Jurnal Maklumatika
Vol. 8, No. 1, Juli 2021 ISSN : 2407-5043

PERANCANGAN *FIREWALL* MENGGUNAKAN FORTIGATE DI PT. SWADHARMA DUTA DATA

Ahmad Riduan[1], Nanang Sadikin[2]

[1,2] Program Studi Teknik Informatika, Sekolah Tinggi Teknologi Informasi NIIT
[1,2] Asem Dua No. 22, Kel. Cipete Selatan, Kec. Cilandak, Jakarta Selatan
Email: ahmadriduan.work@gmail.com[1], nanang.sadikin@gmail.com[2]

Abstrak

Zaman era komputeriasi saat ini yang berkembang dan menyebar luas hampir semua layanan komunikasi seperti media internet sebagai alat untuk mencari informasi. Seiring kemajuan teknologi timbul permasalahan dan berdampak negatif, seperti kejahatan siber yang berasal dari dalam maupun dari luar melalui sistem jaringan komputer. Adanya Kejahatan komputer akan menyebabkan kerugian khususnya berhubungan data-data yang merupakan informasi yang sangat penting dan diketahui oleh orang-orang tertentu di dalam perusahaan atau organisasi tersebut. Sehingga keamanan data merupakan informasi berharga menjadi prioritas utama untuk diperhatikan dan terjamin dari segala kemungkinan kerusakan ataupun penyalahgunaan dari pihak-pihak yang tidak bertanggung jawab, sehingga perlu adanya pengamanan sistem dengan menggunakan teknologi firewall. Tujuan penelitian ini adalah merancang *firewall* menggunakan *foretigate* sebagai pengamanan sistem informasi untuk sejumlah data-data penting perusahaan. Metode penelitian yang digunakan diantaranya adalah studi kepustakaan, observasi dan wawancara serta metode pengembangan jaringan menggunakan *Network Development Life Cylce* (NDLC). Hasil yang akan dicapai penelitian ini yaitu mengimplementasikan perangkat dari brand Fortinet yaitu *FortiGate*. Simpulan dari penelitian ini adalah implementasi firewall menggunakan *Fortigate* memiliki fitur keamanan untuk sistem jaringan yang lengkap, diantaranya pengamanan *antivirus, web-filtering, application control, network trafic policy*, dan *Intrusion Prevention*.

Kata Kunci: *Perancangan, Firewall, FortiGate*

1. PENDAHULUAN

1.1 Latar Belakang

Saat ini era komputeriasi sudah berkembang dan menyebar dengan luas yang meliputi hampir semua layanan komunikasi yang ada, salah satunya seperti media internet yang menyebabkan semua orang menggunakan media ini sebagai bahan untuk mencari informasi, dan ada pula yang menggunakannya sebagai bahan untuk mencari informasi dengan tujuan-tujuan tertentu. Perkembangan dan kemajuan teknologi, khususnya teknologi komputer yang ada memang banyak keuntungan dalam membantu kehidupan manusia. Seiring dengan kemajuan teknologi masih ada permasalahan serius yang membawa dampak negatif, seperti adanya kejahatan siber baik yang berasal dari dalam (internal) maupun yang berasal dari luar (eksternal) sistem jaringan komputer.

Kejahatan komputer akan menyebabkan kerugian dari pengelola atau administrator sistem jaringan komputer, yang khususnya berhubungan dengan sejumlah data-data yang merupakan informasi yang sangat penting, dan hanya diperbolehkan untuk diketahui oleh orang-orang tertentu di dalam perusahaan tersebut. (Karpen, 2012)

Untuk itu keamanan data yang merupakan informasi berharga menjadi prioritas utama untuk diperhatikan dan harus terjamin dari segala kemungkinan kerusakan ataupun penyalahgunaan dari pihak-pihak yang tidak bertanggung jawab, sehingga menyebabkan sistem informasi menjadi rusak dan tidak bisa digunakan lagi sebagaimana yang diinginkan.

Keamanan jaringan menjadi hal yang penting untuk semua industri dan perusahaan untuk menjaga keamanan jaringan, data dan informasi yang berada didalamnnya. Berdasarkan perlindungan keamanan data/informasi dalam suatu jaringan, umumnya semua teori keamanan berbasis data dibuat dan diaplikasikan untuk mengamankan suatu jaringan tertentu. (Pandu Pratama Putra, 2016)

Salah satu yang dapat digunakan sebagai pengamanan sistem informasi untuk sejumlah data-data penting adalah dengan menggunakan teknologi firewall. Sebagian orang mungkin sudah akrab dengan istilah firewall dan mungkin sebagian masih menggap sesuatu hal yangbaru dalam sistem jaringan

komputer. Keamanan komputer tidak hanya mengandalkan *firewall* yang paling canggih, karena untuk itu harus memiliki pengetahuan yang lebih luas tentang network security. (karpen, 2012)

Menurut I Gede Suputra Widharma (2020) yang dikutip dari researchgate.net, definisi Firewall adalah sebuah pembatas antara suatu jaringan local dengan jaringan lainnya yang sifatnya public (dapat diakses oleh siapapun) sehingga setiap data yang masuk dapat diidentifikasi untuk dilakukan penyaringan sehingga aliran data dapat dikendalikan untuk mencegah bahaya/ancaman yang datang dari jaringan publik.

