Jurnal Informatika: Jurnal Pengembangan IT (JPIT), Vol.04, No.02, Mei 2019 ISSN: 2477-5126
DOI: 10.30591/jpit.v4i2.1103, pp:81-86 e-ISSN: 2548-9356

Penerapan Syslog Monitoring Jaringan Menggunakan *The Dude* dan EoIP *Tunnel*

Taufik Rahman[1*)], Herman Kuswanto[2]
[1]Jurusan Sistem Informasi, Fakultas Teknologi Informasi, Universitas Bina Sarana Informatika, Jakarta
[2]Jurusan Teknik Informatika, STMIK Nusa Mandiri, Jakarta
[1]Jln. Kamal Raya No.18 Ringroad Barat, Cengkareng, Jakarta Barat, 11730, Indonesia
[2]Jln. Damai No.8, Warung Jati Barat (Margasatwa), Jakarta Selatan, 12550, Indonesia
email: [1]taufik@bsi.ac.id, [2]herman.hko@nusamandiri.ac.id

***Abstract* – In the era of technology 4.0, the use of the internet is very quickly followed by the development of increasingly complex supporting devices, each activity of devices that are connected or disconnected in the network will send or issue messages that will affect the devices around them because each device has a different role on the network . Messages issued by the device must be considered, especially by network administrators. In general, the message is stored locally in the memory or drive of the device, it will be very dangerous if the device is turned off so the message is lost. or messages sent over the network to a centralized server. One technology that can be used to collect messages is the Dude application through a virtual private network, EoIP Tunnel. From the results of research that has been done, it can be said that system messages (syslog) from computer network devices both internet or intranet using the dude server can be implemented and are very safe because all activities that occur on switches are manageable, access points and routers on campus will be stored. When problems occur regarding network connections, syslog on the dude server can be opened using wordpad or similar applications. Virtual tunnel network, EoIP Tunnel can be configured on MikroTik routers by network administrators, so that syslog can be sent and entered into the dude server. EoIP tunnel development can be used or running simultaneously with OSPF routing.**

***Abstrak* – Pada era teknologi 4.0 ini penggunaan internet sangat cepat diikuti dengan perkembangan perangkat pendukung yang semakin komplek, setiap kegiatan dari perangkat yang terhubung atau terputus dalam jaringan akan mengirimkan atau mengeluarkan pesan sehingga akan mempengaruhi perangkat yang ada disekitarnya karena setiap perangkat itu memiliki peran yang berbeda di jaringan. Pesan yang dikeluarkan oleh perangkat harus diperhatikan, terutama oleh network administrator. Pada umumnya, pesan tersimpan secara lokal di memori atau drive perangkat, akan sangat berbahaya jika perangkat nya mati sehingga hilang pesan nya. atau pesan dikirim melalui jaringan ke server terpusat. Salah satu teknologi yang dapat digunakan untuk mengumpulkan pesan yakni aplikasi The Dude melalui jaringan pribadi virtual, EoIP Tunnel. Dari hasil penelitian yang telah dilakukan maka dapat dikatana bahwa Pesan sistem (syslog) dari perangkat jaringan komputer baik internet atau intranet menggunakan the dude server dapat diimplementasikan dan sangat aman karena semua aktifitas yang terjadi pada switch manageable, access point dan router pada kampus akan tersimpan. Ketika terjadi permasalahan terkait koneksi jaringan, maka syslog pada server the dude dapat dibuka dengan menggunakan wordpad atau aplikasi sejenisnya. Jaringan virtual tunnel, EoIP Tunnel dapat dikonfigurasi pada router MikroTik oleh administrator jaringan, sehingga syslog dapat terkirim dan masuk ke server the dude. Pengembangan EoIP tunnel dapat digunakan atau berjalan bersamaan dengan routing OSPF.**

***Kata Kunci* – Syslog, The Dude, EoIP, *Tunnel*, MikroTik**

*) **penulis korespondensi**: Taufik Rahman
Email: taufik@bsi.ac.id

I. PENDAHULUAN

Dalam jaringan modern sejumlah besar pesan dapat dihasilkan yang membuat analisis informasi ini menjadi tugas tersendiri. Pesan Syslog adalah salah satu sumber informasi paling kaya data mengenai kesehatan sistem. Informasi yang dicatat oleh utilitas syslog mencakup berbagai macam aktivitas sistem. Pesan syslog dianalisis secara manual oleh operator jaringan setelah kegagalan terjadi untuk menemukan petunjuk tentang penyebab masalah. Satu kejadian atau kegagalan dalam jaringan dapat mempengaruhi banyak perangkat, dan pada masing-masing perangkat itu dapat mempengaruhi fitur yang berbeda tergantung pada fungsi perangkat di jaringan. Korelasi yang tepat dari pesan-pesan tersebut bukanlah tugas yang sepele, bahkan untuk para ahli jaringan. Pesan disimpan secara lokal di perangkat atau dikirim melalui jaringan ke server terpusat. Jaringan yang digunakan untuk mengirim pesan syslog dapat melalui internet atau *virtual private network* (VPN). Pengiriman syslog dengan vpn yakni dengan membangun sebuah *tunnel* atau terowongan, sehingga syslog aman sampai pada server kantor pusat. Tujuan dari penelitian adalah untuk menyimpan log dari perangkat jaringan seperti router, *switch* core, *switch* distribusi dan *switch* akses.

