ANALISIS *PERFORMANCE NEXT GENERATION FIREWALL* DAN *MIKROTIK RB1100* SEBAGAI *FIREWALL* UNTUK KEAMANAN JARINGAN

Muhammad Lutfi Yusuf, Kundang Karsono, Nugroho Budhisantosa
Program Studi Teknik Informatika Fakultas Ilmu Komputer Universitas Esa Unggul, Jakarta
Jalan Arjuna No.9 Kebon Jeruk Jakarta Barat DKI Jakarta
Email: muhlutfiyusuf@gmail.com

Abstract

Network security is a form of prevention or detection of interference and unauthorized access to a computer network system. At present, the network security system in the core business of PT. Royal Lestari Utama (RLU) uses a traditional firewall that cannot detect data packets based on behavior and content so that network security on the internal and external networks of PT. RLU is very risky. Where this time the attacks carried out increasingly varied such as Distributed Denial Of Service and Wannacry ransomware. Next Generation Firewall can inspect data packets based on behavior and content so that suspicious data packages can be detected through the Intrusion Prevention System, Anti-Bot, Antivirus, and Anti-Spam & Email Security features. The waterfall approach is a model used to ensure success in repairing network security issues at PT. RLU The research conducted is analysis of performance Next Generation Firewall and Mikrotik RB1100 as firewalls for network security (case study of PT.RLU). The results of this study aim to prevent the risk of data loss, material loss, and paralysis of public services. And to be efficient and effective in scanning variations of attacks without affecting network performance. The implication of the results found is expected to be able to solve the problem faced perfectly.

Keywords*: Network Security, Waterfall, Next Generation Firewall*

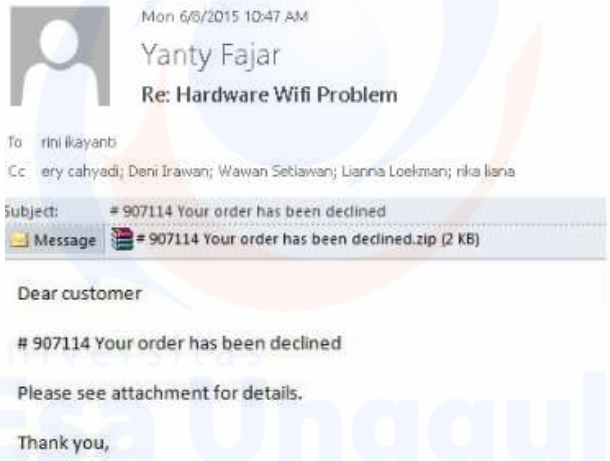
Abstrak

Keamanan jaringan adalah bentuk pencegahan atau deteksi pada hal yang bersifat gangguan dan akses tak seharusnya pada sistem jaringan komputer. Saat ini, sistem keamanan jaringan dalam *core business* PT. Royal Lestari Utama (RLU) menggunakan *traditional firewall* yang tidak dapat mendeteksi paket data berdasarkan *behavior* dan *content* sehingga keamanan jaringan di jaringan internal dan eksternal PT. RLU sangatlah riskan. Dimana saat ini serangan yang dilakukan semakin bervariatif seperti *Distributed Denial Of Service* dan *Wannacry ransomware*. *Next Generation Firewall* dapat melakukan inspeksi paket data berdasarkan *behaviour* dan *content* sehingga paket data yang mencurigakan dapat dideteksi melalui fitur *Intrusion Prevention System, Anti-Bot, Antivirus,* dan *Anti-Spam & Email Security*. Pendekatan *waterfall* adalah model yang digunakan untuk memastikan keberhasilan memperbaiki permasalahan keamanan jaringan di PT. RLU. Penelitian yang dilakukan yaitu Analisis *Performance Next Generation Firewall* Dan *Mikrotik RB1100* Sebagai *Firewall* Untuk Keamanan Jaringan (Studi Kasus PT.RLU). Hasil penelitian 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-hasil yang ditemukan diharapkan dapat menyelesaikan masalah yang dihadapi dengan sempurna.

Kata kunci*: Keamanan Jaringan, Waterfall, Next Generation Firewall*

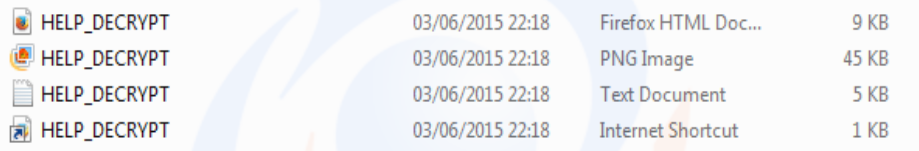
Pendahuluan

Pada tanggal 8 Jun 2015 jam 17:28 wib, *IT* menemukan *file* yang terinfeksi *wannacry ransomware* di *file server* PT. Royal Lestari Utama (RLU). *Wannacry ransomware* menginfeksi *file server* melalui pesan *email* dan lampiran palsu.



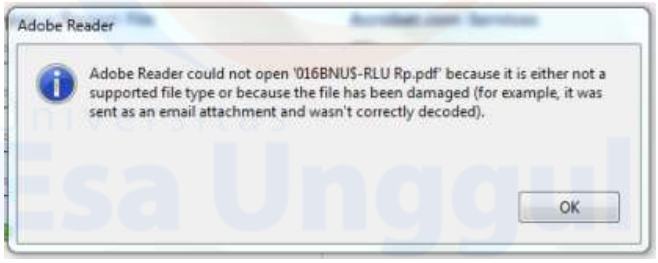
Gambar 1
Pesan *email* dan lampiran palsu yang digunakan dalam distribusi *wannacry ransomware.*

Ketika lampiran palsu di ekstrak dan di klik akan berisi *wannacry ransomware* seperti Gambar 2, *ransomware* akan mengenkripsi *file* (* .doc, * .docx, * .xls, * .ppt, * .psd, * .pdf, * .eps, * .ai, * .cdr , * .jpg, dll.) yang disimpan di *file server*.



