ANALISIS DAN MONITORING LAYANAN INTERNET KEPADA PELANGGAN MENGGUNAKAN APLIKASI BERBASIS OPEN SOURCE (STUDI KASUS: PT JAYA KARTHA SOLUSINDO)

Kevin Christopher Bakkara[a1], I Made Agus Dwi Suarjaya [a2], A.A Ngurah Hary Susila [b3]
[a]Program Studi Teknologi Informasi, Fakultas Teknik, Universitas Udayana Bali
e-mail: [1]kevinchristopher78@yahoo.com, [2]agussuarjaya@it.unud.ac.id, [3]harysusila@unud.ac.id

Abstrak

PT Jaya Kartha Solusindo merupakan salah satu perusahaan internet service provider (ISP) di Bali dengan jumlah lebih dari 80 client. Sebagai perusahaan ISP, layanan internet yang diberikan kepada pelanggan menjadi prioritas utama untuk menciptakan internet yang stabil. PT Jaya Kartha Solusindo untuk melakukan pemantuan trafik pelanggan saat ini menggunakan The Dude dan winbox untuk melakukan kontrol jaringan. Kedua aplikasi tersebut memiliki kelemahan untuk melakukan analisis kualitas jaringan pelanggan, dikarenakan tidak adanya fungsi penyimpanan data trafik jaringan. Maka dari itu perlu penambahan aplikasi monitoring jaringan Cacti yang dapat melihat history pengguna trafik jaringan pelanggan dan aplikasi netflow NfSen yang melakukan identifikasi awal terhadap anomali jaringan pelanggan. Penelitian ini dapat mempermudah kinerja network administrator dalam menganalisa kualitas jaringan dan mendeteksi anomali jaringan pelanggan. Pada pengujian pertama melakukan pengumpulan data trafik jaringan yaitu Delay, throughput, dan packet loss selama 3 bulan dengan interval trafik jaringan selama 5 menit pada pelanggan yang menggunakan perangkat Mikrotik sebanyak 13 client. Penggunaan standarisasi TIPHON untuk penilaian kualitas jaringan ISP PT Jaya Kartha Solusindo masuk dalam kategori sangat bagus dengan hasil rata rata parameter *delay* < 150 ms, *throughput* > 100m dan *packetloss* < 3 %. Pengujian tahapan kedua melakukan identifikasi anomali jaringan antara komunikasi botnet terhadap pelanggan dengan memanfaatkan filter pada aplikasi NfSen. Hasil identifikasi anomali jaringan terdapat alamat IP yang mencurigakan berkomunikasi dengan pelanggan STIKes Bali dan pelanggan Megajaya.

Kata kunci**:** quality of service, Netflow, Cacti, NfSen, Anomali Jaringan

Abstract

PT Jaya Kartha Solusindo is one of the internet service provider(ISP) companies in Bali with more than 80 clients. As an ISP company, internet services provided to customers are a top priority to create a stable internet. PT Jaya Kartha Solusindo to monitor customer traffic currently uses The Dude and Winbox to control the network. Both applications have a weakness to analyze the quality of the customer network, due to the absence of a network traffic data storage function. Therefore, it is necessary to add a Cacti network monitoring application that can view the user history of customer network traffic and the NfSen netflow application which performs initial identification of customer network anomalies. This research can facilitate network administrator performance in analyzing network quality and detecting customer network anomalies. In the first test, we collected network traffic data, namely Delay, throughput, and packet loss for 3 months with network traffic intervals of 5 minutes on customers using Mikrotik devices as many as 13 clients. The use of TIPHON standardization to assess the quality of PT Jaya Kartha Solusindo's ISP network is in the very good category with the average parameter delay < 150 ms, throughput > 100m and packet loss < 3 %. The second stage of testing is to examine network anomalies between botnet communications to customers by using filters in the NfSen application. The results of the identification of network anomalies contained suspicious IP addresses communicating with STIKes Bali customers and Megajaya customers.