Cara kerja Firewall pada dasarnya diumpamakan sebuah satpam yang menjaga pintu gerbang rumah anda untuk menyaring pengunjung yang datang ke tempat anda. Demikian pula dengan Firewall adalah sebuah software atau hardware yang menyaring informasi (paket) yang datang melalui internet ke komputer pribadi anda atau jaringan komputer. (Ahmad Maurits Radhiyya, 2011)

Firewall melakukan penyaringan paket data di dalam jaringan komputer (Packet Filter). Hal ini berarti bahwa firewall melakukan proses penyaringan (Filtering) paket-paket data ke dalam sebuah tabel aturan. Adanya filtering paket data ini akan memudahkan di dalam membedakan antara paket data mana yang diperbolehkan untuk masuk ke dalam jaringan komputer dengan paket data yang harus dibuang (congesti) atau dilarang (block).

Perangkat firewall yang digunakan pada penelitian ini menggunakan perangkat dari *brand Fortinet* yaitu *FortiGate*. Fortigate adalah sebuah sistem keamanan yang dikeluarkan oleh perusahaan Fortinet. Fortinet memiliki keunggulan dalam penerapan Firewall, yang saat ini mereka sebut sebagai Next Generation Firewall. (Surya Aprihansah , Iwan Krisnadi, 2016).

Fortigate memiliki fitur keamanan untuk sistem jaringan yang lengkap, seperti antivirus, web-filtering, application control, network trafic policy, dan Intrusion Prevention.

.

1.2 Rumusan Masalah

Berdasarkan latar belakang masalah di atas maka dapat dirumuskan suatu masalahnya adalah Bagaimana merancang firewall dan fitur-fitur apa saja yang dapat mengamankan sistem jaringan pada PT. Swadharma Duta Data ?

2. METODE PENELITIAN

Metode penelitian yang digunakan untuk melakukan penelitian adalah:

1. Kepustakaan

   Pengertian studi pustaka atau studi kepustakaan menurut R. Poppy Yaniawati (2020) Penelitian kepustakaan merupakan suatu jenis penelitian yang digunakan dalam pengumpulan informasi dan data secara mendalam melalui berbagai literatur, buku, catatan, majalah, referensi lainnya, serta hasil penelitian sebelumnya yang relevan, untuk mendapatkan jawaban dan landasan teori mengenai masalah yang akan diteliti.

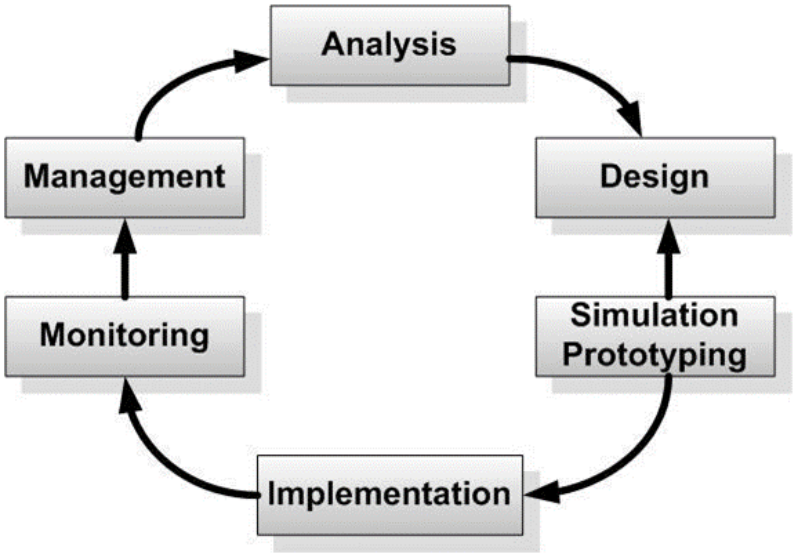
2. Wawancara dan Observasi

   Menurut Imami Nur Rachmawati (2017) Wawancara pada penelitian kualitatif merupakan pembicaraan yang mempunyai tujuan dan didahului beberapa pertanyaan informal. Wawancara penelitian lebih dari sekedar percakapan dan berkisar dari informal ke formal. Dalam teknik wawancara ini, peneliti melakukan tanya jawab kepada pemilik perusahaan secara tatap muka. Melalui wawancara ini, peneliti akan mengetahui lebih dalam mengenai aktivitas proses kerja perusahaan. Sugiyono (2016) mengemukakan bahwa dengan wawancara, maka peneliti akan mengetahui hal-hal yang lebih mendalam tentang partisipan dalam menginterpretasikan situasi dan fenomena yang terjadi, dimana hal ini tidak dapat ditemukan melalui observasi.

