Jurnal Informatika Universitas Pamulang **ISSN: 2541-1004**
Penerbit: Program Studi Teknik Informatika Universitas Pamulang **e-ISSN: 2622-4615**
Vol. 8, No. 2, Juni 2023 (322-329) **10.32493/informatika.v8i2.33656**

Implementasi Perangkat Next Generation Firewall untuk Melindungi Aplikasi dari Serangan Malware

Herika Andini Putri [1], Rohmat Tulloh [2], Nazel Djibran [3]

[1,2]Program Studi Teknik Telekomunikasi, Telkom University, Jl. Telekomunikasi No. 1,Terusan Buah Batu Bandung, Jawa Barat, Indonesia, 40257
e-mail: [1]herikasembiring06@gmail.com, [2]rohmatth@telkomuniversity.ac.id

[3]PT. Datacomm Diangraha, Jl. Kapten Tendean 18A Jakarta, Indonesia, 12790
e-mail: [3]nazel.djibran@datacomm.co.id

Submitted Date: June 16th, 2023 Reviewed Date: June 22nd, 2023
Revised Date: June 27th, 2023 Accepted Date: June 30th, 2023

Abstract

Based on the rapid development of technology, which has positive and negative impacts, one of the negative impacts is data leakage, called cybercrime. This is very dangerous and causes huge losses. In addition, the most commonly found cybercrimes are malware threats, phishing, DDoS, and others. In this study, the implementation of the Paloalto firewall is carried out by configuring the firewall, as is the attack testing stage using malware such as Eicar, ransomware, Trojans, Dos, and web filtering. The results of this test aim to prevent the risk of data loss, material loss, and the paralysis of public services. And to be efficient and effective in scanning for a variety of attacks without affecting network performance. The implications of the results found are expected to solve the problem at hand perfectly. NGFW performs prevention by blocking access to malware that enters its network traffic. This research also implements NGFW, where firewall configuration is carried out, namely by creating a rule policy on the firewall. In this study, an evaluation of network performance was carried out after the implementation of NGFW and firewall configuration. The results show that the use of NGFW and rule policies on firewalls can improve network security efficiently and effectively. It is hoped that these results can overcome the paralysis of public services due to malware attacks and improve network performance.

Keywords: Cybercrime; Next Generation Firewall; Malware; Paloalto; Testing

Abstrak

Berdasarkan Perkembangan teknologi yang begitu pesat memiliki dampak yang positif dan negatif, salah satu dampak negatifnya adalah adanya kebocoran data yang disebut dengan kejahatan siber. Hal tersebut sangatlah berbahaya dan menimbulkan kerugian yang begitu besar. Selain itu juga, kejahatan siber yang paling sering ditemukan adalah seperti ancaman malware, phishing, DDoS, dan lainnya. Pada penelitian ini melakukan implementasi Paloalto firewall dengan melakukan konfigurasi pada firewall dan juga tahap pengujian serangannya dengan menggunakan malware seperti Eicar, ransomware, Trojan, Dos, dan juga adanya web filtering. Hasil pengujian ini bertujuan untuk mencegah risiko kehilangan data, kerugian material, lumpuhnya layanan publik. Dan agar efisien dan efektif dalam melakukan scanning dari variasi serangan tanpa mempengaruhi performa jaringan. Implikasi hasil yang ditemukan diharapkan dapat menyelesaikan masalah yang dihadapi dengan sempurna. NGFW melakukan pencegahan dengan memblokir akses malware yang masuk pada traffic jaringannya. Pada penelitian ini juga melakukan implementasi NGFW di mana dilakukan konfigurasi firewall yaitu dengan pembuatan rule policy pada firewall tersebut. Pada penelitian ini, dilakukan evaluasi terhadap performa jaringan setelah implementasi NGFW dan konfigurasi firewall. Hasilnya menunjukkan bahwa penggunaan NGFW dan rule policy pada

firewall dapat meningkatkan keamanan jaringan dengan efisien dan efektif. Diharapkan hasil ini dapat mengatasi lumpuhnya layanan publik akibat serangan malware serta memperbaiki performa jaringan.

Kata Kunci: kejahatan siber; next generation firewall; malware; Paloalto; Testing

1 Pendahuluan

Seiring dengan perkembangan teknologi yang sangat pesat dan tak luput dari inovasi serta riset yang berlangsung, tentu ada sisi positifnya seperti kemudahan dalam melakukan komunikasi dan pertukaran data, dan sisi negatifnya adalah adanya kejahatan siber yaitu serangan dan pencurian data. Hal tersebut sangat menarik perhatian publik dikarenakan semakin maju teknologi, maka serangan dan pencurian data menjadi semakin tinggi dengan model yang canggih. Salah satu bentuk kejahatan siber adalah serangan zero day, di mana serangan tersebut merupakan ancaman yang berpotensi tinggi karena memanfaatkan kerentanan yang belum pernah diketahui. (Yasin, n.d.)

