FIREWALL FILTERING BERBASIS *DEEP PACKET INSPECTION* DALAM MENDETEKSI DAN MENCEGAH ANCAMAN *MALWARE*

Mochammad Syafi'i Bachtiar [1], Nining Rahaningsih [2], Raditya Danar Dana [3]
[1] Teknik Informatika, [2] Komputerisasi Akuntansi, [3] Manajemen Informatika
STMIK IKMI CIREBON
Jalan Perjuangan No.10B, Karyamulya Cirebon, Indonesia
syafiibachtiar124@gmail.com

ABSTRAK

Ancaman *Malware* sudah menjadi masalah serius bagi keamanan sistem komputer bagi suatu organisasi, karena dapat menyebabkan kerugian finansial dan gangguan operasional. Deep Packet Inspection adalah teknologi yang memungkinkan firewall untuk memeriksa konten aktual dari paket data yang akan melewatinya, bukan hanya header paketnya. Teknologi DPI pertama kali diperkenalkan pada tahun 1990-an untuk memfilter konten web. Saat ini, DPI digunakan secara luas oleh firewall tingkat enterprise, Intrusion Prevention System, dan perangkat keamanan jaringan lainnya untuk mendeteksi ancaman yang mungkin tidak terlihat oleh firewall tradisional. Sebagai kontribusi untuk membantu organisasi ataupun individu dari ancaman siber. Penelitian yang digunakan mengusung pendekatan eksperimental yang secara sistematis menguji kinerja *Firewall* berbasis DPI untuk mendeteksi dan mencegah serangan *Malware*. Variabel yang mungkin mempengaruhi hasil digunakan untuk mendapatkan kesimpulan sebab akibat yang kuat. Hasil pengujian menunjukkan bahwa menambahkan sistem DPI ke *Firewall Fortigate* meningkatkan deteksi situs web berbahaya dan membatasi akses sebesar 25%. Namun agar DPI dapat bekerja secara maksimal, ada beberapa faktor yang harus diperhatikan seperti kemungkinan terjadinya gangguan jaringan ataupun trouble pada alat yang digunakan dan perlunya regulasi untuk penerapan DPI di Indonesia. Oleh karena itu, penerapan DPI harus tetap mempertimbangkan standar etika dan kepatuhan terhadap peraturan perundang-undangan yang berlaku.

Kata kunci : *Fortigate, Firewall, Deep Packet Inspection, Malware*

1. PENDAHULUAN

Pada era digitalisasi yang telah berkembang dengan pesat keamanan sebuah jaringan komputer merupakan hal yang patut dipertimbangkan untuk melindungi jaringan komputer dari ancaman *Malware*. *Malware* merupakan jenis perangkat berbahaya yang dirancang untuk menyusup kedalam sistem jaringan komputer yang sudah ditargetkan untuk tujuan kejahatan. Ancaman *Malware* merupakan ancaman yang cukup serius bagi keamanan dan integritas sistem komputer. Terutama bagi pengguna komputer didalam sebuah organisasi. Ancaman ini dapat menyebabkan kerugian finansial, kehilangan data, serta gangguan operasional.

Firewall filtering menjadi metode yang umum digunakan untuk melindungi jaringan komputer dari ancaman *Malware*. *Malware* menggunakan cara yang cerdik untuk menyusup kedalam sebuah sistem, seperti menyembunyikan diri didalam file yang baru saja didownload atau menggunakan *enkripsi* yang rumit. Oleh karena itu, ancaman *Malware* begitu sulit untuk dideteksi menggunakan *Firewall* tradisional, tetapi dengan adanya metode *Firewall Filtering* berbasis *Deep Packet Inspection* (DPI) dimana paket data yang melewati *Firewall* dianalisis secara mendalam untuk mengidentifikasi dan mencegah ancaman *Malware*. Metode ini memungkinkan *Firewall* untuk memahai konteks isi dari paket data yang melewat jaringan dan akan diperiksa secara detail yang dikirim melalui jaringan komputer untuk bisa mengambil tindakan seperti memberikan, memblokir, atau merutekan ulang.[1]

Dengan memahami kinerja *Firewall Filtering* berbasis *Deep Packet Inspection* (DPI), maka dapat mengidentifikasi kelebihan dan kekurangan metode ini, Informasi ini dapat digunakan untuk meningkatkan efektifitas dan efisiensi *Firewall Filtering* berbasis DPI dalam melindungi jaringan dari ancaman *Malware*. Sehingga pada penelitian ini dapat memberikan pemahaman yang lebih baik tentang berapa persentase peningkatan tingkat deteksi ancaman *Malware* sebelum dan sesudah penerapan DPI, serta berapa banyak faktor yang mempengharui penerapan DPI dalam mencegah serangan *Malware*.

