JURNAL PINTER
VOL. 1 NO. 1 JUNI 2017
e-ISSN: 2597- 4475
http://doi.org/10.21009/pinter.1.1.7

Monitoring Lalu Lintas Jaringan Demilitarized Zone Universitas Negeri Jakarta Menggunakan Sensor Packet Sniffer Pada PRTG Network Monitor

M. Ficky Duskarnaen,Aditya Rie Pratama
Universitas Negeri Jakarta
duskarnaen@unj.ac.id, aditya.rie16@yahoo.co.id

Abstrak

Universitas Negeri Jakarta mendapat pemberitahuan bahwa server yang berada pada jaringan UNJ melakukan serangan ke server milik NETpilot GmbH pada layanan postfix. Sementara itu jaringan tempat server tersebut berada belum terdapat sistem yang dapat memantau lalu lintas jaringan yang terjadi. Penelitian ini bertujuan untuk melakukan monitoring lalu lintas jaringan pada jaringan Demilitarized Zone Universitas Negeri Jakarta. Penelitian yang dilakukan di Laboratorium Komputer Jurusan Teknik Elektro dan Pustikom (Pusat Teknologi Informasi dan Komputer) Universitas Negeri Jakarta pada bulan April sampai dengan Juni 2014 menggunakan metode eksperimen. Dari hasil monitoring tersebut diketahui terdapat server dengan alamat IP 192.168.XXX.XXX menghasilkan lalu lintas data yang sangat besar, beberapa koneksi yang berasal dari server dengan alamat IP 192.168.XXX.XXX memiliki destination port 10026 yang merupakan port default dari salah satu layanan yang diberikan oleh aplikasi postfix. Sehingga kesimpulannya, monitoring lalu lintas jaringan menggunakan sensor Packet Sniffer pada PRTG Network monitor telah dapat menghasilkan laporan lalu lintas data yang terjadi pada jaringan DMZ UNJ setiap hari dan hasil monitoring tersebut dapat digunakan untuk membantu menyelesaikan masalah yang terjadi pada jaringan.

Kata kunci : *monitoring jaringan, demilitarized zone, packet sniffer, dan PRTG network monitor*

1. PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi yang disebabkan oleh tingginya kebutuhan manusia akan sebuah informasi telah membuat lalu lintas data di dalam sebuah jaringan meningkat, baik di jaringan lokal maupun jaringan internet. Untuk menjaga kinerja infrastruktur jaringan dibutuhkan satu solusi yang secara kontinu dapat memantau aktivitas di setiap *node* pada infrastruktur jaringan. Jawaban atas kebutuhan ini yaitu dengan adanya *network monitoring* untuk memantau lalu lintas pada jaringan. Monitoring yang paling umum adalah monitoring penggunaan *bandwidth* dari *router*, *switch*, dan *modem* melalui SNMP *(Simple Network Monitoring Protocol), netflow, atau packet sniffing*.

Dengan menggunakan SNMP informasi yang diperoleh berupa besaran lalu lintas yang terjadi pada sebuah *interface* yang dimonitor tanpa mengetahui informasi detail dari lalu lintas yang terjadi seperti asal dan tujuan serta besaran paket data yang dikirimkannya. Sedangkan *packet sniffing* dapat memberikan informasi yang lebih lengkap dari SNMP. Salah satu aplikasi yang dapat digunakan untuk melakukan

e-ISSN: 2597- 4475
http://doi.org/10.21009/pinter.1.1.7

monitoring jaringan melalui *packet sniffing* adalah PRTG (Paessler Router Traffic Grapher) Network Monitor dengan sensor yang bernama Packet Sniffer.