Gambar 2
Bentuk *wannacry ransomware*

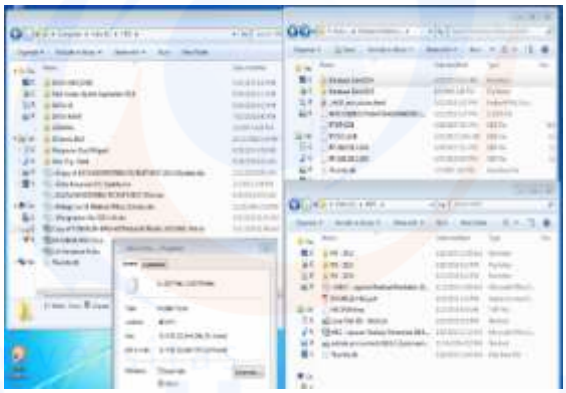
Gambar 3 dan Gambar 4 adalah contoh *format file .pdf dan .xlsx* yang terinfeksi *wannacry ransomware.*



Gambar 3
file .pdf yang telah terinfeksi *wannacry ransomware*

Gambar 4
file excel yang telah terinfeksi *wannacry ransomware*

Wannacry ransomware mengunci data sehingga tidak dapat diakses oleh pengguna. Ketika data telah benar – benar terkunci, *wannacry ransomware* meminta bayaran dalam bentuk *bitcoin* karena lebih sulit dilacak untuk pengembalian data. Satu atau dua *bitcoin*, setara dengan $500[2]. Akibat permasalahan ini perusahaan mengalami kehilangan 11.265 data. Dan jika dikonversikan ke uang, perusahaan mengalami kerugian sebesar 11.265 files x $500 = $5.632.500.

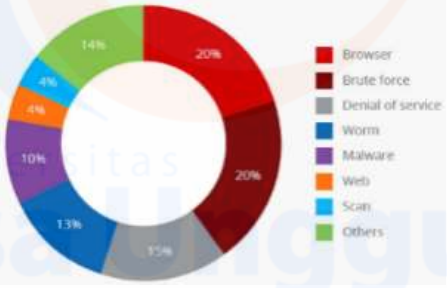


Gambar 5
Jumlah data yang telah terinfeksi virus *ransomware*

Sistem keamanan jaringan dalam *core business* PT. RLU saat ini menggunakan *traditional firewall* yang tidak dapat mendeteksi paket data berdasarkan *behavior* dan *content* sehingga keamanan jaringan komunikasi di jaringan internal dan eksternal PT. RLU sangatlah riskan. Dimana saat ini serangan yang dilakukan semakin bervariatif seperti *Distributed Denial Of Service* (DDOS) dan *wannacry ransomware.*

Next Generation Firewall (NGFW) dapat melakukan inspeksi paket data berdasarkan *behaviour* dan *content* sehingga paket data yang mencurigakan dapat dideteksi melalui fitur *Intrusion Prevention System* (*IPS*), *Anti-Bot, Antivirus,* dan *Anti-Spam & Email Security*. Pendekatan *waterfall* adalah model yang digunakan untuk memastikan keberhasilan memperbaiki permasalahan keamanan jaringan di PT. RLU.

Metode Serangan Pada Jaringan Komunikasi Data
DDOS dan *malware* menjadi metode serangan yang paling sering digunakan.

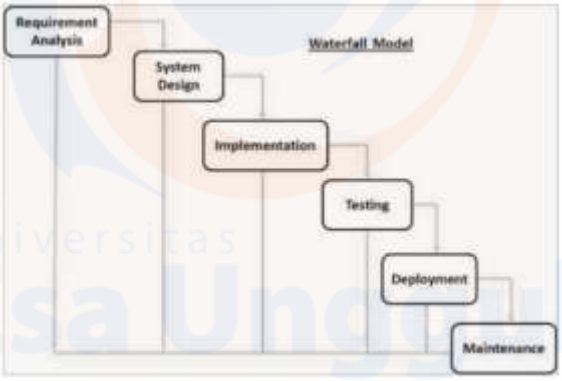


Gambar 6
Metode Serangan Yang Sering Dilakukan [4]

Penelitian ini akan berfokus pada kedua serangan tersebut. [3] *DDOS* memiliki jenis serangan yang umumnya digunakan yaitu *UDP Flood Attack*: Serangan ini dilakukan terus menerus oleh *attacker* hingga *bandwidth* dan *resource* target mengalami *overload* sehingga target menjadi *down.* Ada cara yang dapat digunakan untuk menghadapi *DDOS* yaitu Implementasi *Firewall NGFW* sudah memiliki fitur *Intrusion Prevention System (IPS)* yang dapat menangkap paket data mencurigakan. *NGFW* akan melakukan blokir terhadap paket yang memiliki *behaviour* seperti pada *signature attack* yang ada pada *database NGFW*. Sedangkan *wannacry ransomware* merupakan *trojan* yang mengambil data pada komputer yang telah terinfeksi dan mengirimkannya pada pembuat trojan itu sendiri. Ada cara untuk menghalau *wannacry ransomware* yaitu melakukan implementasi *NGFW* sebagai *gateway* zona *untrusted. NGFW* saat ini memiliki fitur *antivirus* yang dapat digunakan untuk menghalau *wannacry ransomware* .

A. Software Development Life Cycle (SDLC) – *Waterfall Model*

Pendekatan *waterfall* adalah model yang digunakan untuk memastikan keberhasilan memperbaiki permasalahan keamanan jaringan di PT. RLU. Berikut adalah ilustrasi dari fase model w*aterfall*.



Gambar 7 *Waterfall Model* [6]

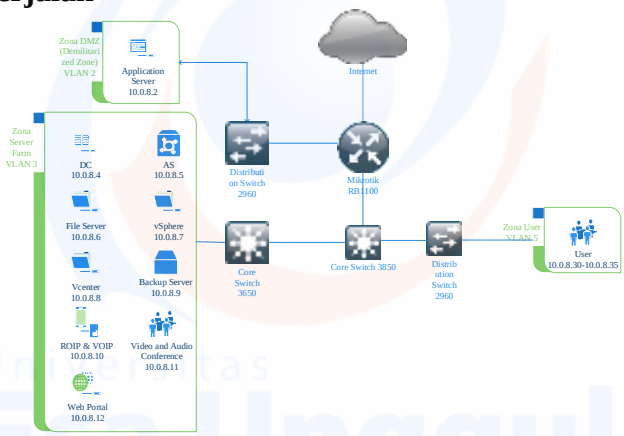
PIECES

PIECES meruapakan singkatan dari *Performance, Information, Economic, Control, Efficiency, and* Services. PIECES merupakan kerangka kerja untuk mengklasifikasi *problem* yang tidak diinginkan yang mencegah organisasi dalam mencapai visi, misi, tujuan, dan objektif.

