Analisis Penerapan Fitur *Unified Threat Management* (UTM) FortiGate sebagai *Firewall* untuk Meningkatkan Kinerja Jaringan dengan Pembatasan Akses Aplikasi Sosial Media dan *Platform Streaming* pada PT. Sanipak Indonesia

Dessy Nur Hastuti [1]*, Andy Triwinarko [2]**
* Teknik Informatika, Politeknik Negeri Batam
** Rekayasa Keamanan Siber, Politeknik Negeri Batam
dessy.4332001006@students.polibatam.ac.id [1], andy@polibatam.ac.id [2]

Article Info

Article history:

Received …
Revised …
Accepted …

Keyword:

Firewall, Fortigate 80F, Keamanan jaringan, UTM, QoS

ABSTRACT

In the era of open internet connectivity, enterprises are faced with increasing security threats in the digital world. Therefore, protecting sensitive data and network performance are top priorities to achieve optimal operational performance. By implementing policies to restrict access to social media applications and streaming platforms, companies can strengthen defenses against cyber attacks such as phishing and optimize network infrastructure performance more effectively. This research uses the features provided by Fortigate 80F to block unauthorized applications and streaming platforms, as well as to perform real-time network traffic monitoring. Network performance is measured by applying Quality of Service (QoS) calculations that include throughput, packet loss, and delay parameters, which use TIPHON standards. The results of the research conducted at PT Sanipak Indonesia show that network security has been successfully improved by blocking phishing activities and network performance has also improved significantly, as evidenced by reaching index 4 on the TIPHON scale which indicates a high level of satisfaction.

I. PENDAHULUAN

Seiring dengan kemajuan teknologi internet, acaman kejahatan *cyber* semakin kompleks. Meskipun internet menawarkan banyak keuntungan, terdapat pula kelemahan yang perlu diperhatikan. Keterbukaan internet memungkinkan akses bebas ke aplikasi sosial media dan *platform streaming* oleh semua orang, yang membuat lingkungan kerja di perusahaan menjadi tidak aman. Hal ini dapat mengakibatkan penurunan kualitas jaringan untuk mengirimkan informasi rahasia dan bahkan dapat menghambat produktivitas karyawan di perusahaan.

Dalam konteks ini, meskipun internet memberikan keuntungan besar dalam hal konektivitas dan akses informasi, perusahaan harus mengambil tindakan proaktif dan preventif untuk melindungi diri dari ancaman keamanan yang semakin meningkat di dunia digital saat ini. Tindakan ini tidak hanya berkontribusi pada menjaga keamanan data sensitif, tetapi juga melibatkan perlindungan kualitas jaringan dalam mencapai kinerja operasional yang optimal.

Salah satu tindakan yang dapat digunakan untuk melindungi jaringan dari serangan digital adalah dengan pemasangan *firewall*. Dengan *firewall*, perusahaan dapat mengontrol, memonitor aktivitas jaringan, serta melindungi sistem dari serangan *cyber*.

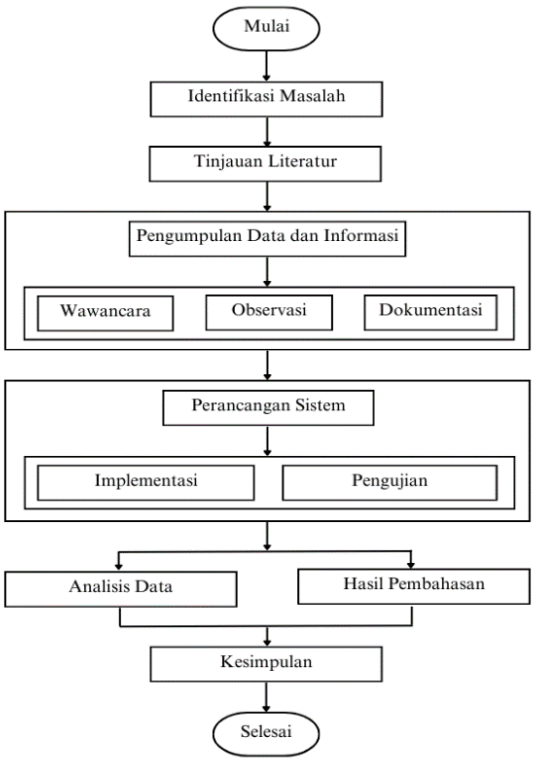
Berdasarkan penelitian terdahulu disimpulkan bahwa pemblokiran aplikasi sosial media dan *platform streaming* yang disalahgunakan karyawan dapat meningkatkan keamanan jaringan dari ancaman siber, sehingga berpotensi memperbaiki kualitas jaringan dan operasional perusahaan [1][2][3][4].

PT. Sanipak Indonesia berusaha menciptakan kondisi yang optimal untuk menjalankan aktivitas dari jarak jauh dengan lancar dan aman antara Batam dan Jepang. Namun, setelah melakukan wawancara dengan salah satu *staff* IT dan melakukan observasi di lapangan, narasumber mengatakan keadaan yang terjadi pada PT. Sanipak Indonesia 1 tahun yang lalu, terjadi serangan siber seperti *phishing* yang menyebabkan penyebaran infeksi *malware* dan merusak data pada komputer. Selain itu, ditemukan juga permasalahan pada kualitas jaringan di perusahaan yang mengalami penurunan akibat penyebaran virus dan penggunaan berlebihan terhadap aplikasi sosial media dan *platform streaming*. Hal ini menyebabkan kinerja jaringan menjadi buruk dan mengakibatkan penundaan dalam proses bisnis. Oleh karena itu, perusahaan perlu mengambil tindakan dengan menetapkan kebijakan keamanan yang jelas terkait penggunaan akses internet oleh karyawan dengan Penerapan Fitur *Unified Threat Management* (UTM) Fortigate Sebagai Firewall [5].