Dalam penelitian ini akan menggunakan metode dan pendekatana yang relevan dengan analisis *Firewall Fitering* berbasis *Deep Packet Inspection* (DPI) dalam mendeteksi ancaman *Malware*. Penelitian ini akan memulai dengan melihat paket data dalam lalu lintas jaringan yang akan diambil dari lingkungan jaringan yang representatif untuk menghadapi ancaman *Malware* modern. Selain itu penelitian ini akan mempertimbangkan aspek-aspek keamanan dan privasi dalam penggunaan DPI, serta merancang sebuah solusi agar dapat meminimalkan dampak terhadap privasi pengguna.

Penelitian analisis kinerja *Firewall Filtering* berbasis *Deep Packet Inspection* (DPI) dalam mendeteksi dan mencegah ancaman *Malware* menjadi penting untuk memperkuat keamanan jaringan komputer. Penelitian ini diharapkan dapat

memberikan kontribusi dalam pengembangan solusi keamanan yang lebih efektif dan dapat diandalkan untuk melindungi jaringan dari serangan *Malware.*

2. TINJAUAN PUSTAKA

2.1. Penelitian Terdahulu

Ban Mohammed Khammas, dkk. Penelitian yang berjudul "Pre-filters in-transit *Malware* packets detection in the network". Tujuan dari penelitian ini adalah untuk mengembangkan teknik deteksi *Malware* pada jaringan sebagai garis pertahanan pertama untuk melindungi sistem yang terhubung ke jaringan dari penyebaran *Malware*. Penelitian ini juga bertujuan untuk mempercepat proses deteksi *Malware* pada level jaringan dan meningkatkan akurasi deteksi dengan menggunakan teknik *Machine Learning*. Hasil dari penelitian ini menunjukkan bahwa teknik yang diusulkan dapat mendeteksi lebih dari 97% paket *Malware* dan meningkatkan kecepatan transmisi lebih dari 98% paket normal tanpa mengirimkannya ke jalur lambat. Selain itu, teknik yang diusulkan juga dapat mendeteksi lebih dari 75% paket *Malware Metamorfik* pada dataset uji.[2]

Penelitian selanjutnya oleh Sari Dewi dan Adam Iqbal Islami dengan judul "Implementasi Web Filtering Menggunakan Router Fortigate FG300D". Tujuan dari penelitian ini adalah untuk mengimplementasikan web filtering menggunakan router Fortigate FG300D pada PT. Karlin Mastrindo dengan tujuan untuk membatasi akses pengguna dalam mengakses website yang tidak relevan dengan pekerjaan mereka, sehingga dapat meningkatkan efektivitas kinerja perusahaan dan menjaga keamanan jaringan secara keseluruhan. Penelitian ini juga bertujuan untuk memberikan solusi terhadap ketidakdisiplinan karyawan dalam bekerja dan kurangnya akses internet yang belum sepenuhnya berjalan dengan baik di PT. Karlin Mastrindo.[3]

Penelitian selanjutnya oleh Canny Siska Georgina, dkk. Dengan judul "Deception Based Techniques Against Ransomwares: A Systematic Review". Tujuan dari Tujuan dari penelitian yang dilakukan adalah untuk memberikan tinjauan komprehensif dan metodologis mengenai penelitian terbaru yang dilakukan pada pencegahan, deteksi, dan mitigasi *Ransomware* menggunakan *Deception-Based Techniques* yang dipublikasikan antara tahun 2016-2022. Penelitian ini juga bertujuan untuk memberikan referensi yang berguna bagi para peneliti dan praktisi dalam mengembangkan, menggunakan, dan mengukur *Deception-Based Techniques* pada ransomware.[4]