Metode penelitian

A. *Requirement Analysis*

A.1 Topologi Jaringa Berjalan



Gambar 8 *Topology* Jaringan Berjalan [8]

Dikarenakan luasnya topologi jaringan PT. RLU, maka akan dilakukan batasan topologi jaringan tersebut mencakup *file server* dan *user.*

Identifikasi Masalah Menggunakan Metode *PIECES*

Berikut adalah analisis kelemahan sistem berjalan dengan metode *PIECES* sehingga membantu dalam membuat rancang bangun sistem baru yang lebih baik:

1. *Performance*
   Tidak dapat melakukan *filtering* terhadap akses dari jaringan internal dan eksternal.
2. *Information*
   Belum dapat menghasilkan informasi yang akurat, relevan, dan tepat waktu untuk mengetahui apakah jaringan perusahaan telah atau sedang diserang.
3. *Economy*
   Bisa menanggung kerugian operasional, baik skala besar maupun kecil.
4. *Control*
   Tidak dapat melindungi suatu jaringan dari berbagai ancaman fisik maupun logik yang dapat menganggu aktivitas yang sedang berlangsung.
5. *Efficiency*

Laporan yang disajikan tidak disediakan secara cepat danmempunyai tingkat keakuratan dan konsistensi yang rendah.

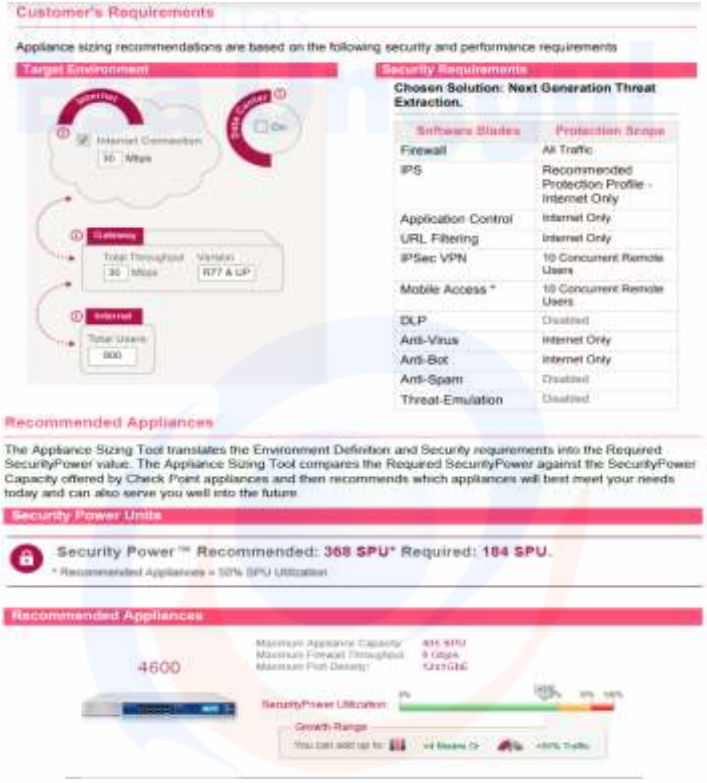
6. *Services*

Kerusakan sistem dan kehilangan data dapat melumpuhkan sejumlah layanan publik.

System Design

Spesifikasi Kebutuhan

Spesifikasi *NGFW* yang digunakan berdasarkan kapasitas *user*, *bandwidth*, dan fitur-fitur sebagai berikut:

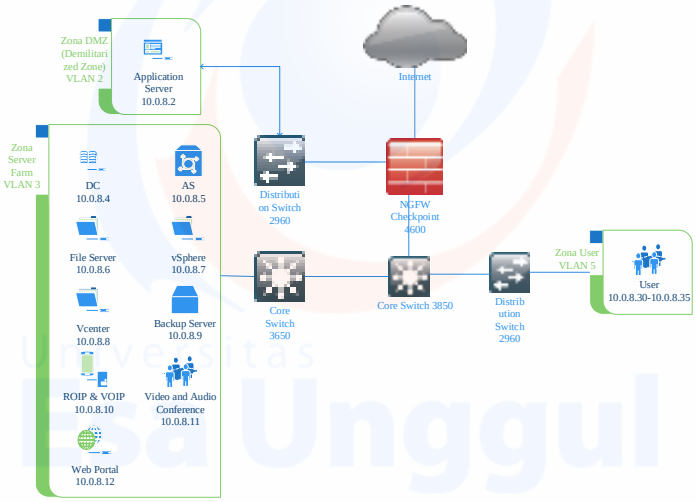


Gambar 9

Chek Point Appliance Sizing Recommendation

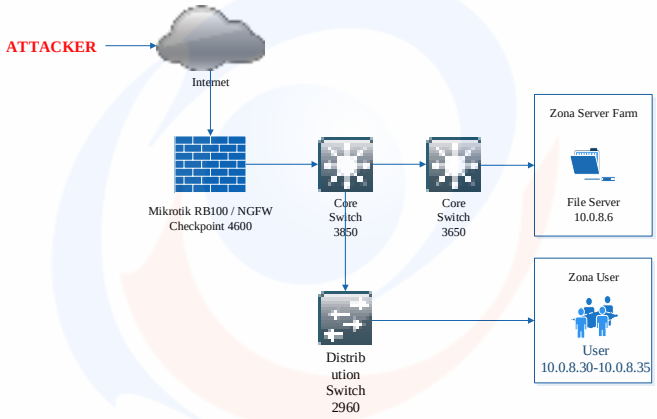
Berdasarkan informasi Gambar 9 yang dimasukkan ke dalam *Check Point Sizing Tool*, maka didapatkan tipe perangkat *Check Point Security Gateway* yang direkomendasikan adalah *Check Point* 4600. *Bill of quantity* dari *Check Point* 4600 *Next Generation Threat Prevention* (NGTP) *Bundle* adalah **$29.389.**

Topologi Jaringan Usulan



Gambar 10
Topologi Jaringan Usulan

Flow Chart Uji Coba Serangan



Gambar 12
Flow chart serangan *file server* dan *user*

Rancangan Konfigurasi *NGFW*

Gambar 13
Langkah – Langkah Merancang Konfigurasi Dasar *NGFW*

Metode Uji Coba *Firewall*

Metode serangan yang dilakukan dapat dilihat pada tabel 1, kemudian akan dilihat efek yang dihasilkan dari serangan yang dilakukan dan tindakan yang dilakukan oleh kedua *firewall* yang diuji.

