya beberapa *firewall* yang masih kurang diperhatikan sehingga memungkinkan *user* (internal) atau pihak ketiga (eksternal) mengakses sesuatu hal yang tidak diizinkan, oleh karena itu *Next-Generation Firewall* ini diimplementasikan guna untuk menjaga keamanan jaringan internet, menangkal serangan siber dari pihak ketiga, membatasi akses internal yang berpotensi menyebabkan serangan atau hal yang berdampak negatif bagi *user* internal serta dapat meninjau *traffic* di berbagai *platform* yang ada pada jaringan.

Untuk itu keamanan jaringan yang menjadi prioritas utama selalu diperhatikan dan harus terjaga dari segala kemungkinan serangan ataupun penyalahgunaan dari pihak-pihak yang tidak bertanggung jawab, sehingga menyebabkan sistem informasi pada suatu perusahaan menjadi rusak dan tidak bisa digunakan lagi sebagaimana mestinya [3].

Maksud penulis mengangkat tema Perancangan Keamanan Jaringan *Next-Generation Firewall* Menggunakan *Router Fortinet* Pada PT. Alodokter Teknologi Solusi adalah: Menjaga keamanan jaringan internet pada PT. Alodokter Teknologi Solusi, menangkal serangan siber dari pihak ketiga, membatasi akses internal yang berpotensi menyebabkan serangan atau hal yang berdampak negatif bagi *user* internal, meninjau *traffic* di berbagai *platform* yang ada pada jaringan. Sedangkan tujuan dari penulis adalah sebagai salah satu syarat kelulusan pada program studi strata satu (S1) untuk Program Studi Teknik Informatika di Universitas Nusa Mandiri Jakarta.

Konsep Dasar Jaringan

Jaringan komputer merupakan gabungan komputer berjumlah banyak yang terpisah-pisah akan tetapi tetap saling berhubungan dalam melaksanakan tugasnya. Beberapa komputer bisa dikatakan saling terhubung bila sesama komputer dapat saling bertukar informasi [4].

Prinsip dasar dalam suatu sistem jaringan ini adalah proses pengiriman data atau informasi dari pengirim kepada penerima melalui suatu media komunikasi tertentu. Tujuan dibangunnya suatu jaringan komputer adalah untuk membawa data-informasi dari pengirim menuju kepada penerima secara cepat dan tepat tanpa adanya gangguan melalui media transmisi atau media komunikasi tertentu [5].

Topologi Jaringan Komputer

Topologi jaringan merupakan berbagai *node*, perangkat, dan koneksi jaringan yang saling berkaitan antara satu dengan yang lainnya secara logis dan teratur. Dimana untuk menghubungkan berbagai jenis *node*, perangkat, dan koneksi jaringan ini bisa dengan kabel maupun nirkabel [6].

IP Address

IP Address *(Internet Protocol Address)* adalah deretan angka biner antara 32 *bit* sampai dengan 128 *bit* yang digunakan untuk alamat identifikasi pada tiap komputer *host* dalam suatu jaringan internet. Angka 32 *bit* berguna untuk alamat *IP Address* versi *IPv4* dan angka 128 *bit* berguna untuk *IP Address versi IPv6* untuk menunjukkan alamat dari suatu komputer pada jaringan internet yang berbasis *TCP/IP* [7].

Komsep Penunjang Usulan

Perancangan dan implementasi *Next-Generation Firewall* dengan *router Fortinet*. Penulis menggunakan *software Cisco Packet Tracer* untuk membuat topologi jaringan perusahaan dan *console* Fortinet untuk simulasi cara kerja *Next-Generation Firewall*. Disini penulis akan menjelaskan fungsi dari aplikasi penunjang untuk konsep *Next-Generation Firewall.*