Penelitian selanjutnya oleh Danaswara Prawira Harja, dkk. Dengan judul "Implementasi Metode Deep Packet Inspection untuk Meningkatkan Keamanan Jaringan pada Software Defined Networks". Tujuan dari penelitian ini adalah untuk meningkatkan keamanan jaringan pada *Software Defined Networks* (SDN) dengan mengimplementasikan metode *Deep Packet Inspection* (DPI). Penelitian ini bertujuan untuk mengatasi kelemahan *Intrusion Prevention System* (IPS) dalam hal waktu proses pemblokiran dengan menitikberatkan pada *pattern matching* yang terjadi akibat adanya *false positive*. Dalam penelitian ini, DPI diaktifkan dengan *tools ntopng* yang diletakkan di *control plane* pada arsitektur jaringan SDN. Proses yang dilakukan DPI terdiri dari empat tahapan, yaitu *getting original packet*, untuk mendapatkan paket yang sebelumnya ada di *Floodlight* untuk di analisa. Diharapkan dengan implementasi metode DPI pada SDN dapat meningkatkan keamanan jaringan dengan melakukan *monitoring, analyzing* dan *controlling traffic* dari *layer 2* atau data link hingga *layer 7* atau *application*.[5]

Penelitian selanjutnya oleh Saputra Dio Azmi, dkk. Dengan judul "Implementasi Sistem Deteksi Ransomware Menggunakan Deep Packet Inspection pada Layanan SMK Negeri 1 Palembang". Tujuan dari penelitian ini adalah untuk mengimplementasikan sistem deteksi *Ransomware* menggunakan *Deep Packet Inspection* (DPI) pada layanan SMK Negeri 1 Palembang. Penelitian ini bertujuan untuk mendeteksi serangan *Ransomware* pada jaringan dengan mengidentifikasi pola paket serangan dan mengklasifikasikannya dengan paket normal. Selain itu, penelitian ini juga bertujuan untuk memvisualisasikan data paket dalam bentuk *diagram* untuk memudahkan analisis dan pemahaman. Diharapkan hasil dari penelitian ini dapat membantu meningkatkan keamanan jaringan dan mencegah serangan *Ransomware* pada layanan SMK Negeri 1 Palembang.[6]

Penelitian selanjutnya oleh Ahmad Riduan dan Nanang Sadikin dengan judul "Perancangan Firewall Menggunakan Fortigate di PT. Swadharma Duta Data". Tujuan dari penelitian ini adalah merancang *Firewall* menggunakan *FortiGate* sebagai pengamanan sistem informasi untuk sejumlah data-data penting perusahaan. Metode penelitian yang digunakan antara lain adalah studi kepustakaan, observasi, dan wawancara serta metode pengembangan jaringan menggunakan *Network Development Life Cycle* (NDLC). Dengan adanya *Firewall* ini diharapkan sistem jaringan komputer internal PT. Swadharma Duta Data lebih aman dalam mengantisipasi terkena *Malware* dan tim *Security Operational Center* (SOC) dapat dengan lebih mudah dan cepat mendeteksi ancaman keamanan siber pada jaringan komputer internal.[7]

2.2. Fortigate

FortiGate adalah *Next Generation Firewall* (NGFW) yang menyediakan keamanan jaringan cerdas dan *real-time* terhadap *Malware* dan ancaman baru. *FortiGate* adalah komponen dari *Fortinet Security Fabric* yang bekerja sama dengan solusi keamanan mitra *Fabric-Ready* lainnya untuk meningkatkan visibilitas dan kontrol jaringan serta mengurangi kompleksitas infrastruktur jaringan. Dibandingkan dengan *Firewall* lainnya, *FortiGate* memiliki sistem kecerdasan ancaman yang lebih baik

dan memiliki fitur keamanan yang lebih banyak dan lebih canggih. Selain itu, antarmuka manajemen *FortiGate* juga lebih mudah untuk digunakan dan lebih mudah untuk dipahami.[8]

2.3. Firewall

Firewall adalah komponen keamanan jaringan yang memiliki fungsi sebagai dinding keamanan antara jaringan internal suatu organisasi dan jaringan internet. Sistem *Firewall* bertujuan untuk memfilter paket data yang masuk dan keluar dari jaringan untuk mencegah serangan dan akses ilegal dari sumber luar. *Firewall* memiliki cara kerja dengan memblokir atau menolak paket jaringan menggunakan aturan keamanan yang dibuat oleh *Network Administrator*. Dengan demikian, *Firewall* memastikan bahwa semua akses ke sumber daya di dalam jaringan internal hanya dimiliki oleh pihak yang berwenang dan tidak memungkinkan pihak lain untuk mengaksesnya.