II. SYSLOG & EoIP Tunnel

Pesan Syslog dihasilkan oleh berbagai jenis komunikasi dan perangkat komputasi untuk menunjukkan status dari beberapa proses internal atau peristiwa apa pun yang harus dilaporkan. Kejadian-kejadian ini bisa berhubungan dengan operasi normal, kegagalan, alarm, informasi debug dan lain-lain. Ada beberapa RFC (*Request for Comments*) yang menyediakan kerangka kerja untuk standardisasi protokol.

Khususnya, RFC 5424 menjelaskan *format* standar untuk pesan syslog dan pemetaan transportasi yang harus didukung untuk transmisi [1].

Ethernet over IP (EoIP) *Tunneling* adalah protokol MikroTik RouterOS yang membuat terowongan *Ethernet* antara minimal dua router di atas koneksi IP. *Tunnel* EoIP dapat berjalan di atas terowongan IPIP, *tunnel* PPTP atau koneksi lain yang mampu mengangkut IP. Ketika fungsi bridging dari router diaktifkan, semua lalu lintas *Ethernet* (semua protokol *Ethernet*) akan dijembatani seolah-olah ada di mana *interface Ethernet* fisik dan kabel antara dua router (dengan bridging diaktifkan). Protokol ini memungkinkan skema jaringan ganda. Pengaturan jaringan dengan *interface* EoIP: Kemungkinan untuk *bridge* LAN melalui Internet, Kemungkinan untuk *bridge* LAN di atas terowongan terenkripsi, Kemungkinan untuk *bridge* LAN melalui jaringan nirkabel 802.11b '*ad-hoc*'. Protokol EoIP mengenkapsulasi frame *Ethernet* dalam paket GRE (IP *Protocol* number 47) (seperti PPTP) dan mengirimnya ke sisi *remote* dari *tunnel* EoIP dengan standar GRE RFC 1701[2].

III. ICMP & SNMP

Metode pertama tidak memerlukan konfigurasi tambahan dari perangkat yang dipantau. Ini didasarkan pada penggunaan protokol ICMP (Internet *Control Message Protocol*). Dengan menggunakan alat ping dan pesan ICMP yang digunakan, adalah mungkin untuk menentukan apakah perangkat atau aplikasi jarak jauh dalam keadaan operasional, dan bagaimana ia merespons pesan permintaan echo ICMP. Tergantung pada respons yang diterima dari perangkat yang dipantau dan sesuai dengan pesan ICMP standar, *platform* pemantauan memberikan informasi yang tepat tentang status perangkat yang dipantau [3].

Metode kedua didasarkan pada penggunaan protokol SNMP (*Simple Network Management Protocol*). SNMP beroperasi di lapisan aplikasi OSI dan menggunakan protokol UDP (User Datagram *Protocol*) pada lapisan transport OSI. Oleh karena itu, protokol SNMP adalah satu dari protokol yang dapat selalu digunakan untuk memantau sumber daya jaringan. Metode ini ditandai dengan komunikasi antara agen yang berjalan pada perangkat yang dipantau dan server pemantauan. Server pemantauan adalah bagian dari *platform* perangkat lunak untuk pemantauan jaringan yang biasanya terletak di lokasi pusat yang memungkinkan pemantauan berkelanjutan dari sumber daya jaringan terdistribusi. Dengan perkembangan teknologi, dan terutama aspek keamanan komunikasi dalam jaringan komputer, protokol SNMP terus berkembang. Dengan versi ketiga dari protokol, SNMPv3, kemajuan signifikan telah dibuat dibandingkan dengan versi sebelumnya, sehubungan dengan keamanan komunikasi antara agen pada perangkat yang dipantau dan server pemantauan [4].

IV. PENELITIAN YANG TERKAIT

Beberapa penelitian yang berkaitan dengan penelitian ini diantaranya yaitu, Varaandi,R.,dkk (2018) Log sistem menyediakan informasi berharga tentang status kesehatan sistem TI dan jaringan komputer. Oleh karena itu, pemantauan file log telah diidentifikasi sebagai sistem yang penting dan teknik manajemen jaringan. Sementara banyak solusi telah dikembangkan untuk memantau pesan log yang diketahui, deteksi kondisi kesalahan yang tidak diketahui sebelumnya tetap menjadi masalah yang sulit[5].