Penilaian dan pemantauan kinerja jaringan mengacu pada fitur yang tersedia dalam Fortigate, seperti *FortiView* dan *Dashboard* [6]. Kedua fitur ini memungkinkan pemantauan real-time yang mendalam terhadap aktivitas jaringan, termasuk tampilan lalu lintas, aplikasi, pengguna, atau *all session*, serta data-data seperti *bandwidth*, paket, dan lainnya. Untuk mengevaluasi performa jaringan, pengukuran dilakukan melalui metode *Quality of Service* (QoS) [7], sementara pengolahan data dilakukan dengan membandingkan hasil pengukuran menggunakan standar TIPHON (*Telecommunications and Internet Protocol Harmonization Over Network*) [8].

II. METODE

Dalam penelitian ini menggunakan *Metode Research & Development* (R&D) [9]. Metode ini dapat membantu mengumpulkan data dan informasi terkait dengan penerapan *Unified Threat Management* (UTM) dilengkapi dengan beberapa fitur yang akan digunakan pada penelitian ini yang terdiri dari *Web Filtering, Application Control, dan Deep Inspection* sebagai *firewall* [5]. Dengan menggunakan pendekatan R&D, penelitian ini akan melakukan analisis terhadap penerapan fitur tersebut untuk meningkatkan keamanan dan kualitas jaringan, khususnya dalam memblokir akses ke aplikasi sosial media dan *platform streaming*. Metode R&D akan memberikan landasan yang kuat untuk mengidentifikasi, menganalisis, dan mengatasi permasalahan yang mungkin muncul seiring dengan implementasi solusi keamanan yang diusulkan [9]. Desain penelitian yang digunakan dalam menyelesaikan Tugas Akhir ini, sebagai berikut:



Gambar 1. *Flowchart* Desain Penelitian

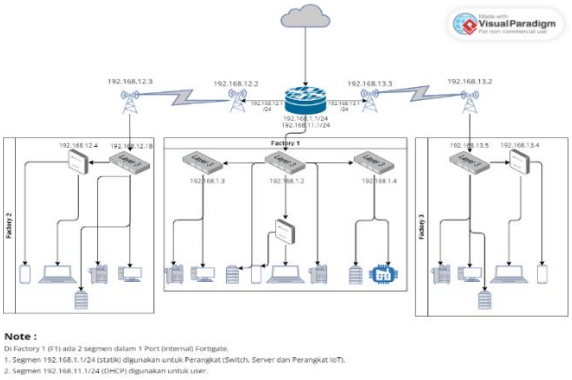
III. PERANCANGAN SISTEM

Pada bab ini merupakan proses yang melibatkan perencanaan, pengembangan, alur dari proses-proses yang akan diimplementasikan, kebijakan keamanan yang akan diterapkan, pemilihan teknologi dan perangkat keras yang akan digunakan, konfigurasi yang diperlukan unuk menjalankan sistem dengan efisien dan efektif serta pengujian

Tahap ini dilakukan konfigurasi pada Fortigate dengan fitur UTM untuk menjalankan sistem dengan efisien dan efektif [3]. Model Fortigate yang digunakan adalah Fortigate 80F v7.0.14.

A. Skema Jaringan Perusahaan

Pada jaringan PT. Sanipak Indonesia menggunakan topologi *tree*. Topologi ini menggunakan satu titik pusat yang mengendalikan dan mengatur akses ke cabang-cabang, yang memungkinkan fleksibilitas dan dapat diperluas dengan relatif mudah, memungkinkan jalur alternatif untuk komunikasi, manajemen jaringan dapat dilakukan dengan lebih efisien dalam operasi jaringan perusahaan. Pada penelitian ini penulis menggunakan *Software Visual Paradigm*.



Gambar 2. Skema Jaringan

Dapat dilihat pada Gambar 2 router yang digunakan adalah perangkat FortiGate. FortiGate ini tidak hanya berfungsi sebagai router, tetapi juga sebagai perangkat keamanan multifungsii yang menyediakan berbagai fitur untuk melindungi dan mengoptimalkan jaringan perusahaan.

