fundamental **management journal**
FUNDAMENTAL MANAGEMENT JOURNAL **ISSN: 2540-9220 (online)** Volume: 5 No 1. 2020

Implementasi dan Analisis Sistem Monitoring Networking Internet Dengan Hardware Hillstone Di Universitas Kristen Indonesia

Implementation and Analysis of Internet Networking Monitoring System with Hillstone Hardware at Indonesian Christian University

Rutman Lumbantoruan
rutman.toruan@uki.ac.id

Fakultas Ekonomi dan Bisnis, Universitas Kristen Indonesia

Jakarta, Indonesia

Abstract

Computer Internet Network Monitoring is a computer system managing activity connected to many servers in an organization. This monitoring system is used to help adjusting and monitoring server network continuously. Internet connection monitoring has benefit in bandwidth usage monitoring for every user, either it is being used or not. Network monitoring is created by installing Hillston Hardware in Information System Implementation Unit. A trouble usually happened when slow loading time occurred in online registration hence error network in consequence. A result obtained after Hillstone Hardware implementation is centre of data staffs could detect network trouble and simplify its handling. Hillstone is reliable to monitor undergoing internet data services in user and network, also activates warning system to user connecting to improper internet network or bandwidth.

Keywords: Monitoring, Internet connection analysis, Hillstone, server, bandwidth

PENDAHULUAN

Untuk mendeteksi pengguanaan *network Internet* dan alokasi penggunaan *Badwith* serta prilaku konsumen dalam penggunaan layanan internet yang di sediakan oleh organisasi perlu dianalisis data yang sangat penting bagi tugas audit system dan audit prilaku konsumen, jadi untuk analisis dalam pekerjaan tersebut sangat dibutuhkan. Pemasangan hardware atau perangkat yang dapat membantu membuat laporan secara otomatis sesuai dengan instruksi yang diberikan kepada alat yang di sebut Hillstone . *Administrator* jaringan *dengan* bantuan *hardware* Hillstone dapat mendeteksi bentuk bentuk layananan,prilaku konsumen,gangguan,user yang terkoneksi yang menggunakan segala fasilitas jaringan penggunaan Badwith, sehingga dapat memaksimalkan menjaga pelayanan yang maksimal dalam penggunaan kelancaran jaringan. Jika layanan jaringan mengalami gangguan terkait dengan gangguan, meskipun dengan jangka waktu yang singkat, maka segera dapat dipastikan produktivitas dalam suatu organisasi akan memberikan dampak yang tidak baik dalam pelayanan.,untuk departemen pelayanan teknis di departemen layanan publik kemampuan untuk menyediakan layanan sangat penting. Oleh karena itu diperlukan sebuah fasilitas pendukung yaitu sistem *monitoring* agar *administrator Networking* dapat mendeteksi jaringan (Rasyid, 2011). Salah satu aplikasi *monitoring* trafik jaringan dengan menggunakan Hillstone

Hillstone merupakan salah satu perangkat komputer yang dapat digunakan sebagai alat untuk monitoring jaringan computer yang terkoneksi ke internet. Sistem operasi tersebut mencakup berbagai fitur lengkap untuk *wireline* dan *wireless*, salah satunya adalah *monitoring* jaringan. Dengan fitur-fitur yang terdapat dalam perangkat. Pihak perusahaan dalam hal ini *admin* dapat mendeteksi dan menganalisis penggunaan badwith *inbound* dan *outbound* sehingga dapat melakukan tindakan untuk segala yang dapat memberikan dampak yang tidak baik terhadap kelancaran jaringan internet dalama pelayanan. Report yang dapat di tampilakan *tool graph* yang dimiliki oleh Hillstone untuk *monitoring* badwith,user terkoneksi, dimana dengan pemasangan hardware Hillstone fitur tersebut dapat di informasikan *Staft* bagian Teknologi Informasi yang sudah terlatih untuk mengoperasikan serta dapat melihat trafik secara *real time* . Dalam penelitan ini *monitoring* trafik dilakukan dengan menggunakan teknik *Router Based.* Dan tidak hanya trafik yang dapat di-*monitor*, *admin* pun dapat me-*monitoring* utilisasi dari perangkat tersebut seperti *CPU, Disk dan Memory Usage.*

TINJAUAN PUSTAKA

Teknik Analisa dan *Monitoring*

Analisis jaringan adalah proses menangkap lalu lintas jaringan dan memeriksanya secara cermat untuk mengetahui apa yang terjadi pada jaringan. (Orebaugh, 2006). Dua teknik *monitoring* jaringan dibagi menjadi 2 bagian yaitu: *Router Based* dan *Non-Router*. Berdasarkan fungsi pemantauan yang dibangun di dalam *router* itu sendiri dan tidak memerlukan perangkat keras atau perangkat lunak tambahan disebut sebagai teknik berbasis *Router*. Sedangkan teknik berbasis *non-Router* memerlukan perangkat keras dan perangkat lunak tambahan, dipasang dan memberikan fleksibilitas yang lebih besar. (Anagnostakis, K.G, 2002).

Hillstone merupakan hardware untuk menganalisis user-user pengguna setiap user telah diklasifikasikan dan dikarakterisasi berdasarkan multiple dimensi dan identifikasi serta menggambarkan tindakan, user. Dengan alat Hilstone ini dalam lingkungan jaringan internet, dianalisis sejuta sampel malware yang dapat di Identifikasi "dikenal". , dikarakterisasi dan diklasifikasikan.,dibandingkan dengan database sampel malware yang sudah teridentifikasi yang sudah dianalisis. Sampel yang tidak diketahui cocok dengan sampel yang diketahui - semakin tinggi tingkat kepercayaannya bahwa varian dari sampel malware yang dikenal. Proses ini disebut "pengelompokan statistik" dan memberikan hasil yang akurat metode untuk mengidentifikasi malware baru.

Deteksi Perilaku Pengguna jaringan Internet,badwith Internet

Untuk mendeteksi perilaku User-user pengguna Internet Hillstone terus memantau jaringan untuk mempelajari seperti apa trafik jaringan normal dari hari ke hari dan bulan, dan memberikan peringatan saat aktivitas jaringan melebihi ambang batas yang dihitung. Ini menggunakan 50+ array dimensi untuk menghitung lalu lintas jaringan normal dari lapisan L4-L7, yang disebut "**pemodelan perilaku**." Selain itu, sudah tersedia dengan alat peretasan nyata untuk memastikan bahwa alat dapat membaca mengenali aktivitas berbahaya. Teknik-teknik ini membatasi pengguna memberi peluang dan menghentikan serangan..