Penelitin selanjutnya oleh Ljubojevic dan Mijic (2018) terkait pemantauan dan *admini*strasi jaringan komputer yang efisien didasarkan pada penggunaan informasi yang tepat waktu tentang status perangkat dan layanan jaringan. Mempertimbangkan perkembangan teknologi informasi dan komunikasi dan integrasi layanan komunikasi yang berbeda, perlu untuk menyediakan pemantauan terpusat lingkungan jaringan heterogen. Dalam makalah ini kami menganalisis persyaratan dasar untuk pemantauan jaringan dan kemungkinan menggunakan *platform open source Zenoss Core* untuk implementasi pemantauan terpusat dari parameter yang diperlukan. Telah ditunjukkan bahwa *platform* Zenoss memungkinkan pemantauan yang efisien dan visualisasi parameter perangkat jaringan menggunakan ICMP, SNMP dan protokol syslog. Selain itu, dengan menggunakan manipulasi dan representasi data yang tepat, adalah mungkin untuk memenuhi persyaratan khusus dari pemantauan jaringan dan manajemen[6].

Kobayashi, M.,dkk (2017) meneliti terkit dengan Pesan log jaringan (mis., Syslog) diharapkan menjadi informasi yang berharga dan berguna untuk mendeteksi perilaku tak terduga atau anomali dalam jaringan berskala besar. Namun, karena banyaknya data log sistem yang dikumpulkan dalam operasi sehari-hari, tidak mudah untuk mengekstrak kegagalan sistem yang tepat atau untuk mengidentifikasi penyebabnya. Dalam studi ini, kami mengusulkan metode untuk mengekstraksi kegagalan pinpoint dan mengidentifikasi penyebabnya dari data syslog jaringan. Metodologi yang diusulkan dalam studi ini bergantung pada inferensi kausal yang merekonstruksi kausalitas peristiwa jaringan dari serangkaian rangkaian waktu kejadian. Inferensi kausal dapat menyaring kejadian yang tidak sengaja berkorelasi, sehingga menghasilkan lebih banyak peristiwa kausal yang masuk akal daripada pendekatan pendekatan lintas korelasi tradisional. Kami menerapkan metode kami untuk data jaringan syslog senilai 15 bulan yang diperoleh dari jaringan akademis nasional di Jepang. Metode yang diusulkan secara signifikan mengurangi jumlah kejadian terkait pseudo dibandingkan dengan metode tradisional. Juga, melalui tiga studi kasus dan perbandingan dengan data masalah tiket, kami menunjukkan efektivitas metode yang diusulkan untuk operasi jaringan praktis[7]

Penelitian dilakukan Zhang, S.,dkk (2017) mengenai Syslog pada *switch* merupakan sumber informasi yang kaya untuk diagnosis post mortem dan prediksi proaktif kegagalan *switch* dalam jaringan pusat data. Namun, informasi tersebut dapat secara efektif diekstraksi hanya melalui pemrosesan syslog yang tepat, misalnya, menggunakan teknik pembelajaran mesin yang sesuai. Pendekatan umum untuk pemrosesan syslog adalah mengekstrak (yaitu, membangun) templat dari pesan syslog historis dan kemudian mencocokkan pesan syslog ke templat ini. Namun, teknik ekstraksi template yang ada memiliki akurasi rendah dalam mempelajari kumpulan template yang "benar", atau tidak mendukung pembelajaran tambahan dalam arti seluruh rangkaian template harus dibangun kembali (dari memproses semua pesan syslog historis lagi) ketika baru template akan

ditambahkan, yang sangat mahal jika digunakan untuk jaringan pusat data besar. Untuk mengatasi dua masalah ini, kami mengusulkan model pohon template (FT-tree) yang sering digunakan di mana kombinasi kata-kata (syslog) yang sering diidentifikasi dan kemudian digunakan sebagai template pesan. FTtree secara empiris mengekstraksi template pesan lebih akurat daripada pendekatan yang ada, dan secara alami mendukung pembelajaran tambahan. Untuk membandingkan kinerja FT-tree dan tiga teknik pembelajaran template lainnya, kami bereksperimen pada tiket kegagalan dua tahun dan syslog yang dikumpulkan dari *switch* yang digunakan di lebih dari 10 pusat data dari penyedia layanan cloud tier-1. Percobaan menunjukkan bahwa FT-tree meningkatkan estimasi / akurasi prediksi (yang diukur oleh F1) sebesar 155% hingga 188%, dan efisiensi komputasi sebesar 117 hingga 730 kali[8].