B. *Network* dan WAN *routing design*

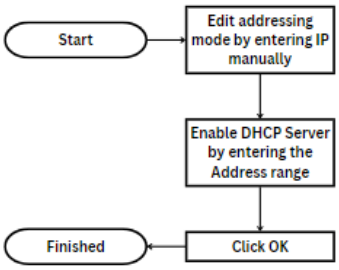
TABLE I KONFIGURASI JARINGAN

Network Jaringan Internal	
Network IP	192.168.11.1
Subnet	255.255.255.0
Broadcast IP	192.168.11.255
Address Range	192.168.11.21-192.168.11.254
Network Jaringan External/WAN	
Network IP	XXX.XXX.XXX.XXX
Subnet	255.255.255.248
Port WAN Interface IP	XXX.XXX.XXX.XXX

C. Konfigurasi Dasar *Network*

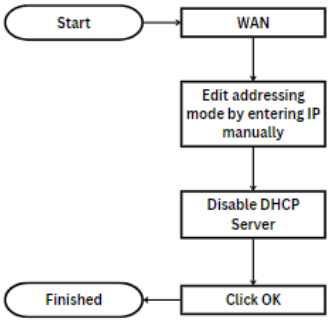
Sebelum melakukan konfigurasi *routing*, langkah pertama yang perlu dilakukan adalah konfigurasi dasar *network*. Ini melibatkan penetapan IP yang diperlukan, dan kemudian melakukan konfigurasi *network* sesuai dengan kebutuhan tersebut.

Berikut adalah langkah-langkah Konfigurasi *Network Internal*:



Gambar 3. Konfigurasi Dasar Network Internal

Langkah-langkah Konfigurasi *Network External*/WAN:

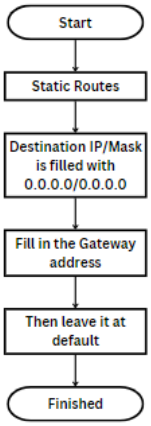


Gambar 4. Konfigurasi WAN

D. Konfigurasi *Routing*

Konfigurasi ini diperlukan untuk memungkinkan perangkat yang terhubung dibelakang Fortigate dapat mengakses jaringan luar Fortigate, seperti internet.

Berikut adalah langkah-langkah untuk melakukan konfigurasi tersebut:

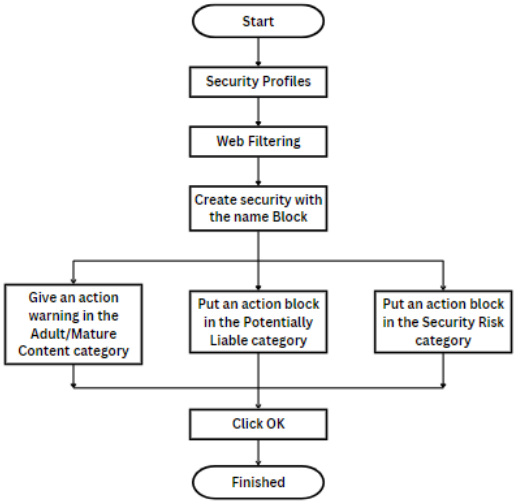


Gambar 5. Konfigurasi Routing

E. Konfigurasi *Web Filtering*

Konfigurasi *Web Filtering* diperlukan untuk mengontrol dan mengelola akses pengguna ke situs web berdasarkan kriteria tertentu, seperti *Potentially Liable*, *Adult/Mature Content*, dan *Security Risk*. Hal ini akan mencegah akses ke situs yang tidak diinginkan atau berbahaya, serta mematuhi kebijakan penggunaan internet yang ditetapkan oleh perusahaan.

Berikut adalah rancangan konfigurasinya:

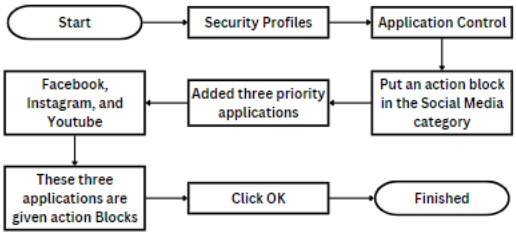


Gambar 6. Konfigurasi Security Profiles pada Web Filtering

F. Konfigurasi *Application Control*

Application Control memiliki kemampuan untuk memblokir lalu lintas HTTPS berdasarkan kategori yang telah ditentukan. Misalnya, kategori yang mencakup situs web atau aplikasi berbahaya, ilegal, atau tidak sesuai dengan kebijakan perusahaan dapat diblokir untuk akses melalui protokol HTTPS. Dalam hal ini akan dicoba untuk memblokir situs *Facebook*, *Instagram*, dan *Youtube*.

Berikut adalah detail langkah-langkah konfigurasinya:



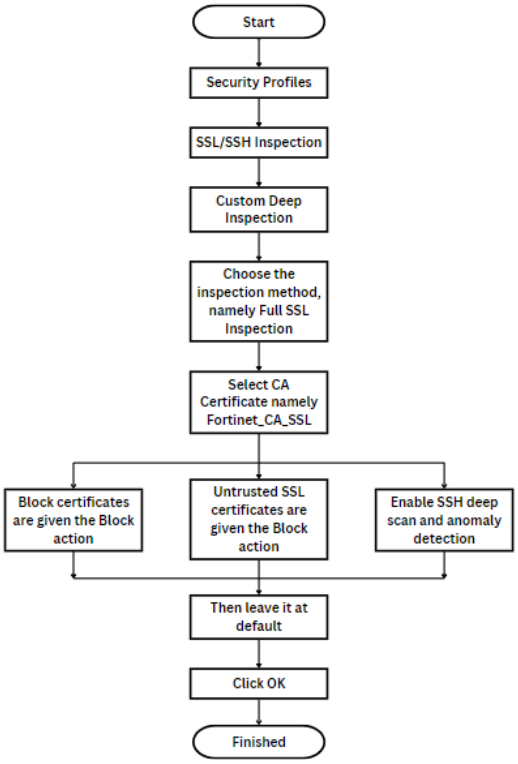
Gambar 7. Konfigurasi Security Profiles pada Application Control

G. Konfigurasi *SSL/SSH Inspection*/

SSL/SSH Inspection berguna pada keamanan jaringan untuk mencegah serangan berbasis enkripsi, seperti serangan *malware* atau serangan *phishing* yang

menggunakan lalu lintas yag dienkripsi untuk menyembunyikan aktivitas jahat.