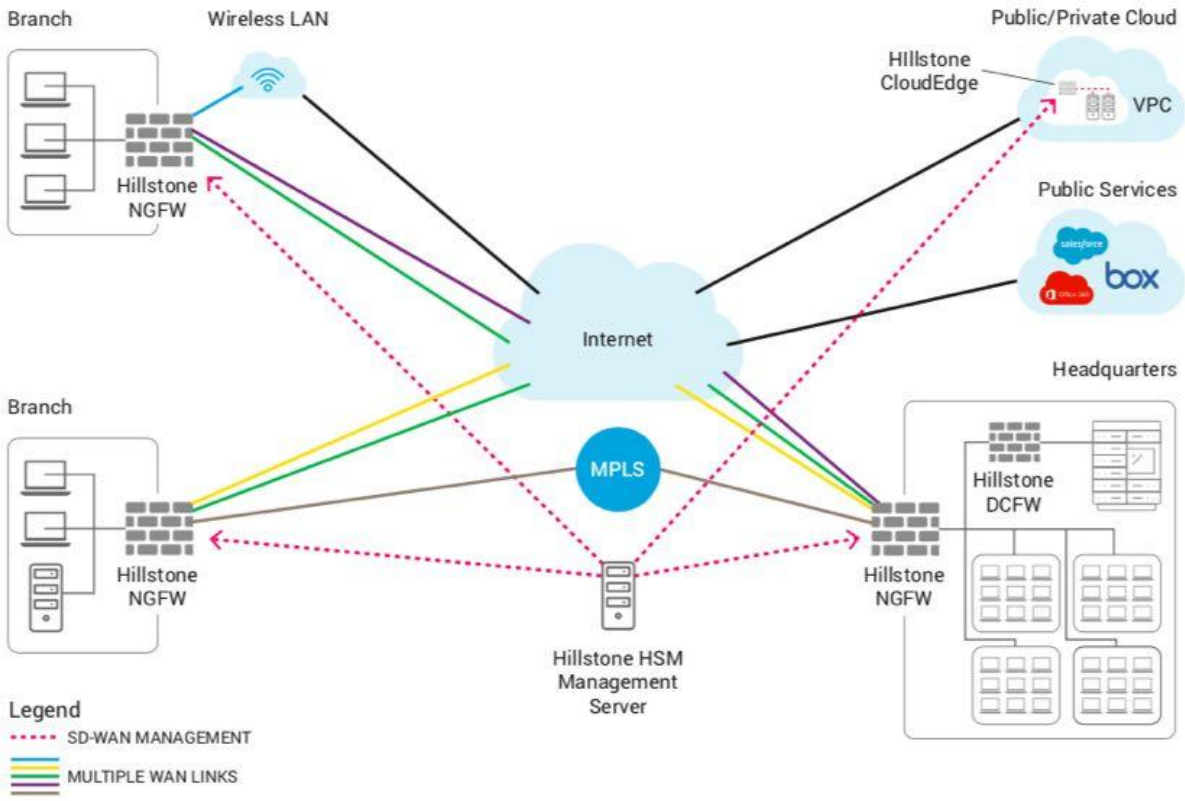
Analisis Forensik Dengan Hislstone

Hillstone memberikan cara baru untuk memvisualisasikan dan menganalisis serangan. Setiap tindakan diambil oleh kode yang berpotensi berbahaya secara otomatis dikaitkan ke langkah-langkah dalam "Bunuh Rantai". Dengan informasi forensik yang kaya yang memungkinkan analis keamanan untuk menentukan asal dari serangan dan resiko dari serangan. Metodologi yang digunakan. menyediakan file paket capture, yang, ketika terikat dengan syslog dan traffic log, administrator *Networking* akan memberikan informasi, data pengguna seperti situs web yang dikunjungi, aplikasi yang digunakan, tingkat risiko aplikasi. Paling penting, Hillstone mengidentifikasi kebijakan firewall yang tepat yang memungkinkan penyerang untuk melewati firewall.

Mitigasi Preemptive

Selain kemampuan untuk membuat perubahan kebijakan untuk mencegah serangan, Hillstone memiliki beberapa mitigasi otomatis bawaan fitur. Fitur-fitur ini terdiri dari templat yang telah ditentukan yang secara otomatis memperlambat atau memblokir serangan jika perilaku serangan terdeteksi. Administrator dapat memodifikasi template untuk membatasi bandwidth atau jumlah rekap sesi penyerang. Dan dapat mempersiapkan dan menyesuaikan terhadap kendala sumber daya jaringan berdasarkan pada jenis serangan. Dalam kasus di mana serangan kritis dan tingkat kepercayaan tinggi, mitigasi dapat mencakup lengkap penyumbatan semua sumber daya jaringan. Dan, jika templat tidak ada atau tidak aktif, administrator dapat dengan cepat mengatur mitigasi sementara untuk penyerangan tersebut.

Fitur Intalasi



Analisis Korelasi Ancaman

- Korelasi antara ancaman yang belum diketahui/terdeteksi, abnormal perilaku dan perilaku aplikasi untuk ditemukan ,potensi ancaman atau serangan
- Aturan korelasi multi-dimensi

Deteksi Ancaman Tingkat Lanjut

- Deteksi malware tingkat lanjut yang berbasis perilaku
- Deteksi diketahui dan tidak diketahui,dari malware termasuk Virus, Worm, Trojan dan lainya
- Model perilaku malware, real-time, online,pembaruan basis data

Deteksi Perilaku Abnormal

- Pemodelan perilaku berdasarkan lalu lintas dasar L3-L7 untuk mengungkapkan perilaku jaringan yang tidak normal, seperti Pemindaian HTTP, Spider, SPAM, SSH / FTP lemahnya kata sandi
- Deteksi DDoS termasuk Flood, Sockstress, zip of death, reflect, permintaan DNS, SSL DDos dan aplikasi DDoS
- Mendukung inspeksi lalu lintas tunneling terenkripsi untuk aplikasi yang tidak dikenal
- Mendeteksi serangan C&C menggunakan Generasi Domain Algoritma (DGA)
- Real-time, online, model perilaku abnormal pembaruan basis data.

Visibilitas Ancaman dan Mitigasi

- Indeks risiko jaringan, aset penting, dan risiko host status, host dan keparahan risiko ancaman dan kepastian
- Menghapus pemetaan rantai kejadian ancaman pada setiap host
- Aturan *mitigasi* yang telah ditentukan dan disepakatin dalam standard organsasi
- Membuat daftar ancaman.