2.4. Deep Packet Inspection

Deep Packet Inspection (DPI) adalah teknologi yang memungkinkan operator jaringan mengidentifikasi serta menganalisis secara akurat terhadap *traffic* internet yang ada didalam jaringan yang sudah dibentuk secara *real-time*. Perangkat DPI memiliki kemampuan untuk melihat semua lalu lintas yang berasal dari alamat *IP* tertentu, dan mengambil lalu lintas *HTTP*. Alat DPI dirancang untuk menentukan program pembuatan paket waktu nyata untuk ratusan ribu transaksi per detik. [9]

2.5. *Malware*

Malicious software atau perangkat lunak berbahaya atau bisa disebut dengan *Malware*. *Malware* adalah jenis program komputer yang dibentuk untuk menyusup ke sistem komputer tanpa pengguna komputer sadari lalu merusaknya. *Malware* dapat menyebar melalui iklan pada website, mendownload file sembarang pada website yang tidak terpercaya, melalui *flashdisk*, dan media lainnya. *Malware* dirancang untuk melakukan tindakan yang merugikan pengguna, seperti mencuri data pribadi, merusak sistem, atau mengambil kendali atas komputer. *Virus, Worm, Trojan, Spyware,* dan *Ransomware* adalah beberapa jenis *Malware* yang sering ditemui.[10]

2.6. GNS3

GNS3 alah program simulator jaringan yang memiliki kemampuan untuk mensimulasikan jaringan kompleks. *GNS3* dapat berjalan di berbagai sistem operasi, termasuk *Windows, Linux,* dan *Mac OS X*. Prinsip kerja *GNS3* adalah mengemulasi *Cisco IOU* pada komputer, sehingga PC dapat bertindak sebagai router atau bahkan switch dengan mengaktifkan fungsi Kartu *Switch Ethernet*. *GNS3* memiliki beberapa kelebihan, termasuk akses penuh ke *Cisco IOU* dan desain topologi yang lebih *real*, yang bisa menjalankan *router high end (seri 3600, macintosh, dll.)* serta dapat berinteraksi dengan sistem lain. Namun, kekurangan *GNS3* adalah instalasinya yang cukup sulit dan membutuhkan banyak sumber daya komputer.[11]

3. METODE PENELITIAN

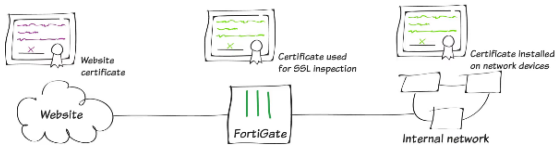
Pada penelitian ini mengusung pendekatan ekperimental dengan tujuan menguji secara sistematis kinerja *Firewall Filtering* berbasis *Deep Packet Inspection* (DPI) dalam mendeteksi dan mencegah ancaman *Malware*. Pendekatan ekperimental memberikan kontrol yang cermat terhadap variabel-variabel yang mungkin mempengaruhi hasil, memungkinkan penarikan kesimpulan *kausal* yang kuat. Dalam konteks ini, penelitian juga mengintegrasikan kombinasi metode kuantitatif untuk memperoleh pemahaman yang lebih mendalam dan terukur. Dengan pola metode sebagai berikut:

Gambar 1. Alur Metode Penelitian

4. HASIL DAN PEMBAHASAN

4.1. Pembahasan

Malware merupakan ancaman utama bagi keamanan komputer untuk saat ini. Sehingga deteksi dan pencegahan *Malware* memiliki fungsi yang sangat penting bagi keamanan untuk melindungi perangkat dan jaringan dari serangan luar. *Fortigate firewall* adalah *tools* yang digunakan dalam penelitian ini, fortigate berfungsi untuk mendeteksi serta mencegah *Malware* atau anomali yang tidak dikenali dalam lalu lintas paket.



Gambar 2. *Fortigate Firewall*
(Sumber : *www.fortinet.com*)

Fortigate Firewall menyediakan fitur pencegahan *intrusi* dan perlindungan *Malware* yang dapat menganalisis lalu lintas jaringan secara mendalam. Temuan pada penelitian ini adalah *anomali* yang tidak diketahui, *virus* yang terdeteksi, dan web yang diblokir karena berbahaya.