Keywords: *Quality of Service, Netflow, Cacti, Nfsen, Network Anomaly*

1. Introduction

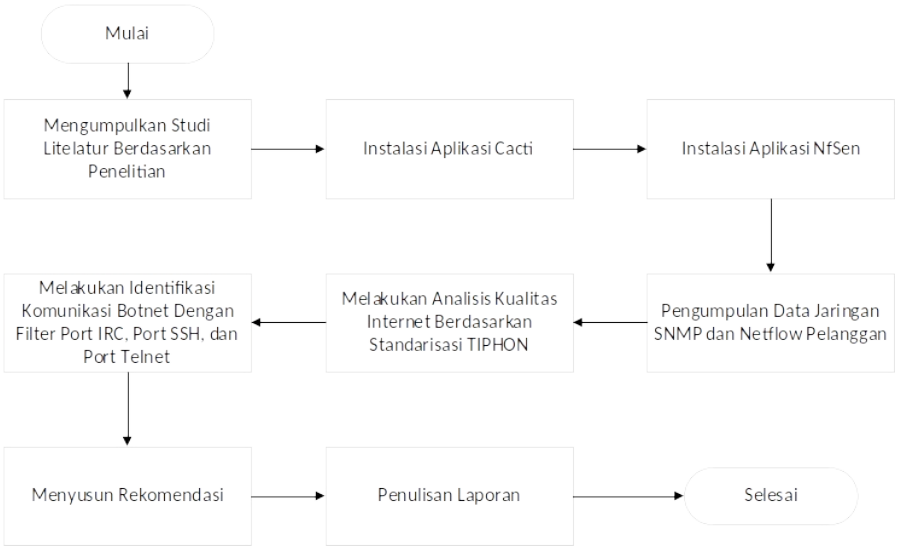
Peningkatan pengguna internet didasarkan oleh kebutuhan manusia pada zaman globalisasi ini. PT Jaya Kartha Solusindo sebagai penyedia layanan internet harus mampu mengakomodasi kualitas layanan internet yang stabil. Dalam menjamin kualitas internet, seorang *administrator* membutuhkan aplikasi yang mampu melakukan pemantuan kondisi suatu jaringan setiap saat kemudian memberikan informasi pada *administrator*[4]. Salah satu aplikasi yang dapat diandalkan untuk melakukan pemantauan jaringan dan berbasis *open source* yaitu Cacti.

Cacti merupakan aplikasi pemantauan jaringan yang menyimpan dan menampilkan data jaringan dalam bentuk grafik dengan memanfaatkan fungsi RRDTool. Kegunaan RRDTool sebagai alat *database* untuk mengelola dan mengambil data dalam urutan waktu. Data tersebut selanjutnya siap untuk ditampilkan dalam bentuk grafik. Data jaringan dapat dilakukan analisa untuk menentukan seberapa baik jaringan internet dari layanan yang diberikan atau disebut *quality of service* [8]. Parameter pengukuran *quality of service* pada jaringan diantaranya *delay*, *throughput*, dan *packetloss*.

Kualitas internet yang diberikan harus mampu meningkatkan keamanan jaringan terhadap layanan pelanggan. Peningkatan yang signifikan terhadap serangan jaringan harus mampu diidentifikasi oleh penyedia jasa layanan internet, sehingga penelitian ini memberikan rekomendasi aplikasi *open source* untuk mencegah serangan tersebut. Aplikasi NfSen merupakan aplikasi berbasis *netflow* yang melakukan *capture* terhadap aliran komunikasi jaringan dalam bentuk grafik aliran data. Fitur yang tersedia pada NfSen dapat melakukan identifikasi anomali jaringan pelanggan dengan memanfaatkan berbagai sintaks *filter* yang ingin dicapai pada penelitian ini. Tahapan ini melakukan identifikasi anomali jaringan terhadap komunikasi *botnet* kepada komputer pelanggan dengan klasifikasi komunikasi dengan *web* berbahaya, *port* IRC, *port* SSH, dan *port* Telnet.

2. Metode Penelitian

Metode peneltian menjelaskan langkah yang akan dilakukan dalam merancang analisis kualitas jaringan internet berdasarkan parameter *Delay*, *packet loss*, *throughput,* dan anomali jaringan. Hasil dari analisis jaringan pada PT Jaya Kartha Solusindo akan memberikan layanan internet yang bagus bagi pelanggan.