Baseman, S.,dkk (2016) meneliti mengenai pemantauan sistem komputasi kinerja tinggi menjadi semakin sulit karena peneliti dan analis sistem menghadapi tantangan untuk mensintesiskan berbagai informasi pemantauan untuk mendeteksi masalah sistem pada mesin yang lebih besar. Kami menyajikan metode untuk deteksi anomali pada data syslog, salah satu aliran data yang paling penting untuk menentukan kesehatan sistem. Pesan Syslog menimbulkan pertanyaan sulit untuk analisis karena mereka menyertakan campuran teks bahasa alami terstruktur serta nilai-nilai numerik. Kami menyajikan kerangka deteksi anomali yang menggabungkan analisis grafik, pembelajaran relasional, dan estimasi kepadatan kernel untuk mendeteksi pesan syslog yang tidak biasa. Kami merancang detektor blok peristiwa, yang menemukan grup pesan syslog terkait, untuk mengambil seluruh bagian pesan syslog yang terkait dengan satu baris anomali. Pendekatan baru kami berhasil mengambil perilaku anomali yang dimasukkan ke dalam file syslog dari mesin *virtual*, termasuk pesan yang menunjukkan masalah sistem yang serius. Kami juga menguji pendekatan kami pada pesan syslog dari superkomputer Trinity dan menemukan bahwa metode kami tidak menghasilkan *false positive* yang signifikan[9].

Penelitian selanjutnya dilakukan oleh Tan, T.,dkk (2017), bahwa syslog router adalah urutan peristiwa yang diamati dan dicatat oleh router. Mereka telah banyak digunakan di bidang keamanan sistem. Makalah ini berfokus pada mendeteksi perilaku anomali dari router dengan menganalisis syslog router. Untuk pra-pemrosesan data syslog, pengelompokan hierarkis berdasarkan penghitungan jarak sepupu antara pola peristiwa digunakan untuk mengelompokkan acara. Untuk membuat deret waktu, panjang untuk jangka waktu ditetapkan dan setiap jendela waktu memiliki skor yang terkait dengan gugus acara di dalamnya. Alih-alih hanya memperlakukan setiap acara cluster secara bersamaan di jendela waktu, kami menetapkan bobot untuk setiap kelompok acara dengan menggunakan empat metode pembobotan jangka. Dua dari mereka (IDF) dan metode residual (RIDF) - secara luas digunakan dalam bidang pencarian informasi. Karena kekurangan mereka, makalah ini mengusulkan dua metode pembobotan baru. Metode pertama, IDFVAR, adalah modifikasi dari metode RIDF dan mengambil distribusi data, frekuensi, dan beberapa faktor tambahan menjadi pertimbangan. Dalam metode kedua, IDFJMP, nilai JMP diusulkan untuk mengevaluasi tingkat perubahan tiba-tiba dari suatu gugus peristiwa. Untuk membandingkan metode pembobotan jangka itu, eksperimen dilakukan pada sekumpulan data yang diperkirakan. Kemudian, kami mendeteksi perilaku anomali dengan menggunakan metode yang berasal dari standar deviasi pada deret waktu yang dipilih dengan melakukan percobaan pada syslogs router nyata[10].

Vuong, Q.,dkk (2015) meneliti mengenai perangkat lunak yang didefinisikan jaringan memisahkan data dan kontrol yang memfasilitasi fungsi manajemen jaringan, terutama mengaktifkan fungsi kontrol jaringan yang dapat diprogram. Pemantauan acara adalah fungsi manajemen kesalahan yang terlibat dalam mengumpulkan dan memfilter pesan pemberitahuan acara dari perangkat jaringan. Penelitian ini menyajikan pendekatan pemantauan acara terdistribusi untuk jaringan yang ditentukan perangkat lunak. Peristiwa pemantauan biasanya berhubungan dengan sejumlah besar data log peristiwa, proses pengumpulan dan penyaringan log sehingga memerlukan otomatisasi dan efisiensi tingkat tinggi. Pendekatan ini memanfaatkan protokol OpenFlow dan syslog untuk mengumpulkan dan menyimpan peristiwa log yang diperoleh dari perangkat jaringan pada server syslog. Ia juga menggunakan metode penyaringan semantik adaptif untuk memfilter dan menyajikan kejadian-kejadian tidak biasa bagi *administrator* sistem untuk mengambil tindakan lebih lanjut. Kami telah mengevaluasi pendekatan ini pada *platform* simulasi jaringan dan menyediakan beberapa pengumpulan log dan menyaring hasil dengan analisis[11].

Kimura, T.,dkk (2015) meneliti bahwa dengan pertumbuhan layanan dalam jaringan IP, operator jaringan diharuskan melakukan operasi proaktif yang cepat mendeteksi tanda-tanda kegagalan kritis dan mencegah masalah di masa depan. Data log jaringan, termasuk router syslog, adalah sumber yang kaya untuk operasi semacam itu. Namun, tidak mungkin menemukan log yang benar-benar penting yang menyebabkan masalah serius karena volume besar dan kompleksitas data log[12].