Tabel 1 Metode Uji Coba *Firewall*

No	Jenis Serangan	Metode Serangan	Target Serangan	Efek yang Dihasilkan	Response oleh *Firewall*
1	*DDOS*	*UDP Flooding*	*File Server* dan *user*	*Bandwidth server overload*	*Drop/Accept*
2	*Wannacry ransomware*	Mendownload, mengekstrak, dan menjalankan *wannacry ransomware*	*File Server* dan *user*	Pengujian kualitas firewall traditional dan NGFW	*Drop/Accept*

Hasil dan Pembahasan

Identifikasi Aset

Identifikasi asset terhadap perangkat apa saja yang akan dilindungi oleh kedua *firewall* tersebut. Asset yang akan dilindungi berupa *file server* dan *user* dengan penggunaan port sebagai berikut:

Tabel 2
List Aset PT. Royal Lestari Utama

No	*Server*	*Destination*	*Protocol*	*Port*
1	*File server*	10.0.8.6	*TCP*	80, 443
			UDP	>1023, 161, 53, 138, 80, 389
			ICMP	ICMP Request, Echo Reply
2	*User*	10.0.8.30-10.0.8.35	*TCP*	80,443, 25, 465, 143, 993, 110, 995, 53, 389
			UDP	>1023, 161, 53, 138, 80, 389
			ICMP	ICMP Request, Echo Reply

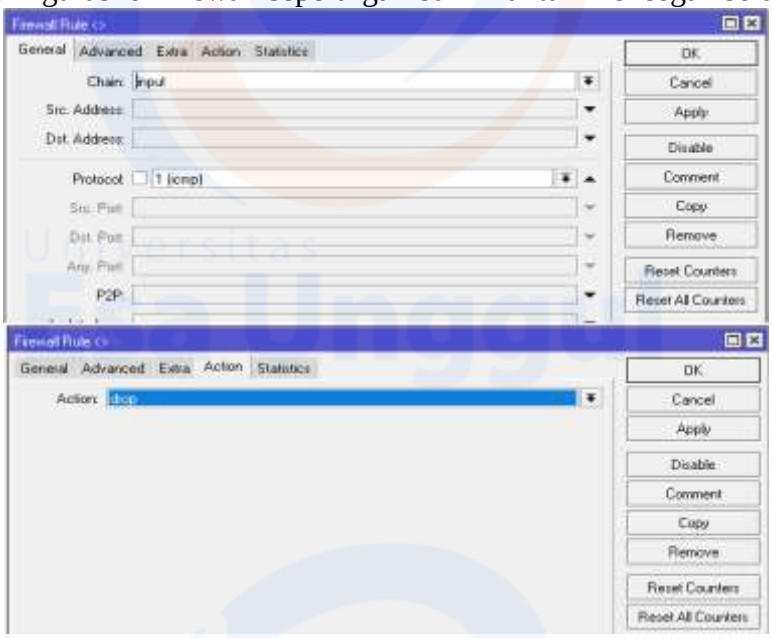
Konfigurasi *Mikrotik RB1100* dan *Stateful Firewall NGFW Checkpoint*

Konfigurasi *Mikrotik RB1100*

1. Ketika *login mikrotik* meminta *username* dan *password.* Masukkan *username: admin* dan *password:* kosong.
2. Melakukan konfigurasi *Internet Protocol* (IP) agar *mikrotik* bisa diakses melalui *winbox* versi 2.2.18. Ketikkan perintah-perintah berikut: # ip add print, # inter print, # ip add address interface=ether1 address=10.0.8.13 netmask=255.255.255.0
3. Menambahkan *NAT* di *firewall Mikrotik RB1100* dengan cara: *IP* > *Firewall*, Pilih tab *NAT*, Klik tanda "+" untuk menambahkan konfigurasi, *Chain: srcnat* > *out. Interface: ether1* > *action: masquerade.*
4. Menambahkan *IP Address* 10.0.8.13/24 dan 10.0.7.1/24 di mikrotik dengan cara: *IP* > *Address list*, Klik tanda "+", Masukkan *address*: 10.0.8.13/24 > *interface*: ether1 > klik ok, Klik tanda

"+" lagi untuk menambahkan IP 10.0.7.1/24, Masukkan *address*: 10.0.7.1/24 > *interface*: ether3 > klik ok.

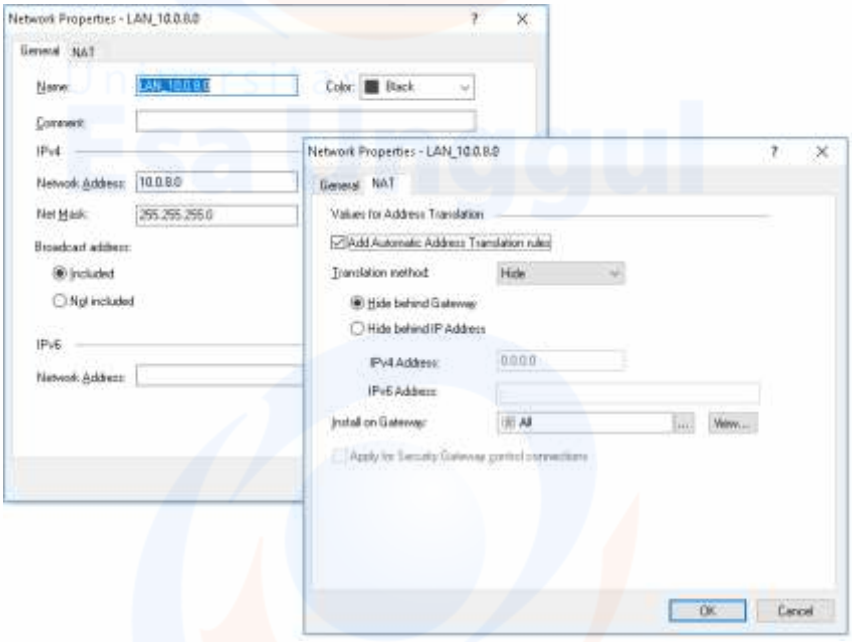
5. Menambahkan konfigurasi di firewall seperti gambar 14 untuk mencegah serangan DDOS