Gambar 1. Alur Penelitian

Pada Gambar 1 menampilkan alur penelitian dengan 7 tahapan diantaranya melakukan mengumpulkan studi literatur berdasarkan judul penelitian, melakukan instalasi aplikasi Cacti dan NfSen, melakukan pengumpulan data pelanggan (*Delay*, *packet loss*, *throughput*, dan data netflow), melakukan analisa kualitas jaringan pelanggan berdasarkan standrisasi TIPHON,

melakukan identifikasi komunikasi botnet dengan menggunakan sintaks *filter* NfSen, menyusun rekomendasi berdasarkan hasil yang didapat.

3. Kajian Pustaka

Bagian kajian pustaka memberikan ilmu teori dasar yang berkaitan dengan penelitian ini. Teori-teori penunjang yang akan dipaparkan antara lain *monitoring* jaringan, *quality of service*, dan anomali jaringan.

3.1 Monitoring Jaringan

Aktivitas untuk mengatur atau mengelola sistem jaringan yang berada pada tempat tertentu dan topologi jaringan disebut monitoring jaringan [1]. *Monitoring* jaringan menggunakan trafik jaringan untuk menampilkan paket data jaringan sebenarnya pada suatu topologi jaringan. Manfaat *monitoring jaringan* yaitu mengumpulkan data jaringan dari setiap *node* jaringan yang bertujuan untuk pengambilan keputusan dari data jaringan yang terkumpul [10]

3.2 Quality of Service

Quality of Service (QoS) merupakan metode untuk mengetahui kemampuan suatu jaringan, mengontrol layanan jaringan yang berkualitas, dan mengetahui karakteristik suatu jaringan. QoS memiliki fungsi untuk mengetahui kinerja setiap *node* yang telah ditentukan dalam memberikan layanan internet. Terdapat beberapa parameter dalam mengetahui QoS dalam suatu jaringan sebgai berikut.

Throughput merupakan waktu pengiriman data dari sumber ke tujuan yang berhasil yang diukur dengan satuan bps. Perhitungan menentukan parameter *throughput* ialah paket data yang diterima pada setiap *node* dibagi dengan lama pengamatan tertentu. Perhitungan untuk mengukur nilai throughput digunakan dengan persamaan berikut ini.

$$Throughput = \frac{\text{Paket data yang diterima}}{\text{Lama pengamatan}}$$

Table 1. Kategori Nilai Throughput

Nilai Throughput (bps)	Indeks	Kategori
<25	1	Buruk
50	2	Cukup
75	3	Efektif
100	4	Sangat Efektif

Delay merupakan keterlambatan waktu untuk menempuh pengiriman data dari sumber ke tujuan. Penyebab terjadinya *delay* dipengaruhi oleh media fisik, jarak, dan waktu proses yang lama. Penilaian kategori parameter *delay* menggunakan standarisasi TIPHON diantaranya sebagai berikut.

Table 2. Kategori Nilai Delay

Nilai Delay (ms)	Indeks	Kategori
<450 ms	1	Buruk
300 ms s/d 450 ms	2	Cukup
150 ms s/d 300 ms	3	Efektif
<150 ms	4	Sangat Efektif

Perhitungan menentukan parameter *Delay* ialah total waktu lama pengiriman dibagi dengan total paket data yang diterima. Pada Tabel 2 menampilkan bahwa semakin besar nilai *delay* maka kualitas jaringan semakin buruk dan semakin kecil nilai *delay* maka kualitas jaringan sangat efektif. Rumus untuk mengukur parameter *delay* dengan persamaan berikut ini.

$$Delay = \frac{\text{Total } delay}{\text{Total paket data yang diterima}}$$

Packet loss merupakan keadaan dimana total persentase paket data yang hilang dalam pengiriman dari sumber ke tempat tujuan. Penyebab terjadinya *packetloss* dipengaruhi oleh antrian pengiriman data yang berlebih, *node* yang bekerja melebihi kapasitas *buffer*, dan tidak adanya kontrol untuk memastikan trafik jaringan berjalan baik. Penilaian kategori parameter *packet loss* menggunakan standarisasi TIPHON diantaranya sebagai berikut.