a) *Fortigate*
   Fortigate merupakan suatu sistem keamanan yang diluncurkan oleh perusahaan *Fortinet*. *Fortinet* adalah perusahaan, penyedia layanan, dan badan pemerintahan di seluruh dunia, termasuk mayoritas dari perusahaan *Fortune Global* 100 di tahun 2009. *Fortinet* adalah pemimpin pasar untuk *unified threat management (UTM). Fortigate* sebagai perangkat yang menjamin keamanan jaringan secara keseluruhan dan berfungsi sebagai *gateway* dan *router* bagi jaringan *LAN* sehingga tidak dibutuhkan *router* atau perangkat tambahan *load balancing* lain bila ada lebih dari satu koneksi *WAN* [8].
b) *Firewall*
   Firewall pada dasarnya dimaksudkan untuk melindungi jaringan internal terhadap berbagai gangguan ataupun serangan yang berasal dari luar, *firewall* melindungi perangkat *router* dan *client-client* yang terhubung pada suatu jaringan. *Firewall* dapat menyeleksi paket yang melewatinya, berdasarkan aturan yang dibuat administrator [9].
c) *Next-Generation Firewall*
   Next-Generation Firewall atau sering disebut *NGFW* lebih kuat dibandingkan dengan *Traditional Firewall*. *NGFW* memiliki kemampuan *Traditional Firewall* dan

juga memiliki beberapa fitur tambahan untuk menangani lebih banyak variasi ancaman. *Firewall* ini disebut *"Next-Generation"* untuk membedakan dari *firewall* lama atau biasa disebut *Traditional Firewall* yang tidak mempunyai kemampuan tambahan tersebut [10].

Next-Generation Firewall adalah bagian dari teknologi *firewall* generasi ketiga, yang menggabungkan *firewall* tradisional dengan fungsi penyaringan perangkat jaringan lainnya, seperti *Application Firewall* yang menggunakan *Deep Packet Inspection (DPI) in-line, Intrusion Prevention System (IPS).* Teknik lain juga bisa digunakan, seperti inspeksi lalu lintas terenkripsi *TLS/SSL*, memfilterkan situs *web*, manajemen *QoS/bandwidth*, inspeksi *antivirus* dan integrasi manajemen identitas untuk pihak ketiga (yaitu *LDAP, RADIUS, Active Directory)* [11].

2. METODE PENELITIAN

Akan hal ini penulis mengumpulkan data dan informasi yang sangat mendukung di dalam penyusunan penelitian, antara lain:

2.1 Metode Pengumpulan Data

a) Observasi
Penulis melakukan pengumpulan data di PT. Alodokter Teknologi Solusi dengan cara melakukan pengamatan terhadap sistem keamanan jaringan pada perusahaan secara langsung pada pihak terkait dan memanfaatkan data dengan cara memperhatikan dan mencari kekurangan pada keamanan jaringan di *console router Fortinet* untuk meninjau permasalahan yang ada pada perusahaan.

b) Wawancara
Mendokumentasikan data dengan melakukan tanya jawab tentang topologi dan sistem keamanan jaringan secara langsung dengan pihak yang terkait yaitu, Bapak Rangga Yudasmara selaku *Manager IT Operation*.

c) Studi Pustaka
Metode ini penulis dapatkan dari berbagai sumber terutama dari internet yang membahas jaringan komputer yang sesuai dengan tema yang penulis bahas di penelitian ini dan pengumpulan data yang tertuju pada buku-buku yang bersumber, jurnal dan lainnya yang dapat mendukung di dalam penyusunan penelitian.

2.2 Tahapan Penelitian

a) Analisa Kebutuhan
Pada PT. Alodokter Teknologi Solusi membutuhkan sistem keamanan jaringan yang lebih ketat agar dapat menjaga keamanan jaringan, menangkal serangan dari pihak ketiga, membatasi akses internal yang berpotensi menyebabkan serangan atau hal yang berdampak negatif bagi *user* internal dan meninjau *traffic* di berbagai *platform* pada jaringan perusahaan.