Layanan Jaringan

- Rute Network dikendalikan dari aplikasi
- DHCP, NTP, Server DNS dan proksi DNS

Firewall

- Mode operasi: NAT / rute, transparan (jembatan),dan mode campuran
- Objek kebijakan: sudah ditentukan sebelumnya, khusus, dan objek pengelompokan
- Kebijakan keamanan berdasarkan aplikasi, peran dan lokasi geografis
- Gateway Tingkat Aplikasi dan dukungan sesi: MSRCP, PPTP, RAS, RSH, SIP, FTP, TFTP, HTTP,dcerpc, dns-tcp, dns-udp, H.245 0, H.245 1, H.323
- Dukungan NAT dan ALG: NAT46, NAT64, NAT444, SNAT, DNAT, PAT, NAT Cone Penuh, STUN
- Konfigurasi NAT: sesuai kebijakan dan NAT
- VoIP: SIP / H.323 / SCCP NAT traversal, pin RTP Holing
- Pandangan manajemen kebijakan global
- Inspeksi redundansi kebijakan keamanan, kebijakan grup, kembalikan konfigurasi kebijakan
- Analisis kebijakan dan pembersihan kebijakan yang tidak valid
- Kebijakan DNS yang komprehensif
- Jadwal: satu kali dan berulang

Pencegahan intruksi

• Protokol deteksi anomali, deteksi berbasis tingkat,tanda tangan kustom, manual, push otomatis atau tarik pembaruan tanda tangan, ancaman terintegrasi encyclo-pedia
• Tindakan IPS: default, monitor, blokir, reset (IP penyerang atau IP korban, antarmuka masuk) dengan waktu kedaluwarsa
• Opsi pendataan paket
• Pemilihan Berbasis Filter: OS, aplikasi atau protokol
• Pembebasan IP
• mode sniffer IDS
• Proteksi DoS berbasis tingkat IPv4 dan IPv6 dengan pengaturan toleransi terhadap koneksi TCP Syn, TCP /Pemindaian port UDP / SCTP
• Pemintas aktif dengan antarmuka pemintas
• Konfigurasi pencegahan yang telah ditentukan sebelumnya

Anti Virus

• Pembaruan manual, push otomatis.
• Antivirus berbasis aliran: protokol termasuk HTTP,SMTP, POP3, IMAP, FTP / SFTP
• Identifikasi virus file terinfeksi

Serang Pertahanan

• Protokol pertahanan serangan abnormal
• Anti-DoS / DDoS, termasuk SYN Flood, DNS Query
• Pertahanan serangan ARP

Penyaringan URL

• Inspeksi penyaringan web berbasis aliran
• Penyaringan web yang ditentukan secara manual berdasarkan URL, web konten dan header MIME
• Penyaringan web dinamis dengan real-time berbasis cloud basis data kategorisasi: lebih dari 140 juta URL dengan 64 kategori (8 di antaranya terkait keamanan)
• Fitur penyaringan web tambahan:
- Filter Java Applet, ActiveX atau cookie
- Blokir Posting HTTP
- Log kata kunci pencarian
- Memberi tanda koneksi terenkripsi aktif kategori tertentu untuk privasi

• Penimpaan profil pemfilteran web: memungkinkan administrator untuk sementara menetapkan profil yang berbeda untuk pengguna /grup / IP
• Filter web kategori lokal

Anti-Spam

• Klasifikasi dan Pencegahan Spam Real-time
• Spam Terkonfirmasi, Spam Yang Diduga, Spam Massal,Massal yang Valid
• Perlindungan isi pesan
• Mendukung protokol email SMTP dan POP3
• Deteksi masuk dan keluar
• Daftar email yang resmi dari domain tepercaya.

Cloud-Sandbox

• Unggah file berbahaya ke cloud sandbox untuk dianalisis
• Protokol dukungan termasuk HTTP / HTTPS, POP3,IMAP, SMTP dan FTP
• Jenis file Dukungan termasuk PE, ZIP, RAR, Office,PDF, APK, JAR dan SWF
• Arah transfer file dan kontrol ukuran file
• Berikan laporan analisis perilaku lengkap untuk file berbahaya
• Pembagian intelijen ancaman global, ancaman waktu-nyata pemblokiran
• Mendukung mode deteksi saja tanpa mengunggah file

Pencegahan C&C Botnet

• Temukan host botnet intranet dengan memonitor C&C koneksi dan blok ancaman lanjutan lebih lanjut seperti botnet dan ransomware
• Perbarui alamat server botnet secara teratur
• Pencegahan untuk C&C IP dan domain
• Mendukung deteksi lalu lintas TCP, HTTP, dan DNS
• Daftar putih IP dan domain

Reputasi IP

• Identifikasi dan filter lalu lintas dari IP berisiko seperti host botnet, pengirim spam, simpul Tor, dilanggar host, dan serangan brute force
• Logging, menjatuhkan paket, atau memblokir berbagai jenis lalu lintas IP berisiko
• Peningkatan basis data tanda tangan reputasi IP regular

Dekripsi SSL

• Identifikasi aplikasi untuk lalu lintas terenkripsi SSL
• Pemberdayaan IPS untuk lalu lintas terenkripsi SSL
• Pemberdayaan AV untuk lalu lintas terenkripsi SSL
• Filter URL untuk lalu lintas terenkripsi SSL

• Daftar putih lalu lintas terenkripsi SSL
• Mode pembongkaran proxy proxy

Identifikasi dan Kontrol Titik Akhir

• Dukungan untuk mengidentifikasi IP titik akhir, jumlah titik akhir,waktu on-line, waktu off-line, dan durasi on-line
• Mendukung 10 sistem operasi termasuk Windows,iOS, Android, dll.
• Permintaan dukungan berdasarkan IP, jumlah titik akhir,kontrol kebijakan dan status dll.
• Mendukung identifikasi titik akhir yang diakses kuantitas melintasi lapisan 3, logging dan interferensi pada overrun IP
• Redirect tampilan halaman setelah gangguan kustom operasi
• Mendukung operasi pemblokiran pada IP overrun

Keamanan data

• Kontrol transfer file berdasarkan jenis file, ukuran dan nama
• Identifikasi protokol file, termasuk HTTP, FTP,SMTP dan POP3
• Mengajukan tanda tangan dan identifikasi akhiran untuk lebih dari 100 jenis file
• Identifikasi Intermet Manajemen dan audit perilaku jaringan
• Memfilter file yang dikirim oleh HTTPS menggunakan Proxy SSL