   Definisi Observasi Sugiyono (2016) menyatakan bahwa, “through observation, the researcher learn behavior and the meaning attached to those behavior”. Melalui observasi, peneliti belajar tentang perilaku, dan makna dari perilaku tersebut. Dalam melakukan observasi, peneliti akan terlibat kegiatan sehari-hari proses kerja dan orang yang diamati sebagai sumber data penelitian.

3. Metode Pengembangan Sistem

Menurut Hendra Kurniawan dan Sandy Kosasi (2015) Metode analisis dan perancangan menggunakan *Network Development Life Cycle* (NDLC) dengan pendekatan Top Down Approach. Tahapan *Network Development Life Cycle* (NDLC) mencakup tahapan: a) Analisis, menganalisis kebutuhan untuk melakukan penelitian, permasalahan yang ada, topologi jaringan; b) Desain, merancang jaringan dalam skala waktu tertentu; c) Simulasi prototype; d) melakukan eksekusi penelitian (monitoring jaringan); e) Implementasi; dan f) Manajemen , pengelolaan alokasi bandwidth jaringan yang dilakukan administrator"

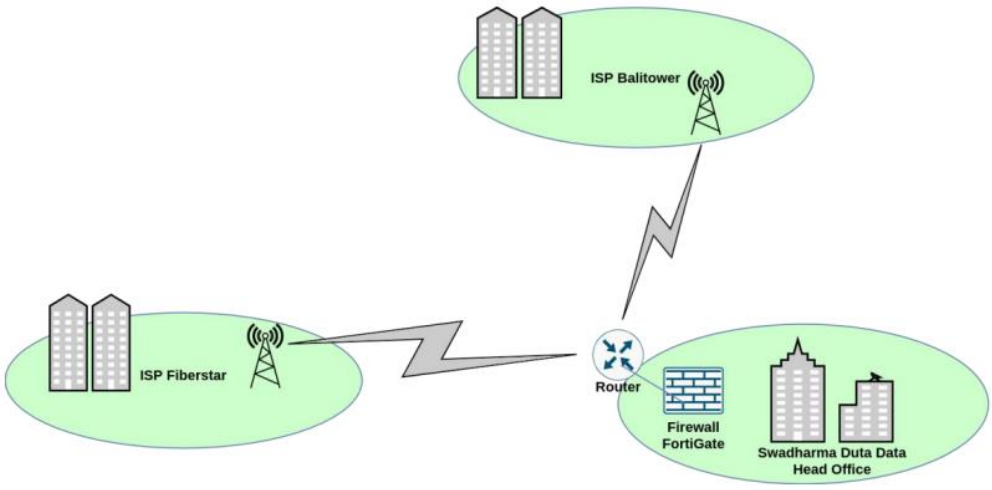


Gambar 1. Metode NDLC

3. HASIL DAN PEMBAHASAN

3.1. Topologi Jaringan Yang Di Usulkan

Sistem jaringan komputer PT. Swadharma Duta Data menggunakan dua (2) *Internet Service Provider* yaitu Fiberstar dan Balitower, berikut gambar topologi firewalll yang dirancang pada PT. Swadharma Duta Data:



Gambar 2. Topology Jaringan PT. Swadharma Duta Data

Secara alur sistem jaringan komputer pada gambar topologi, posisi perangkat Router terletak di paling depan dan terhubung dengan 2 (dua) *Internet Service Provider*, posisi *firewall Fortigate* tepat berada dibelakang perangkat Router guna untuk memeriksa paket data/trafic yang keluar dan masuk ke sistem jaringan komputer internal PT. Swadharma Duta Data. Fitur keamanan yang digunakan

pada perangkat *firewall Fortigate* yaitu antivirus, web filter, application control dan Intrusion Prevention. Pada saat penelitian ini berfokus pada 2 (dua) fitur saja, yaitu *antivirus* dan *intrusion prevention*.