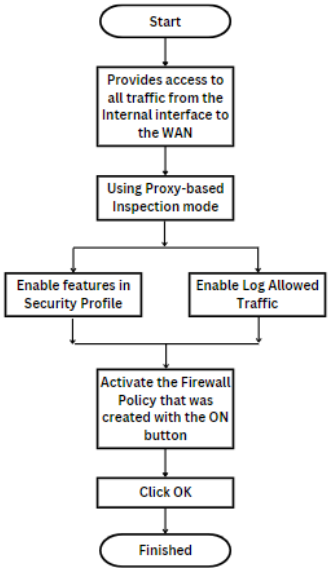
Untuk konfigurasinya adalah sebagai berikut:



Gambar 8. Konfigurasi Security Profiles pada SSL/SSH Inspection

H. *Firewall Policy* dengan UTM

Apabila semua fitur sudah dikonfigurasikan sesuai dengan kebijakan keamanan perusahaan, setelah itu membuat profil keamanan yang menggabungkan semua fitur UTM yang sudah dikonfigurasikan sebelumnya dan dapat menetapkan profil keamanan ini ke *interface* tertentu atau ke grup perangkat yang ditentukan.



Gambar 9. Setting Firewall Policy

I. Pemantuan Kinerja Jaringan

Proses pemantauan dan evaluasi kinerja jaringan secara terus-menerus untuk memastikan bahwa jaringan beroperasi dengan optimal dan memenuhi kebutuhan pengguna. Hal ini dilakukan dengan memanfaatkan fitur-fitur seperti *Dashboard* dan *FortiView* untuk menyediakan analisis yang mendalam terhadap performa jaringan. Dalam menilai kualitas kinerja jaringan yang optimal, diperlukan penggunaan metode seperti *Quality of Service* (QoS) untuk melakukan perhitungan yang sesuai [10].

Quality of Service (QoS) adalah sebuah metode evaluasi yang berkaitan dengan efektivitas suatu jaringan komputer. QoS digunakan untuk mengevaluasi sekelompok atribut kinerja yang telah ditentukan dan terkait dengan suatu layanan. Metode ini mengacu pada standar penilaian yang telah ditetapkan oleh TIPHON (*Telecommunications and Internet Protocol Harmonization Over Network*) [7], sebuah badan standar yang dikeluarkan oleh ETSI (*European Telecommunications Standards Institute*). Adapun standar persentase dan nilai QoS oleh TIPHON sebagai berikut.

TABLE I STANDARISASI QoS

Nilai	Persentase	Indeks
3,8 – 4	95 – 100	Sangat Memuaskan
3 – 3,79	75 – 94,75	Memuaskan
2 – 2,99	50 – 74,75	Kurang Memuaskan
1 – 1,99	25 - 49,75	Buruk

Sumber: TIPHON [8]

Berdasarkan penelitian sebelumnya dan jurnal yang umum ditemukan, dengan menggunakan tiga parameter QoS yaitu *throughput*, *packet loss*, dan *delay*, telah terbukti memberikan penilaian dengan akurat terhadap kualitas kinerja jaringan [11]. Ini menandakan bahwa parameter-parameter tersebut telah menjadi standar yang dapat dipercaya untuk menyevaluasi kualitas layanan dalam jaringan. Berikut parameter yang digunakan pada pengujian:

1. *Throughput*

   Throughput adalah kecepatan efektif transfer data, diukur dalam bit per detik (bps) [12]. Ini mencakup jumlah total paket yang sukses dikirim dan diterima pada tujuan selama interval waktu tertentu, dibagi dengan durasi interval waktu tersebut.

$$Throughput = \frac{jumlah\ data\ yang\ dikirim\ (byte)}{waktu\ pengirim\ data\ (s)}$$

TABLE II KATEGORI THROUGHPUT

Kategori Throughput	Throughput (bps)	Indeks
Sangat Baik	100	4
Baik	75	3
Cukup	50	2
Buruk	<25	1

Sumber:TIPHON [8]

2. *Packet Loss*

Packet Loss adalah parameter yang mengindikasikan jumlah total paket data yang hilang dalam jaringan, yang dapat disebabkan oleh *collision dan congestion* [10]. Hal ini dapat berdampak pada semua aplikasi karena dapat mengurangi efisiensi jaringan secara keseluruhan, meskipun *bandwidth* yang cukup tersedia untuk aplikasi-aplikasi tersebut [11].

$$Packet\ Loss = \frac{(packet\ dikirim - paket\ diterima)}{paket\ data\ yang\ dikirim} \times 100\%$$

TABLE III KATEGORI PACKET LOSS

Kategori Packet Loss	Packet Loss	Indeks
Sangat Baik	0-2%	4
Baik	3-14%	3
Cukup	15-24%	2
Buruk	>25%	1

Sumber: TIPHON [8]