Gambar 14
Tampilan Konfigurasi *Firewall* Untuk Mencegah Serangan DDOS

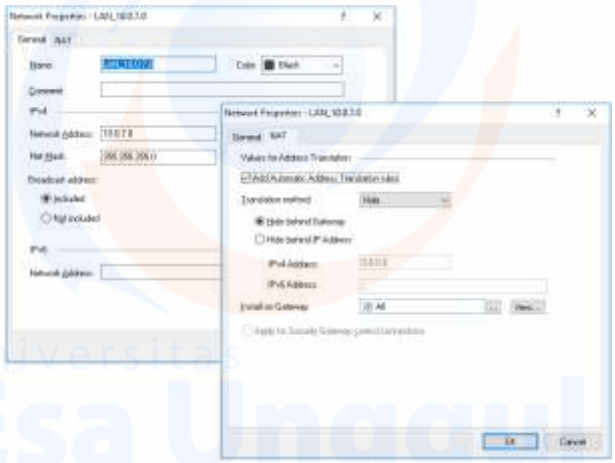
Konfigurasi *NGFW Checkpoint 4600*

1. Buka aplikasi *Checkpoint SmartDashboard R77.30*. *Username*: whcheckpoint dan *Password*: laj12345, dan *Server Name or IP Address*: 10.0.8.13. kemudian tekan *enter*.
2. Pilih ***Network Objects*** > ***Networks*** > ***klik kanan, pilih Networks***:
   a. *Tab* ***General*** > ***Name: LAN_10.0.8.0*** > ***Network Address:10.0.8.0*** > ***Net Mask: 255.255.255.0*** > *Tab* ***NAT*** > ***checked Add Automation Address Translation Rules*** > ***ok.***



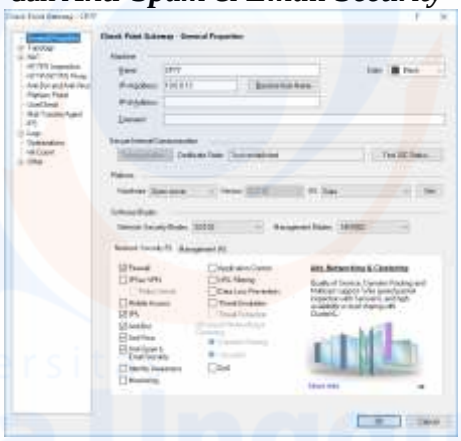
Gambar 15
Penambahana *IP Public* di *Network Objects*

   b. *Tab* ***General*** > ***Name: LAN_10.0.7.0*** > ***Network Address:10.0.7.0*** > ***Net Mask: 255.255.255.0*** > *Tab* ***NAT*** > ***checked Add Automation Address Translation Rules*** > ***ok.***



Gambar 16
Penambahana *IP 10.0.7.0*

3. Pilih ***Network Objects*** > ***Chekpoint*** > CP77 > ***Edit*** > ***Topology*** > ***Get*** > ***Interface with Topology*** > ***Yes*** > ***Accept*** > *Double click* masing-masing ***eth0, eth1,*** dan ***eth2*** >***Topology*** *tab* > ***Anti-Spoofing action is set to Detect*** > ***ok.***
4. Menambahkan fitur *Intrusion Prevention System (IPS), Anti-Bot, Antivirus,* dan *Anti-Spam & Email Security* untuk mencegah serangan *Wannacry ransomware* dan *DDOS.* Dengan cara pilih *group* ***Network Objects*** > ***Check Point*** > ***Double Click CP77*** > ***General Properties*** > *Checklist* fitur ***IPS, Anti-Bot, Antivirus,*** dan ***Anti-Spam & Email Security*** > *ok.*

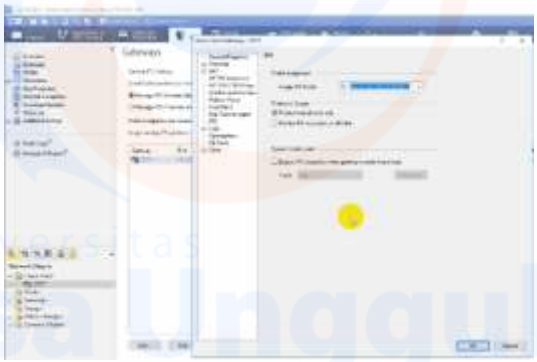


Gambar 17
Checkpoint SmartDashboard R77.30

5. Konfigurasi *Antispam & Mail NGFW Checkpoint.* Konfigurasi yang harus dilakukan pada *NGFW Checkpoint* sebagai berikut:

Gambar 18
Konfigurasi *Anti-Spam & Mail*

6. Langkah selanjutnya adalah konfigurasi *IPS*, konfigurasi yang dilakukan adalah sebagai berikut:
   a. Pilih *group* ***IPS*** > ***Gateways*** > *Double click* ***CP77*** > ***IPS*** > ***Assign IPS Profile: Recommended Protection*** > ***Ok***.



Gambar 19
Konfigurasi *IPS*

Fitur *IPS NGFW Checkpoint* memiliki *database* yang di dalamnya berisikan *signature attack* yang didapat dari *Checkpoint Database Center*.*Database* ini digunakan oleh *NGFW* untuk mendeteksi paket data yang tidak diinginkan atau paket data yang dicurigai sebagai serangan dengan melakukan komparasi antara paket data yang datang dengan *signature attack* yang ada pada *database NGFW*. Oleh karena itu *database* ini harus selalu di-*update* untuk mendapatkan *signature attack terbaru* sehingga dapat menjaga jaringan komunikasi data menjadi lebih aman terhadap ancaman dari *internet.*

7. Menambahkan *Rule* ***Firewall*** di ***Firewall*** > ***Policy*** > ***Add Rule Above Current*** > tambahkan ***Policy*** seperti gambar 20 > ***Install Policy*** > ***Ok.***

Gambar 20
Konfigurasi *Firewall Policy*

Fitur ini digunakan untuk menentukan paket data yang diizinkan melewati *NGFW* sesuai dengan *rule* yang telah dikonfigurasi.

Metode Serangan

Metode serangan yang akan dilakukan pada tugas akhir ini meliputi *Distributed Denial of Services* (*DDOS)* dan *wannacry ransomware* dan pada sub-bab ini dijelaskan pula *tool* yang akan digunakan pada tugas akhir ini.

Serangan *DDOS – UDP Flooding*

Untuk melakukan serangan *DDOS*, penulis menggunakan *tool* yaitu *Low Orbit Ion Canon* (*LOIC*) yang dapat mengirimkan paket data secara cepat dengan tujuan membuat *resource processor* ataupun *bandwidth* dari *file server* dan *user* yang menjadi target mengalami *overload*.