Bagas31, Kuyhaa dan Deretan Situs Download Software Ilegal

Berdasarkan laporan BSA Global Software Survey 2018, tingkat pemakaian perangkat lunak bajakan di Indonesia mencapai 83%. Angka tersebut merupakan yang tertinggi dibandingkan dengan rata-rata di Asia Pasifik sebesar 57%.

Berikut situs software bajakan gratis di Indonesia yang perlu kamu hindari:

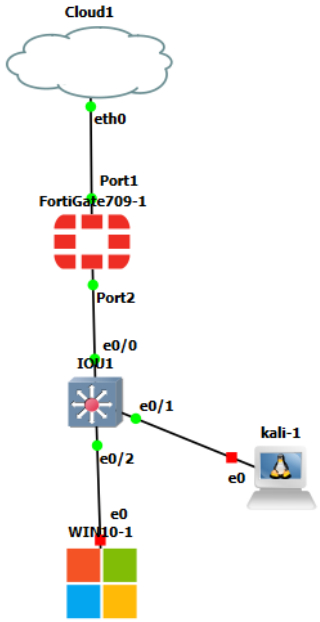
- Bagas31.info
- Kuyhaa-me.com
- Gigapurbalingga.net
- Yashir252.com
- ipeenk.com
- Ad4msan.com
- Siberuang.com
- Alex71.com
- Kuyhaabagas31.blogspot.com
- Hienzo.com
- Ibrasoftware.com

Gambar 3. Situs Software Ilegal
(Sumber : *www.cnbcindonesia.com*)

Pada Gambar 3. adalah list website yang terindikasi adanya *Malware* atau berbahaya menurut cnbcindonesia dengan referensi artikel dibawah ini *https://www.cnbcindonesia.com/tech/20200710105017-37-171675/bagas31-kuyhaa-dan-deretan-situs-download-software-ilegal*. Referensi lainnya bisa dilihat melalui link berikut *https://www.cloudcomputing.id/berita/bssn-ungkap-software-bajakan-akibat-serangan-Malware*. Dengan referensi diatas pada penelitian ini akan dilakukan uji coba untuk mengakses beberapa list website yang sudah disediakan untuk mendapatkan hasil perbandingan sebelum dan sesudah penerapan DPI. Beberapa list website yang akan digunakan adalah sebagai berikut:

a. wicar.org
b. eicar.eu
c. sophostest.com
d. mikrotik.com
e. gigapurbalingga.net
f. kuyhaa-me.com
g. reddit.com
h. fortinet.co
i. ikmi.ac.id
j. alex71.com

Pada penelitian ini menggunakan software simulasi *GNS3* untuk melakukan uji coba dengan gambar topologi yang digunakan seperti dibawah ini:

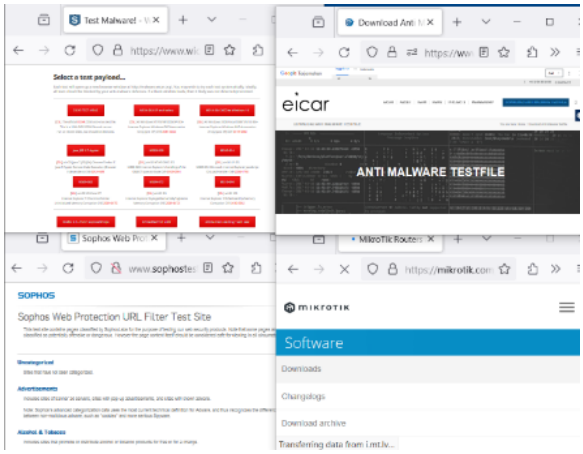


Gambar 4. Topologi Jaringan

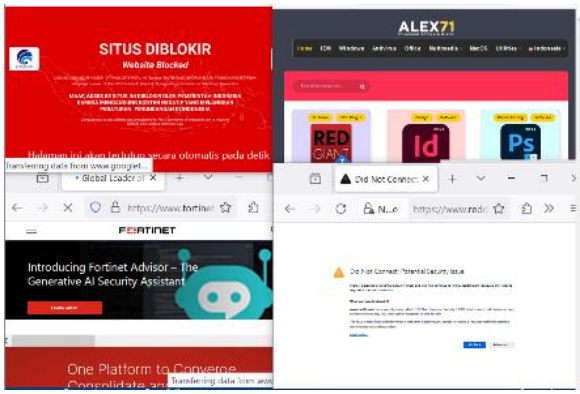
Penjelasan gambar 4. Sebagai berikut:

1) *Cloud* ⟶ Sumber Internet
2) *Fortigate* ⟶ Router Firewall
3) *Cisco IOU L2* ⟶ Switch
4) *OS Kali Linux* ⟶ Client/User 1
5) *OS Windows 10* ⟶ Client/User 2

4.2. Sebelum Penerapan *Deep Packet Inspection*



Gambar 5. Sebelum DPI *test* 1

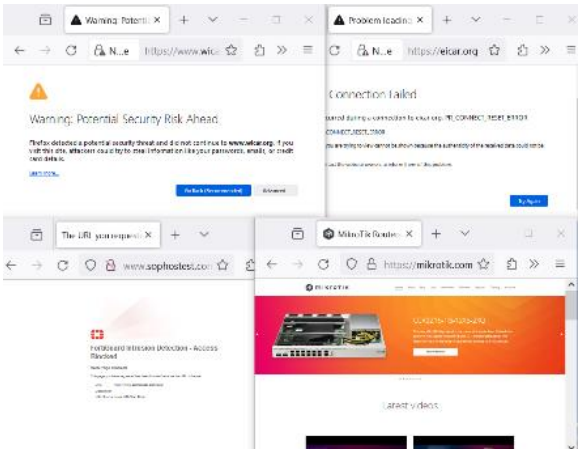


Gambar 6. Sebelum DPI *test* 2

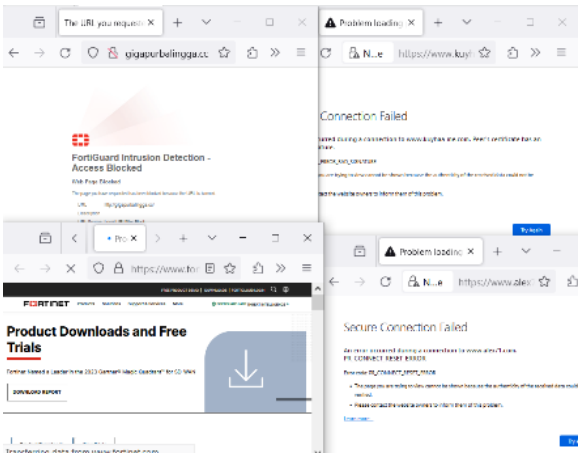
Gambar 7. Sebelum DPI *test* 3

Pada Gambar 5. Gambar 6. Dan Gambar 7. Adalah hasil *test* sebelum diterapkannya DPI dari 10 list website yang akan di uji coba hanya 2 website yang tidak bisa diakses yaitu *gigapurbalingga.net* dan *reddit.com*

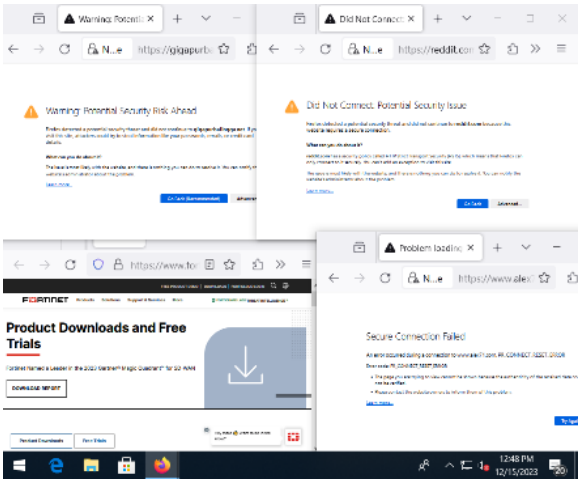
4.3. Sesudah Penerapan Deep Packet Inspection



Gambar 8. Sesudah DPI *test* 1



Gambar 9. Sesudah DPI *test* 2



Gambar 10. Sesudah DPI *test* 3

Pada Gambar 8. Gambar 9. dan Gambar 10. adalah hasil *test* sesudah diterapkannya DPI dari 10 list website yang akan di uji coba ada 7 website yang tidak bisa diakses sedangkan 3 website sisanya bisa diakses seperti *mikrotik.com, fortinet.com,* dan *ikmi.ac.id.*

4.4. Hasil sebelum dan sesudah penerapan DPI Uji coba dilakukan pada 10 website dengan isi konten yang berbeda dari setiap website yang akan di uji coba.