Dampak negatif dari perkembangan teknologi tersebut dapat mengakibatkan kerugian khusunya yang berhubungan dengan sejumlah data-data yang merupakan informasi penting dan hanya diperbolehkan untuk diketahui oleh orang-orang tertentu di dalam sebuah perusahaan. Selain itu, serangan zero day juga dapat merusak reputasi perusahaan dan mengganggu operasional bisnis secara keseluruhan. Oleh karena itu, penting bagi perusahaan untuk memiliki sistem keamanan yang kuat dan terus memperbarui perlindungan mereka terhadap serangan semacam ini. Kasus kebocoran data terbesar di dunia berdasarkan laporan CSO yaitu kebocoran data Yahoo pada agustus 2013 di mana ada sekitar 3 miliar akun yang berada di layanan mereka bocor (Khalisah & Kirana, 2022), sehingga keamanan data adalah prioritas utama untuk diperhatikan dari kerusakan ataupun penyalahgunaan dari pihak tanggung jawab.

Salah satu langkah yang dapat digunakan untuk mencegah adanya pencurian data atau informasi dalam suatu jaringan, yaitu dengan menggunakan teknologi firewall(Ramos Brandao & Almeida, 2021). Fungsi firewall adalah menjaga jaringan dari trafic yang berbahaya, di mana bentuk dari firewall dapat berupa hardware maupun software. Jika diilustrasikan firewall dapat digambarkan seperti pintu gerbang. Jadi ketika kita mengirimkan paket dari internet, sebelum sampai dikirimkan kepada user, firewall menyarinng paket tersebut dan memutuskan apakah paket tersebut diterima atau ditolak.

Firewall merupakan suatu sistem yang dapat menerapkan access control policy pada lalu lintas jaringan, yang dapat membantu melindungi dari serangan lalu lintas jaringan dan serangan lainnya, serta dapat memfilter lalu lintas jaringan yang masuk pada jaringan. Implementasi firewall sangat penting diterapkan pada perangkat komputer untuk menghindari dari pencurian data-data yang ada di dalam perangkat yang sifatnya rahasia. Implementasi firewall penting untuk diterapkan pada jaringan untuk menjaga dari ancaman serangan. Dasar kinerja yang dimiliki firewall, yaitu dapat mendeteksi traffic jaringan yang sah. Seingga dapat diberikan akses ke dalam sistem dengan melewati firewall untuk dibatasi. Pembatasan akses yang masuk ke dalam jaringan lokal, kemudian melakukan pencegahan jaringan yang tidak terdaftar pada sistem. Pembatasan dilakukan dengan diaturnya rules atau policy pada konfigurasi firewall. The next-generation firewall (NGFW).

Next Generation Firewall merupakan firewall yang memiliki kemampuan dalam mendeteksi dan memblokir suatu serangan yang berbahaya. Kemampuan NGFW dengan memberikan proteksi dan perlindungan yang tinggi, serta dapat menerapkan keamanan yang terdapat pada tingkat protocol, port, dan aplikasi. Next generation firewall adalah bagian dari generasi ketiga firewall, perbedaan paling jelas antara keduanya adalah kemampuan next generation firewall untuk menyaring setiap trafic berdasarkan aplikasi. Pengguna next generation firewall dapat menggunakan white list atau signature-based IPS untuk membedakan antara aplikasi yang aman dan yang tidak aman, dan juga next generation firewall dapat membuat policy sampai Layer 7 dengan menggabungkan konten AI (IPS, Antivirus, Antispyware, dll) dalam policy.

Berdasarkan fenomena kasus di atas yaitu, rentannya pencurian data dan kebocoran data sehingga saya mengangkat judul tentang implementasi next generation firewall dan cara kerjanya untuk bertahan terhadap serangan

malware. Dikarenakan next generation firewall memiliki fitur yang lebih kompleks dalam pertahanan terhadap malware, saya menggunakan next generation firewall pada penelitian ini.

