

Filtering Firewall Menggunakan Untangle untuk Sistem Keamanan Jaringan di Berlin Komputer

Filtering Firewalls Using Untangle for Network Security Systems at Berlin Computer

Heru Eko Saputro¹⁾; Khairil²⁾; Hari Aspriyono³⁾

^{1,2)} Department of Informatics, Faculty of Computer Science, Universitas Dehasen Bengkulu

Email: ¹⁾ herueko212121@gmail.com

How to Cite :

Saputro, H. E., Khairil., Aspriyono, H. (2021). *Filtering Firewalls Using Untangle for Network Security Systems at Berlin Computer*. Gatotkaca Journal, 2(1) page: 45-54. DOI: <https://doi.org/10.37638/gatotkaca.2.1.45-54>

ARTICLE HISTORY

Submitted [29 Desember 2021]
Received [29 Desember 2021]
Revised [30 Desember 2021]
Accepted [31 Desember 2021]

KEYWORDS

Filtering, Firewall, Untangle,
Network Security, Berlin
Computer

This is an open access article
under the [CC-BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license



ABSTRAK

Berlin Komputer merupakan salah satu toko komputer yang terdapat di Kota Bengkulu. Dalam proses pengolahan data barang dan penjualan barang di Berlin Komputer sudah menggunakan aplikasi easy pos manager lite yang berbasis jaringan client server. Selain itu pada Berlin Komputer sudah memiliki jaringan internet yang dapat diakses oleh staf karyawan di Berlin Komputer untuk mencari dan mendapatkan informasi. Akses internet menggunakan Telkom, dimana modem indihome terkoneksi dengan komputer dan laptop di lingkungan kerja Berlin Komputer melalui akses LAN dan Wifi. Namun jaringan komputer yang telah dibangun oleh Berlin Komputer belum menerapkan sistem keamanan sehingga sangat rentan jika terjadi suatu serangan yang tidak diinginkan pada jaringan tersebut. Untuk mencegah atau mengantisipasi sebelum terjadi, maka dibutuhkan suatu sistem keamanan yang akan diterapkan pada jaringan komputer yang telah di bangun oleh Berlin Komputer, salah satunya adalah penggunaan firewall. Penerapan Untangle pada Berlin Komputer Bengkulu berhasil dilakukan dimana server telah diinstal, dan sisi client dapat mengakses internet. Dalam penerapan Untangle di Berlin Komputer, didapatkan hasil yang dapat diuji yaitu untangle mampu melakukan blok/filter beberapa situs dengan mengaktifkan web blocker, sedangkan yang belum dapat diuji yaitu phishing, virus blocker, dan ad blocker, dikarenakan report untangle tidak tercatat adanya hal tersebut. Berdasarkan pengujian yang dilakukan, dapat disimpulkan bahwa proses pengamanan sistem jaringan dapat dilakukan dengan baik sesuai dengan harapan dan client tidak dapat mengakses situs-situs yang sudah di blok oleh Untangle. Namun jika client mengaktifkan VPN, situs-situs tersebut masih dapat dibuka dan diakses oleh client. Berdasarkan implementasi yang telah dilakukan, Untangle belum bisa sepenuhnya mengamankan jaringan sebagai firewall, karena sifatnya yang berbayar dan juga masih dapat diakses situs jika mengaktifkan vpn.

ABSTRACT

The purpose of this study is to create an expert system application that can be used to diagnose diseases caused by the coxsackie virus in children using the certainty factor method. Viral infectious disease is a collection of types of diseases caused by viruses that easily attack children. Diseases that often occur in children are caused by very vulnerable viruses, this is because the immune system in the child's body has not been fully developed. One of the viruses that often attack children, among others, is the Coxsackie Virus. Coxsackie is a type of disease caused by the Coxsackie virus, which is a type of RNA virus. This virus is transmitted through the fecal oral route, namely bacteria from feces or feces that move from one person to another and enter the mouth of the other person. This system is designed using PHP Programming Language and MySQL Database. With this expert system, it is easier for users to consult about diseases caused by the Coxsackie Virus in children.

PENDAHULUAN

Banyaknya kemudahan yang didapat oleh pengguna internet menyebabkan teknologi tersebut tumbuh dengan sangat cepat. Hampir semua aspek informasi dapat diperoleh melalui internet mulai dari

pendidikan, hiburan, olahraga, pemerintahan, sekolah, dan lain-lain. Internet bisa diakses hampir semua kalangan baik anak-anak maupun dewasa untuk mencari informasi.