Kontrol Aplikasi

• Lebih dari 3.000 aplikasi yang dapat difilter oleh nama, kategori, subkategori, teknologi dan risiko
• Setiap aplikasi berisi deskripsi, risiko

Kualitas Layanan

• Terowongan bandwidth maks / terjamin atau IP / pengguna Dasar
• Alokasi terowongan berdasarkan domain keamanan, antarmuka, alamat, grup pengguna / pengguna, server / server grup, grup aplikasi / aplikasi, KL, VLAN
• *Bandwidth* yang dialokasikan berdasarkan waktu, prioritas, atau sama berbagi bandwidth
• Jenis Layanan (KL) dan Layanan Berbeda (DiffServ) dukungan
• Alokasi bandwidth yang tersisa diprioritaskan
• Koneksi bersamaan maksimum per IP
• Alokasi bandwidth berdasarkan kategori URL
• Batas bandwidth dengan menunda akses untuk pengguna atau IP
• Pembersihan kedaluwarsa otomatis dan pembersihan manual lalu lintas yang digunakan pengguna

Server Load Balancing
• hashing berbobot, koneksi-terbobot, dan round-robin tertimbang
• Perlindungan sesi, kegigihan sesi dan pemantauan status sesi

• Pemeriksaan kesehatan server, pemantauan sesi dan perlindungan sesi

Tautan Penyeimbangan Beban

• Penyeimbangan beban tautan dua arah
• Perimbangan beban tautan keluar mencakup kebijakan Routing berbasis, ECMP dan tertimbang, tertanam Perutean ISP dan deteksi dinamis
• Penyeimbangan beban tautan masuk mendukung SmartDNS dan deteksi dinamis
• Peralihan tautan otomatis berdasarkan bandwidth,latensi, jitter, konektivitas, aplikasi dll.
• Tautkan inspeksi kesehatan dengan ARP, PING, dan DNS

VPN

• IPSec VPN:
- Mode IPSEC Phase 1: ID agresif dan utama mode perlindungan
- Opsi penerimaan teman: ID apa saja, ID spesifik, ID dalam grup pengguna dialup
- Mendukung IKEv1 dan IKEv2 (RFC 4306)
- Metode otentikasi: sertifikat dan kunci yang dibagikan sebelumnya
- Dukungan konfigurasi mode IKE (sebagai server atau klien)
- DHCP melalui IPSEC
- Masa berlaku kunci enkripsi IKE yang dapat dikonfigurasi, NAT traversal menjaga frekuensi tetap hidup
- Enkripsi Proposal Tahap 1 / Tahap 2: DES,3DES, AES128, AES192, AES256
- Otentikasi Proposal Tahap 1 / Tahap 2:MD5, SHA1, SHA256, SHA384,SHA512
- Fase 1 / Fase 2 Dukungan Diffie-Hellman: 1,2,5
- XAuth sebagai mode server dan untuk pengguna dialup
- Deteksi rekan sebaya yang mati
- Autokey tetap hidup untuk Fase 2 SA

• Dukungan ranah IPSEC VPN: memungkinkan banyak kustom Login VPN SSL yang terkait dengan grup pengguna (URL jalur, desain)
• Opsi konfigurasi VPN IPSEC: berbasis rute atau berbasis kebijakan
• Mode penyebaran IPSEC VPN: gateway-to-gateway, full mesh, hub-and-spoke, redun dan terowongan, penghentian VPN dalam mode transparan • Satu kali login mencegah masuk bersamaan dengan nama pengguna yang sama
• Pembatasan pengguna bersamaan portal SSL
• Modul penerusan port SSL VPN mengenkripsi klien data dan mengirimkan data ke server aplikasi
• Mendukung klien yang menjalankan iOS, Android, dan Windows XP / Vista termasuk OS Windows 64-bit
• Pemeriksaan integritas host dan pemeriksaan OS sebelum Koneksi terowongan SSL
• Pemeriksaan host MAC per portal
• Opsi pembersihan cache sebelum mengakhiri SSL VPN sidang
• L2TP client dan mode server, L2TP over IPSEC,dan GRE atas IPSEC
• Melihat dan mengelola koneksi IPSEC dan SSL VPN
• PnPVPN

IPv6

• Manajemen atas IPv6, logging IPv6 dan HA
• Penerowongan IPv6, DNS64 / NAT64 dll
• IPS, Identifikasi Aplikasi, Antivirus, Akses kontrol, pertahanan serangan ND, iQoS
• Melacak deteksi alamat

VSYS

• Alokasi sumber daya sistem untuk setiap VSYS
• virtualisasi CPU
• VSYS non-root mendukung firewall, IPSec VPN, SSL VPN, IPS, pemfilteran URL
• Pemantauan dan statistik VSYS

Ketersediaan Tinggi

- Port, lokal & pemantauan tautan jarak jauh
- Kegagalan network internet negara
- Kegagalan kedua
- Pemberitahuan kegagalan
• Opsi penempatan:
-

Identitas Pengguna dan Perangkat

• Database pengguna lokal
• Otentikasi pengguna jarak jauh: TACACS +, LDAP,Radius, Aktif
• Sistem masuk tunggal: Windows AD
• otentikasi 2-faktor: dukungan pihak ke-3,token server terintegrasi dengan fisik dan SMS
• Kebijakan berbasis pengguna dan perangkat
• Sinkronisasi kelompok pengguna berdasarkan AD dan LDAP
• Dukungan untuk 802.1X, SSO Proxy
• Kustomisasi halaman WebAuth
• Otentikasi berbasis antarmuka
• ADSSO Agentless (Polling AD)
• Gunakan sinkronisasi otentikasi berdasarkan Monitor SSO
• Mendukung otentikasi pengguna berbasis MAC

Administrasi

• Akses manajemen: HTTP / HTTPS, SSH, telnet,menghibur
• Manajemen Pusat: Manajer Keamanan Hillstone (HSM), API layanan web

• Integrasi Sistem: SNMP, syslog, aliansi kemitraan
• Penyebaran cepat: USB auto-install, lokal dan eksekusi skrip jarak jauh
• Status dasbor real-time dinamis dan drill-in memonitor widget
• Dukungan bahasa: Inggris