Pada penelitian ini saya memilih mengamankan sistem dengan next generation firewall dibandingkan dengan firewall tradisional dikarenakan firewall tradisional tidak dapat memblokir malware (*PENGAMANAN SISTEM JARINGAN KOMPUTER DENGAN TEKNOLOGI FIREWALL I Gede Suputra Widharma and The A Team*, n.d.). Penelitian ini melakukan implementasi seperti penelitian, yaitu melakukan implementasi web filter, antivirus, IPS, dan antiDDoS. Pada penelitian ini, juga melakukan pengujian ketahanan next-generation firewall terhadap serangan malware.

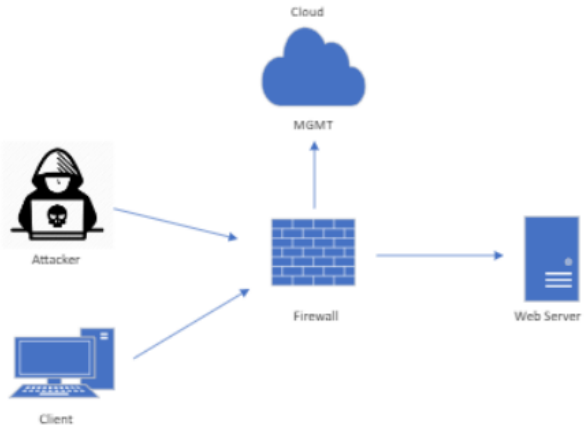
Pengujian ketahanan terhadap serangan malware pada next generation firewall pada penelitian ini menggunakan randsomware, Wannacry, dan malware lainnya. Penelitian ini menggunakan Wannacry dikarenakan menurut laporan ancaman ransomware unit 42 paloalto, mengemukakan bahwa trend randsomware terus meningkat. Jika diilihat dari laporan pada tahun 2022, kasus randsomware meningkat 144% dari tahun sebelumnya dan terdapat 85% jumlah peningkatan korban.

Wannacry terjadi pada sejak mei 2017 sampai saat ini telah melumpuhkan lebih dari 200.000 komputer di lebih dari 150 negara, dengan estimasi total kerugian mulai dari ratusan juta hingga miliaran US dollar. Cara kerja wannacry sendiri adalah dengan mengenkripsi semua dokumen yang dimiliki korban, sehingga korban tidak dapat mengakses dokumen tersebut dan juga menuntun tebusan kepada korban untuk dapat mengakses dokumen yang dia miliki. Target dari Proyek Akhir ini diharapkan dapat meningkatkan pertahanan sebuah firewall dari serangan malware dan juga membantu dalam mendeteksi dan mencegah serangan malware lebih awal.

2 Metode Penelitian

2.1 Model Sistem

Penelitian ini merupakan pengimplementasian dan pengujian ketahanan Next Generation Firewall terhadap serangan malware.

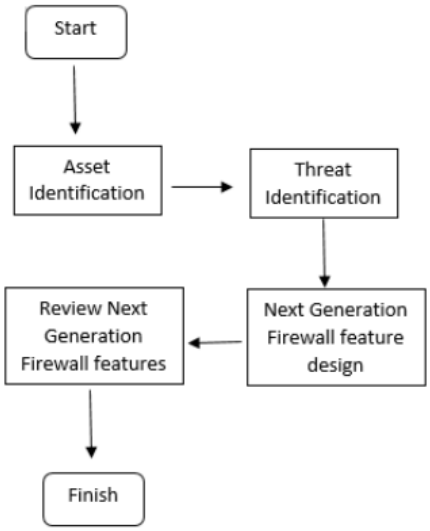


Gambar 1. Blok diagram sistem

Berdasarkan gambar 1 dapat dilihat bahwa pengujian ketahanan firewall dilakukan dari attacker dengan mengirimkan file malware ke webserver dalam bentuk zip. Setelah itu ketika client akses ke webserver dan si attacker mengubah file malware tersebut menjadi file unzip sehingga ketika client akses webserver dan membuka file tersebut otomatis malware masuk ke client tersebut dan dikarenakan web server melewati firewall sehingga log traffic malwarenya terdeteksi oleh firewall

Tahap pengujian dilakukan dengan tujuan untuk melihat ketahanan next generation firewall apakah sistem yang dibuat sudah sesuai dengan yang diharapkan. Untuk itu, diperlukan suatu metode pengujian yang menjadi ukuran atau parameter agar dapat diambil kesimpulan bahwa sistem yang dibuat telah berjalan sesuai dengan tujuan. Beberapa pengujian yang dilakukan antara lain:

1. Pengujian antivirus dilakukan dengan mencoba mendownload malware seperti Eicar, Randsomeware, dan Trojan untuk melihat apakah NGFW dapat melakukan pemblokiran.
2. Pengujian web filter dilakukan dengan mencoba mengakses website dengan memasukkan kategori blocking pada web filter untuk melihat apakah pada web filter untuk melihat apakah NGFW dapat mencegah pengguna mengakses website yang masuk ke dalam kategori blokir.