Keamanan jaringan saat ini menjadi isu yang sangat penting dan terus berkembang. Perkembangan teknologi komputer, selain menimbulkan banyak manfaat juga memiliki banyak sisi buruk. Salah satunya adalah serangan terhadap sistem komputer yang terhubung ke Internet. Sebagai akibat dari serangan itu, banyak sistem komputer atau jaringan yang terganggu bahkan menjadi rusak. Untuk menanggulangi hal tersebut, diperlukan sistem keamanan yang dapat menanggulangi dan mencegah kegiatan-kegiatan yang mungkin menyerang sistem jaringan.

Berlin Komputer merupakan salah satu toko komputer yang terdapat di Kota Bengkulu. Dalam proses pengolahan data barang dan penjualan barang di Berlin Komputer sudah menggunakan aplikasi *easy pos manager lite* yang berbasis jaringan *client server*. Selain itu pada Berlin Komputer sudah memiliki jaringan internet yang dapat diakses oleh staf karyawan di Berlin Komputer untuk mencari dan mendapatkan informasi. Akses internet menggunakan Telkom, dimana modem *indihome* terkoneksi dengan komputer dan laptop di lingkungan kerja Berlin Komputer melalui akses LAN dan Wifi. Namun jaringan komputer yang telah dibangun oleh Berlin Komputer belum menerapkan sistem keamanan sehingga sangat rentan jika terjadi suatu serangan yang tidak diinginkan pada jaringan tersebut. Untuk mencegah atau mengantisipasi sebelum terjadi, maka dibutuhkan suatu sistem keamanan yang akan diterapkan pada jaringan komputer yang telah di bangun oleh Berlin Komputer, salah satunya adalah penggunaan *firewall*.

Firewall digunakan sebagai pertahanan pertama yang ditujukan untuk melindungi sebuah komputer atau sebuah *network* dari *traffic internet* atau *intranet* yang tidak diinginkan. Untuk membangun *firewall* diperlukan *hardware* (Perangkat Keras) dan *software* (Perangkat Lunak), dimana *software* yang digunakan dalam penelitian ini menggunakan *firewall Untangle*.

Untangle Firewall NG mengambil kompleksitas dari keamanan jaringan menghemat waktu dan uang. *Untangle* adalah sebuah *appliance* yang bersifat *open source* dan dapat diunduh secara bebas. *Untangle* memberikan kemudahan bagi *system administrator* dalam melakukan manajemen *firewall*. Administrator bisa melakukan manajemen lewat *web GUI administration* yang sudah *untangle* sediakan (Putra, 2019).

LANDASAN TEORI

Jaringan Komputer

Jaringan komputer secara istilah adalah kumpulan komputer yang saling berkaitan dan memiliki hubungan komunikasi antar mereka. Hubungan antara komputer memungkinkan terjadinya operasi yang tidak mungkin dilakukan dalam keadaan *stand alone*. Kata kunci dari jaringan komputer adalah komunikasi (Amien & Mukhtar, 2020).

Terdapat beberapa definisi jaringan komputer yang dikutip (Wicaksono, 2019), antara lain :

- 1) Jaringan komputer adalah desain sistem untuk dapat berbagi, berkomunikasi dan mengakses informasi dari komputer satu dengan komputer
- 2) Jaringan komputer adalah hubungan dua buah simpul atau lebih yang tujuan utamanya adalah untuk melakukan pertukaran data

Topologi Jaringan

Topologi atau arsitektur jaringan merupakan pola hubungan antar terminal dalam suatu sistem jaringan komputer. Topologi jaringan adalah istilah yang digunakan untuk menguraikan cara bagaimana komputer terhubung dalam suatu jaringan (Khasanah, 2016).

Keamanan Jaringan Komputer

Keamanan jaringan komputer sebagai bagian dari sebuah sistem informasi adalah sangat penting untuk menjaga validitas dan integritas data serta menjamin ketersediaan layanan bagi penggunaannya. Sistem harus dilindungi dari segala macam serangan dan usaha-usaha penyusupan atau pemindaian oleh pihak yang tidak berhak dimana usaha tersebut bisa dilakukan baik dari dalam maupun dari luar sistem (Khasanah, 2016).