Log & Pelaporan

• Fasilitas logging: memori dan penyimpanan lokal (jika tersedia), beberapa server syslog dan banyak Platform Hillstone Security Audit (HSA)
• Pencatatan terenkripsi dan integritas log dengan HAS mengunggah log bets terjadwal
• Pencatatan yang andal menggunakan opsi TCP (RFC 3195)
• Log lalu lintas terperinci: diteruskan, sesi dilanggar,lalu lintas lokal, paket tidak valid, URL dll.
• Log peristiwa komprehensif: sistem dan administrasi-audit aktivitas tratif, perutean & jaringan, VPN,otentikasi pengguna, acara terkait WiFi
• Opsi resolusi IP dan port layanan
• Opsi format log traffic singkat
• Tiga laporan yang telah ditentukan: Keamanan, Aliran dan Laporan jaringan
• Pelaporan yang ditentukan pengguna
• Laporan dapat diekspor dalam PDF, Word dan HTML via Email dan FTP

Statistik dan Pemantauan

• Aplikasi, URL, statistik peristiwa ancaman dan pemantauan
• Statistik dan analitik lalu lintas waktu-nyata
• Informasi sistem seperti sesi bersamaan,CPU, memori, dan suhu
• statistik dan pemantauan lalu lintas iQOS, status tautan pemantauan
• Mendukung pengumpulan informasi lalu lintas dan penerusan melalui Netflow (v9.0)

CloudView

• Pemantauan keamanan berbasis cloud
• Akses 24/7 dari aplikasi web atau seluler
• Status perangkat, lalu lintas, dan pemantauan ancaman
• Retensi dan pelaporan log berbasis cloud

Permasalahan Sistem Jaringan

1. Permasalahan pada jaringan server yang digunakan ,sebagai tempat pusat informasi sering tidak stabil koneksinya .
2. Sistem informasi dari setiap user, bila terjadinya maintenance tidak bisa diperbaiki dengan cepat dan kurangnya informasi.

Alternatif Pemecahan Masalah Dengan adanya monitoring server ini menggunakan hardware Hillstone untuk memonitoring keseluruhan jaringan di server jika ada maintenance pada jaringan tersebut bisa mengetahui dalam sistem monitoring sehingga bisa mengetahui informasi melalui

notifikasi handpohe via email. Skema jaringan server yang ada di Universitas Kristen Indonesia menggunakan topologi star yang menggunakan router, switch, TP-LINK, PC di ruang server, lab dan kantor. Di antaranya alur jaringan dari swicth tersebut sebagai berikut:

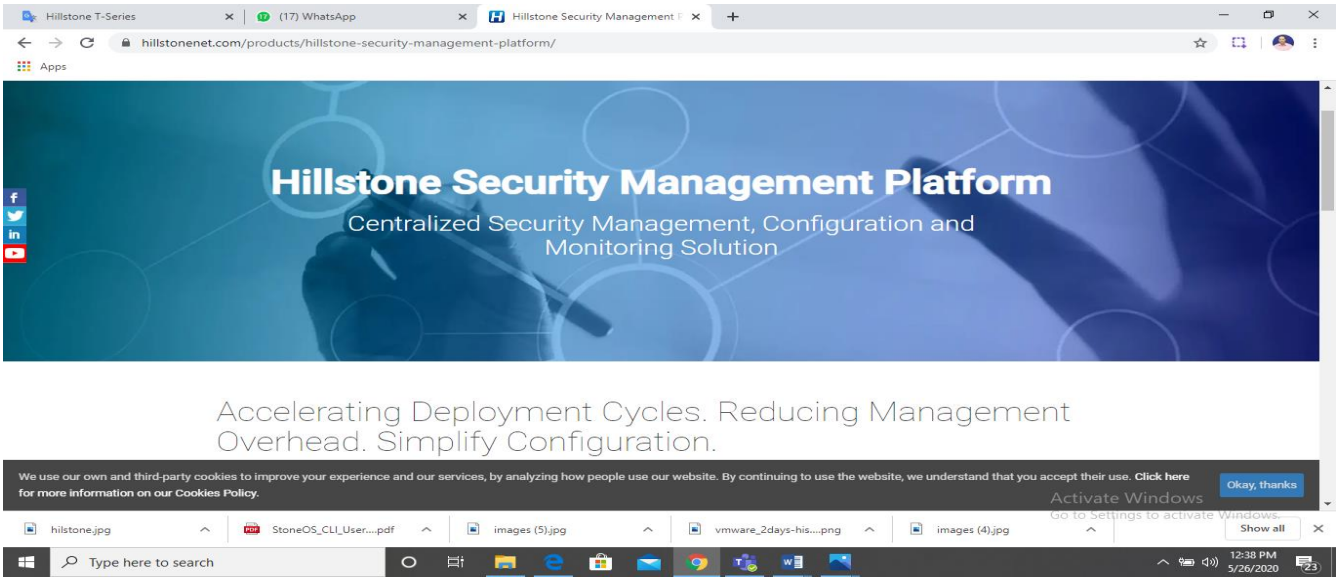
1. Router server menggunakan IP Address
2. Switch server menghubungkan jaringan komputer pada setiap user pengguna baik ruangan lab, kantor, ruangan akademik
3. Switch lab satu dan dua yang menghubungkan jaringan komputer lokal pada ruang lab letak switch ini berada di setiap unit.
4. Switch kantor menghubungkan khusus ruangan akademik, yang kemudian terpecah untuk jaringan kantor itu sendiri dan hotspot atau wifi yang bisa digunakan semua user mahasiswa,tenaga Kependidikan dan Tenaga Pendidik.