Gambar 2. Metode penelitian

Pada gambar 2 dijelaskan langkah untuk pengimplementasian next generation firewall di mana untuk pengimplementasian dilakukan sesuai dengan yang dibutuhkan di mana dilakukan konfigurasi pada firewall dan membuat rule policy sesuai dengan yang telah ditetapkan. Rule policy yang dibuat seperti antivirus dan web filtering. Beberapa fitur keamanan yang diterapkan antara lain Intrusion Prevention System (IPS), antivirus berbasis jaringan, dan web filter.

Fitur keamanan yang pertama adalah Intrusion Prevention System (IPS) yang berfungsi untuk memindai dan memblokir aktivitas yang dianggap mencurigakan dan berbahaya di dalam computer jaringan seperti kegiatan mengeksploitasi kelemahan sistem operasi untuk menemukan pintu belakang (backdoors).

Fitur keamanan kedua adalah antivirus berbasis jaringan yang berfungsi untuk memindai virus dengan memindai semua koneksi jaringan yang melewati perangkat Next-Generation.

Dalam melakukan pengujian ketahanan next generation firewall ini, ada beberapa skenario diujicobakan untuk mengetahui keandalan, efisiensi, dan ketersediaan sistem yang diuji. Berikut adalah beberapa skenario dalam penelitian ini:

1) Sistem pengujian menggunakan malware Eicar, Randsomeware, dan kemudia yang terakhir adalah dengan Trojan
2) Pengujian ini dilakukan dengan mengirimkan file malware ke webserver, sehingga ketika client mengunduh file tersebut terdeteksi pada log firewall.
3) Analisa log traffic pada firewall digunakan untuk mengetahui apakah malware tersebut terdeteksi pada firewall atau tidak dan setelah adanya malware yang terdeteksi, maka selanjutnya firewall akan memutuskan apakah file malware tersebut akan di allow atau di drop sesuai dengan rule policy yang telah dibuat
4) Pengujian web filtering yaitu dengan memblok website yang berbahaya sehingga ketika seseorang membuka website tersebut otomatis diblok.
5) Selain pengujian malware ada juga pengujian zero-day malware, di mana pengujian tersebut menggunakan malware yang belum dikenal atau malware jenis baru.

2.2 Metode Penyerangan

A. Skenario pengujian malware

Skenario pengujian malware ini dilakukan dengan menginstal file malware pada windows dan mendownload file tersebut di webserver, sehingga ketika proses download file malware tersebut berlangsung maka muncul traffic pada Next Generation Firewall.

Metode serangan yang dilakukan dapat dilihat pada table 1, kemudian dapat dilihat efek yang dihasilkan dari serangan yang dilakukan dan tindakan yang dilakukan oleh firewall yang diuji.

Pada tabel 1 dapat dilihat bahwa pengujian ketahanan Next Generation Firewall dilakukan dengan tiga jenis malware yaitu Eicar, Ransomware, dan juga Trojan.

Tabel 1. Skenario pengujian

No	Jenis Serangan	Metode Serangan	Target Serangan	Efek yang Dihasilkan	Response oleh Firewall
1	Eicar	Mendownload, mengekstrak, dan menjalankan malware	File Server dan user	Pengujian kualitas NGFW	Drop/Accept
2	Ransomware	Mendownload, mengekstrak, dan menjalankan malware	File Server dan user	Pengujian kualitas NGFW	Drop/Accept
3	Trojan	Mendownload, mengekstrak, dan menjalankan malware	File Server dan user	Pengujian kualitas NGFW	Drop/Accept