Universitas Negeri Jakarta memiliki jaringan komputer yang berpusat di Pustikom. Secara garis besar, jaringan komputer di UNJ terbagi menjadi 2 yaitu jaringan LAN (*Local Area Network*) dan DMZ (*Demilitarized Zone*), kedua jaringan tersebut sama-sama dapat terhubung ke internet. Pada jaringan LAN terdapat sebuah *bandwidth management* yang digunakan untuk melakukan pemantauan dan pengaturan penggunaan *bandwidth*. Sementara itu untuk jaringan DMZ belum dapat dimonitor. Padahal DMZ merupakan jaringan yang cukup penting karena didalamnya terdapat *server-server* yang merupakan bagian dari layanan sebuah perguruan tinggi, seperti *web server* dan *database server*. Selain itu, UNJ pernah mendapat surat pemberitahuan bahwa server yang dimiliki UNJ melakukan serangan ke server milik pihak lain yang berada di internet. Dalam surat tersebut, UNJ diminta untuk melakukan pengecekan terhadap server yang dimiliki oleh UNJ. Akan tetapi banyaknya jumlah server yang dimiliki oleh UNJ dan semua server menggunakan alamat yang sama ketika mengirimkan data ke internet membuat *administrator* mengalami kesulitan untuk menentukan server mana yang melakukan serangan terhadap server milik pihak lain yang berada di internet.

Oleh karena itu, dibutuhkan sebuah *network monitoring* yang dapat memantau aktivitas yang terjadi dalam jaringan khususnya jaringan DMZ UNJ agar *administrator* dapat melakukan evaluasi terhadap kinerja jaringan. Hal tersebut yang melatarbelakangi dibuatnya sebuah monitoring lalu lintas jaringan menggunakan sensor Packet Sniffer pada PRTG Network Monitor.

2. JARINGAN KOMPUTER

2.1 Definisi Jaringan Komputer

Jaringan komputer merupakan sekumpulan komputer berjumlah banyak yang terpisah-pisah akan tetapi saling berhubungan dalam melaksanakan tugasnya (Tanenbaum, 1997: 1). Lebih lengkapnya, jaringan komputer merupakan sekelompok komputer otonom yang saling berhubungan antara yang satu dengan yang lainnya menggunakan protokol komunikasi melalui media komunikasi sehingga dapat saling berbagi informasi dan sumber daya.

2.2 Jaringan DMZ

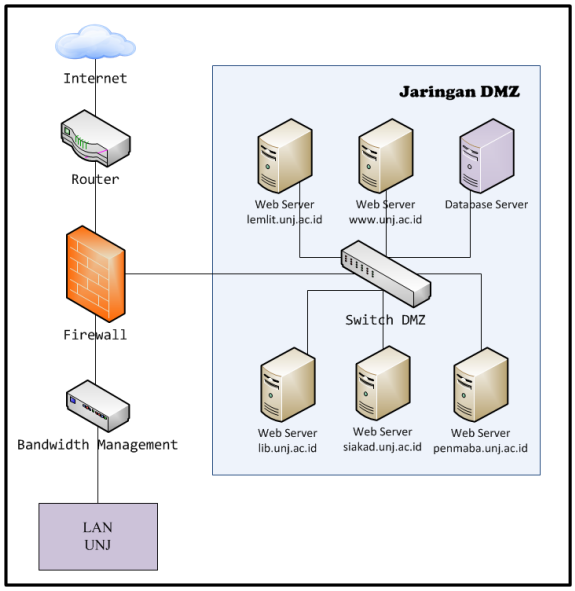
DMZ (*Demilitarized Zone*) merupakan area netral diantara jaringan publik (internet) dan jaringan intranet perusahaan yang dilindungi oleh firewall yang membatasi akses dari jaringan luar menuju host yang terletak di jaringan LAN (Lammle dan Timm, 2003: 368). Tujuan dari adanya DMZ adalah sebagai pembatas jaringan yang dapat diakses dari luar (internet) sehingga ketika terjadi serangan atau penyusupan, yang terganggu hanya jaringan DMZ saja dan tidak sampai ke jaringan internal dari organisasi atau perusahaan.

2.3 Lalu Lintas Jaringan DMZ UNJ

Dalam kamus besar bahasa Indonesia, lalu lintas di definisikan sebagai berjalan bolak balik (Pusat Pembinaan dan Pengembangan Bahasa, 1999: 556). Dalam ensiklopedia Computer Desktop, *traffic* adalah data yang ditransmisikan melalui sebuah jaringan (Freedman dan Morrison, 2014).