Langkah-langkah uji coba *UDP Flooding* yang akan dilakukan untuk menyerang *file server* dan *user*:

1. Jalankan *tool DDOS LOIC* pada *notebook attacker* sebanyak 5 aplikasi,
2. Masukkan *IP Address Target*, setelah itu *lock on* untuk mendapatkan *IP Target*,
3. Masukkan 1000 *thread*,

4. Jalankan *service port* 80 dan *protocol UDP*,
5. Jalankan *tool DDOS LOIC* selama 1 menit dan lakukan observasi pada *resource processor file server* dan *user*,
6. Lihat log report dan tindakan apa yang dilakukan kedua *firewall* saat serangan terjadi.

Bagian yang harus dikonfigurasi pada *tool LOIC UDP Flooding* yang akan dilakukan untuk menyerang *file server* dan *user* seperti pada Gambar 16 dan Gambar 17:

1. *IP: File Server* atau *User*
2. *Method: UDP*
3. *Klik Lock On*
4. *Port:* 80
5. *Thread:* 1000
6. *Klik IMMA Chargin Mah Lazer*

Serangan *Wannacry Ransomware*

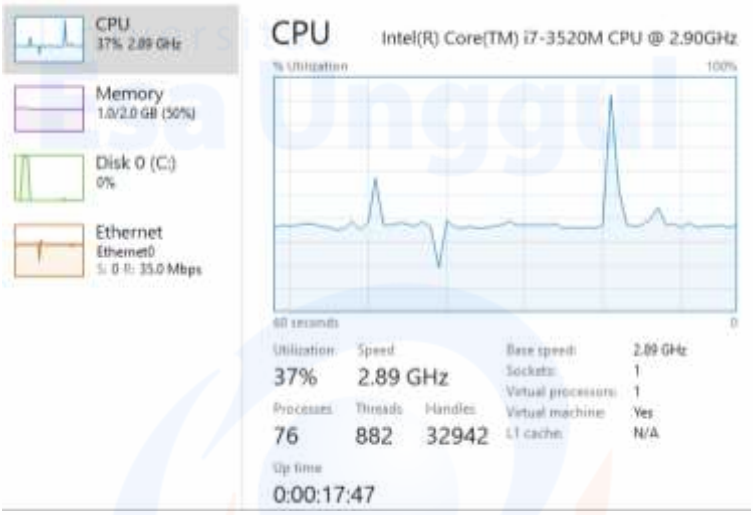
Penulis akan menguji kedua *firewall* yang ada, deskripsi serangan *wannacry ransomware* yang akan dilakukan adalah dengan menjalankan *sample wannacry ransomware* di *file server* dan *user*. Penulis akan melihat *log report* kedua *firewall* yang diuji apakah *wannacry ransomware* yang dijalankan terdeteksi dan apa tindakan yang dilakukan kedua *firewall* yang diuji.

Hasil Uji Coba Serangan

Hasil uji coba serangan pada *file server* dan *user* yang akan dijelaskan pada tugas akhir ini meliputi *DDOS UDP Flooding* dan *wannacry ransomware* dimana jenis serangan ini mempunyai hasil yang berbeda.

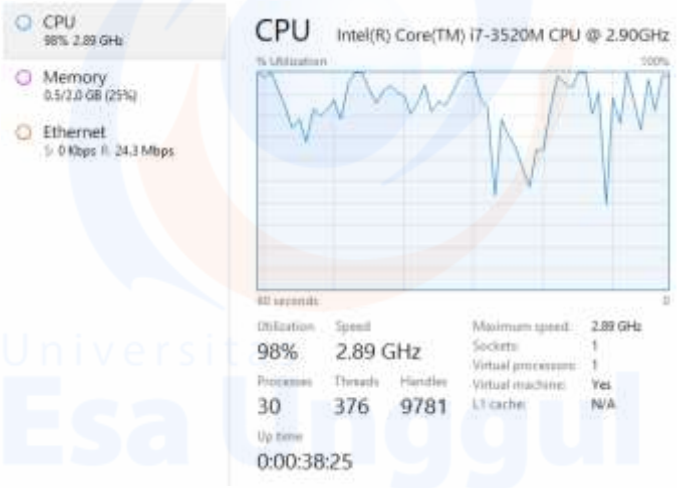
Hasil Uji Coba Serangan *DDOS – UDP Flooding*

Pada uji coba serangan *DDOS – UDP Flooding* pada *Mikrotik RB1100* tidak dapat mendeteksi *behavior* dari serangan *DDOS – UDP Flooding* dikarenakan fitur *statefull firewall* tidak dapat melakukan inspeksi *behavior* suatu paket data. Dapat dilihat pada gambar 21 hasil serangan *DDOS* yang dilakukan pada *file server* dan *user* membuat kinerja *processor* tidak stabil dan membuat sistem kesulitan untuk beroperasional.



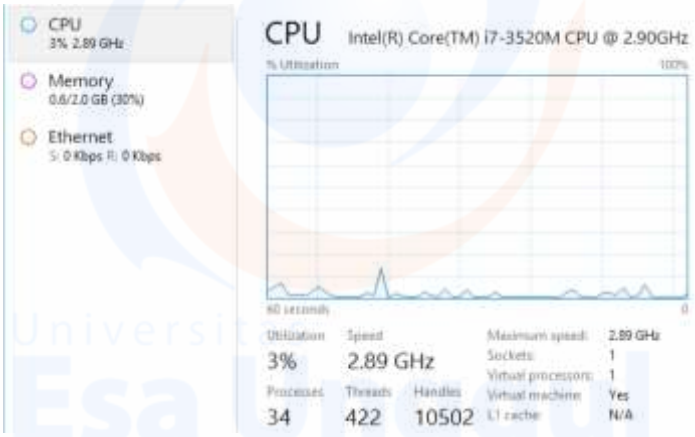
Gambar 21a

Kinerja *Processor User* Saat *DDOS UDP Flooding – Mikrotik RB1100*



Gambar 21b
Kinerja *Processor File Server* Saat *DDOS UDP Flooding – Mikrotik RB1100*

Hasil dari uji coba serangan *DDOS – UDP Flooding* pada *NGFW* mendeteksi paket data yang dikirimkan dan seketika itu juga paket data yang dikirim di-*drop*. Serangan *DDOS - UDP Flooding* tidak memberikan dampak yang berarti pada *file server* dan *user*, karena serangan yang dilakukan di-*drop* oleh *NGFW* terlebih dahulu sebelum mencapai *file server* dan *user*. Dapat dilihat pada Gambar 22 bahwa tidak ada kenaikan kinerja *resource processor* yang signifikan.