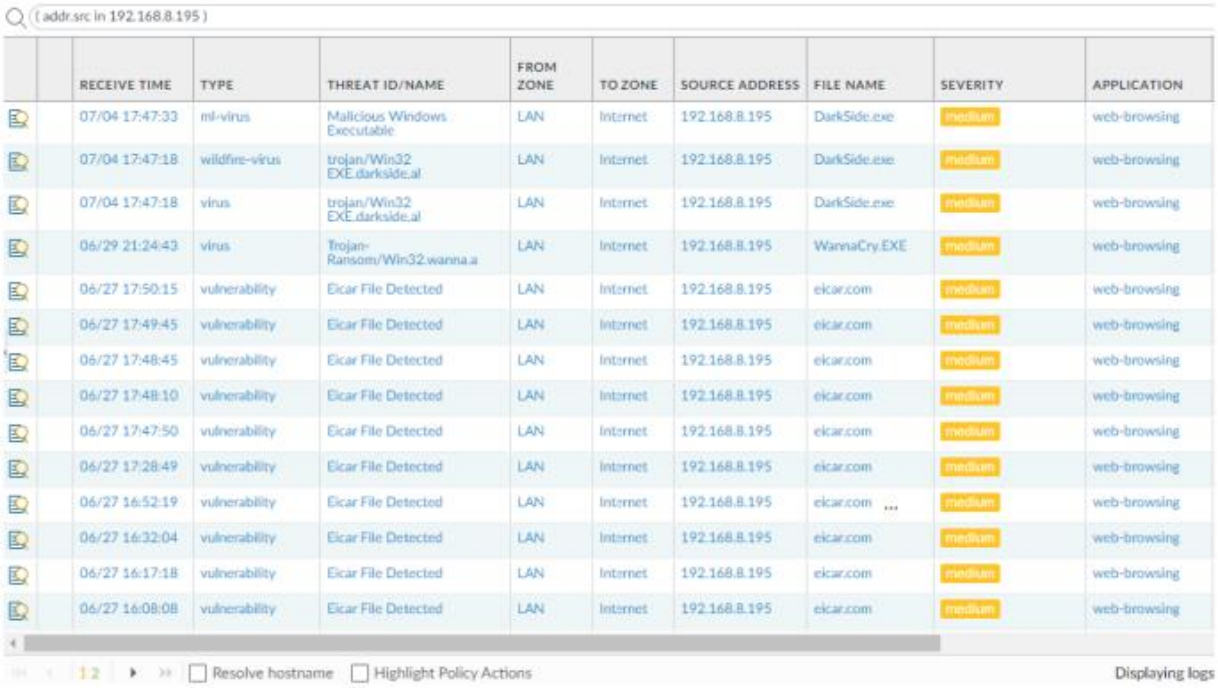
B. Skenario pengujian web filtering

Untuk menguji apakah fungsi web filter berjalan dengan baik, sebuah situs web yang mengandung unsur perbelanjaan online dilakukan pemblokiran. Jika konektivitas perangkat pengguna dapat melakukan ping, membuktikan bahwa pada lapisan jaringan, pengguna dapat mengakses shopping.com tetapi karena ada aturan untuk memblokir website dengan kategori perbelanjaan online, maka website tersebut tidak dapat diakses.

Namun, jika pengguna mencoba mengakses situs web lain yang tidak termasuk dalam kategori perbelanjaan online, seperti news.com, pengguna masih dapat mengaksesnya dengan lancar. Hal ini menunjukkan bahwa fungsi web filter berjalan dengan baik dalam memblokir akses ke situs web yang memiliki unsur perbelanjaan online.

3 Hasil dan Pembahasan

Pada bagian ini akan dijelaskan bagaimana ketahanan sebuah firewall untuk memblokir akses malware yang telah diuji.Untuk melakukan pengujian ketahanan NGFW terhadap malware adalah dengan membuat suatu webserver yang melewati suatu traffic jaringan yang dilindungi oleh fitur NGFW di mana awalnya webserver tersebut akan diberikan oleh attacker file malware berbentuk zip, seperti yang ketahui bahwa file berbentuk zip tidak akan bias dideteksi oleh firewall. Dan ketika file zip malware telah berada pada webserver maka attacker akan melakukan proses unzip pada file tersebut sehingga ketika client akan mencoba untuk mengakses file tersebut akan terdeteksi oleh NGFW bahwa file yang diakses adalah suatu file malware sehingga file tersebut akan langsung diblok oleh NGFW dan log traffic akan muncul pada firewall.


(addr.src in 192.168.8.195)