Jaringan DMZ Universitas Negeri Jakarta adalah sebuah area jaringan yang terletak diantara jaringan internal dan eksternal Universitas Negeri Jakarta, yang didalamnya terdapat server-server yang dapat diakses baik dari dalam maupun dari luar jaringan Universitas Negeri Jakarta (internet). Untuk lebih jelasnya dapat dilihat pada Gambar 1.

e-ISSN: 2597- 4475
http://doi.org/10.21009/pinter.1.1.7



Gambar 1. Jaringan DMZ UNJ

Lalu lintas jaringan DMZ Universitas Negeri Jakarta adalah perpindahan data secara bolak balik (dua arah) yang terjadi pada jaringan yang terletak diantara jaringan internal dan jaringan eksternal Universitas Negeri Jakarta.

3. Monitoring Jaringan

Monitoring adalah suatu proses mengukur, mencatat, mengumpulkan, memproses, dan mengkomunikasikan informasi untuk membantu pengambilan keputusan manajemen program/proyek (Clayton dan Petry, 1983: 2). Monitoring jaringan komputer adalah proses pengumpulan dan melakukan analisis terhadap data-data pada lalu lintas jaringan dengan tujuan memaksimalkan seluruh sumber daya yang dimiliki jaringan komputer.

Monitoring jaringan ini merupakan bagian dari manajemen jaringan. Monitoring jaringan memiliki peranan yang penting dalam upaya pencegahan insiden. Monitoring jaringan juga dapat memantau kondisi jaringan setiap saat, memperoleh laporan statistik, dan memperkirakan apakah ada perangkat yang perlu diganti, ditambah, atau ditiadakan. *Network monitoring* tidak dapat digunakan untuk menyelesaikan masalah ketika terjadi insiden, namun berbagai informasi yang sangat berharga dapat disajikan oleh sebuah aplikasi *network monitoring* (Sofana, 2012: 481).

Tujuan monitoring jaringan komputer adalah untuk mengumpulkan informasi yang berguna dari berbagai bagian jaringan sehingga jaringan dapat diatur dan dikontrol dengan menggunakan informasi yang telah terkumpul. Dengan begitu diharapkan jika terjadi permasalahan dalam jaringan akan cepat diketahui dan diperbaiki sehingga stabilitas jaringan lebih terjamin. Monitoring jaringan perlu dilakukan karena beberapa alasan utama berikut:

a. Menjaga stabilitas jaringan
b. Sulitnya mengawasi apa yang sedang terjadi dalam jaringan yang memiliki sejumlah besar mesin *(host)* tanpa alat pengawas yang baik.
c. Mendeteksi kesalahan pada infrastruktur jaringan, *gateway*, *server*, maupun *user*.
d. Memberikan peringatan dengan segera kepada *administrator* ketika terjadi kesalahan dalam jaringan
e. Mendokumentasikan jaringan

Terdapat banyak hal yang dapat dimonitoring dalam jaringan komputer. Salah satu yang paling sering dimonitoring adalah *load traffic* jaringan yang melewati sebuah *router* atau *interface* komputer. Untuk melakukan *monitoring load traffic* pada jaringan, dapat menggunakan *SNMP* dan *packet sniffer*.

SNMP singkatan dari *Simple Network Management Protocol*. Protokol ini digunakan untuk memonitor *device-device* yang terhubung ke jaringan akan kondisi-kondisi systemnya yang penting. Sebagai contoh penggunaan *CPU*, penggunaan *harddisk*, penggunaan *memory*, *traffic* jaringan dan lain-lain. Untuk *device-device* yang dapat dipantau adalah perangkat seperti *PC*, *Server*, atau *router*. Sedangkan untuk sistem operasi yang dapat dipantau meliputi *Linux*, **Nix*, *Windows*, atau yang lain.