3. *Delay (Latency)*

Delay (latency) adalah waktu yang diperlukan bagi data untuk melakukan perjalanan dari titik awal ke titik tujuan. Faktor-faktor yang dapat mempengaruhi delay termasuk jarak fisik antara kedua titik, jenis media fisik yang digunakan, tingkat kongesti dalam jaringan, dan lamanya waktu proses [13].

$$Rata - rata\ delay = \frac{total\ delay}{total\ paket\ yang\ dikirim} x\ 1000$$

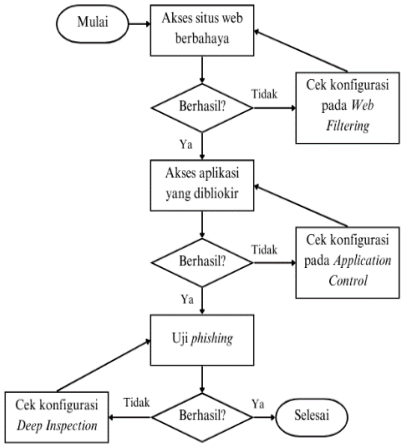
TABLE IV KATEGORI DELAY

Kategori Delay	Delay	Indeks
Sangat Baik	<150 ms	4
Baik	150 - 300 ms	3
Cukup	300 - 450 ms	2
buruk	>450 ms	1

Sumber: TIPHON [8]

IV. ANALISIS HASIL DAN PEMBAHASAN

Hal yang akan dianalisis dari pengujian ini mencakup evaluasi kinerja jaringan dan efektivitas implementasi fitur *Web Filtering*, *Application Control*, dan *Deep Inspection* pada *Unified Threat Management* (UTM) FortiGate. Pengujian dirancang untuk menguji kinerja, keamanan, atau fungsionalitas sistem atau aplikasi secara sistematis. Berikut ini skenario pengujian berdaasarkan metode testing UTM dari NSS Labs [14].



Gambar 10. Skenario Pengujian

A. Pengujian *Web Filtering*

Pada tahap ini pengujian *Web Filtering* dilakukan dengan mengakses situs yang diblokir oleh Fortigate. Kategori-kategori situs tersebut ialah *hackforums.net* dan *blog.elhacker.net*, yang akan di *block* oleh *Web Filtering*.

Gambar 11. Hackforums.net yang diblock oleh FortiGate

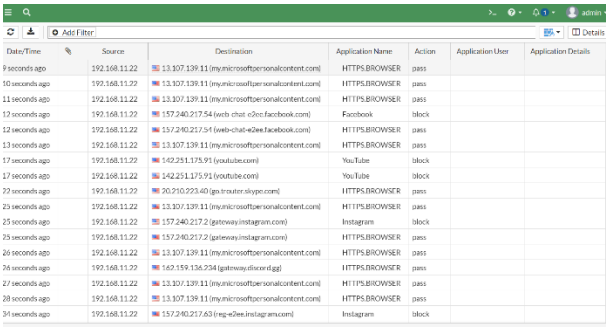
Gambar 12. blog.elhacker.net yang diblock oleh FortiGate

Pengguna dapat melihat catatan aktivitas yang mencakup detail tentang setiap akses ke internet yang diblokir oleh fitur *Web Filter*. Pemblokiran situs berbahaya ini merupakan langkah yang penting untuk meningkatkan keamanan dan mengurangi risiko dalam lingkungan jaringan serta melindungi pengguna dari berbagai ancaman online.

B. Pengujian *Application Control*

Pengujian *Application Control* berbeda dengan pengujian *Web Filtering* dalam hal bahwa pada pengujian ini, pemblokiran langsung dilakukan oleh aplikasi. Aplikasi yang akan diblokir ialah *Facebook, Youtube,* dan *Instagram.*

Pemblokiran langsung terhadap aplikasi ini memungkinkan organisasi untuk mengendalikan risiko terkait dengan penggunaan aplikasi tertentu dalam jaringan, termasuk risiko keamanan, kepatuhan, atau reputasi. Selain itu, tindakan ini juga dapat berdampak pada kinerja jaringan. Dengan memblokir aplikasi tertentu, organisasi dapat mengelola lalu lintas jaringan dengan lebih efisien, mengalokasikan *bandwidth* dengan lebih baik, dan menghindari kelebihan beban jaringan yang disebabkan oleh penggunaan aplikasi yang tidak terkendali.



Gambar 13. Log Application Control

Gambar diatas menunjukkan bahwa dalam proses pemblokiran aplikasi, Fortigate mencatatnya dalam *log application control* dengan *action "block*", menunjukkan keberhasilan pemblokiran.

C. Pengujian *Phishing*

Pengujian ini menggunakan *Kali Linux* di *Virtual Box* dengan meng-*install Tool Zphisher* [15]. *Tool* ini akan berguna untuk membuat situs phishing yang menyerupai situs yang diinginkan yaitu *Facebook* untuk mendapatkan kredensial (ID pengguna dan kata sandi).