Gambar 22a
Kinerja *Processor File Server* Saat *DDOS UDP Flooding – NGFW*

Gambar 22b
Kinerja *Processor User* Saat *DDOS UDP Flooding – NGFW*

Selain itu, pada *NGFW* dapat dilihat pada *log report*, dimana serangan *DDOS* pada *file server* dan *user* di-*drop* oleh *NGFW* karena serangan *DDOS* tidak memenuhi syarat dari konfigurasi *statefull firewall rule* No. 1. Dapat dilihat pada gambar 23 dan gambar 24, detail paket dapat dijabarkan sebagai berikut:

1. Gambar 23:
   a. *Source IP Address*: 10.0.7.2 (*Attacker*)
   b. *Source Port*: 60723
   c. *Destination IP Address*: 10.0.8.6 (*File server*)
   d. *Destination Port*: 80
   e. *Protocol*: UDP (17)
   f. *Action*: Drop with *NGFW*

Gambar 23
Respon *NGFW* Terhadap Serangan *DDOS UDP Flooding File Server*

2. Gambar 24:
   a. *Source IP Address*: 10.0.7.2 (*Attacker*)
   b. *Source Port*: 138
   c. *Destination IP Address*: 10.0.8.30 (*User*)
   d. *Destination Port*: 138
   e. *Protocol*: UDP (17)
   f. *Action*: Drop with *NGFW*

Gambar 24
Respon *NGFW* Terhadap Serangan *DDOS UDP Flooding User*

Hasil Uji Coba Serangan *Wannacry Ransomware*

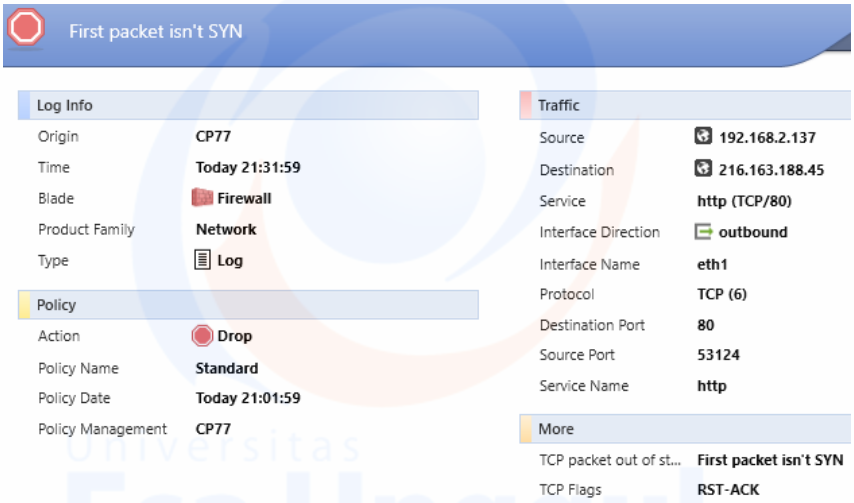
Pada sub-bab ini akan ditunjukkan hasil dari uji serangan *wannacry ransomware* dan respon dari kedua *firewall* yang diuji. Pada uji *firewall Mikrotik RB1100*, dikarenakan *traditional firewall Mikrotik RB100* tidak memiliki fitur *antivirus* seperti pada *NGFW*, *firewall Mikrotik RB100* tidak

dapat mengidentifikasi dan melakukan pengecekan setiap serangan *wannacry ransomware* yang datang. *File* yang berisikan *trojan* dapat dengan mudah masuk dan mengeinfeksi *file server* dan *user*. Setelah *file server* dan *user* terinfeksi, *trojan* melakukan *scanning LAN* dan *WAN* yang terhubung untuk menemukan dan menginfeksi *host* rentan lainnya

Sedangkan hasil pada uji serangan *wannacry ransomware* dengan *NGFW*, *NGFW* melakukan tindakan *drop* terhadap *wannacry ransomware*, karena *NGFW* mendeteksi adanya *pattern* menyerupai *Trojan* dan setelah dicocokkan dengan *database antivirus* yang dimiliki oleh *NGFW, NGFW* menyimpulkan bahwa *file* mengandung *trojan* dan *fle* tersebut di-*drop.*

Detail serangan (Gambar 25) yang terdeteksi pada *NGFW* adalah sebagai berikut:

1. Gambar 25a:
   a. *Source IP Address User* : 10.0.8.6
   b. *Source Port* : 53124
   c. *Destination IP Address* : 216.163.188.45
   d. *Destination Port* : 80
   e. *Protocol* : *TCP*
   f. *Action* : *Drop*
   g. *TCP packet out of state* : *First packet isn't SYN*
   h. *TCP Flags* : *RST-ACK*



Gambar 25a
Respon *NGFW* Terhadap Serangan *Wannacry Ransomware File Server*

2. Gambar 25b:
   a. *Source IP Address User* : 10.0.8.30
   3. *Source Port* : 80
   4. *Destination IP Address* : 64.62.202.101
   5. *Destination Port* : 10264
   6. *Protocol* : *TCP*
   7. *Action* : *Drop*
   8. *TCP packet out of state* : *First packet isn't SYN*
   9. *TCP Flags* : *ACK*

Gambar 25b
Respon *NGFW* Terhadap Serangan *Wannacry Ransomware User*

Rekapitulasi Pengujian Yang Diperoleh

Dari serangkaian uji coba serangan yang dilakukan pada tugas akhir ini, dapat disimpulkan respon dari kedua *firewall* yang diujikan pada tabel 3:

Tabel 3
Rekapitulasi Hasi Pengujian

No	Zona	IP	Jenis Serangan	*Duration*	*CPU Usage*		*Respon Wannacry Ransomware*	
					Mikrotik RB1100	*NGFW*	*Mikrotik RB1100*	*NGFW*
1	File Server	10.0.8.6	*DDOS - UDP Flooding*	2 minutes	98%	3%		
			Wannacry ransomware				Accept	Drop
2	Users	10.0.8.30	*DDOS - UDP Flooding*	2 minutes	37%	5%		
			Wannacry ransomware				Accept	Drop
		10.0.8.31	*DDOS - UDP Flooding*	2 minutes	74%	4%		
			Wannacry ransomware				Accept	Drop
		10.0.8.32	*DDOS - UDP Flooding*	2 minutes	46%	2%		
			Wannacry ransomware				Accept	Drop
		10.0.8.33	*DDOS - UDP Flooding*	2 minutes	35%	2%		
			Wannacry ransomware				Accept	Drop
		10.0.8.34	*DDOS - UDP Flooding*	2 minutes	35%	2%		
			Wannacry ransomware				Accept	Drop
		10.0.8.35	*DDOS - UDP Flooding*	2 minutes	46%	6%		
			Wannacry ransomware				Accept	Drop

Berdasarkan tabel 3 pada hasil pengujian serangan *DDOS – UDP Flooding* pada *Mikrotik RB1100* tidak dapat mendeteksi *behavior* dari serangan *DDOS – UDP Flooding* dikarenakan fitur *statefull firewall* pada *Mikrotik RB1100* tidak dapat melakukan inspeksi *behavior* suatu paket data. Dapat dilihat pada tabel 3 hasil serangan *DDOS* yang dilakukan pada *file server* dan *user* membuat kinerja *processor* mencapai persentase dari 35% - 98% yang dapat membuat sistem kesulitan untuk beroperasional. Pada tabel 3 ditunjukkan hasil pengujian serangan *wannacry ransomware* dan respon pada *Mikrotik RB1100, firewall Mikrotik RB100* tidak dapat mengidentifikasi dan melakukan pengecekan setiap serangan *wannacry ransomware* yang dating dan dapat dengan mudah masuk dan mengeinfeksi *file server* dan *user*. Setelah *file server* dan *user* terinfeksi, *trojan* melakukan *scanning LAN* dan *WAN* yang terhubung untuk menemukan dan menginfeksi *host* rentan lainnya.

Hasil pengujian pada tabel 3 *DDOS – UDP Flooding* pada *NGFW* mendeteksi paket data yang dikirimkan dan seketika itu juga paket data yang dikirim di-*drop*. Serangan *DDOS - UDP Flooding* tidak memberikan dampak yang berarti pada *file server* dan *user*, karena serangan yang dilakukan di-*drop* oleh *NGFW* terlebih dahulu sebelum mencapai *file server* dan *user*. Dapat dilihat pada tabel 3 bahwa tidak ada kenaikan kinerja *resource processor* yang signifikan, range resource processor antara 2% - 6%. Sedangkan hasil pada uji serangan *wannacry ransomware* pada *NGFW*, *NGFW* melakukan tindakan *drop* terhadap *wannacry ransomware*, karena *NGFW* mendeteksi

adanya *pattern* menyerupai *trojan* pada *file* dan setelah dicocokkan dengan *database antivirus* yang dimiliki oleh *NGFW, NGFW* menyimpulkan bahwa *file* mengandung *trojan* dan *fle* tersebut di-*drop.*

Rekapitulasi *Benefit* yang Diperoleh

Berdasarkan rekapitulasi hasil pengujian pada tabel 3 *Benefit* yang diperoleh dari biaya yang perlu dikeluarkan sebesar $29.389 mempunyai manfaat yang sangat besar dibandingkan kerugian yang diperoleh oleh perusahaan sebesar $5.632.500.

Manfaat yang diperoleh oleh perusahaan sebagai berikut:

1. Dapat mencegah dan mendeteksi serangan dari *DDOS* dan *wannacry ransomware*.
2. Mencegah kerusakan sistem dan kehilangan data pada beberapa department yang akan mengakibatkan sejumlah layanan publik terganggu seperti laporan keuangan perusahaan ke pihak ekternal (bank, konsultan, mitra kerjasama, dsb).

Simpulan

Setelah melakukan penelitian dapat disimpulkan bahwa:

1. Analisis dan perancangan sistem keamanan jaringan dengan menggunakan *waterfall,* dapat menetapkan fitur yang akan digunakan sehingga dapat menghindari *misconfiguration* dan dapat digunakan dengan optimal dalam menghadapi serangan/ancaman dari pihak internal dan eksternal.
2. Pada uji coba serangan *DDOS* dan *wannacry ransomware* yang diujikan pada *file server* dan *user* terhadap kedua *firewall*:
   a. Serangan *DDOS* dan *wannacry ransomware* pada *traditional firewall* dapat dengan mudah dilewati dikarenakan ketidakmampuan fitur *statefull firewall* yang ada dalam mendeteksi *behavior* suatu paket data dan *trojan* pada *file* yang dibuktikan dalam tabel 3.
   b. Serangan *DDOS* dan *wannacry ransomware* pada *Next Generation Firewall* (*NGFW*) dapat mendeteksi *new signature* dan *behavior attack* pada setiap paket data yang melewati *NGFW* sehingga *NGFW* dapat melakukan *drop* sebelum paket data dan *trojan* masuk ke dalam jaringan komunikasi data PT. RLU yang dibuktikan dalam tabel 3.
3. *Prototype NGFW* telah berhasil dibangun sehingga bisa dijadikan alternatif solusi dari sistem keamanan jaringan di PT. RLU sehingga meningkatkan keamanan dalam lalu lintas data di jaringan PT. RLU.

Daftar Pustaka

M. Labs, “Top 8 Network Attacks by Type in 2017,” Calyptix Security. pp. 3–5, 2017. jenis virus baru yang bisa memeras A. Ransomware, “BBC.pdf.” 15 Desember 2015, 2015.

A. . Fallis, “Bab Ii Landasan Teori,” J. Chem. Inf. Model., vol. 53, no. 9, pp. 1689–1699, 2016.

NEWS-News Analysis, “Hacking Critical Infrastructure How-To Guide.” 2015.

Check Point Software Technologies Ltd, “Fact vs hype top 10 considerations for choosing a strategic cybersecurity partner table of contents,” 2016.

G. W. Sasmito, “Penerapan Metode Waterfall Pada Desain Sistem Informasi Geografis Industri Kabupaten Tegal,” J. Inform. Pengemb. IT, vol. 2, no. 1, pp. 6–12, 2017.

R. A. N. Laily, “Bab II Landasan Teori Bisnis,” J. bisnis, vol. 67, no. 6, pp. 14–21, 2016.

PT. Royal Lestari Utama, “Sistem Integration Feasiblity Study,” 2018.

PT Royal Lestari Utama, “Check Point Appliance Sizing Recommendation,” 2015.