METODE PENELITIAN

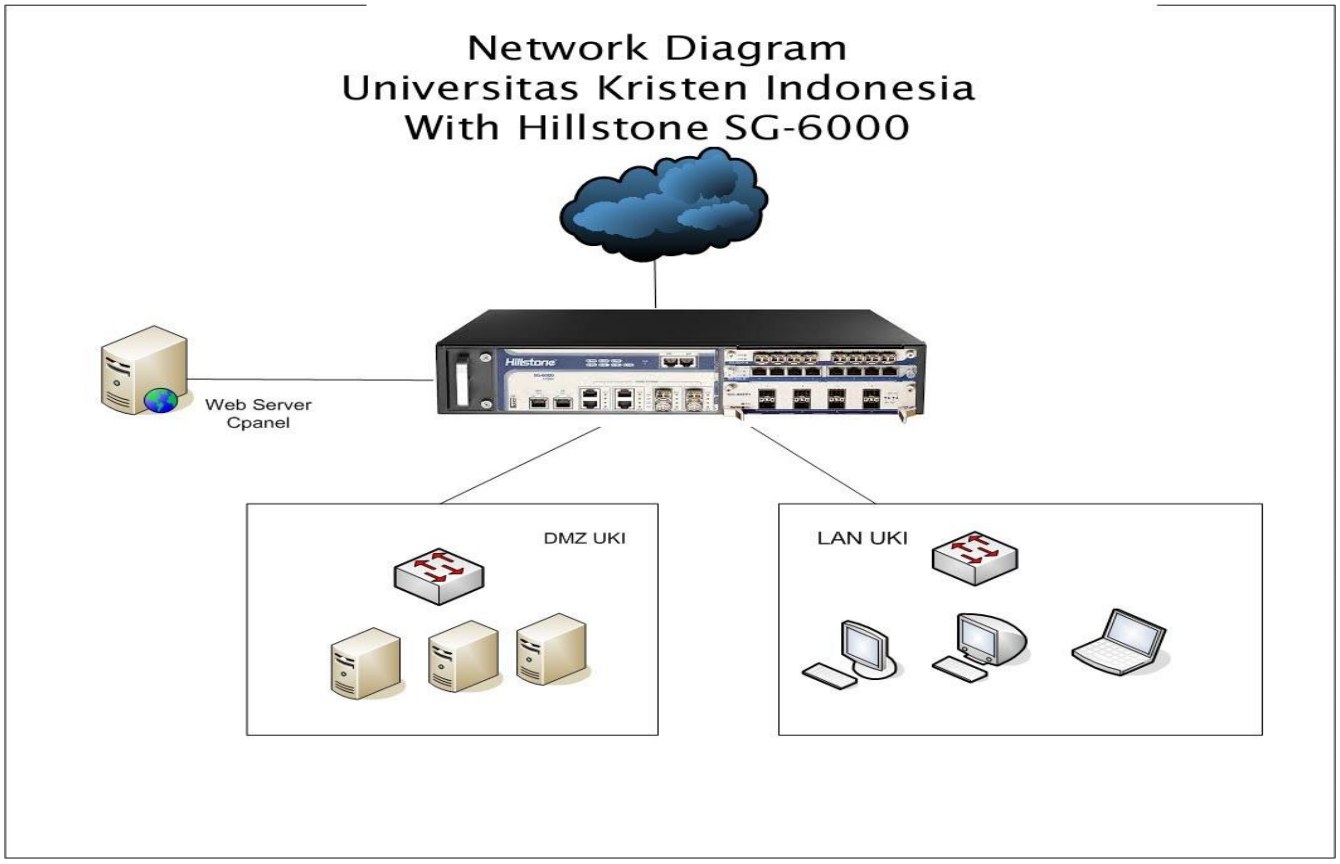
Metode pengembangan sistem yang digunakan dalam penelitian ini adalah NDLC (*Network Development Life Cycle*) yaitu suatu pendekatan proses dalam komunikasi data yang menggambarkan siklus yang tiada awal dan akhir dalam mengamati jaringan.

Tahapan untuk proses penelitian ini adalah dengan melakukan beberapa tahapan seperti :

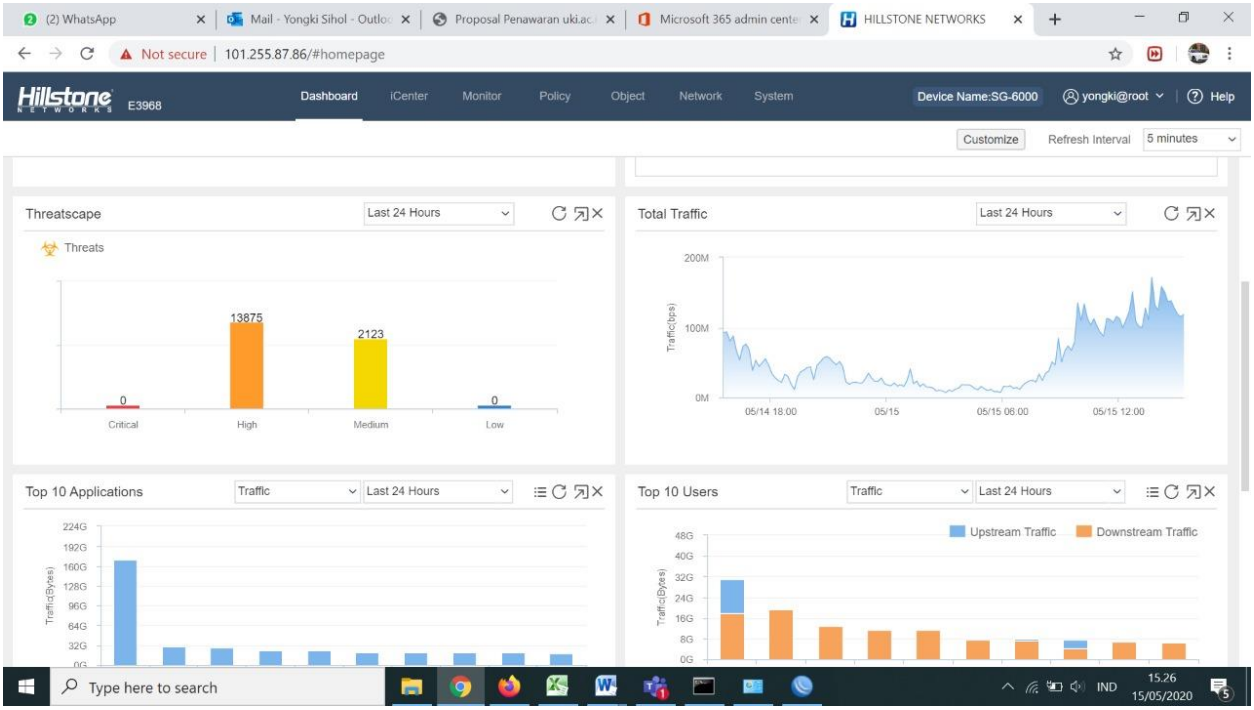
1. *Analysis*, menganalisa kebutuhan untuk melakukan penelitian permasalahan yang ada.
2. *Design*, rancangan topologi jaringan berikut jadwal melakukan *monitoring*
3. Implementasi berupa instalasi/*setting* perangkat yang diperlukan untuk proses *capturing* data
4. *Monitoring*, melakukan *monitoring incoming* dan *outgoing* trafik
5. Managemen , pengelolaan alokasi *bandwidth* jaringan yang sudah ditentukan sesuai dengan standard organiasasi