Packet sniffer adalah sebuah aplikasi yang dapat melihat lalu lintas data pada jaringan komputer. *Packet sniffer* bekerja

e-ISSN: 2597- 4475
http://doi.org/10.21009/pinter.1.1.7

dengan cara mendengarkan seluruh paket yang lewat pada media komunikasi, baik itu media kabel maupun tanpa kabel. Setelah paket-paket tersebut didapatkan, kemudian paket-paket tersebut disusun ulang sehingga data yang dikirimkan dapat dibaca oleh komputer yang menjadi *sniffer*. Hal ini dapat dilakukan karena pada dasarnya semua koneksi *ethernet* adalah koneksi yang bersifat *broadcast*, di mana semua *host* dalam sebuah kelompok jaringan akan menerima paket yang dikirimkan oleh sebuah *host*. Pada keadaan normal, hanya *host* yang menjadi tujuan paket yang akan memproses paket tersebut sedangkan *host* yang lainnya akan mengabaikan paket-paket tersebut. Namun pada keadaan tertentu, sebuah host bisa merubah konfigurasi sehingga host tersebut akan memproses semua paket yang dikirimkan oleh host lainnya.

Untuk melakukan *monitoring* jaringan, terdapat banyak *software* yang tersedia baik yang gratis maupun berbayar. Berikut adalah beberapa contohnya:

a. Nagios (*http://www.nagios.org/*)
b. Cacti (*http://www.cacti.net/*)
c. MRTG (*http://oss.oetiker.ch/mrtg/*)
d. PRTG (*http://www.paessler.com/PRTG/*)

3.1 Monitoring Lalu Lintas Jaringan DMZ Universitas Negeri Jakarta

Monitoring lalu lintas jaringan DMZ Universitas Negeri Jakarta adalah proses pengumpulan dan melakukan analisis terhadap perpindahan data secara bolak balik (f*ull duplex*) yang terjadi pada jaringan yang terletak diantara jaringan internal dan jaringan eksternal Universitas Negeri Jakarta.

4. PRTG Network Monitor

PRTG *(Paessler Router Traffic Grapher)* Network Monitor merupakan sebuah perangkat lunak *monitoring* jaringan yang dibuat oleh perusahaan Paessler yang berpusat di Jerman. PRTG Network Monitor telah digunakan oleh lebih dari 150.000 *administrator* jaringan untuk memantau LAN, WAN, *server*, *website*, peralatan, URL, dan banyak lagi (Paessler AG, 2014: 17). PRTG network monitor tersedia dalam empat pilihat lisensi, yaitu *Freeware Edition*, *Special Edition*, *Trial Edition*, dan *Commercial Editions*.

PRTG Network Monitor berjalan pada mesin Windows dalam jaringan, PRTG mengumpulkan berbagai statistik dari mesin, perangkat lunak, dan perangkan lain yang ditentukan. PRTG juga menyimpan data statistik yang telah dikumpulkan sehingga penggunanya dapat melihat riwayat kerja perangkat yang dimonitor sehingga dapat merespon perubahan yang terjadi. PRTG mendukung beberapa protokol untuk mengumpulkan data berikut (Paessler AG, 2014: 21):

a. SNMP dan WMI
b. Packet Sniffing
c. Netflow, IPFIX, jFlow, dan sFlow

Secara garis besar, PRTG dapat digunakan untuk melakukan hal-hal berikut (Paessler AG, 2014: 16):

a. Pengawasan terhadap koneksi sumber daya pada jaringan
b. Mengawasi dan mengukur penggunaan bandwidth pada perangkat jaringan
c. Mencari dan menemukan serta mengakses perangkat yang ada pada jaringan
d. Mendeteksi aktivitas yang tidak seharusnya (*suspicious and malicious*) baik dari *user* maupun dari *device* yang ada dalam jaringan
e. Pengawasan terhadap penggunaan sumber daya sistem, seperti konsumsi *CPU*, penggunaan *memory*, dan sisa kapasitas *storage* yang tersedia.
f. Mengelompokkan paket-paket yang lewat pada lalu lintas jaringan berdasarkan sumber dan tujuannya.