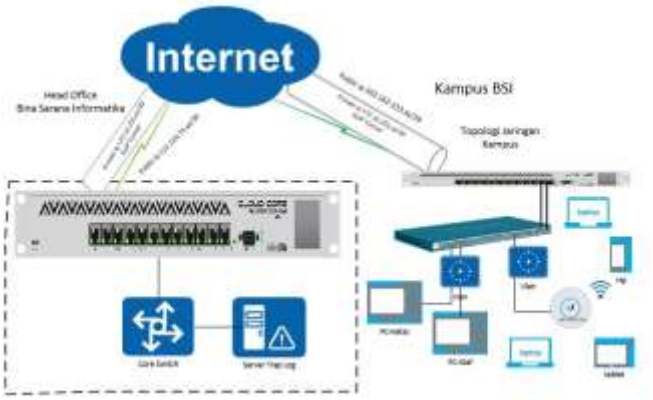
Berdasarkan penelitian yang dilkukan oleh Aeri, A.,dkk (2015), saat ini banyak alat manajemen log tersedia di pasar untuk menganalisis, melaporkan, dan mengelola data. Untuk mengetahui alat manajemen log terbaik itu harus tetap ditentukan. Log adalah informasi mendetail tentang aplikasi apa pun, aktivitas pengguna, dan kinerja sistem. Hari-hari ini organisasi berinvestasi dalam alat manajemen log untuk mengawasi jaringan karena dapat melacak aktivitas apa pun yang sedang berlangsung di jaringan. Dalam makalah penelitian ini, lima alat manajemen log yang berbeda telah dilihat dengan tujuan untuk menentukan fitur-fitur dan memberi peringkat dalam berbagai metrik. Saat melakukan penelitian kami, kami mengetahui bahwa Kiwi syslog hadir dengan persyaratan metrik lebih banyak. Jadi sesuai penelitian kami, server log Kiwi sys adalah alat manajemen log terbaik[13].

V. METODE PENELITIAN

Penelitian ini menggunakan *Network Development Life Cycle* (NDLC) adalah metode yang digunakan pada pembuatan atau mendesain infrastruktur jaringan yang dapat memonitoring untuk mengetahui statistik dan *performance*

jaringan[14], yang digunakan lima tahapan: analisa, desain, implementasi, monitoring dan manajemen. Sebelum masuk pada tahap analisa, terlebih dahulu tahap studi pustaka dengan mengumpulkan data data teoritis dan mempelajari buku atau literatur artikel jurnal yang berkaitan[15] tentang syslog, the dude dan EoIP *Tunnel*.

Tahap perancangan dalam penggunaan *hardware* adalah disesuaikan dengan yang support EoIP Tunnel yakni Router MikroTik dengan tipe 1100AHX2 dan *Switch Manageable* untuk menjalankan *Vlan.*



Gbr. 1 Topologi Jaringan ke Server Log

Pada Gbr. 1, adalah topologi jaringan berjalan dan topologi jaringan vpn dari kantor pusat ke kampus untuk penerapan syslog monitoring jaringan menggunakan the dude, log pada router MikroTikRB 1100AHX2 pada kampus dikirim ke server the dude yang berada di kantor pusat melalui EoIP *Tunnel*. Kemudian pada tahap desain, topologi jaringan usulan dibuat, mengalokasikan ip *Address* yang digunakan untuk EoIP *Tunnel*, menambahkan jalur route *network*, membuka port dan protokol, memilah jenis rule *logging* dan *action* pada MikroTik RB1100AHX2 kampus. Selanjutnya pada tahap implementasi, menggabungkan topologi fisik berjalan dengan topologi yang baru. Diawali dengan membuat *interface virtual*, konfig ip *Address*, menambahkan route, menghubungkan jaringan kampus dengan kantor pusat pada tahap ini.

VI. HASIL DAN PEMBAHASAN

Implementasi *The Dude* sebagai *server syslog* setelah membuat rancangan topologi jaringan dari kampus ke kantor pusat, selanjutnya melakukan konfigurasi, seperti yang ditunjukkan pada Tabel I.

TABEL I
KONFIGURASI ROUTER

Router Kampus	Router Pusat
Interface EoIP *Tunnel*	*Interface* EoIP *Tunnel*
Vlan	*Vlan*
IP *Address*	IP *Address*
System Logging	The Dude Server

A. Konfigurasi detail *interface* eoip *tunnel* pada router kampus

```
[taufik@MT_Kampus] > interface eoip pr detail
Flags: X - disabled, R - running
 0  R name="eoip-to-dwsa" mtu=1500 actual-mtu=1500
l2mtu=65535 mac-Address=02:D8:C7:DB:A2:D0
arp=enabled arp-timeout=auto loop-protect=default
loop-protect-status=off loop-protect-send-
interval=5s loop-protect-disable-time=5m local-
Address=202.162.223.x remote-Address=115.124.73.x
tunnel-id=133 dscp=inherit clamp-tcp-mss=no don't-
fragment=no allow-fast-path=no
```

Pembuatan eoip *tunnel* menggunakan *tunnel*-id yang sama di kedua sisi.