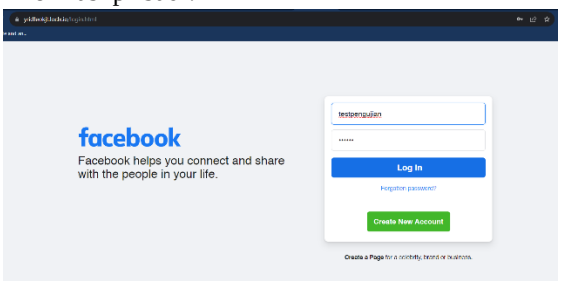
Berikut adalah langkah-langkah untuk meng-*install tool Zphisher* [16]:

1. Cukup dengan kloning repositori ini:
   git clone --depth=1 https://github.com/htr-tech/zphisher.git
2. Apabila sudah masuk ke direktori kloning, selanjutnya jalankan:
   cd zphisher
   bash zphisher.sh
3. Ketika alat sudah mulai berjalan, selanjutnya memilih opsi dari alat yang diperlukan untuk membuat halaman phishing, kemudian memilih untuk membuat halaman *phishing Facebook*
4. Setelah mendapatkan tautan, selanjutnya menyiapkan dan mengirimkan *email* atau pesan pemancing yang mengarahkan target ke halaman *phishing* yang telah dibuat:

Gambar 14. Mendapatkan Link dari Tool Zphisher

Dapat dilihat pada Gambar 14 terdapat tiga URL yang dapat digunakan untuk menarik korban. Pada kesempatan kali ini opsi yang dipilih ialah opsi pertama yaitu https://yridfeokjt.loclx.io

5. Target meng-klik tautan *phising* dan memasukkan informasi pribadi:



Gambar 15. Tampilan Login Page dari Tautan Palsu Facebook

6. Informasi pribadi target seperti detail ID dan kata sandi akan terlihat diterminal *Zphisher*; Dengan menggunakan informasi ini, pelaku *thread* dapat memperoleh akses ke situs web korban dan mungkin seluruh jaringan [16].

Untuk hal ini akan dilakukan dua kali pengujian *phishing*, yaitu pengujian sebelum pemblokiran dan setelah pemblokiran dengan UTM. Tujuannya adalah untuk mengevaluasi efektivitas UTM dalam mengurangi atau mencegah serangan *phishing* di lingkungan jaringan. Dengan demikian, dapat diukur seberapa baik UTM dalam melindungi jaringan dari ancaman *phishing* setelah penerapan pemblokiran.

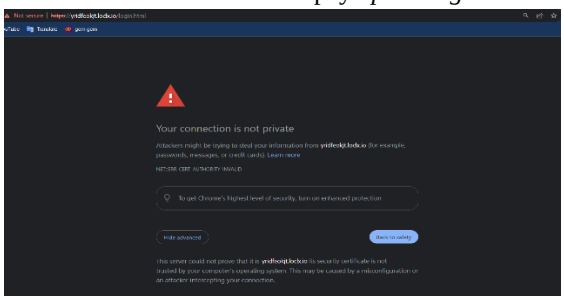
a. Pengujian Sebelum Pemblokiran

Pada pengujian sebelum dilakukan pemblokiran tautan *phishing* dapat terbuka dan menampilkan *login page* yang menyerupai halaman website resmi. Kemudian, ketika target telah mengisi informasi

pribadi seperti *username*, *password*, dan alamat IP pada halaman tersebut maka informasi pribadi tersebut juga akan terlihat diterminal *Zphisher*. Hal ini yang dapat menyebabkan pencurian identitas, penipuan keuangan, atau bahkan akses ilegal ke akun *online* tersebut.

b. Pengujian Setelah Pemblokiran dengan UTM

Tautan tidak dapat terbuka dikarenakan FortiGate dapat mengenali *link phishing* atau tautan berbahaya, sehingga FortiGate dengan langsung mendeteksi dan memblokir upaya *phishing* tersebut.



Gambar 16. Tautan Telah Terblokir Fortigate

Gambar 16 menjelaskan bahwa apabila terdapat masalah saat memvalidasi sertifikat keamanannya yang tidak dipercaya, maka kesalahan akan muncul sebagai "*Your connection is not private*". Dalam hal ini penyerang mencoba mencuri informasi pribadi dari tautan tersebut seperti sandi, pesan, atau kartu kredit yang disebut percobaan *phishing*.

Ketika sebuah *link phishing* diblokir oleh FortiGate, hal ini akan tercatat dalam log keamanan FortiGate sebagai tindakan pemblokiran yang dilakukan oleh fitur keamanan yang sudah dikonfigurasikan. Dengan demikian, administrator jaringan dapat melacak dan menganalisis aktivitas tersebut untuk memastikan perlindungan yang tepat terhadap jaringan.

D. Penilaian Performa Kinerja Jaringan

Dalam penilaian ini, kinerja jaringan diamati menggunakan fitur *Dashboard* dan *FortiView*. Penelitian ini melibatkan perbandingan performa jaringan sebelum dan setelah pembatasan akses aplikasi media sosial dan platform streaming dengan perhitungan QoS dan standar penilaian yang ditetapkan oleh TIPHON.