4.1 Kebutuhan Minimal PRTG

Untuk menginstall dan bekerja dengan PRTG Network Monitor, diperlukan

e-ISSN: 2597- 4475
http://doi.org/10.21009/pinter.1.1.7

persyaratan sebagai berikut (Paessler AG, 2014: 21):

a. *PC server* atau *virtual machine* dengan kinerja rata-rata *CPU* dari sebuah *PC* rata-rata yang dibangun pada tahun 2007 atau lebih baru. Dan *RAM* paling sedikit 1024MB.
b. Sistem operasi Microsoft Windows 7, Windows 8, Server 2012, Server 2012 R2, Windows 2003 SP1 atau lebih baru, atau Windows 2008 R2 (all 32-bit or 64-bit). Windows Vista or 2008 R1 dapat digunakan tapi tidak direkomendasikan karena isu performa keduanya.
c. Peramban web *(web browser)* untuk mengakses web interface. *Browser* yang didukung diantaranya:
    i. Google Chrome 34 or later (direkomendasikan)
    ii. Mozilla Firefox 28 or later
    iii. Microsoft Internet Explorer 10 or 11

4.2 Sensor PRTG

Di dalam PRTG, sensor merupakan bagian dari *device*. Sebuah *device* bisa memiliki sejumlah sensor. Setiap sensor memantau satu aspek dari sebuah *device* yang meliputi (Paessler AG, 2014: 86):

a. Satu layanan jaringan seperi *SMTP, FTP, HTTP*.
b. Satu trafik *switch* jaringan.
c. Beban *CPU* sebuah *device.*
d. Beban *memory* sebuah *device*
e. *Traffic* pada sebuah kartu jaringan

4.3 Sensor Packet Sniffer PRTG

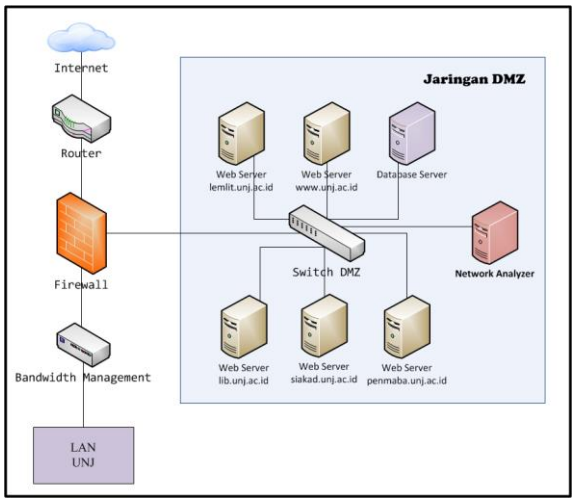
Packet sniffer adalah sebuah sensor di *PRTG* yang berfungsi untuk menginformasikan aplikasi maupun *IP Address* yang membuat lalulintas data pada jaringan. Sensor ini akan memeriksa setiap data tunggal yang berjalan melalui jaringan (Paessler AG, 2014: 714).

Sensor ini hanya dapat ditambahkan pada perangkat *probe* (perangkat yang diinstall *PRTG*) baik *local probe* maupun *remote probe*. Lalu lintas yang dapat dimonitor hanyalah lalu lintas data yang melewati *probe* yang telah dipasang sensor *packet sniffer*. Untuk memonitor lalu lintas dalam jaringan dapat dengan cara mengkonfigurasi *port monitoring* pada *switch* (jika tersedia), yang dapat mengirimkan salinan dari semua lalu lintas jaringan. Kemudian *port* tersebut dihubungkan (secara fisik) ke komputer *probe PRTG*. Dengan cara ini *PRTG* akan dapat menganalisis seluruh *traffic* pada switch. Fitur seperti ini pada hardware dapat disebut *Switched Port Analyzer (SPAN)* atau *Port Monitoring* (Paessler AG, 2014: 714).

5. Perancangan

Untuk melakukan monitoring terhadap jaringan DMZ UNJ, sebagai langkah awal perlu dilakukan observasi terhadap perangkat jaringan yang terdapat di Pustikom UNJ, khusunya perangkat jaringan yang termasuk ke dalam jaringan DMZ.