Table 3. Kategori Nilai Packet Loss

Nilai Packet Loss (%)	Indeks	Kategori
25 %	1	Buruk
15 %	2	Cukup
3 %	3	Efekf
0 %	4	Sangat Efektif

Perhitungan menentukan parameter *packet loss* ialah selisih paket data dikirim dengan paket data yang diterima lalu dibagi paket data yang diterima dan dikali dengan 100%. Rumus untuk mengukur parameter *packet loss* dengan persamaan berikut ini.

$$\textit{Packet loss} = \frac{\text{Paket data dikirim} - \text{paket data diterima}}{\text{Paket data diterima}} x\ 100\ \%$$

3.3 Anomali Jaringan

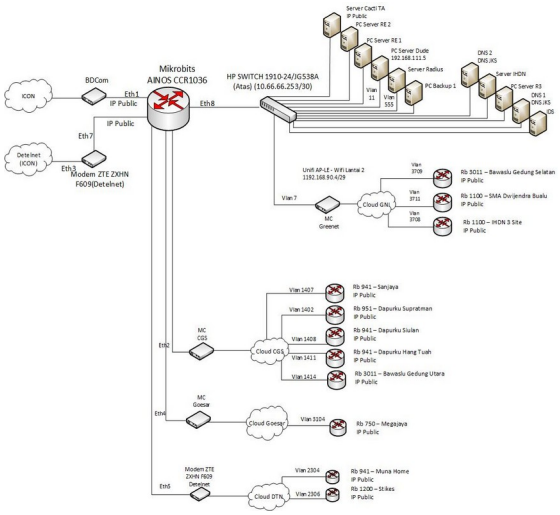
Anomali jaringan dilakukan untuk mendeteksi terjadinya gangguan keamanan jaringan komputer berdasarkan pola – pola anomali yang ditimbulkan. Serangan keamanan jaringan terdiri atas 2 yaitu serangan pasif yang melakukan serangan hanya untuk mendapatkan informasi dari sumber daya sistem tetapi tidak diubah dan serangan aktif melakukan penyerangan untuk mengakses, mengubah, menonaktifkan atau menghancurkan sumber daya sistem korban. *Botnet* adalah suatu program atau skrip yang diracang untuk melakukan fungsi yang telah ditentukan secara berulang dan otomatis setelah dipicu secara sengaja atau menyeluruh terhadap infeksi sistem. *Botnet* terdiri dari server bot (*Command and Conquer*) atau *server* yang dikendalikan oleh *botmaster* dan beberapa *botclients*. Botclients disebut dengan *zombie* atau *drone*.

Metode menggunakan algoritma non-intrusif yang dapat diskalakan dengan menganalisis data secara pasif pada tautan jaringan. Analisis menggunakan aktivitas *host* yang mencurigakan seperti melakukan pemindaian, mengirim *spam*, dan pembuatan lalu lintas DDoS. Aliran koneksi mencurigakan antara *bot* dan *host* disebut sebagai *candidate controller conversation* (CCC). CCC adalah aliran yang menggunakan IRC nomor port TCP/6667, TCP/6668, dan TCP/7000. Analisa CCC terdiri dari tiga bagian utama yaitu perhitungan jumlah *bot* yang dicurigai untuk alamat atau *port* server jarak jauh, perhitungan jarak antara lalu lintas ke *port* server jauh dan lalu lintas model, dan perhitungan skor heuristik untuk alamat server yang tetap menjadi kandidat dari bagian sebelumnya. Setelah jumlah *bot* unik yang dicurigai server jarak jauh dihitung dan diurutkan berdasarkan jumlah *bot* yang dicurigai.

4. Hasil dan Pembahasan

Adapun hasil dari penelitian ini berisi tentang topologi jaringan, kualitas jaringan, dan anomali jaringan pelanggan ISP PT Jaya Kartha Solusindo. Analisa kualitas tersebut menggunakan dua aplikasi berbasis *open source* yaitu aplikasi Cacti dan aplikasi NfSen.