Firewall

Terdapat beberapa definisi *firewall* yang dikutip (Khasanah, 2016), antara lain :

- a. *Firewall* merupakan suatu cara atau mekanisme yang diterapkan baik terhadap *hardware*, *software* ataupun sistem itu sendiri dengan tujuan untuk melindungi, baik dengan menyaring, membatasi atau

- bahkan menolak suatu atau semua hubungan atau kegiatan suatu segmen pada jaringan lokal dengan jaringan luar yang bukan merupakan ruang lingkungannya
- b. Firewall adalah sebuah sistem atau kelompok sistem yang menerapkan sebuah *access control policy* terhadap lalu lintas jaringan yang melewati titik-titik akses dalam jaringan. Tugas *firewall* adalah untuk memastikan bahwa tidak ada tambahan di luar ruang lingkup yang diizinkan. *Firewall* bertanggung jawab untuk memastikan bahwa *access control policy* yang diikuti oleh semua pengguna di dalam jaringan tersebut. *Firewall* sama seperti alat-alat jaringan lain dalam hal untuk mengontrol aliran lalu lintas jaringan. Namun, tidak seperti alat-alat jaringan lain, sebuah *firewall* harus mengontrol lalu lintas *network* dengan memasukkan faktor pertimbangan bahwa tidak semua paket-paket data yang dilihatnya adalah apa yang seperti terlihat. *Firewall* digunakan untuk mengontrol akses antara *network* internal sebuah organisasi Internet.

Untangle

Untangle adalah sebuah software atau perangkat lunak untuk Next Generation Firewall (NGFW) / Unified Threat Management (UTM). Untangle adalah satu bagian dari generasi ketiga teknologi firewall. Untangle menyatukan semua yang dibutuhkan untuk jaringan yang dikelola, seperti web content dan spam filtering, virus scanning, VPN, multi WAN fail over, dan lain-lain (Putra, 2019).

NDLC (Network Development Life Cycle)

NDLC mendefinisikan siklus proses perancangan atau pengembangan suatu sistem jaringan komputer. NDLC mempunyai elemen yang mendefinisikan fase, tahapan, langkah atau mekanisme proses spesifik. Kata cycle merupakan kunci deskriptif dari siklus hidup pengembangan sistem jaringan yang menggambarkan secara keseluruhan proses dan tahapan pengembangan sistem jaringan yang berkesinambungan. (Kurniawan, 2016).

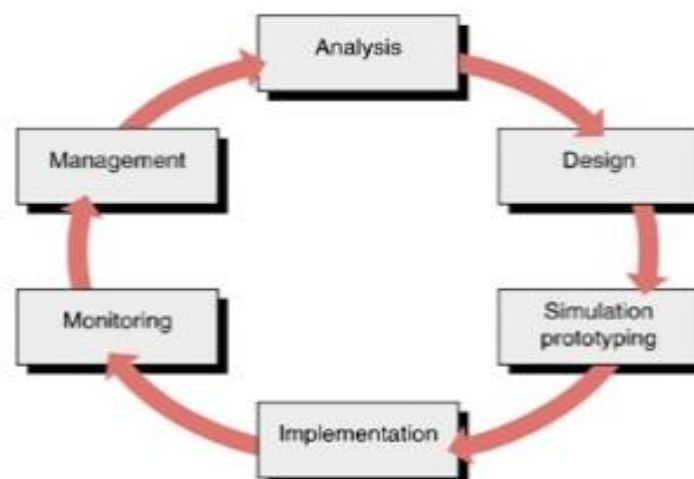
Flowchart

Flowchart adalah dalam bahasa Indonesia diagram alir, merupakan diagram yang memuat simbol-simbol grafis yang menyatakan aliran algoritma atau proses dari langkah-langkah instruksi dalam bentuk-bentuk kotak persegi dan bulat dan pernyataan instruksi, dimana hubungan dan urutan proses tiap instruksi ditunjukkan dengan simbol tanda panah (Anggrawan, 2018)

METODE PENELITIAN

Dalam melaksanakan penelitian ini, penulis menggunakan metode *Network Development Life Cycle* (NDLC) yang merupakan sebuah metode yang bergantung pada proses pembangunan sebelumnya seperti perencanaan strategi bisnis, daur hidup pengembangan aplikasi, dan analisis pendistribusian data.