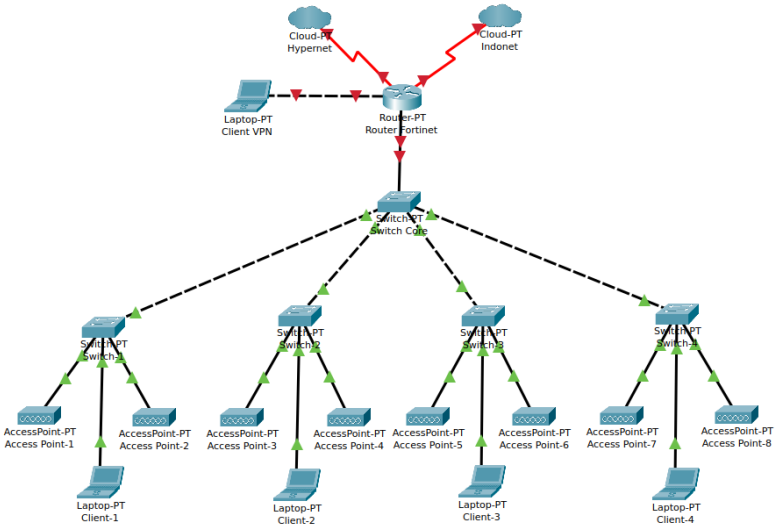
b) Desain
Penulis akan melakukan perancangan keamanan jaringan dengan menggunakan *software Cisco Packet Tracer* untuk menggambarkan skema jaringan yang diusulkan dengan membuat topologi keamanan jaringan.

c) Testing
Pengujian dilakukan dengan menggunakan *router Fortinet* yang dihubungkan dengan laptop dan terhubung dengan *ISP*. Untuk melihat sistem keamanan jaringan tersebut berjalan dengan baik, penulis menggunakan aplikasi pada laptop untuk melakukan *test* sistem keamanan jaringan tersebut.

d) Implementasi
Setiap ruangan akan menggunakan *access point* atau kabel *LAN* pada setiap komputer *client*, lalu dari sana akan di hubungkan ke *switch* dan di teruskan ke *router*. Di *router* inilah *Next-Generation Firewall* akan diimplementasikan, jika user internal atau pihak ketiga ingin mengakses sesuatu yang tidak diizinkan maka otomatis akan di *block* oleh *firewall.*

3. HASIL DAN PEMBAHASAN

3.1 Topologi Jaringan



Gambar 1. Topologi Jaringan

Gambar 1 di atas menggunakan 2 buah *ISP* yang menuju ke dalam *router Fortinet* yang di dalamnya menggunakan *firewall* agar mengamankan akses jaringan. Lalu dari *router Fortinet* dihubungkan dengan *core switch* sebagai inti penghubung antara perangkat lain. Dari *core switch* dihubungkan ke 4 buah *switch* dan dari *switch* tersebut dihubungkan kembali ke 8 *access point* dan *client* yang berada pada lingkungan kerja pada PT. Alodokter Teknologi Solusi. Untuk yang berada di luar kantor PT. Alodokter Teknologi Solusi dapat menggunakan *VPN* agar terhubung ke dalam jaringan perusahaan.

Tabel 1. *Hardware* Jaringan

No	Hardware
1	*Fortinet Fortigate 300E*
2	*Switch US-16-150W*
3	*Switch US-48-500W*
4	*Access Point UAP-HC-AD*
5	Komputer dan Laptop

Pada tabel 1 di atas adalah daftar *hardware* yang dipakai untuk topologi jaringan komputer pada perusahaan PT. Alodokter Teknologi Solusi.