4.1. Topologi Jaringan



Gambar 2. Topologi Penelitian PT Jaya Kartha Solusindo

Gambar 2 dijelaskan bahwa router mikrobits AINOS CCR1036 merupakan router utama yang mendapatkan bandwidth dari ICON dan backup Detelnet (ICON) untuk menyalurkan ke pelanggan. Router mikrobits AINOS CCR1036 terhubung dengan 2 switch yaitu HP SWITCH 1910-24/JG538A untuk memberikan layanan internet ke server PT Jaya Kartha Solusindo dengan media transmisi kabel LAN serta pelanggan terhubung melalui transmisi *fiber optic* dan HP SWITCH 1910-24/JG538A (Bawah)10.11.11.2/30) memberikan layanan internet ke *office* PT Jaya Kartha Solusindo dengan media transmisi kabel LAN. Router Dari router utama juga terhubung langsung ke perusahaan penyedia *link*(*fiber optic*) untuk menyebarkan jaringan internet kepada pelanggan yang terhubung menggunakan router mikrotik. Penelitian ini menggunakan miniPC sebagai server yang dapat terhubung langsung kepada router utama dan mendapatkan IP *public* 103.207.96.3 sehingga penulis dapat melakukan akses secara *mobile*. Daftar pelanggan dalam penelitian ini khusus yang menggunakan router mikrotik yang terdiri atas 13 *client* diantaranya sebagai berikut.

Tabel 3. Daftar Pelanggan PT Jaya Kartha Solusindo

No	IP	Nama Pelanggan	Bandwidth		Link
			Dedicated / Up To	Kecepatan	
1	103.207.96.94	Vlan 1407 Sanjaya	Up To	5 Mbps	PT CGS
2	103.207.97.30	Vlan DTN 2304 - Muna Home	Up To	5 Mbps	PT Detelnet
3	103.207.96.254	Vlan DTN 2306 Stikes Bali	Dedicated	100 Mbps	PT Detelnet
4	103.207.96.82	Vlan 3709 Greenet - Bawaslu Gedung Selatan	Dedicated	50 Mbps	PT Greenet
5	103.207.96.74	Vlan 1414 Bawaslu Gedung Utara	Dedicated	50 Mbps	PT CGS
6	103.207.97.238	Vlan 3711SMA Dwijendra Bualu	Dedicated	50 Mbps	PT Greenet
7	103.207.96.26	Vlan Ratna Dedi	Dedicated	200 Mbps	PT Greenet
8	103.207.96.66	3708 Greenet –	Dedicated	75 Mbps	PT Greenet

No	IP	Nama Pelanggan	Bandwidth		Link
			Dedicated / Up To	Kecepatan	
9	103.207.96.78	IHDN Pasca 3708 Greenet – IHDN Brahma	Dedicated	75 Mbps	PT Greenet
10	103.207.96.150	Vlan Megajaya	Dedicated	100 Mbps	PT Goesar
11	103.207.96.242	VLAN 1411 Dapurku Hangtuah	Dedicated	5 Mbps	PT CGS
12	103.207.96.70	Vlan 1408 Dapurku Siulan	Dedicated	5 Mbps	PT CGS
13	103.207.96.146	Vlan 1414 Dapurku Supratman	Dedicated	5 Mbps	PT CGS

4.2. Hasil *Quality of Service*

Pengumpulan data jaringan *client* menggunakan apliksi Cacti dengan waktu nilai rata-rata 5 menit dalam sehari dari tanggal 4 Juni 2020 pukul 06:00 WITA sampai tanggal 3 September 2020 pukul 23:55 WITA. Pengolahan data jaringan *client* PT Jaya Kartha Solusindo dilakukan penilaian berdasarkan standrisasi TIPHON. Berikut hasil kualitas jaringan ISP PT Jaya Kartha Solusindo pada Tabel 4.