	RECEIVE TIME	TYPE	THREAT ID/NAME	FROM ZONE	TO ZONE	SOURCE ADDRESS	FILE NAME	SEVERITY	APPLICATION
	07/04 17:47:33	ml-virus	Malicious Windows Executable	LAN	Internet	192.168.8.195	DarkSide.exe	medium	web-browsing
	07/04 17:47:18	wildfire-virus	trojan/Win32 EXE.darkside.al	LAN	Internet	192.168.8.195	DarkSide.exe	medium	web-browsing
	07/04 17:47:18	virus	trojan/Win32 EXE.darkside.al	LAN	Internet	192.168.8.195	DarkSide.exe	medium	web-browsing
	06/29 21:24:43	virus	Trojan-Ransom/Win32.wanna.a	LAN	Internet	192.168.8.195	WannaCry.EXE	medium	web-browsing
	06/27 17:50:15	vulnerability	Eicar File Detected	LAN	Internet	192.168.8.195	eicar.com	medium	web-browsing
	06/27 17:49:45	vulnerability	Eicar File Detected	LAN	Internet	192.168.8.195	eicar.com	medium	web-browsing
	06/27 17:48:45	vulnerability	Eicar File Detected	LAN	Internet	192.168.8.195	eicar.com	medium	web-browsing
	06/27 17:48:10	vulnerability	Eicar File Detected	LAN	Internet	192.168.8.195	eicar.com	medium	web-browsing
	06/27 17:47:50	vulnerability	Eicar File Detected	LAN	Internet	192.168.8.195	eicar.com	medium	web-browsing
	06/27 17:28:49	vulnerability	Eicar File Detected	LAN	Internet	192.168.8.195	eicar.com	medium	web-browsing
	06/27 16:52:19	vulnerability	Eicar File Detected	LAN	Internet	192.168.8.195	eicar.com	medium	web-browsing
	06/27 16:32:04	vulnerability	Eicar File Detected	LAN	Internet	192.168.8.195	eicar.com	medium	web-browsing
	06/27 16:17:18	vulnerability	Eicar File Detected	LAN	Internet	192.168.8.195	eicar.com	medium	web-browsing
	06/27 16:08:08	vulnerability	Eicar File Detected	LAN	Internet	192.168.8.195	eicar.com	medium	web-browsing

1 2 Resolve hostname Highlight Policy Actions Displaying logs

Gambar 3. Log traffic pada next generation firewall

Berdasarkan gambar 3 dapat dilihat secara detail jenis malware yang masuk pada jaringan firewall seperti tanggal, waktu, jenis malware, IP jaringan, dan juga tingkat bahaya jenis malware tersebut. Tingkatan jenis malware pada next generation firewall terdiri atas critical tingkat yang paling berbahaya, medium adalah tingkat yang sedang da nada tingkat low, yaitu jenis malware yang tidak berbahaya.

A. Hasil dari Eicar Attack

Hasil dari uji coba eicar malware, next generation firewall melakukan aksi penolakan terhadap file yang mengandung virus yang dikirim dari penyerang, next generation firewall menolak

file yang dikirim ke web server, karena next generation firewall mendeteksi adanya malware di mana pattern pada attachment (eicar.com) tersebut dan setelah disesuaikan dengan database next generation firewall bahwa dapat disimpulkan bahwa file tersebut mengandung virus dan file ditolak.

B. Hasil dari Ransomware Attack

Hasil pada uji serangan wannacry ransomware dengan next generation firewall, karena next generation firewall mendeteksi adanya pattern ataupun bentuk file yang menyerupai ransomware dan setelah dicocokkan dengan database antivirus yang dimiliki oleh next generation firewall, maka akan next generation firewall menyimpulkan bahwa file tersebut mengandung malware dan file tersebut di drop ataupun langsung di blok.

C. Hasil dari Trojan Attack

Hasil dari uji coba trojan dengan next generation firewall, next generation firewall melakukan aksi reject terhadap file yang mengandung virus yang dikirim dari penyerang, next generation firewall menolak file yang dikirim ke file server, karena next generation firewall mendeteksi adanya virus like pattern pada attachment tersebut dan setelah dicocokkan dengan database antispam yang dimiliki oleh next generation firewall, maka next generation firewall menyimpulkan bahwa attachment tersebut mengandung virus dan file ditolak.