1) Hasil sebelum DPI diterapkan:

Tabel 1. akses web sebelum DPI diterapkan

website	bisa atau tidak	Value
https://www.eicar.eu/	bisa	1
https://www.wicar.org/	bisa	1
https://sophostest.com/	bisa	1
https://mikrotik.com/	bisa	1
https://gigapurbalingga.net/	tidak	0
https://www.kuyhaa-me.com/	bisa	1
https://www.alex71.com/	bisa	1
https://www.fortinet.com/	bisa	1
https://www.reddit.com/	tidak	0
https://ikmi.ac.id/	bisa	1

Dari tabel 1 maka dapat disimpulakan sebelum diterapkan DPI dari 10 website yang diuji coba 8 website bisa diakses dan 2 website tidak bisa diakses.

2) Hasil sesudah DPI diterapkan:

Tabel 2. akses web sesudah DPI diterapkan

website	bisa atau tidak	Value
https://www.eicar.eu/	tidak	0
https://www.wicar.org/	tidak	0
https://sophostest.com/	tidak	0
https://mikrotik.com/	bisa	1
https://gigapurbalingga.net/	tidak	0
https://www.kuyhaa-me.com/	tidak	0
https://www.alex71.com/	tidak	0
https://www.fortinet.com/	bisa	1
https://www.reddit.com/	tidak	0
https://ikmi.ac.id/	bisa	1

Dari tabel 2 maka dapat disimpulakan setelah diterapkannya DPI dari 10 website yang diuji 3 website bisa diakses dan 7 website tidak bisa diakses. Berdasarkan hasil data dari tabel diatas maka didapatkan sebuah pola, sebelum penerapan DPI website yang tidak bisa diakses berjumlah 2, sedangkan setelah penerapan DPI website yang tidak bisa diakses bertambah menjadi 5 website sehingga memiliki total 7 website yang tidak bisa diakses pada saat DPI diterapkan. Berikut adalah laporan perhitungan persentase sebelum DPI dan sesudah DPI diterapkan:

1) Variabel:
   - Website yang tidak bisa diakses sebelum penerapan DPI $= x_1$
   - Website yang tidak bisa diakses sesudah penerapan DPI $= x_2$
   - Total uji website $= y$

2) Persentase website yang tidak bisa diakses sebelum penerapan DPI:
   - Website yang tidak bisa diakses $= 2$
   - Total uji website $= 10$
   - Persentase $= \left(\frac{x_1}{y}\right) x100\%$
     $= \left(\frac{2}{10}\right) x100\%$
     $= 20\%$

3) Persentase website yang tidak bisa diakses sesudah penerapan DPI:
   - Website yang tidak bisa diakses $= 7$
   - Total uji website $= 10$
   - Persentase $= \left(\frac{x_1}{y}\right) x100\%$
     $= \left(\frac{7}{10}\right) x100\%$
     $= 70\%$

4) Persentase peningkatan website tidak bisa diakses:
   $x_1 = 2\ website\ (20\%)$
   $x_2 = 7\ website\ (70\%)$

5) Persentase peningkatan:
   $= x_2 - x_1$
   $= 70\% - 20\%$
   $= 50\%$

Dari hasil diatas maka dapat diambil kesimpulan secara garis besar bahwa penerapan DPI pada sistem jaringan menyebabkan peningkatan yang *signifikan*, *persentase* website yang tidak bisa diakses padda awalnya hanya 20% setelah DPI diterapkan pada sistem menjadi 70% hal ini meningkat 50% dan nilai ini lebih besar dari sebelumnya yang hanya 20% serta menunjukan penerapan DPI dapat membatasi akses ke website yang diindikasikan berbahaya.

Dengan menggunakan sistem *Deep Packet Inspection* (DPI) terdapat beberapa faktor yang mempengaruhi kinerja dari *Router Fortigate*. Disisi lain, ada faktor lain yang berpengaruh pada penerapan DPI ini, diantaranya sebagai berikut:

a. Memperlambat jaringan internet atau bahkan bisa mengganggu jaringan.
b. *Versi Firmware* yang digunakan harus versi terbaru, *CPU* dan *Memory* yang digunakan harus memiliki *space* yang cukup besar agar bisa optimal dan tidak memberatkan beban pada sisi *router*.
c. Belum ada regulasi yang membahas secara *spesifik* tentang penerapan *Firewall Filtering* berbasis *Deep Packet Inspection.*