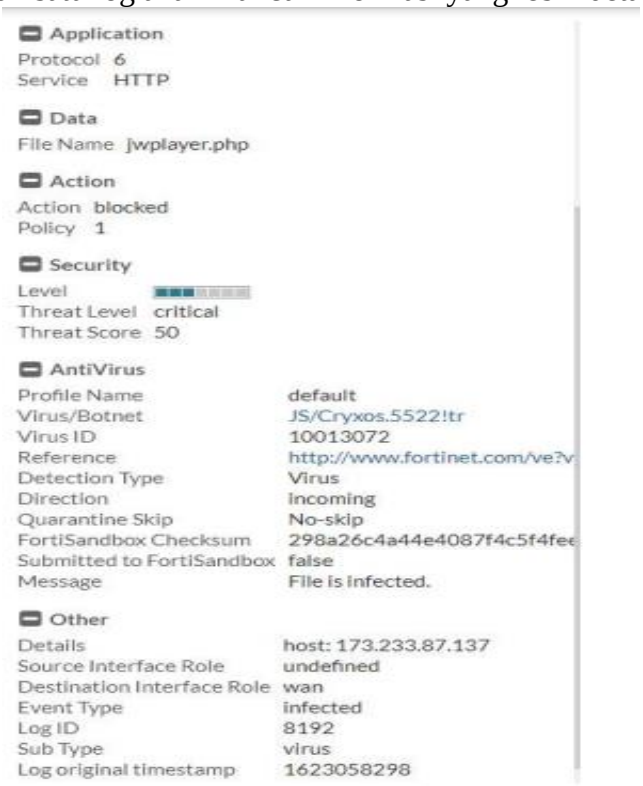
3.2. Analisa Log Antivirus

Tim *Security Operation Center* (SOC) PT. Swadharma Duta Dataditugaskan untuk melakukan analisa jika ada log atau alert pada perangkat *security* yang berbahaya, tim SOC akan melakukan action terkait dengan peringatan (alert) tersebut dan membuat laporan analisa untuk dieskalasi.

Date/Time	Service	Source	Virus/Botnet	Details	Action
06-07 16:31	HTTP	10.70.11.238	JS/Cryxos.5522!tr	host: 173.233.87.137	blocked
06-07 16:31	HTTP	10.70.11.238	JS/Cryxos.5522!tr	host: 173.233.87.137	blocked
06-07 16:31	HTTP	10.70.11.238	JS/Cryxos.5522!tr	host: 173.233.87.137	blocked
06-07 14:16	HTTP	10.70.11.238	JS/Cryxos.5522!tr	host: 173.233.87.137	blocked
06-07 14:16	HTTP	10.70.11.238	JS/Cryxos.5522!tr	host: 173.233.87.137	blocked
06-07 14:16	HTTP	10.70.11.238	JS/Cryxos.5522!tr	host: 173.233.87.137	blocked
06-07 11:17	HTTP	10.70.11.238	JS/Cryxos.5522!tr	host: 173.233.87.137	blocked
06-07 11:17	HTTP	10.70.11.238	JS/Cryxos.5522!tr	host: 173.233.87.137	blocked
06-07 11:17	HTTP	10.70.11.238	JS/Cryxos.5522!tr	host: 173.233.87.137	blocked
06-07 10:49	HTTP	10.70.11.238	JS/Cryxos.5522!tr	host: 173.233.87.137	blocked
06-07 10:49	HTTP	10.70.11.238	JS/Cryxos.5522!tr	host: 173.233.87.137	blocked
06-07 10:49	HTTP	10.70.11.238	JS/Cryxos.5522!tr	host: 173.233.87.137	blocked
06-07 10:38	HTTP	10.70.11.238	JS/Cryxos.5522!tr	host: 173.233.87.137	blocked
06-07 10:38	HTTP	10.70.11.238	JS/Cryxos.5522!tr	host: 173.233.87.137	blocked
06-07 10:38	HTTP	10.70.11.238	JS/Cryxos.5522!tr	host: 173.233.87.137	blocked
06-07 10:33	HTTP	10.70.11.238	JS/Cryxos.5522!tr	host: 173.233.87.137	blocked
06-07 10:33	HTTP	10.70.11.238	JS/Cryxos.5522!tr	host: 173.233.87.137	blocked
06-07 10:33	HTTP	10.70.11.238	JS/Cryxos.5522!tr	host: 173.233.87.137	blocked
06-05 01:01	HTTP	10.70.76.75	HTML/FakeAlert.MF!tr	host: 68.183.181.111	blocked
06-04 13:45	HTTP	10.70.128.69	HTML/ScrInject.B!tr	host: 62.149.9.44	blocked
06-04 13:45	HTTP	10.70.128.69	HTML/ScrInject.B!tr	host: 62.149.9.44	blocked
06-04 13:44	HTTP	10.70.128.69	HTML/ScrInject.B!tr	host: 62.149.9.44	blocked
06-04 13:44	HTTP	10.70.128.69	HTML/ScrInject.B!tr	host: 62.149.9.44	blocked
06-03 23:14	HTTP	10.70.8.155	JS/Cryxos.4162!tr	host: 99.198.108.198	blocked
06-02 22:00	HTTP	10.70.17.63	HTML/ScrInject.B!tr	host: 103.194.171.18	blocked
06-02 22:00	HTTP	10.70.17.63	HTML/ScrInject.B!tr	host: 103.194.171.18	blocked
06-02 22:00	HTTP	10.70.17.63	HTML/ScrInject.B!tr	host: 103.194.171.18	blocked
06-02 21:42	HTTP	10.70.17.81	HTML/ScrInject.B!tr	host: 103.194.171.18	blocked
06-02 21:42	HTTP	10.70.17.81	HTML/ScrInject.B!tr	host: 103.194.171.18	blocked