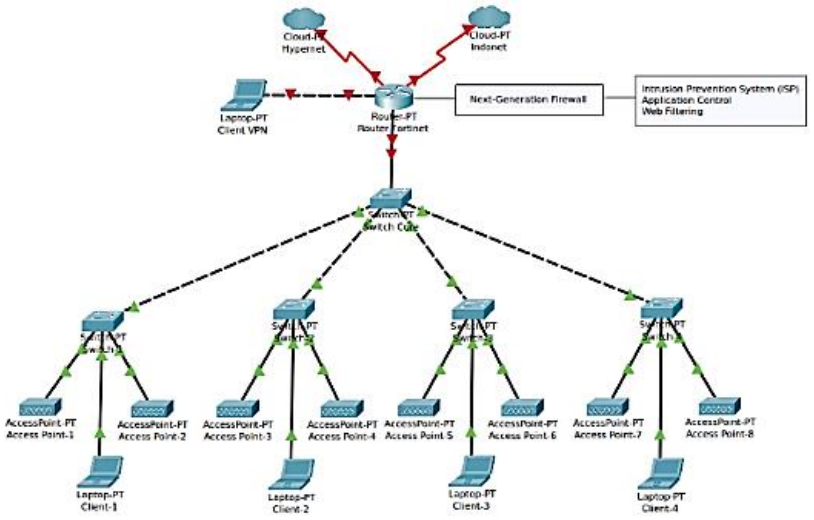
Tabel 2. *Software* Jaringan

No	Software
1	*Windows 10 Pro*
2	*Linux Ubuntu*
3	*MacOS*
4	*FortiClient VPN*
5	*Panda Security*

Pada tabel 2 di atas adalah daftar *software* yang dipakai untuk topologi jaringan komputer pada perusahaan PT. Alodokter Teknologi Solusi.

3.2 Skema Jaringan

Pada skema keamanan jaringan usulan ini penulis akan menggambarkan dengan menggunakan simulasi *Cisco Packet Tracer*, penulis hanya mengusulkan dan menambahkan fitur *Next-Generation Firewall* pada *router* Fortinet sebagai pengaman jaringan. Pada PT. Alodokter Teknologi Solusi penulis akan menerapkan *Next-Generation Firewall* dengan *Fortigate* pada *router Fortinet*, berikut skema jaringan yang diusulkan pada gambar 2 berikut:



Gambar 2. Skema Jaringan

3.3 Keamanan Jaringan

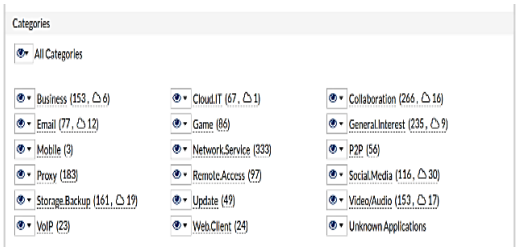
Di dalam keamanan jaringan pada PT. Alodokter Teknologi Solusi yaitu menggunakan *firewall* secara *default* dalam fitur *Web Filtering* dan *Application Control*, oleh karena itu penulis mengusulkan untuk menerapkan *Next-Generation Firewall* yaitu dengan fitur tambahan *Intrusion Prevention System (IPS)* dan menambahkan fitur dalam *Web Filtering* dan *Application Control* yang sudah diterapkan secara *default* pada keamanan jaringan PT. Alodokter Teknologi Solusi.

3.4 Rancangan Aplikasi

Pada rancangan ini penulis akan membuat dan mengimplementasikan *Next-Generation Firewall* dengan *router* Fortinet, *Next-Generation Firewall* yaitu *firewall* dengan sejumlah fitur tambahan untuk menangani ancaman dari dalam dan luar jaringan. Dengan menggunakan *router Fortinet* penulis akan melakukan konfigurasi pada *console Fortigate*.

a) *Application Control*

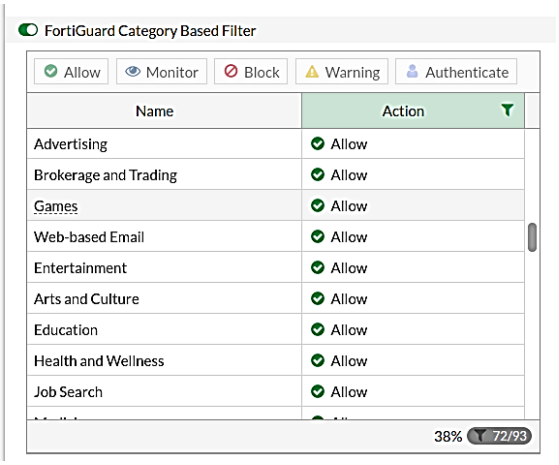
Pada *Application Control* penulis akan konfigurasi aplikasi apa saja yang ingin diberikan akses atau *allow*, *monitoring* dan *block*. Pilih *Firewall Policy* yang akan dituju untuk menggunakan *firewall Application Control* yang sudah dikonfigurasi, seperti yang dapat dilihat pada gambar 3 berikut.