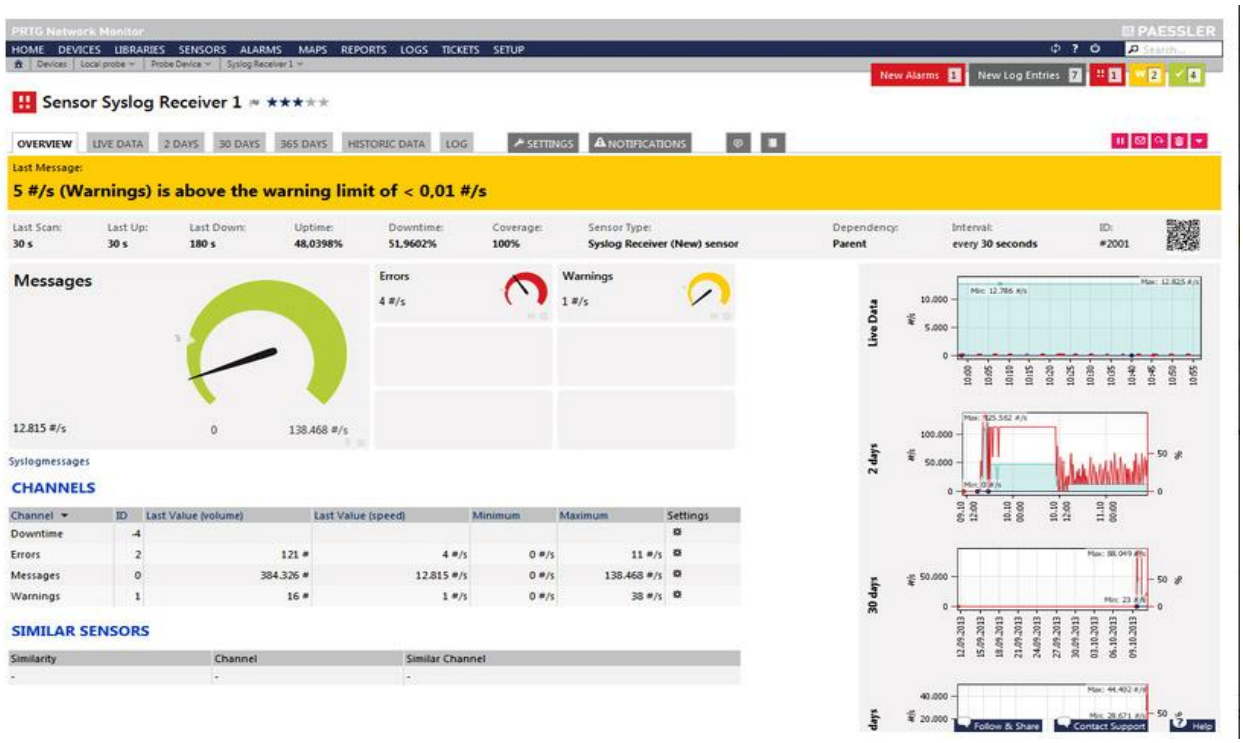
Hasil Penelitian dan Pembahasan



Hasil Monitoring Penggunaan Dengan Hillstone

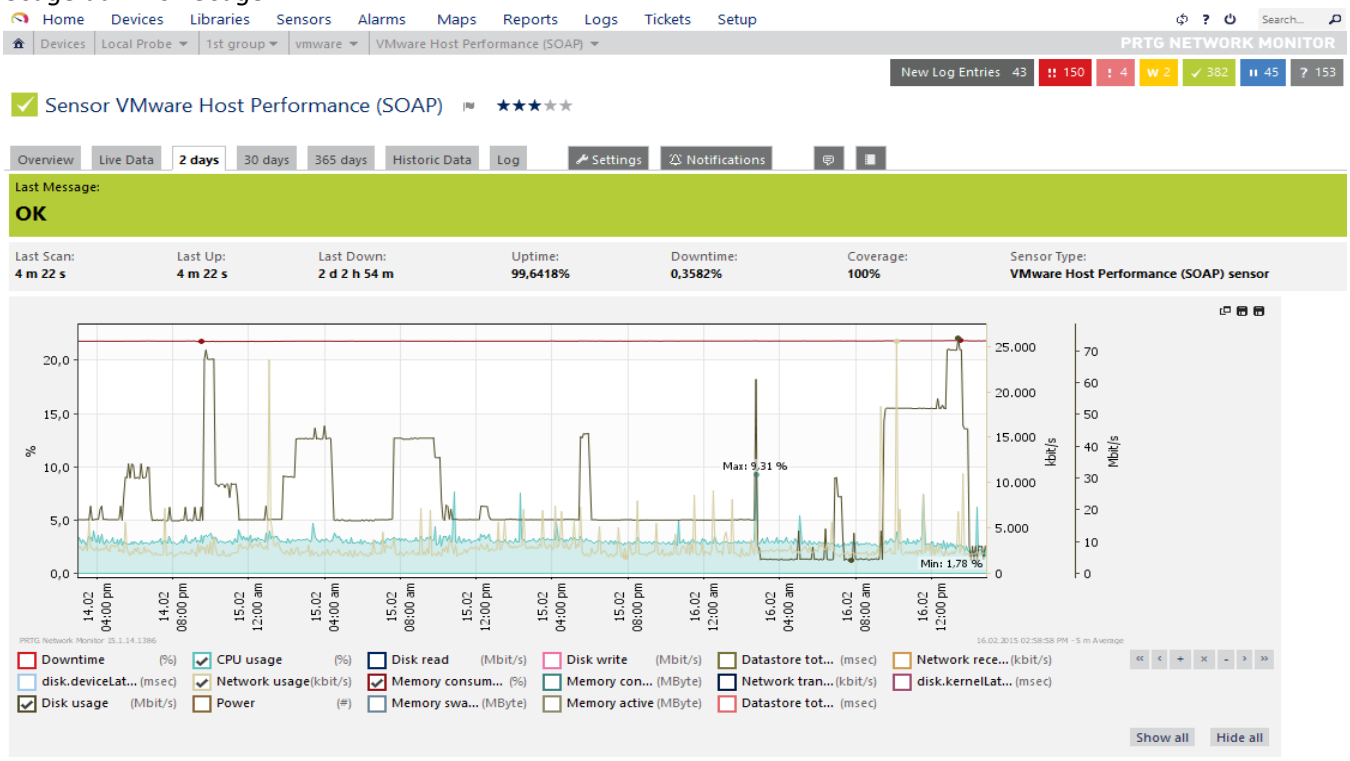


Hasil Monitoring Sensor Syslog dan Grafik



Hasil *Monitoring* dan Analisis Grafik

Laporan *monitoring* dilakukan harian dan mingguan yang meliputi *monitoring* trafik, *memory usage*. *CPU Usage* dan *Disk Usage*