Adapun tahapan yang dilakukan dalam NDLC terdiri dari *Analysis, Design, Simulation Prototyping, Implementation, Monitoring, dan Management*, seperti terlihat pada Gambar 3.1.



Gambar 1. Tahapan Metode NDLC

Keterangan :

1. *Analysis*

Tahap awal ini dilakukan analisa kebutuhan, analisa permasalahan yang muncul, analisa keinginan pengguna, dan analisa topologi jaringan yang sudah ada saat ini.

2. *Design*

Membuat gambaran desain topologi jaringan yang akan dibangun sesuai dengan analisa kebutuhan yang telah dilakukan

3. *Simulation Prototype*

Tahap dimana dilakukan simulasi dengan bantuan *tools* khusus di bidang jaringan yang digunakan untuk melihat kinerja awal jaringan yang akan dibangun.

4. *Implementation*

Tahap dimana akan dilakukan penerapan rancangan yang telah dibuat agar dapat diuji di lapangan agar dapat menyelesaikan masalah teknik dan non teknis.

5. *Monitoring*

Tahap dimana dilakukan pengamatan terhadap infrastruktur perangkat keras, dan memperhatikan jalannya aplikasi *Untangle* di dalam jaringan yang telah dibangun

6. *Management*

Tahap dimana menentukan kebijakan untuk membuat/mengatur agar sistem yang telah dibangun dapat berjalan dengan baik dan berlangsung lama.

HASIL DAN PEMBAHASAN

Hasil dan Pembahasan

Penerapan *Untangle* di Berlin Komputer Bengkulu dapat membantu proses lalu-lintas data internet ke LAN atau sebaliknya menjadi lebih aman dan cepat. Konfigurasi *Untangle* pun juga sudah berbasis GUI menggunakan aplikasi web browser seperti *Google Chrome*, *Mozilla Firefox*, dan lain-lain.

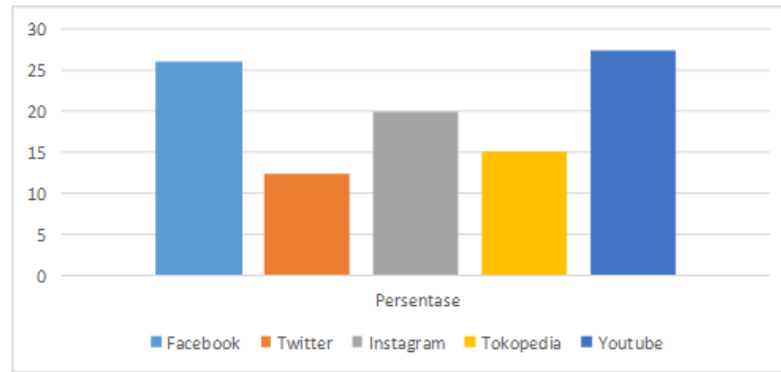
Dengan adanya *untangle* ini, dapat membantu Berlin Komputer dalam melakukan blok/filter beberapa situs yang dapat menurunkan kinerja karyawan dengan mengaktifkan web *blocker*, dan juga dapat mengamankan jaringan internal dari virus atau ancaman lain dengan mengaktifkan virus *blocker*, *ads blocker*, dan *phish blocker*.

Implementasi dilakukan di Berlin Komputer, dengan menggunakan akses internet *Indihome* dan jaringan yang ada di Berlin Komputer. Koneksi Internal menggunakan LAN Adaptor yang akan dikoneksikan ke *client* yang terdapat di Berlin Komputer. Sedangkan eksternal menghubungkan *untangle* ke koneksi internet. Setelah semua terkoneksi, dilakukan penerapan selama 3 hari di Berlin dengan mengaktifkan *Untangle* sebagai Firewall untuk mencatat semua aktivitas lalu lintas yang masuk dan keluar di jaringan berlin. Dimana jumlah karyawan yang bekerja di Berlin Komputer sebanyak 5 orang yang mengakses internet menggunakan laptop atau pun smartphone. Selama 3 hari memantau aktivitas berlin dimana terdapat kuisisioner yang diberikan ke karyawan berlin untuk diisi, sehingga diperoleh seperti Tabel 1.