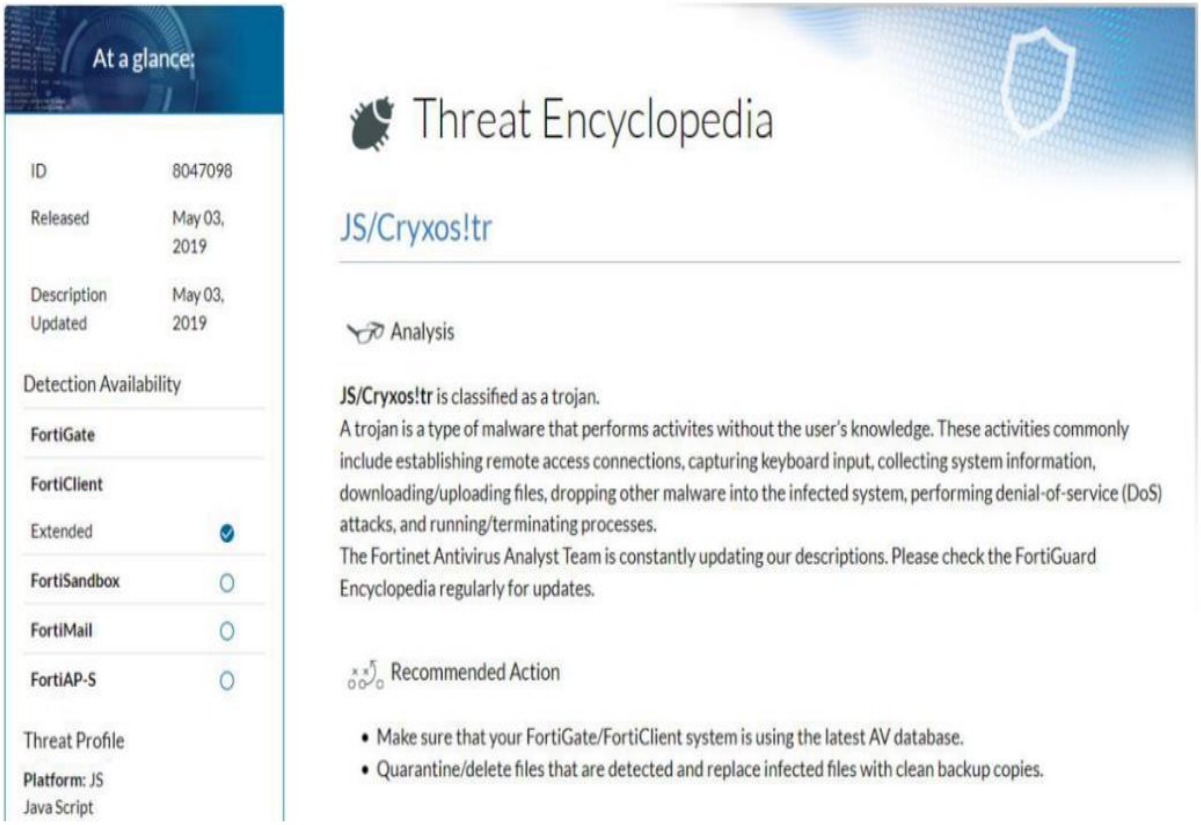
Gambar 3. Log Antivirus

Jika kita klik pada salah satu log akan muncul informasi yang lebih detail dari log tersebut.



Gambar 4. Detail Log Antivirus

Tim SOC akan membuat laporan analisa berdasarkan log *antivirus* tersebut, analisa yang dilakukan adalah dengan melihat info lebih detail, seperti jenis malwarenya, *action* yang dilakukan *firewall*, *threat level* (tingkat bahaya dari virus tersebut), *source address* dan *service*. Info detail virus tersebut bisa kita dapatkan dari detail *log* pada *firewall* dan *reference* dari website fortigate (www.fortiguard.com).



Gambar 5. Virus Ensiklopedia fortiguard.com

Berdasarkan gambar diatas dapat dilaporkan detail dari threat JS/Cryos!tr adalah sebuah malware yang diklasifikasikan sebagai trojan. Trojan adalah jenis malware yang melakukan aktivitas tanpa sepengetahuan pengguna. Aktivitas ini biasanya termasuk membuat koneksi akses jarak jauh, menangkap input keyboard, mengumpulkan informasi sistem, mengunduh / mengunggah file, memasukkanmalware lain ke sistem yang terinfeksi, melakukan serangan penolakan layanan (DoS), dan menjalankan / menghentikan proses. Platform dari malware ini yaituJS (JavaScript).

3.3. Analisa Intrusion Prevention

Analisa lainnya yang dilakukan Tim *Security Operation Center* (SOC) pada perangkat firewall FortiGate adalah analisa log pada fitur intrusion prevention.