Gambar 3. *Application Control*

b) *Web Filtering*

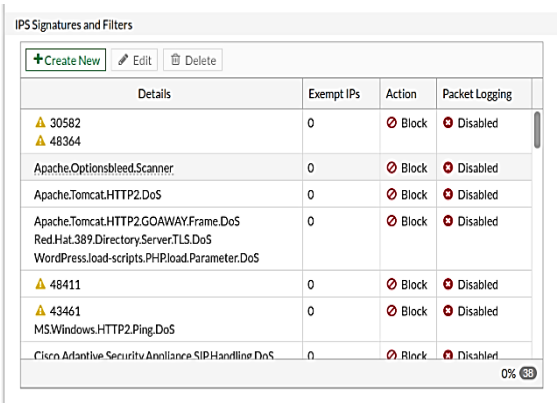
Pada *Web Filtering* penulis akan mengonfigurasi *website* apa yang diizinkan dan tidak diizinkan untuk diakses menggunakan jaringan. Pada gambar 4, pilih *Firewall Policy* yang akan dituju untuk menggunakan *firewall Web Filtering* yang sudah dikonfigurasi.



Gambar 4. *Web Filtering*

c) *Intrusion Prevention System (IPS)*

Pada *Intrusion Prevention System* akan konfigurasi *traffic* yang berpotensi membahayakan jaringan perusahaan. Pada gambar 5, pilih *Firewall Policy* yang akan dituju untuk menggunakan *firewall Intrusion Prevention System (IPS)* yang sudah dikonfigurasi.



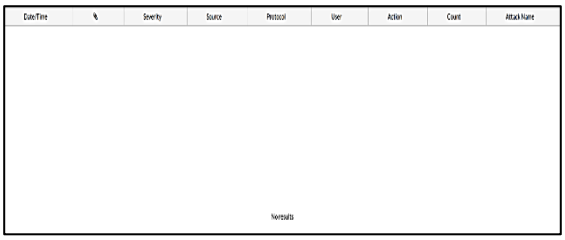
Gambar 5. *Intrusion Prevention System (IPS)*

3.5 Pengujian Jaringan

a) Pengujian Awal

Pada tahap pengujian awal penulis melakukan pengujian terhadap *Application Control, Web Filtering* dan *Intrusion Prevention System (IPS)* yang masih memberikan *action allow*. Hasilnya aplikasi, *website* dan *traffic* yang tidak diizinkan dapat masuk ke dalam jaringan dan tidak terdeteksi pada *log*. Hasil pengujian awal dapat dilihat pada gambar 6 dan gambar 7.

Gambar 6. *Log Allow Application Control*



Gambar 7. *Log Allow Intrusion Prevention System (IPS)*

b) Pengujian Akhir

Pada tahap pengujian akhir penulis melakukan pengujian terhadap *Application Control, Web Filtering* dan *Intrusion Prevention System (IPS)* yang sudah diberikan *action* monitor dan *block*. Hasilnya aplikasi, *website* dan *traffic* yang tidak diizinkan dapat di *monitoring* dan ter-*block* saat masuk ke dalam jaringan dan dapat terdeteksi pada *log*. Hasil pengujian awal dapat dilihat pada gambar 8, gambar 9, dan gambar 10.