Tabel 1. Hasil Kuisisioner

Karyawan	Site Yang Di Akses Selama 3 Hari				
	Facebook	Twitter	Instagram	Tokopedia	Youtube
Responden 1	3	2	2	2	5
Responden 2	5	1	4	2	4
Responden 3	4	2	2	2	4
Responden 4	4	3	2	2	3
Responden 5	3	1	4	3	4
Total	19	9	14	11	20
Persentase	26,03	12,33	19,18	15,07	27,40

Hasil persentase tersebut jika dibuat dalam bentuk grafik menghasilkan nilai seperti Gambar 4.1.



Gambar 2. Hasil Persentase

Perangkat yang digunakan

Perangkat Keras yang digunakan untuk implementasi *Untangle* pada Berlin Komputer, antara lain :

- a) 1 laptop yang akan dijadikan *Server*
- b) 4 laptop yang akan dijadikan *Client*
- c) 1 Modem *Router Indihome* sebagai akses Internet
- d) 1 *Switch* sebagai penghubung antara server dengan *client* melalui LAN
- e) 1 *wifi router* sebagai penghubung antara server dengan client melalui WLAN

Perangkat Lunak yang digunakan untuk implementasi *Untangle* pada Berlin Komputer, yaitu :

- a) Sistem Operasi *Untangle 15.1.0* untuk *Server*
- b) Sistem Operasi Windows 8 dan Windows 10 untuk *Client*

Pengujian Sistem

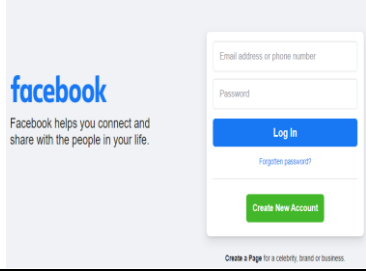
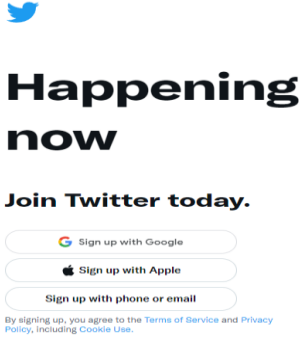


Pada tahap ini dilakukan pengujian terhadap sistem jaringan yang telah diimplementasikan *untangle* apakah berjalan dengan baik atau tidak. Pengujian dilakukan di Berlin Komputer Bengkulu komponen pengujian yang dibagi menjadi 2 bagian yaitu :

1. Pengujian Sebelum dan Sesudah Penerapan *Untangle*

Tabel 2. Hasil Penerapan *Untangle*


No	Report	Keterangan
1		Pada Report ini terlihat bahwa beberapa website telah di blok oleh <i>untangle</i>
2		pada report ini terlihat bahwa aplikasi telah di blok oleh <i>untangle</i>

Tabel 3. Penerapan Untangle Sebelum Melakukan Block Web di Browser

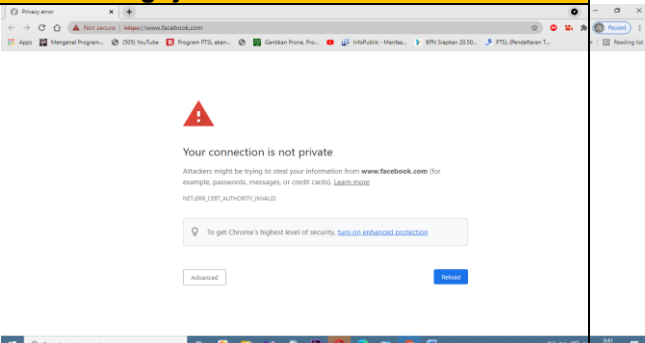
No	Link Web	Hasil	Keterangan
1	www.facebook.com		Masih dapat membuka Facebook
2	www.twitter.com		Masih dapat membuka Twitter
3	www.instagram.com		Masih dapat membuka Instagram
4	www.tokopedia.com		Masih dapat membuka Tokopedia