Date/Time	Severity	Source	Protocol	Action	Attack Name
05-04 13:58		104.17.166.186	tcp	dropped	WebRTC.Local.IP.Addresses.Disclosure
05-04 13:31		104.17.167.186	tcp	dropped	WebRTC.Local.IP.Addresses.Disclosure
05-04 13:31		104.17.167.186	tcp	dropped	WebRTC.Local.IP.Addresses.Disclosure
05-02 18:06		104.17.166.186	tcp	dropped	WebRTC.Local.IP.Addresses.Disclosure
05-02 18:06		104.17.166.186	tcp	dropped	WebRTC.Local.IP.Addresses.Disclosure
04-26 10:48		104.26.5.218	tcp	dropped	WebRTC.Local.IP.Addresses.Disclosure
04-26 10:48		104.26.5.218	tcp	dropped	WebRTC.Local.IP.Addresses.Disclosure
04-26 10:47		104.26.5.218	tcp	dropped	WebRTC.Local.IP.Addresses.Disclosure
04-26 09:45		104.26.5.218	tcp	dropped	WebRTC.Local.IP.Addresses.Disclosure
04-26 09:41		104.26.5.218	tcp	dropped	WebRTC.Local.IP.Addresses.Disclosure
04-26 09:28		104.26.5.218	tcp	dropped	WebRTC.Local.IP.Addresses.Disclosure
04-13 10:05		104.17.166.186	tcp	dropped	WebRTC.Local.IP.Addresses.Disclosure
04-13 10:04		104.17.166.186	tcp	dropped	WebRTC.Local.IP.Addresses.Disclosure
04-12 20:53		10.70.77.186	tcp	dropped	Quest.NetVault.Backup.Multipart.Request.Header.Buffer.Overflow
04-12 20:53		10.70.77.186	tcp	dropped	Quest.NetVault.Backup.Multipart.Request.Header.Buffer.Overflow
04-12 19:50		10.70.77.244	tcp	dropped	Quest.NetVault.Backup.Multipart.Request.Header.Buffer.Overflow
04-12 19:50		10.70.77.244	tcp	dropped	Quest.NetVault.Backup.Multipart.Request.Header.Buffer.Overflow
04-07 00:47		104.17.166.186	tcp	dropped	WebRTC.Local.IP.Addresses.Disclosure
04-06 14:14		10.70.76.73	tcp	dropped	Quest.NetVault.Backup.Multipart.Request.Header.Buffer.Overflow
04-06 14:14		10.70.76.73	tcp	dropped	Quest.NetVault.Backup.Multipart.Request.Header.Buffer.Overflow
03-31 20:27		104.17.166.186	tcp	dropped	WebRTC.Local.IP.Addresses.Disclosure
03-31 20:27		104.17.166.186	tcp	dropped	WebRTC.Local.IP.Addresses.Disclosure
03-26 10:15		104.17.167.186	tcp	dropped	WebRTC.Local.IP.Addresses.Disclosure
03-26 10:15		104.17.167.186	tcp	dropped	WebRTC.Local.IP.Addresses.Disclosure
03-10 19:30		104.17.167.186	tcp	dropped	WebRTC.Local.IP.Addresses.Disclosure
03-10 17:35		104.17.167.186	tcp	dropped	WebRTC.Local.IP.Addresses.Disclosure
03-10 17:35		104.17.167.186	tcp	dropped	WebRTC.Local.IP.Addresses.Disclosure
03-10 17:35		104.17.167.186	tcp	dropped	WebRTC.Local.IP.Addresses.Disclosure
02-27 01:12		10.70.152.131	tcp	detected	TCP.Split.Handshake