5. KESIMPULAN DAN SARAN

Hasil penelitian menunjukkan bahwa firewall filtering Fortigate yang menggunakan teknologi Deep Packet Inspection (DPI) dapat meningkatkan kemampuan mendeteksi dan mencegah *Malware*, seperti yang ditunjukkan oleh analisis data sebelum dan sesudah penerapan DPI. Namun, penerapan DPI membutuhkan biaya infrastruktur yang cukup besar dan berpotensi melanggar privasi pengguna internet karena kemampuannya yang bisa memantau aktifitas trafik data secara detail. Oleh karena itu, sistem Deep packet Inspection (DPI) perlu dipertimbangkan untuk penerapannya serta membutuhkan pembaruan secara berkelanjutan untuk mengikuti standar keamanan siber terbaru. Untuk menerapkan DPI juga harus mempertimbangkan etika dan kepatuhan terhadap hukum yang berlaku di masyarakat.

DAFTAR PUSTAKA

[1] 2017 Rodrigues, et al., "Cybersecurity and Network Forensics Analysis of Malicious Traffic towards a Honeynet with Deep Packet Inspection.pdf," *Cybersecurity Netw. forensics AnalyRodrigues, G. A. P., Oliveira Albuquerque, R., Deus, F. E. G., Sousa, R. T., Oliveira Júnior, G. A., Villalba, L. J. G., Kim, T. H. (n.d.). Cybersecurity Netw. Forensics Anal. Malicious T*, 2017.

[2] B. M. Khammas, I. Ismail, and M. N. Marsono, "Pre-filters in-transit *Malware* packets detection in the network," *Telkomnika (Telecommunication Comput. Electron. Control.*, vol. 17, no. 4, pp. 1706–1714, 2019, doi: 10.12928/TELKOMNIKA.V17I4.12065.

[3] S. Dewi and A. I. Islami, "Implementasi Web Filtering Menggunakan Router Fortigate FG300D," *INSANtek*, vol. 2, no. 1, pp. 22–27, 2021, doi: 10.31294/instk.v2i1.424.

[4] C. S. Georgina, F. Sakinah, M. R. Fadholi, S. Yazid, and W. Syafitri, "Deception Based Techniques Against Ransomwares: a Systematic Review," *J. Tek. Inform.*, vol. 4, no. 3, pp. 529–553, 2023, doi: 10.52436/1.jutif.2023.4.3.886.

[5] D. P. Harja, A. Rakhmatsyah, and M. A. Nugroho, "Implementasi untuk Meningkatkan Keamanan Jaringan Menggunakan Deep Packet Inspection pada Software Defined Networks," *Indones. J. Comput.*, vol. 4, no. 1, p. 133, 2019, doi: 10.21108/indojc.2019.4.1.286.

[6] S. D. Azmi, S. Deris, and S. Tata, "Implementasi Sistem Deteksi Ransomware Menggunakan Deep Packet Inspection pada Layanan SMK Negeri 1 Palembang," *Indones. J. Multidiscip. Soc. Technol.*, vol. 1, no. 2, pp. 176–183, 2023.

[7] A. Riduan and N. Sadikin, "Perancangan Firewall Menggunakan Fortigate Di PT Swadharma Duta Data," *J. Maklumatika*, vol. 8, no. 1, pp. 90–98, 2021, [Online]. Available: https://maklumatika.i-tech.ac.id/index.php/maklumatika/article/view/122

[8] W. Paper, "Powering Security at the Speed of the Business Why the FortiGate Next-Generation Firewall Is at the Apex of the Industry".

[9] M. P. I. Support and C. L. C. B. Cell, "White paper on White Paper," *Cell*, no. 26734, pp. 1–7, 2008.

[10] T. A. Cahyanto, V. Wahanggara, and D. Ramadana, "Analisis dan Deteksi *Malware* Menggunakan Metode *Malware* Analisis Dinamis dan *Malware* Analisis Statis," *J. Sist. Teknol. Inf. Indones.*, vol. 2, no. 1, pp. 19–30, 2017.

[11] H. D. Wijaya, R. R. Hidayat, and T. A. Aliyansyah, "Kegiatan Pembelajaran Jaringan Komputer Dengan Static Routing Protocol Menggunakan Gns3 Untuk Siswa Smk Ymik Pada Wilayah Joglo," *J. Abdi Masy.*, vol. 5, no. 2, p. 10, 2020, doi: 10.22441/jam.2020.v5.i2.003.