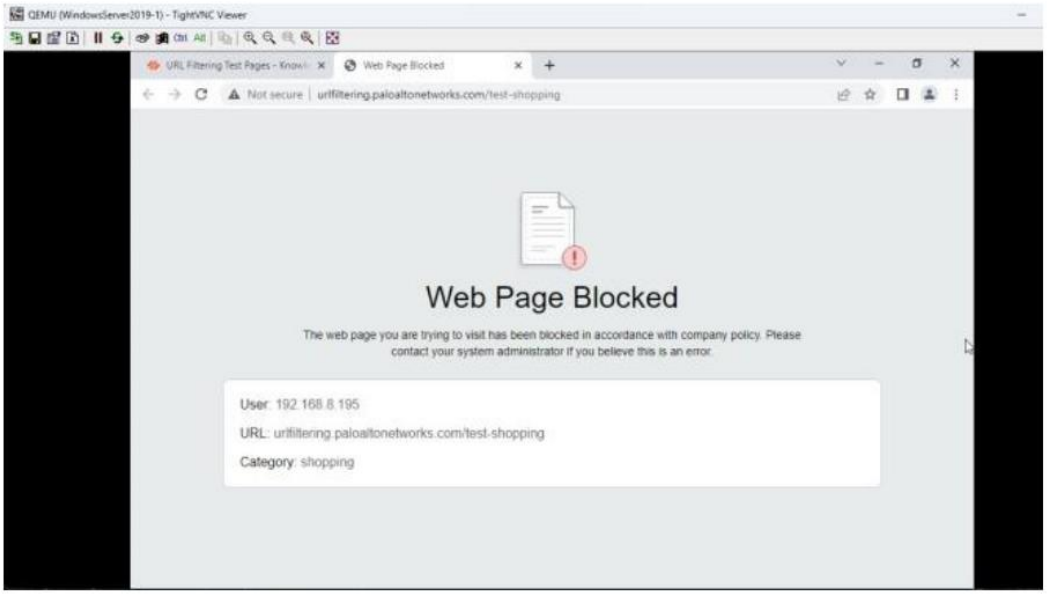
Hasil dari pengujian malware dapat dilihat dari tabel 2 di mana ketiga malware yang telah diuji dapat di drop oleh next generation firewall.

Tabel 2. Hasil pengujian malware pada next generation firewall

No	Jenis Serangan	Metode Serangan	Attack Target	Response NGFW
1	Eicar	Mendownload, mengekstrak, dan menjalankan malware.	File Server dan user	Drop
2	Ransomware	Mendownload, mengekstrak, dan menjalankan malware.	File Server dan user	Drop
3	Trojan	Mendownload, mengekstrak, dan menjalankan malware.	File Server dan user	Drop

D. Hasil dari Pengujian Web filtering

Pengujian web filtering diterapkan dengan memblokir situs atau website yang berbahaya seperti website perjudian, game online dan lain sebagainya, sehingga ketika seorang pengguna membuka sebuah website yang berbahaya walaupun konektivitas perangkatnya dapat melakukan ping yang membuktikan bahwa jaringan dapat diakses maka website berbahaya tersebut tidak dapat diakses.



Gambar 4. Tampilan website perbelanjaan online

Berdasarkan gambar 4 dapat disimpulkan bahwa web filtering berjalan dengan baik dikarenakan dapat memblokir website yang memiliki unsur perbelanjaan online.

Pengujian performa jaringan dapat dilakukan dengan melakukan ping ke situs detik.com. Di mana dapat dilihat bahwa rata-rata latensi yang terjadi adalah 61ms dan ketika trafik internet dilewatkan menuju next generation firewall maka rata-rata latensinya adalah 48ms. Untuk mengetahui kecepatan membuka website dilakukan pengujian dengan cara membuka website detik.com, di mana hasil yang didapatkan adalah terjadinya suatu peningkatan penggunaan jaringan internet unuk mengakses website detik.com adalah 3,25 detik sementara itu ketika trafik internet dilewatkan menuju next generation firewall waktu untuk dapat mengkases website detik.com adalah 1,31 detik.

Pada table 3 diuji dengan membandingkan kecepatan performa jaringan antara jaringan yang dilalui oleh next generation firewall dan jaringan tanpa next generation firewall. Dengan menggunakan next generation firewall yang telah diimplementasikan ada banyak aspek yang dapat ditingkatkan. Hasil dari penelitian tersebut ditampilkan pada tabel 3 yang menunjukkan peningkatan yang sangat baik, di mana adanya jaringan yang awalnya tidak memiliki sistem keamanan untuk melindungi teknologi dan sistem informasi teknologi dan informasi, saat ini telah memiliki Next Generation Firewall.

Tabel 3. Hasil perbandingan dengan NGFW dan tanpa NGFW

Pengukuran	Tanpa Next Generation Firewall	Dengan Next Generation Firewall	Perubahan
Rata-rata latensi	61 ms	48 ms	Penurunan kualitas latensi 27%
Rata-rata kecepatan akses website	3,25 detik	1,31 detik	Penurunan kecepatan waktu akses website 59,68%
Tingkat keamanan	Network Layer (L3)	Network Layer (L7)	100 %
Keamanan next generation firewall	Tidak ada	IPS, Antivirus, Web filter, WAF	100 %

E. Hasil dari pengujian wildfire

Pengujian wildfire dimanfaatkan untuk melihat bagaimana perlindungan Next Generation Firewall dalam melindungi sebuah aplikasi dari serangan malware yang belum diketahui atau zero day malware. Peran Next Generation Firewall disini adalah ketika adanya serangan zero day malware maka wildfire akan mendeteksi malware tersebut dan akan dikirimkan log atau traffic setelah 5 menit serangan karena wildfire membaca log ketika ada pesan yang masuk ke Paloalto, dapat dikatakan bahwa wildfire sama seperti sandbox.