B. Konfigurasi detail ip address pada router kampus

```
[taufik@MT_Kampus] > ip Address pr detail
Flags: X - disabled, I - invalid, D - dynamic
0 Address=202.162.223.x/29 network=202.162.223.x
interface=ether1-to-icon+ actual-interface=ether1-
to-icon+
1 Address=172.16.255.130/30 network=172.16.255.128
interface=eoip-to-dwsa actual-interface=eoip-to-
dwsa
2   Address=10.10.0.1/26 network=10.10.0.0
interface=vlan1 actual-interface=vlan1
3  Address=10.10.1.1/26 network=10.10.1.0
interface=vlan10 actual-interface=vlan10
4   Address=10.10.2.1/26 network=10.10.2.0
interface=vlan20 actual-interface=vlan20
```

Script diatas adalah ip *Address* yang terdapat pada router kampus, terdapat ip public yang didapat dari ISP, ip *Address* eoip *tunnel* dan ip *Address* pada *interface vlan*.

C. Script logging pada router MikroTik kampus detail nya

```
[taufik@MT_Kampus] >  system logging action pr
detail
Flags: * - default
 0 * name="memory" target=memory memory-lines=100
memory-stop-on-full=no
 1 * name="disk" target=disk disk-file-name="log"
disk-lines-per-file=100 disk-file-count=2 disk-
stop-on-full=no
 2 * name="echo" target=echo remember=yes
 3 * name="remote" target=remote
remote=115.124.73.x remote-port=514 src-
Address=0.0.0.0 bsd-syslog=no
     syslog-time-format=bsd-syslog syslog-
facility=daemon syslog-severity=auto
 4 name="todwsa" target=remote remote=192.168.1.16
remote-port=514 src-Address=0.0.0.0 bsd-syslog=no
syslog-time-format=bsd-syslog syslog-
facility=daemon syslog-severity=auto
```

Pada hasil *script* diatas, *flags* no 4 menunjukkan bahwa ada aksi *remote* ke ip *Address* 192.168.1.16(ip server the dude pada kantor pusat) dengan *port* 514 yang berasal dari 0.0.0.0 (semua ip *address*) yang berada dibawah router kampus.

D. Hasil secara detail system logging

```
[taufik@MT_Kampus] > system logging pr detail
Flags: X - disabled, I - invalid, * - default
 0  * topics=info prefix="" action=memory
 1  * topics=error prefix="" action=memory
 2  * topics=warning prefix="" action=memory
 3  * topics=critical prefix="" action=echo
 4    topics=info prefix="" action=todwsa
 5    topics=critical prefix="" action=todwsa
 6    topics=error prefix="" action=todwsa
 7    topics=warning prefix="" action=todwsa
```

```
8    topics=system prefix="" action=todwsa
```

Script yang diatas adalah *topics* atau jenis log yang dipilih, no 4-8 yang akan di kirim ke server the dude yang ada dipusat.

Kemudian konfig pada MikroTik Kantor pusat juga dilakukan, berikut hasil bentukan *interface* eoip *tunnel*.

E. Konfigurasi interface eoip secara detail pada kantor pusat

```
[taufik@MT_Pusat] > interface eoip pr detail
Flags: X - disabled, R - running
0   R name="eoip-to-bdg" mtu=1500 actual-mtu=1500
l2mtu=65535 mac-Address=02:FD:67:04:03:C5
arp=enabled arp-timeout=auto loop-protect=default
loop-protect-status=off loop-protect-send-
interval=5s loop-protect-disable-time=5m local-
Address=115.124.73.x remote-Address=202.162.223.x
tunnel-id=133 dscp=inherit clamp-tcp-mss=no dont-
fragment=no allow-fast-path=no
```

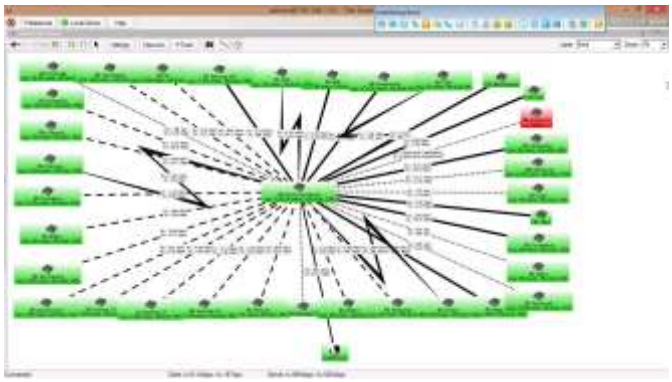
Pada *script* diatas terlihat sama *tunnel*-id nya yaitu133, local-*Address* diisi dengan ip public didapat dari ISP begitu juga dengan *remote-Address* (yang dituju).