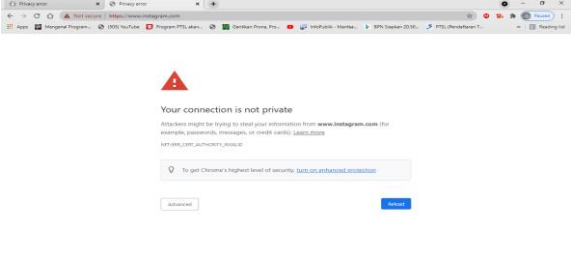
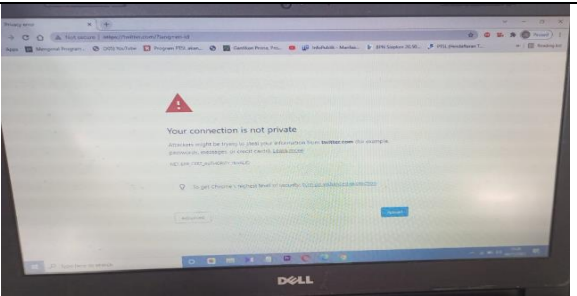
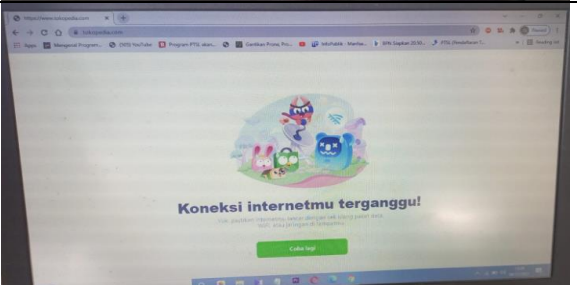
Tabel 3. Penerapan Untangle Sebelum Melakukan Block Aplikasi di Smartphone

No	Aplikasi Smartphone	Hasil	Keterangan
1	Facebook		Masih dapat membuka Facebook

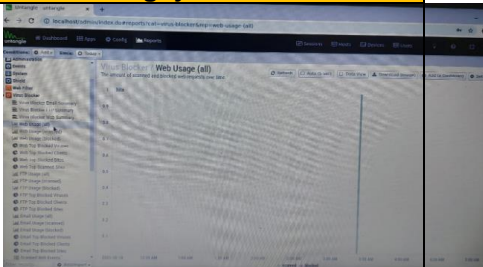
2	Twitter		Masih dapat membuka Twitter
3	Instagram		Masih dapat membuka Instagram
4	Tokopedia		Masih dapat membuka Tokopedia

Tabel 4. Web Blocker

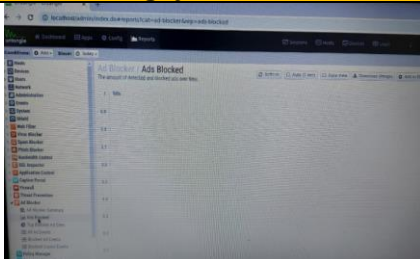
Pengujian	Status	Hasil Pengujian
Web Filter	Enabled	
Site : www.facebook.com	Block	

www.instagram.com	Block	
www.twitter.com	Block	
www.tokopedia.com	Block	

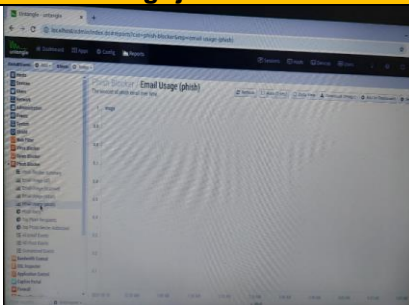
Tabel 5. Virus Blocker

Pengujian	Status	Hasil Pengujian
Virus Blocker	Enabled	
Scan HTTP	Enabled	
Scan SMTP	Enabled	
Scan FTP	Enabled	

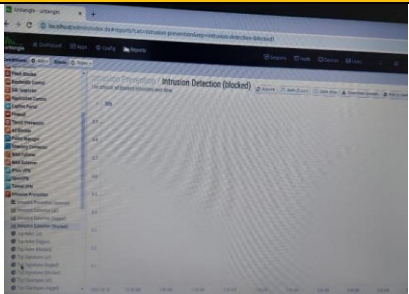
Tabel 6. Ad Blocker

Pengujian	Status	Hasil Pengujian
Ad Blocker	Enabled	
Block ads	Enabled	
Blocks Tracking dan Cookies	Enabled	

Tabel 7. Phish Blocker

Pengujian	Status	Hasil Pengujian
Phish Blocker	Enabled	
Scan SMTP Action	Enabled Quaranti	

Tabel 8. Instrusion Prevention

Pengujian	Status	Hasil Pengujian
Instrusion Prevention	Enabled	

Berdasarkan pengujian yang dilakukan di Berlin Komputer Bengkulu, dapat disimpulkan bahwa proses pengamanan sistem jaringan dapat dilakukan dengan baik sesuai dengan harapan dan *client* tidak dapat mengakses situs-situs yang sudah diblok oleh *Untangle*. Namun jika *client* mengaktifkan VPN, situs-situs tersebut masih dapat dibuka dan diakses oleh *client*.