1. Percobaan Sebelum Pemblokiraan

Percobaan pertama dilakukan di jam kerja. Sepuluh dari 88 user yang terekam dalam satu menit dengan sengaja mengakses aplikasi sosial media yaitu *facebook* dan *instagram* lalu *platform streaming* seperti *youtube*. Data yang dikumpulkan seperti *byte, packet, time*, dan *delay* disajikan ke dalam *microsoft excel.*

Berikut hasil analisis sebelum pemblokiran:

a) Analisis *throughput*

Jumlah *byte* = 1544897

Time span = 344591

Maka *throughput* yang didapat adalah

$$Throughput = \frac{1.544.897}{344.591} = 4{,}48\ byte/s$$

b) Analisis *packet loss*

Paket dikirim = 1359

Paket diterima = 1093

Maka *packet loss* yang didapat adalah

$$Packet\ Loss = \frac{(1359 - 1093)}{1359} \times 100\%$$

Packet Loss = 19%

c) Analisis rata-rata *delay*

Total *delay* = 344591

Paket dikirim = 1359

$$Rata - rata\ delay = \frac{344591}{1359} = 253{,}56\ x\ 1000$$

Rata-rata *delay* = 253 ms

d) Hasil rata-rata parameter QoS

Berdasarkan perhitungan dan penilaian seperti Tabel 5 didapati rata-rata nilai *throughput* 4,48 byte/s dimana kategori berdasarkan standarisasi TIPHON dikatakan **"Buruk"**, kemudian untuk parameter *packet loss* dikategorikan **"Cukup"** karena memiliki nilai 19%. Untuk parameter *delay* percobaan pertama mendapat nilai 253 ms yang artinya **"Baik"**, maka apabila dihitung dengan rata-rata indeks total percobaan pertama mendapat nilai indeks 2 yakni masuk ke dalam kategori **"Kurang memuaskan"**.

TABLE V PENILAIAN QOS PADA PERCOBAAN PERTAMA

Parameter QoS	Nilai	Indeks	Kategori
Throughput (bps)	4,48 byte/s	1	Buruk
Packet Loss (%)	19%	2	Cukup
Delay (ms)	253 ms	3	Baik
Rata-rata Indeks		**2**	**Kurang memuaskan**

2. Percobaan Sesudah Pemblokiran

Pada percobaan ini yakni setelah diimplementasikan pemblokiran terhadap aplikasi sosia media dan *platform streaming*. *User* yang terekam dalam lintas jaringan sebanyak 93 *user* dalam waktu satu menit. Dibawah ini data yang dikumpulkan seperti *byte, packet, time*, dan *delay* disajikan ke dalam *microsoft excel*.

Berikut hasil analisis pada percobaan ini:

a) Analisis *throughput*

Jumlah byte = 36143018

Time span = 206775

Maka *throughput* yang didapat adalah

$$Throughput = \frac{36.143.018}{206.775} = 174{,}79\ byte/s$$

b) Analisis *packet loss*

Paket dikirim = 3250

Paket diterima = 3250

Maka *packet loss* yang didapat adalah

$$Packet\ Loss = \frac{(3250 - 3250)}{3250} \times 100\%$$

Packet Loss = 0%

c) Analisis rata-rata *delay*

Total *delay* = 206775

Paket dikirim = 3250

$$Rata - rata\ delay = \frac{206775}{3250} = 63{,}62\ x\ 1000$$

Rata-rata *delay* = 63 ms

d) Hasil rata-rata parameter QoS

Berdasarkan perhitungan dan penilaian yang dapat dilihat pada Tabel 6 rata-rata nilai *throughput* yaitu 174,79 byte/s dengan kategori **"Sangat baik"**, untuk parameter *packet loss* berada dikategori **"Sangat baik"** dengan nilai rata-rata di 0%, dan kualitas *delay* masuk dalam kategori **"Sangat baik"** dikarenakan memiliki nilai 63 ms. Dengan ini rata-rata indeks total yakni nilai 4 dengan kategori **"Sangat memuaskan"**.

TABLE VI PENILAIAN QOS PADA PERCOBAAN KEDUA

Parameter QoS	Nilai	Indeks	Kategori
Throughput (bps)	174,79 byte/s	4	Sangat baik
Packet Loss (%)	0%	4	Sangat baik
Delay (ms)	63 ms	4	Sangat baik
Rata-rata Indeks		**4**	**Sangat memuaskan**

TABLE VII HASIL PERBANDINGAN OLEH DUA PERCOBAAN

Parameter QoS	Percobaan Sebelum Pemblokiran	Percobaan Sesudah Pemblokiran
Throughput (bps)	4,48 byte/s	174,79 byte/s
Packet Loss (%)	19%	0%
Delay (ms)	253 ms	63 ms
Indeks Berdasarkan TIPHON	**Kurang Memuaskan**	**Sangat Memuaskan**

IV. KESIMPULAN DAN SARAN

Berdasarkan hasil pengujian yang telah dilakukan, dapat disimpulkan bahwa penerapan Fitur-fitur *Unified Threat Management* (UTM) Fortigate sebagai *Firewall* memiliki peran signifikan dalam memperkuat keamanan jaringan internet. Hal ini terwujud melalui kemampuannya dalam menangkal serangan siber yang dilancarkan oleh pihak ketiga, membatasi akses internal yang berpotensi menimbulkan ancaman atau dampak negatif bagi pengguna internal, mampu mencegah serangan *phishing*.

Pembatasan ini juga telah terbukti efektif dalam meningkatkan kinerja jaringan pada PT. Sanipak Indonesia dengan mengimplementasikan pembatasan akses terhadap aplikasi sosial media dan *platform streaming*. Evaluasi yang dilakukan menggunakan parameter *Quality of Service* (QoS) menunjukkan bahwa setelah penerapan pembatasan indeks kinerja jaringan meningkat menjadi 4, dibandingkan dengan sebelumnya yang hanya mencapai indeks 2.