Berikutnya adalah penempatan *Network Analyzer* di jaringan DMZ. *Network Analyzer* dihubungkan ke switch DMZ pada port nomor 11 dengan menggunakan kabel UTP dengan susunan straight. Sedangkan *switch* tersebut terhubung ke *firewall* melalui port nomor 20. Untuk lebih jelasnya mengenai penempatan Network Analyzer pada jaringan DMZ UNJ dapat dilihat pada Gambar 2.



e-ISSN: 2597- 4475
http://doi.org/10.21009/pinter.1.1.7

Gambar 2. Penempatan Network Analyzer pada Jaringan DMZ Universitas Negeri Jakarta

Setelah ditempatkan di jaringan DMZ, *Network Analyzer* kemudian diinstall sistem operasi Microsoft Windows Server 2008 R2 dan juga perangkat lunak PRTG Network Monitor serta menambahkan sensor Packet Sniffer pada PRTG Network Monitor.

Terakhir adalah konfigurasi port mirroring pada *switch* DMZ. *Port mirroring* merupakan fasilitas yang terdapat pada *switch* tertentu yang berfungsi untuk menduplikasi paket data pada satu atau beberapa *port* ke sebuah *port* yang ditentukan. Paket yang diduplikasi bisa paket yang masuk ke dalam *port*, paket yang keluar dari *port*, maupun keduanya. Pada konfigurasi ini, peneliti akan melakukan *mirroring* terhadap paket data yang masuk ke *port* nomor 20 menuju port 11.

Langkah-langkah untuk melakukan konfigurasi *port mirroring* pada *switch* di jaringan DMZ meliputi sebagai berikut.

a. Buka *web browser*, kemudian masukkan alamat IP *switch* pada *address bar*.
b. Masukkan *username* dan *password* kemudian kllik *Log In*.
c. Dari menu *Configure*, pilih *Security* kemudian pilih *Port Mirroring*.
d. Ketikkan *dmz-monitor* pada isian *Analyzer Name*.
e. Dalam isian *Analyzer Port*, klik *Select* untuk memilih ge-0/0/11 sebagai *output interface*.
f. Klik *Add* untuk memilih *ingress interface*. Pilih ge-0/0/20 lalu klik *OK*.
g. Klik *OK* untuk menyimpan konfigurasi.

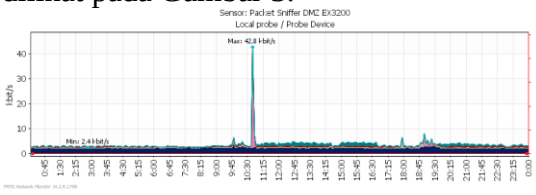
Dari langkah ini akan dihasilkan grafik *transfer rate* data yang melalui *switch* DMZ yang dapat dilihat pada sensor Packet Sniffer PRTG Network Monitor.

Pengujian terhadap hasil monitoring jaringan yang didapatkan dari sensor Packet Sniffer pada perangkat lunak PRTG didasarkan pada dua hal, yaitu:

a. Hasil dari sensor Packet Sniffer dapat menampilkan alamat IP dari perangkat-perangkat yang melakukan komunikasi melalui switch yang terdapat pada jaringan DMZ.
b. Rata-rata data transfer rate data yang masuk ke Network Analyzer harus lebih besar dari 1 Mbps. Hal ini dikarenakan pada saat penelitian berlangsung, server-server yang dimiliki UNJ sedang banyak diakses oleh user.

6. Hasil dan Pembahasan

Rata-rata transfer rate data yang diterima sensor Packet Sniffer ketika melakukan monitoring dengan cara mirroring terhadap satu port switch DMZ mendapatkan hasil 4 kbps, grafiknya dapat dilihat pada Gambar 3.

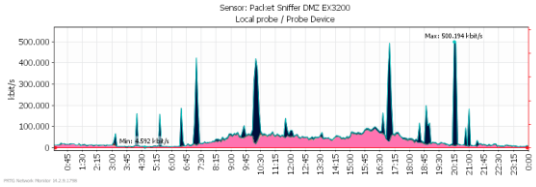


Gambar 3. Transfer Rate Data Sensor Packet Sniffer saat Silakukan Mirroring terhadap Satu Port Switch DMZ

Hasil monitoring dengan mirroring terhadap satu port switch DMZ dinyatakan belum sesuai dengan keadaan lalu lintas data pada jaringan DMZ karena meskipun sudah dapat menampilkan alamat IP dari perangkat-perangkat yang terhubung pada switch DMZ tetapi transfer rate data yang diterima sensor Packet Sniffer masih di bawah 1 Mbps. Untuk itu diperlukan perbaikan pada tahapan implementasi dengan melakukan mirroring terhadap seluruh port yang terdapat pada switch DMZ.