Gambar 6. Log Intrusion Prevention

Application

Protocol	tcp
Service	HTTP

Action

Action	dropped
Policy	6

Security

Level	
Threat Level	critical
Threat Score	50

Intrusion Prevention

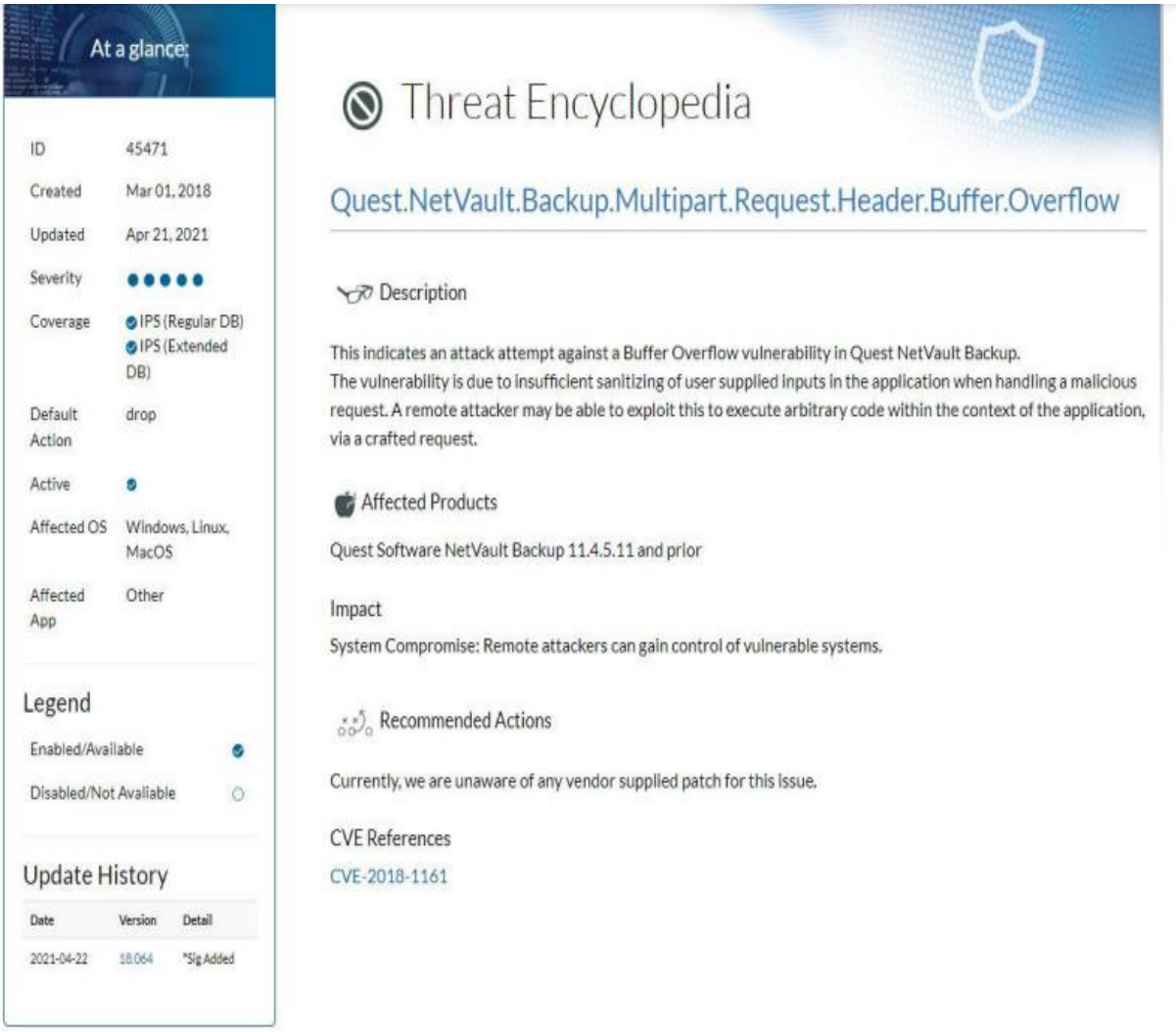
Profile Name	default
Attack Name	Quest.NetVault.Backup.Multipart.Req
Attack ID	45471
Reference	http://www.fortinet.com/ids/VID4547
Incident Serial No.	1539731185
Direction	outgoing
Severity	
Message	applications3: Quest.NetVault.Backup.Multipart.Req

Other

Source Interface Role	undefined
_pcap_id	45471
Destination Interface Role	wan
Event Type	signature
Protocol Number	6
Log ID	16384
Sub Type	ips
Log original timestamp	1618235639

Gambar 7. Detail salah satu Log Intrusion Prevention

Gambar 7 adalah tampilan log dari fitur *intrusion prevention*, analisa yang dilakukan adalah dengan melihat info lebih detail, seperti jenis serangannya (attack name), *action* yang dilakukan *firewall*, *threat level* (tingkat bahaya dari virus tersebut), *source address* dan *service*. Info detail virus tersebut bisa kitadapatkan dari detail *log* pada *firewall* dan *reference* dari website fortigate (www.fortiguard.com).