Gambar 8. *Log Block Web Filtering*

Gambar 9. *Log Monitor Application Control*

Gambar 10. *Log Block Intrusion Prevention System (IPS)*

4. KESIMPULAN

Dari hasil pembahasan dan penelitian yang telah diuraikan, maka penulis dapat mengambil beberapa kesimpulan diantaranya ialah: Mengaktifkan fitur *Next-Generation Firewall* pada *router Fortinet* dapat membantu menjaga keamanan jaringan internet, menangkal serangan siber dari pihak ketiga, membatasi akses internal yang berpotensi menyebabkan serangan atau hal yang berdampak negatif bagi user interal dan dapat memantau *traffic* di berbagai *platform* dalam jaringan. Dengan menambahkan fitur *Intrusion Prevention System (IPS)* dapat membantu secara aktif memasukkan *traffic* mencurigakan ke daftar hitam. Fitur *Web Filtering* dan *Application Control* yang sudah diterapkan secara *default* kurang berperan penting, oleh karena itu harus dimanfaatkan sebaik mungkin agar keamanan jaringan menjadi lebih ketat. Dengan adanya *Next-Generation Firewall* user internal tidak dapat mengakses hal yang tidak diizinkan dan dapat memantau *traffic* yang digunakan serta menangkal serangan siber dari pihak ketiga.

Ucapan Terima Kasih

Terima kasih kami ucapkan kepada Jurnal Informatika Terpadu atas kesempatannya dalam mempublikasikan tulisan ini, dan juga terima kasih kepada PT ALODOKTER yang telah memberikan kesempatan dalam melakukan observasi. Kepada pihak kampus kami yang telah mendukung dalam penyusunan jurnal ini..

DAFTAR PUSTAKA

[1] W. W. Purba, R. Efendi, F. Teknologi, I. Universitas, and K. Satya, “Perancangan dan analisis sistem keamanan jaringan komputer menggunakan SNORT,” vol. 17, no. 2, pp. 143–158, 2021.

[2] I. F. B. Andoro, H. Agung Budijanto, and M. Aidjili, “Analisa Keamanan Jaringan Dengan Mikrotik,” *RISTEK J. Riset, Inov. dan Teknol. Kabupaten Batang*, vol. 6, no. 2, pp. 35–39, 2022.

[3] A. Riduan and N. Sadikin, “Perancangan Firewall Menggunakan Fortigate Di Pt . Swadharma Duta Data,” vol. 8, no. 1, pp. 90–98, 2021.

[4] A. Hidayat and D. S. P. Prakoso, “RANCANGAN TOPOLOGI DAN IMPLEMENTASI JARINGAN INTERNET PADA PERUSAHAAN PT KRESNA GRAHA INVESTAMA Tbk. Akik,” *J. Tek. Inform.*, vol. 3, no. 1, p. 82, 2021.

[5] N. K. Dewi and A. S. Putra, “Pengembangan Sistem Jaringan Menggunakan Local Area Network Untuk Meningkatkan Pelayanan (Studi Kasus di PT . ARS Solusi Utama),” *TEKINFO Vol. 22, No. 1, April 2021*, vol. 22, no. 1, pp. 66–81, 2021.

[6] Edavos, “Pengertian Topologi dan 10 Jenis Perangkat Jaringan Komputer.” .

[7] Pro.co.id, “Pengertian IP Address, Fungsi, Jenis dan Penjelasan Pembagian Kelas IP Adress.” .

[8] A. Darojat and I. Nurhaida, “Analisa Qos Administrative Distance,” *J. Ilmu Tek. dan Komput.*, vol. 3, no. 1, pp. 11–21, 2019.

[9] C. Purnama and P. Astuti, “Implementasi Virtual Private Network Menggunakan Protokol L2TP Untuk Meningkatkan Keamanan Data Pada Fakultas Hukum Universitas Indonesia,” vol. 1, no. 1, pp. 1–11, 2020.

[10] Cloudflare, “Next-generation firewall (NGFW) vs. firewall-as-a-service (FWaaS) | Cloudflare.” .

[11] Herza.id, “Kekuatan NGFW (Next Generation Firewall) Technology - Herza.ID.” .