Rata-rata transfer rate data yang diterima sensor Packet Sniffer ketika melakukan monitoring dengan cara mirroring terhadap seluruh port switch DMZ mendapatkan hasil 50.880 kbps, grafiknya dapat dilihat pada Gambar 4.

e-ISSN: 2597- 4475
http://doi.org/10.21009/pinter.1.1.7



Gambar 4. Transfer Rate Data Sensor Packet Sniffer saat Silakukan Mirroring terhadap Seluruh Port Switch DMZ

Hasil monitoring dengan mirroring terhadap seluruh port switch DMZ dinyatakan telah sesuai dengan keadaan lalu lintas data pada jaringan DMZ karena sudah dapat menampilkan alamat IP dari perangkat-perangkat yang terhubung pada switch DMZ dan menunjukkan rata-rata transfer rate data di atas 1 Mbit/s. Selanjutnya hasil monitoring yang dihasilkan oleh sensor Packet Sniffer dapat digunakan sebagai analisis terhadap lalu lintas jaringan yang terjadi pada jaringan DMZ Universitas Negeri Jakarta.

Monitoring yang dilakukan oleh sensor Packet Sniffer PRTG, menampilkan adanya koneksi dari 192.168.XXX.XXX: 55182 menuju 178.32.137.100:10026 dengan protokol UDP dan size 7,42GB dalam kurun waktu 24 jam.

Port 10026 merupakan *port* default yang biasanya digunakan oleh layanan content filter pada postfix. Dari temuan tersebut, peneliti mengindikasikan IP 192.168.XXX.XXX sebagai alamat dari server yang telah melakukan serangan terhadap server milik pihak lain yang berada di Internet.

7. KESIMPULAN DAN SARAN

Monitoring lalu lintas jaringan menggunakan sensor Packet Sniffer pada PRTG Network Monitor telah dapat menghasilkan laporan lalu lintas jaringan DMZ Universitas Negeri Jakarta setiap hari.

Laporan lalu lintas jaringan yang dihasilkan oleh sensor Packet Sniffer pada PRTG Network Monitor dapat digunakan untuk mendeteksi adanya lalu lintas data yang tidak wajar pada jaringan DMZ UNJ dan juga dapat menginformasikan alamat IP yang menghasilkan lalu lintas data yang tidak wajar tersebut.

Untuk mencegah terulang kembalinya serangan yang dilakukan oleh server milik UNJ ke server yang berada di internet, perlu dibuat sistem keamanan jaringan komputer berupa IPS (*Intrusion Prevention System*) yang dapat mencegah terjadinya terjadinya lalu lintas data yang tidak semestinya, baik ke dalam jaringan di lingkungan Universitas Negeri Jakarta maupun ke luar jaringan Universitas Negeri Jakarta (internet). Salah satu aplikasi *open-source* yang memiliki fungsi sebagai *Intrusion Prevention System* adalah SNORT (*https://www.snort.org/*).

Daftar Pustaka:

[1] Freedman, Alan & Morrison, Irma. 2014. traffic. [terhubung berkala]. http://lookup.computerlanguage.com/host_app/search?cid=C999999&term=trtraff&lookup.x=0&lookup.y=0 [22 Juli 2014]

[2] Lammle, Told & Timm, Carl. 2003. CCSP: Securing Cisco IOS Networks. Alameda : SYBEX Inc..

[3] Paessler AG. 2014. *PRTG Network Monitor User Manual*. Nuremberg: [penerbit tidak diketahui]

[4] Sofana, Iwan. 2012. *Cisco CCNP dan Jaringan Komputer (Materi Route, Switch, & Troubleshooting)*. Bandung: Informatika.

[5] Tanenbaum, Andrew S. 1997 . *Jaringan Komputer*. Terjemahan oleh Priatna, Gurnita; & Indarto, Purnomo Wahyu. Jakarta: Prenhallindo.