Date Time	CPU usage	Disk read	Disk write	Datastore total ReadLatency	Network received	disk.deviceLatency	Network usage	Memory consumed (Percent)	Memory consumed
Averages (of 576 values)	3,04272569444445 %	23 Mbit/s	0,23 Mbit/s	0,0347222222222222 msec	1.353 kbit/s	0 msec	2.795 kbit/s	21,8028993055555 %	42.860 MByte

1 to 50 of 576

Date Time	CPU usage	Disk read	Disk write	Datastore total ReadLatency	Network received	disk.deviceLatency	Network usage	Memory consumed (Percent)	Memory consumed
16.02.2015 02:50:00 PM – 02:55:00 PM	1,78 %	8 Mbit/s	0,18 Mbit/s	0 msec	1.081 kbit/s	0 msec	2.114 kbit/s	21,82 %	42.903 MByte
16.02.2015 02:45:00 PM – 02:50:00 PM	2,33 %	8 Mbit/s	0,12 Mbit/s	0 msec	1.106 kbit/s	0 msec	2.105 kbit/s	21,83 %	42.905 MByte
16.02.2015 02:40:00 PM – 02:45:00 PM	1,82 %	4 Mbit/s	0,11 Mbit/s	0 msec	1.155 kbit/s	0 msec	2.318 kbit/s	21,83 %	42.904 MByte
16.02.2015 02:35:00 PM – 02:40:00 PM	2,06 %	8 Mbit/s	0,07 Mbit/s	0 msec	999 kbit/s	0 msec	1.982 kbit/s	21,82 %	42.897 MByte
16.02.2015 02:30:00 PM – 02:35:00 PM	2,2 %	8 Mbit/s	0,07 Mbit/s	0 msec	1.130 kbit/s	0 msec	2.220 kbit/s	21,82 %	42.903 MByte
16.02.2015 02:25:00 PM – 02:30:00 PM	2,15 %	8 Mbit/s	0,18 Mbit/s	0 msec	1.073 kbit/s	0 msec	2.073 kbit/s	21,83 %	42.906 MByte
16.02.2015 02:20:00 PM – 02:25:00 PM	6,22 %	4 Mbit/s	0,06 Mbit/s	0 msec	1.130 kbit/s	0 msec	2.400 kbit/s	21,82 %	42.902 MByte
16.02.2015 02:15:00 PM – 02:20:00 PM	2,14 %	8 Mbit/s	0,18 Mbit/s	0 msec	1.245 kbit/s	0 msec	2.220 kbit/s	21,82 %	42.899 MByte
16.02.2015 02:10:00 PM – 02:15:00 PM	1,95 %	4 Mbit/s	0,17 Mbit/s	0 msec	1.090 kbit/s	0 msec	2.122 kbit/s	21,82 %	42.899 MByte
16.02.2015 02:05:00 PM – 02:10:00 PM	2,12 %	8 Mbit/s	0,07 Mbit/s	0 msec	1.081 kbit/s	0 msec	2.105 kbit/s	21,82 %	42.899 MByte
16.02.2015 02:00:00 PM – 02:05:00 PM	1,94 %	4 Mbit/s	0,06 Mbit/s	0 msec	1.204 kbit/s	0 msec	2.187 kbit/s	21,82 %	42.898 MByte
16.02.2015 01:55:00 PM – 02:00:00 PM	2,01 %	8 Mbit/s	0,18 Mbit/s	0 msec	999 kbit/s	0 msec	1.917 kbit/s	21,82 %	42.902 MByte
16.02.2015 01:50:00 PM – 01:55:00 PM	2,25 %	45 Mbit/s	0,18 Mbit/s	0 msec	1.130 kbit/s	0 msec	2.163 kbit/s	21,84 %	42.942 MByte
16.02.2015 01:45:00 PM – 01:50:00 PM	2,52 %	45 Mbit/s	0,18 Mbit/s	0 msec	1.114 kbit/s	0 msec	2.171 kb		

Kesimpulan

Setelah hasil analisis dan implementasi sistem monitoring jaringan menggunakan Hillstone, beberapa kesimpulan mengenai implementasi monitoring jaringan server univeritas Kristen Indonesia sebagai berikut: 1. Penggunaan Hillstone sebagai monitoring jaringan di Universitas Kristen Indonesia berhasil dapat dioptimalisasikan penggunaannya sehingga lebih cepat mendeteksi trouble jaringan agar mempercepat dalam penanganannya. 2. Hillstone berjalan pada tiap network dan memberi peringatan pada setiap perubahan dan ancaman serangan. 3 Hillstone dapat memonitor penggunaan Badwith agar sesuai dengan standar penggunaan yang di tentukan oleh Organisasi.

Saran

Saran untuk pengembangan monitoring jaringan menggunakan Hillstone adalah perlu adanya perawatan koneksi server dan pelatihan sumber daya manusia untuk mengetahui secara umum tentang jaringan koneksi internet,penggunaan Badwith tersedia dapat digunakan sesuai kibijakan organisasi dan menghindarkan ancaman dari pihak yang tidak bertanggung jawab pada jaringan,Badwith atau looping sehingga mengganggu aktifitas.

Daftar Pustaka

1. https://kb.hillstonenet.com/en/wp-content/uploads/2017/01/StoneOS_CLI_User_Guide_Monitor_5.5R4.pdf
2. https://manuals.paessler.com/prtgmanual.pdf
3. https://www.youtube.com/watch?v=KYeov9deGwc
4. https://www.hillstonenet.com/products/data-center-protection/
5. (Rasyid B. d., 2011)Realisasi Monitoring Server Menggunakan Nagios Dengan Memanfaatkan Event Handler, email dan SMS Gateway, ACADEMIA Politeknik Telkom, edisi September 2011, Lembaga Penelitian Politeknik Telkom, Bandung
6. (Operations and management Symposium(NOMS), 2002)
7. (Orebaugh A. e.)*Wireshark & Ethereal Network Protocol Analyzer Toolkit*, Syngress Publishing, 2006