Log traffic serangan akan terdeteksi selama 5 menit dikarenakan adanya proses dari wildfire sendiri, fitur wild fire akan mendeteksi malware dengan file hash sehingga prosesnya adalah ketika suatu file yang tidak dikenal dan melewati next generation firewall maka akan dicek dan dianalisis apakah fitur wild fire sudah pernah melihat file tersebut atau tidak. Jika filenya belum pernah diketahui maka akan dilakukan tindakan sesuai dengan ketentuan dari wild fire sendiri akan disesuaikan berapa kapasitas filenya dan apakah file tersebut trusted atau tidak sesuai dengan database pada next generation firewall, sehingga setelah hal tersebut sudah dilakukan maka wild fire akan memutuskan apakah file tersebut sebuah malware atau tidak.

Pengujian wildfire sangat bermanfaat karena dengan adanya fitur wildfire tersebut keamanan jaringan lebih terjaga dari serangan malware yang belum diketahui karena seiring dengan berkembangnya teknologi maka malware juga ikut berkembang dengan bentuk yang baru dan lebih update dari malware sebelumnya.

4 Kesimpulan

Setelah melakukan implementasi dan juga pengujian terhadap next generation firewall dapat disimpulkan bahwa kelengkapan fitur yang tersedia pada next generation firewall seperti Intrusion Prevention System (IPS), Antispam dan Mail, Threat Emulation, URL Filtering & Application Control dapat membuat jaringan komunikasi data menjadi lebih aman.

Dapat dilihat pada hasil uji coba yang telah dilakukan, di mana ketiga serangan yang dilakukan pada tugas akhir ini (ransomeware, trojan, phising dan web filtering) dapat terdeteksi seperti pada hasil yang ditunjukkan oleh tabel 2 dan dapat digerakkan oleh next generation firewall karena next generation firewall dapat melakukan inspeksi berdasarkan konten dan perilaku pada setiap paket data yang melewati next generation firewall sehingga dapat melakukan memblokir sebelum paket data tersebut masuk ke dalam jaringan.

Selain itu dengan adanya next generation firewall kecepatan suatu jaringan untuk mengakses suatu website meningkat karena seperti pada data yang ditunjukkan pada table 3 bahwa rata-rata latensi pada jaringan yang melewati traffic next generation firewall akan lebih kecil dibandingkan dengan nilai average latency yang tidak melewati traffic next generation firewall karena semakin kecil nilai rata-rata latensinya semakin bagus kecepatan akses website suatu jaringan.

Referensi

Almeida, P. R. (2021). Next-Generation Firewall Concept, Features, and Their . *no. doi: 10.31112/kriativ-tech-2021-*.

Khalisah, A. M., & Kirana, P. (2022). Implementasi Norma Hukum Terhadap Tindak Pidana Peretasan (Hacking) di Indonesia. *Jurist-Diction*, *5*(6), 2117–2132. https://doi.org/10.20473/jd.v5i6.40073

Pengamanan Sistem Jaringan Komputer Dengan Teknologi Firewall I Gede Suputra Widharma and The A Team. (n.d.).
https://www.researchgate.net/publication/346965331

Ramos Brandao, P., & Almeida, J. (2021). *Next-Generation Firewalls: Concept, Features, and Their Benefits*. https://doi.org/10.31112/kriativ-tech-2021-10-59

Yasin, M. A. (n.d.). *Respon Insiden dan Deteksi Terhadap Zero-Day*.

Jr, R. M. (2008). Keamanan sistem ionformasi. *Sistem Informasi Salemba*.

Kirana, A. M. (2022). Implementasi Norma Hukum Terhadap Tindak Pidana Peretasan (Hacking) di Indonesia.

Labone, M. (2020). Anomaly-based network intrusion detection using machine learning, . *Institut polytechnique de Paris*.

Sitorus, V. P. (2022). Nunukan State Court's Computer Network Security Improvement Using Centralized Next-Generation Firewall, *Budapest International Research and Critics* .

Team, I. G. (2021). Pengamanan Sistem Jaringan Komputer Dengan Teknologi Firewall.

Ramos Brandao, P., & Almeida, J. (2021). *Next-Generation Firewalls: Concept, Features,*