KESIMPULAN DAN SARAN

Kesimpulan

Penerapan *Untangle* pada Berlin Komputer Bengkulu berhasil dilakukan dimana *server* telah di instal, dan sisi *client* dapat mengakses internet.

1. Dalam penerapan *Untangle* di Berlin Komputer, didapatkan hasil yang dapat diuji yaitu untangle mampu melakukan blok/filter beberapa situr dengan mengaktifkan *web filter*, *application control*, dan *bandwidth control* sedangkan yang belum dapat diuji yaitu *phish blocker*, *virus blocker*, *ad blocker*, dan *threat prevention* dikarenakan report untangle tidak tercatat adanya hal tersebut.
2. Berdasarkan pengujian yang dilakukan, dapat disimpulkan bahwa proses pengamanan sistem jaringan dapat dilakukan dengan baik sesuai dengan harapan dan *client* tidak dapat mengakses situs-situs yang sudah di blok oleh *Untangle*. Namun jika *client* mengaktifkan VPN, situs-situs tersebut masih dapat dibuka dan diakses oleh *client*
3. Berdasarkan implementasi yang telah dilakukan, Untangle belum bisa sepenuhnya mengamankan jaringan sebagai firewall, karena sifatnya yang berbayar dan juga masih dapat diakses situs jika mengaktifkan vpn.

Saran

1. Agar dapat menggunakan *Untangle* untuk menjaga keamanan sistem jaringan dan membantu meningkatkan kinerja karyawan.
2. Perlu adanya perbandingan dengan melakukan instalasi *firewall* yang lain, salah satunya *Zentyal* untuk penelitian selanjutnya.

DAFTAR PUSTAKA

- Amien, J. A. & Mukhtar, H., 2020. *Implementasi Jaringan Komputer*. Yogyakarta: Penerbit Deepublish.
- Anggraini, M. A. N., 2018. Uji Fitur Intrusion Prevention Pada Firewall Untangle Dengan Pengujian DOS dan SSH Brute Force. *Jurnal Manajemen Informatika*, Volume Vol.9 No.1.
- Anggrawan, A., 2018. *Algoritma dan Pemrograman Implementasi Pada VB.Net dan Java*. Pertama penyunt. Yogyakarta: Andi Publisher.
- Khasanah, F. N., 2016. Perancangan dan Simulasi Jaringan Komputer Menggunakan Graphical Network Simulator 3 (GNS3). *Makalah Program Studi Teknik Informatika Universitas Muhammadiyah Surakarta*.
- Khasanah, S. N., 2016. Keamanan Jaringan Dengan Packet Filtering Firewall (Studi Kasus PT. Sukses Berkat Mandiri Jakarta). *JURNAL KHATULISTIWA INFORMATIKA*, Volume VOL. IV, NO. 2 Desember 2016.
- Kurniawan, R., 2016. Analisis Dan Implementasi Desain Jaringan Hotspot Berbasis Mikrotik Menggunakan Metode NDLC (Network Development Life Cycle) Pada Bpu Bagas Raya Lubuklinggau. *Jurnal Ilmiah Betrik*, Volume Vol.7 No.1 April 2016.
- Putra, M. D., 2019. *Next Generation Firewall Berbasis Untangle*. Bekasi Jawa Barat: PT. Excellent Infotama Kreasindo.
- Rajab & Weafandi, A., 2017. Membangun Jaringan Local Area Network Menggunakan Untangle 11.0 di Lembaga Quantum Padang. *Indonesian Journal of Computer Science*, Volume Vol. 6, No. 2 ISSN 2302-4364.
- Sahal, M., 2018. *Administrasi Infrastruktur Jaringan Untuk SMK/MAK Kelas XII*. Jakarta: PT. Gramedia Widiasarana Indonesia.
- Wicaksono, S. R., 2019. *Jaringan Komputer Konsep dan Studi Kasus*. Pertama penyunt. Malang Jawa Timur: CV. Seribu Bintang.