Diperlukan uji coba lanjutan untuk melakukan pengambilan sampel yang lebih luas, termasuk pengumpulan data pada berbagai waktu yang berbeda serta daalam beragam kondisi jaringan internet, baik saat sibuk maupun dalam keadaan normal sehingga dapat memaksimalkan hasil yang diinginkan.

UCAPAN TERIMA KASIH

Ucapan terima kasih yang tulus kepada PT. Sanipak Indonesia atas dukungan dan kesempatan yang telah diberikan dalam penelitian ini. Tanpa bantuan dan akses yang diberikan, penelitian ini tidak akan terlaksana dengan baik. Penulis juga ingin menyampaikan rasa terima kasih kepada dosen pembimbing atas bimbingan dan arahan yang berharga, serta kepada keluarga, rekan-rekan sejawat yang telah memberikan dukungan dan masukaan yang berarti dalam proses penelitian ini. Semua kontribusi daan bantuan anda sangat dihargai. Terima kasih.

DAFTAR PUSTAKA

[1] B. A. Prasetia *et al.*, "Analisa Perangkat Fortinet Sebagai Firewall Untuk Memblokir Aplikasi Sosial Media Dan Platform Streaming Saat Jam Kerja (Studi Kasus : PT . Aplikanusa Lintasarta)," vol. 1, no. 3, pp. 496–504, 2023.

[2] 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.

[3] M. Ikhsan, "Optimalisasi Keamanan Jaringan dan Internet dengan Fitur Unified Threat Management pada Perangkat Firewall," *Sentinel*, vol. 1, no. 1, pp. 21–36, 2018, doi: 10.56622/sentineljournal.v1i1.4.

[4] 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

[5] AVFirewwalls, "Fortinet FortiGate 80D High Performance UTM for Small Networks." https://www.avfirewalls.com.au/

[6] FORTINET, "FortiView Dashboards." https://docs.fortinet.com/document/fortianalyzer/7.4.2/administration-guide/85344/fortiview-dashboards

[7] Satria Turangga, Martanto, and Yudhistira Arie Wijaya, "Analisis Internet Menggunakan Paramater Quality of Service Pada Alfamart Tuparev 70," *JATI (Jurnal Mhs. Tek. Inform.*, vol. 6, no. 1, pp. 392–398, 2022, doi: 10.36040/jati.v6i1.4693.

[8] ETSI, "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON)," *Tec. Rep.*, vol. 1, pp. 1–72, 2002.

[9] Sugiyono, "Sugiyono. 2018. Metode Penelitian Pendidikan," *Revista de Química*, vol. 9, no. 1. pp. 1–14, 2018. [Online]. Available: http://ctic-

cita.es/fileadmin/redactores/Explora/Tecnica_valoriz_ANICE.pdf%0Ahttp://bvssan.incap.org.gt/local/file/T469.pdf%0Ahttps://dspace.ups.edu.ec/bitstream/123456789/1586/15/UPS-CT002019.pdf%0Ahttp://www.bdigital.unal.edu.co/6259/%0Ahttp://onlinelib

[10] M. Hasbi and N. R. Saputra, "Analisis Quality of Service (Qos) Jaringan Internet Kantor Pusat King Bukopin Dengan Menggunakan Wireshark," *Univ. Muhammadiyah Jakarta*, vol. 12, no. 1, pp. 1–7, 2021, [Online]. Available: https://jurnal.umj.ac.id/index.php/just-it/article/view/13596

[11] P. R. Utami, "Analisis Perbandingan Quality of Service Jaringan Internet Berbasis Wireless Pada Layanan Internet Service Provider (Isp) Indihome Dan First Media," *J. Ilm. Teknol. dan Rekayasa*, vol. 25, no. 2, pp. 125–137, 2020, doi: 10.35760/tr.2020.v25i2.2723.

[12] M. Arifar, D. Wiguna, E. Sutanta, and Y. R. K, "Admin-Journal-Manager-41-50-Mahendra-Arifar-Diwan-Wiguna-Edhy-Yuliana1," vol. 7, no. 1, pp. 41–50, 2019.

[13] E. P. Saputra, A. Saryoko, M. Maulidah, N. Hidayati, and S. Dalis, "Analisis Quality of Service (QoS) Performa Jaringan Internet Wireless LAN PT. Bhineka Swadaya Pertama," *EVOLUSI J. Sains dan Manaj.*, vol. 11, no. 1, pp. 13–21, 2023, doi: 10.31294/evolusi.v11i1.14955.

[14] G. Ács and S. Consultant, "Next Generation Firewall Update," 2010.

[15] N. K. A. T. Wahyuni, Putu Putri Cahayani, I Gusti Ngurah Yogi Wicaksana, and Ida Ayu Kadek Bintang Wijayanti, "Analisis Kerentanan Kejahatan Online Phising Menggunakan Tools Zphisher, Shellphish Dan Whphisher," *J. Tek. Mesin, Elektro dan Ilmu Komput.*, vol. 3, no. 1, pp. 23–31, 2023, doi: 10.55606/teknik.v3i1.915.

[16] "Zphisher Tool".