F. Konfigurasi ip Address yang terdapat pada router kantor pusat,

```
[taufik@MT_Pusat] > ip Address pr detail
Flags: X - disabled, I - invalid, D - dynamic
 0 Address=115.124.73.x30 network=115.124.73.x
interface=ether1 BSI-Cawang-primary
1 Address=172.16.255.x/30 network=172.16.255.124
interface=eoip-to-tsk actual-interface=eoip-to-tsk
2 Address=172.16.255.x/30 network=172.16.255.72
interface=eoip-to-tna actual-interface=eoip-to-tna
3 Address=172.16.255.x/30 network=172.16.255.32
interface=eoip-to-ckp actual-interface=eoip-to-ckp
4  Address=172.16.255.x/30 network=172.16.255.128
interface=eoip-to-bdg actual-interface=eoip-to-bdg
```

Pada *script* diatas adalah ip *Address* pada router kantor pusat yang didalamnya ada beberapa ip *Address interface* eoip *tunnel* kampus bina sarana informatika tasik, tanggerang, cikampek dan bandung.

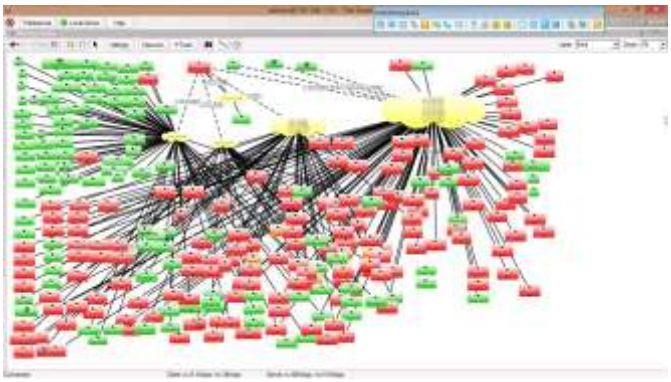
G. Kampus Universitas Bina Sarana Informatika terkoneksi dengan Kantor Pusat



Gbr. 2 koneksi dari kampus ke kantor pusat

Pada gambar 2, adalah *Network Intranet* pada Server The Dude, koneksi router MikroTik kampus Universitas Bina Sarana Informatika menuju router MikroTik kantor pusat, melalui koneksi *wireless*, link metro *ethernet*, link *localloop* dan *internet* (eoip *tunnel*).

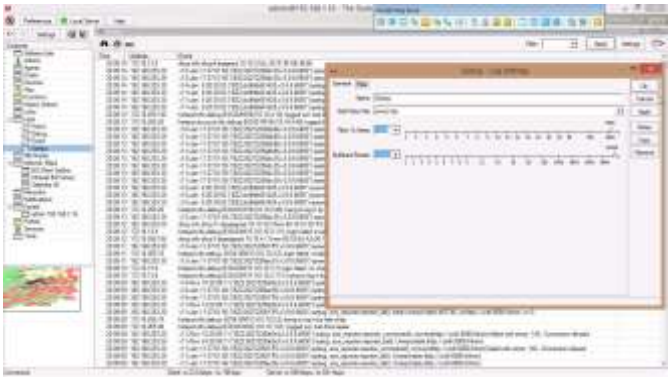
H. Jaringan VLAN pada Kantor Pusat Universitas Bina Sarana Informatika



Gbr. 3 *Discovery Network* dengan The Dude

Pada Gbr. 3, adalah jaringan pada kantor pusat Universitas Bina Sarana Informatika yang telah mendeteksi komputer yang aktif terkoneksi dengan jaringan (warna hijau), komputer yang tidak terkoneksi atau *shutdown* (warna merah). Sedangkan yang berbentuk awan adalah kumpulan *network* atau *vlan* yang saling terhubung.

I. Konfigurasi Syslog dan pada Server The Dude

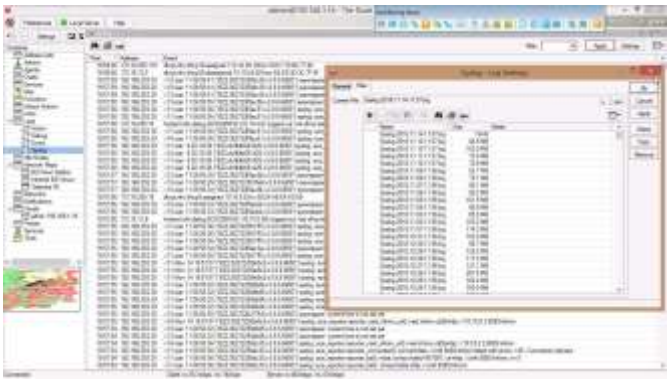


Gbr. 4 Syslog *setting*

Pada gambar 4, log berjalan yang masuk dari router kampus (gambar belakang) dan log *setting* (gambar depan) dengan *start new file every day*, *file to keep* dan *buffered* nya 1000, artinya log akan tersimpan seribu baris dalam 1 file.

J. Syslog dari kampus masuk ke Server The Dude

Pada Gbr. 5 merupakan hasil syslog yang tersimpan pada server the dude dengan penamaan terdiri dari Syslog tahun bulan tanggal jam dan menit, ukuran file nya berbeda sesuai dengan aktifitas yang terjadi.