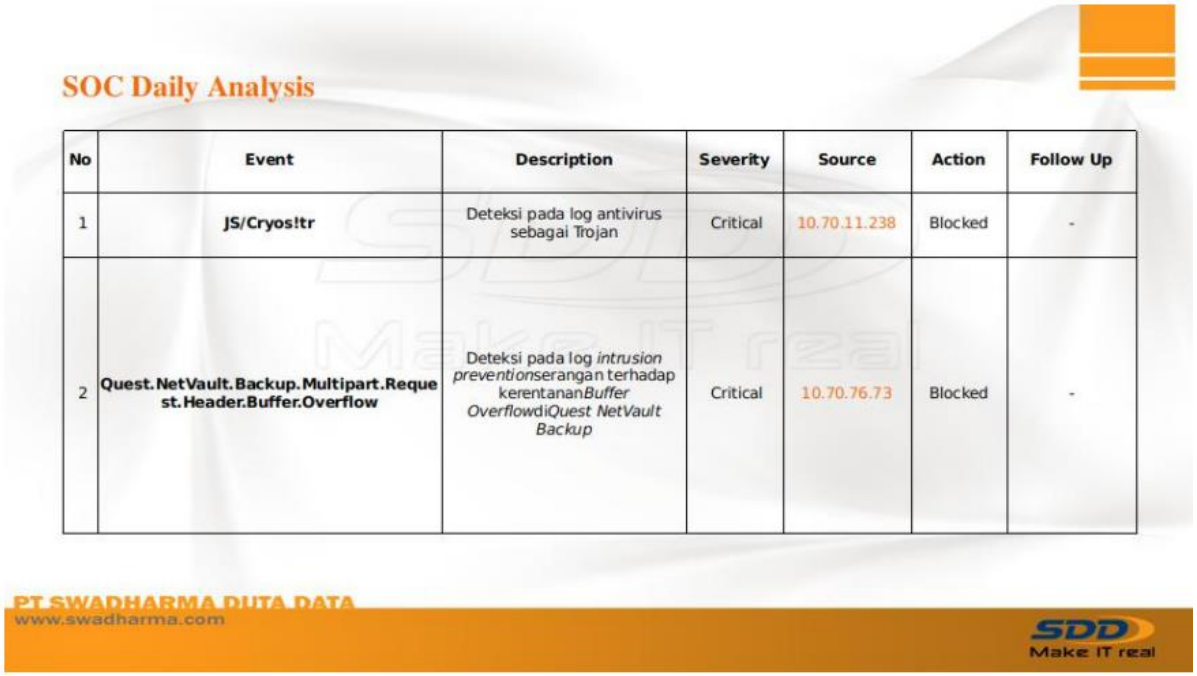


Gambar 8. Threat Ensiklopedia fortiguard.com

Berdasarkan gambar diatas dapat dilaporkan detail dari threat Quest.NetVault.Backup. Multipart.Request.Header.Buffer.Overflow adalah sebuah upaya serangan terhadap kerentanan Buffer Overflow di Quest NetVault Backup. Kerentanan ini disebabkan oleh sanitasi yang tidak memadai dari input yang diberikan pengguna dalam aplikasi saat menangani permintaan berbahaya. Penyerang jarak jauh mungkin dapat memanfaatkan ini untuk mengeksekusi kode arbitrer dalam konteks aplikasi, melalui permintaan yang dibuat.

3.4. Insiden Respon & Report

Pada sub-bab ini Tim SOC akan membuat laporan analisa harian dari beberapa event jika ada *alert* atau *log* dari perangkat *firewall fortigate*. Bentuk laporan yang dibuat seperti gambar dibawah ini:



SOC Daily Analysis

No	Event	Description	Severity	Source	Action	Follow Up
1	JS/Cryos!tr	Deteksi pada log antivirus sebagai Trojan	Critical	10.70.11.238	Blocked	-
2	Quest.NetVault.Backup.Multipart.Request.Header.Buffer.Overflow	Deteksi pada log *intrusion prevention*serangan terhadap kerentanan*Buffer Overflow*di*Quest NetVault Backup*	Critical	10.70.76.73	Blocked	-

Gambar 10. Laporan Analisa Harian

Keterangan gambar:

Event : Nama malware atau jenis serangan.
Description : Deskripsi dari jenis malware atau jenis serangan.
Severity : Tingkat bahaya dari malware atau jenis serangan.
Source : Alamat perangkat sumber malware atau serangan yang terdeteksi.
Action : Tindakan yang dilakukan oleh Fortigate terhadap malware atau jenis serangan tersebut, apakah blocked atau allow.
Follow Up : Saran atau tindakan yang perlu dilakukan jika ada malware atauserangan yang dampaknya sangat berbahaya dan harus diatasi secepatnya.

4. SIMPULAN

Dari pembahasan yang telah dipaparkan, maka dapat di tarik kesimpulan dengan mengimplementasikan perangkat *firewall FortiGate* sistem jaringan komputer internal PT. Swadharma Duta Data lebih aman dalam mengantisipasi terkena malware. Tim *Security Operational Center* (SOC) dapat dengan lebih mudah dan cepat mendeteksi ancaman keamanan siber pada jaringan komputer internal.

DAFTAR PUSTAKA

Imami Nur Rachmawati. (2017). Pengumpulan Data Dalam Penelitian Kualitatif: Wawancara. Retrieved 26 April 2021 from https://media.neliti.com/media/publications/105145-ID-pengumpulan-data-dalam-penelitian-kualit.pdf

Maurits Radhiyya, Ahmad. (2011). Bagaimana Cara Kerja Firewall. retrieved 20 Mei 2021 from https://www.scribd.com/doc/59527010/Bagaimana-Cara-Kerja-Firewall#download

Karpen. (2012). Pengamanan Sistem Jaringan Komputer dengan Teknologi Firewall. Jurnal Sains dan Teknologi Informasi, Vol. 1, No. 1, Juni 2012.

Kurniawan, Hendra, Sandy Kosasi. (2015). Penerapan Network Development Life Cycle Dalam Perancangan Intranet Untuk Mendukung Proses Pembelajaran. Jurnal Ilmiah SISFOTENIKA Vol.x, No. x, Juli 2015.

Pratama Putra, Pandu. (2016). Pengembangan Sistem Keamanan Jaringan Menggunakan Rumusan Snort Rule (Hids) untuk Mendeteksi Serangan Nmap. SATIN - Sains dan Teknologi Informasi, Vol. 2, No. 1, Juni 2016.

Sugiyono. (2016). Metode Penelitian Kuantitatif, Kualitatif dan R&D. Bandung: PT Alfabet.

Surya Aprihansah, Iwan Krisnadi. (2016). Analisis Next Gen Firewall Pada Perangkat Fortigate. Program Studi Magister Teknik Elektro, Fakultas Teknik Universitas Mercu Buana.