Gbr. 5 Hasil Syslog tersimpan

VII. KESIMPULAN

Menerapkan syslog untuk jaringan computer internet dan intranet dengan menggunakan the dude server dapat diimplementasikan dan sangat aman karena semua aktifitas yang terjadi pada *switch manageable*, *access point* dan router pada kampus akan tersimpan semua. Syslog yang masuk pada server the dude dapat dibuka dengan menggunakan wordpad atau aplikasi sejenisnya. Sedangkan penggunaan jaringan *virtual tunnel*, yakni eoip *tunnel* yang bisa di konfigurasi pada router MikroTik oleh *administrator* jaringan, sehingga syslog dapat terkirim dan masuk ke *server the dude*. Saran kedepannya pengembangan atau penggunaan *interface* eoip *tunnel* dapat digunakan atau berjalan bersamaan dengan routing OSPF.

DAFTAR PUSTAKA

[1] G. Slomovitz, "Latent semantic analysis (LSA) *for* syslog correlation," *2017 Int. Conf. Electron. Commun. Comput. CONIELECOMP 2017*, 2017.

[2] W. MikroTik, "Manual:*Interface*/EoIP - MikroTik Wiki," 2018. [Online]. Available: https://wiki.mikrotik.com/wiki/Manual:*Interface*/EoIP. [Accessed: 10-Nov-2018].

[3] C. M. Kozierok, *The TCP/IP Guide: A Comprehensive, Illustrated Internet Protocols Reference*. 2005.

[4] A. Kaushik, "Use of Open Source Technologies *for* Enterprise Server Monitoring Using Snmp," *Technology*, vol. 02, no. 07, pp. 2246–2252, 2010.

[5] R. Vaarandi, B. Blumbergs, M. Kont, R. Vaarandi, B. Blumbergs, and M. Kont, "An Unsupervised Framework *for* Detecting Anomalous *Message*s from Syslog Log Files An Unsupervised Framework *for* Detecting Anomalous *Message*s from Syslog Log Files," *NOMS 2018 - 2018 IEEE/IFIP Netw. Oper. Manag. Symp.*, pp. 1–6, 2018.

[6] M. Ljubojevic, A. Bajic, and D. Mijic, "Centralized monitoring of computer *network*s using Zenoss open source *platform*," *2018 17th Int. Symp. INFOTEH-JAHORINA, INFOTEH 2018 - Proc.*, vol. 2018–Janua, no. March, pp. 1–5, 2018.

[7] S. Kobayashi, K. Otomo, K. Fukuda, and H. Esaki, "Mining Causality of *Network* Events in Log Data," *IEEE Trans. Netw. Serv. Manag.*, vol. 15, no. 1, pp. 53–67, 2018.

[8] S. Zhang *et al.*, "Syslog processing *for switch* failure diagnosis and prediction in datacenter *network*s," *2017 IEEE/ACM 25th Int. Symp. Qual. Serv. IWQoS 2017*, pp. 1–10, 2017.

[9] E. Baseman, S. Blanchard, Z. Li, and S. Fu, "Relational synthesis of text and numeric data *for* anomaly detection on computing *system* logs," *Proc. - 2016 15th IEEE Int. Conf. Mach. Learn. Appl. ICMLA 2016*, vol. 1, pp. 882–885, 2017.

[10] T. Tan, S. Gao, W. Yang, Y. Song, and C. Lin, "Two new term weighting methods *for* router syslogs anomaly detection," *Proc. - 18th IEEE Int. Conf. High Perform. Comput. Commun. 14th IEEE Int. Conf. Smart City 2nd IEEE Int. Conf. Data Sci. Syst. HPCC/SmartCity/DSS 2016*, pp. 1454–1460, 2017.

[11] Q. Vuong, H. M. Tran, and S. T. Le, "Distributed Event Monitoring *for* Software Defined *Network*s," *2015 Int. Conf. Adv. Comput. Appl.*, pp. 90–97, 2015.

[12] T. Kimura, A. Watanabe, T. Toyono, and K. Ishibashi, "Proactive failure detection learning generation patterns of large-scale *network* logs," *Proc. 11th Int. Conf. Netw. Serv. Manag. CNSM 2015*, pp. 8–14, 2015.

[13] A. Aeri and S. Tukadiya, "A comparative study of *network* based *system* log *Management* tools," *2015 Int. Conf. Comput. Commun. Informatics*, pp. 1–6, 2015.

[14] K. Rianafirin and M. T. Kurniawan, "Design *Network* Security Infrastructure Cabling Using *Network Development Life Cycle* Methodology and ISO/IEC 27000 Series in Yayasan Kesehatan (Yakes) Telkom Bandung," in *2017 4th International Conference on Computer Applications and Information Processing Technology (CAIPT)*, 2017, pp. 1–6.

[15] T. Rahman, "Jaringan Hotspot Menggunakan Dua Radius MikroTik dan *Ethernet Over* Internet *Protocol Tunnel*," vol. 2, no. 2, pp. 135–148, 2018.