Table 4. Hasil Rata – Rata Nilai Kualitas Jaringan Pelanggan

Router Pelanggan	Parameter				Kategori
	Bandwidth Inbound (Kbps)	Bandwidth Outbound (Kbps)	Packet Loss (%)	Delay (ms)	
Vlan 1407 Sanjaya	31.4 Kbps	462.9 Kbps	0.012 %	2.2 ms	Sangat Efektif
Vlan DTN 2304 - Muna Home	59.7 Kbps	1,023 Kbps	0.008 %	8.6 ms	Sangat Efektif
Vlan DTN 2306 Stikes Bali	1,760 Kbps	12,788 Kbps	0.008%	8.2 ms	Sangat Efektif
Vlan 3709 Greenet - Bawaslu Gedung Selatan	128.6 Kbps	1,655 Kbps	0.0009 %	0.9 ms	Sangat Efektif
Vlan 1414 Bawaslu Gedung Utara	165.4 Kbps	1,598 Kbps	0.01 %	1.4 ms	Sangat Efektif
Vlan 3711SMA Dwijendra Bualu	32.6 Kbps	322.2 Kbps	0.001 %	1.2 ms	Sangat Efektif
Vlan Ratna Dedi	945.6 Kbps	6,147 Kbps	0.0009 %	0.9 ms	Sangat Efektif
3708 Greenet – IHDN Pasca	132.04 Kbps	1,194 Kbps	0.0009 %	0.9 ms	Sangat Efektif
3708 Greenet – IHDN Brahma	413.5 Kbps	3,491 Kbps	0.0009 %	0.9 ms	Sangat Efektif
Vlan Megajaya	338.3 Kbps	3,444 Kbps	0.0009 %	0.9 ms	Sangat Efektif
VLAN 1411 Dapurku Hangtuah	158.7 Kbps	882.4 Kbps	0.005 %	5.1 ms	Sangat Efektif
Vlan 1408 Dapurku Siulan	67.4 Kbps	428.9 Kbps	0.003 %	3.07 ms	Sangat Efektif
Vlan 1414 Dapurku	228.5 Kbps	1,421 Kbps	0.01 %	16.2 ms	Sangat Efektif

Router Pelanggan	Parameter				Kategori
	Bandwidth Inbound (Kbps)	Bandwidth Outbound (Kbps)	Packet Loss (%)	Delay (ms)	
Supratman					

Tabel 4 menjelaskan bahwa hasil analisa kualitas jaringan berdasarkan TIPHON dengan parameter *latency* pada pelanggan bernilai sangat bagus dengan rata-rata <150 ms, parameter *bandwidth inbound* pada pelanggan bernilai sangat bagus dengan rata rata > 100 bps, parameter *bandwidth outbound* pada pelanggan bernilai sangat bagus dengan rata rata > 100 bps dan parameter *packet loss* bernilai sangat bagus dengan rata rata < 3%. Berdasarkan hasil indeks parameter *quality of service* yang telah diukur didapatkan bahwa kualitas ISP PT Jaya Kartha Solusindo kepada pelanggan bernilai Sangat Efektif berdasarkan standarisasi TIPHON.

4.3. Analisa Anomali Jaringan

Analisis anomali jaringan pelanggan berfokus pada perliku keseluruhan router jaringan pelanggan didasarkan untuk mengetahui ancaman yang akan terjadi dan meningkatkan kemanan jaringan. Analisis ini menggunakan sistem *netflow* yaitu NFSen untuk menganalisis statik dan trafik jaringan. Metode analisis anomali jaringan menggunakan *history* trafik untuk memprediksikan karakteristik jaringan dengan memanfaatkan filter komunikasi jaringan antara lain *port* IRC dan *port* SSH.

Deteksi trafik *botnet* menggunakan port IRC pada penelitian ini didasarkan untuk mengetahui pola yang terjadi pada *anomaly* jaringan pada pelanggan yang dilakukan oleh *bot* IRC. Deteksi adanya komunikasi *botnet* dengan IRC sebelumnya sudah dilakukan dengan menggunakan aplikasi *netflow* NfSen dengan menggunakan sintaks filter “port TCP and (source net ip local) and (not destination net ip local) and ((destination port>6660 and destination port 7000” [3]. Aktifitas *bot* yang menggunakan *port* IRC yang terhubung antara komputer target dengan *bot* bersifat pasif, yang mana *anomaly* jaringan akan timbul ketika akan ada perintah. Pendekatan menggunakan *port* IRC untuk mengetahui *botnet* memliki tingkat positif palsu yang tinggi, tetapi bagus untuk mengetahui *anomaly* jaringan secara mendasar. Pemeriksaan *port* IRC dengan menggunakan filter aplikasi NfSen akan menampilkan alamat IP luar yang berkomunikasi dengan IP jaringan lokal. Berikut deteksi *botnet* dengan komputer pelanggan PT Jaya Kartha Solusindo.

Table 5. Hasil Identifikasi Botnet Port IRC

Pelanggan	Src IP Pelanggan	Total Flow
IHDN Pasca	10.5.50.111	9
	10.5.50.22	1
	10.5.50.127	16
STIKes Bali	10.5.50.239	5
	192.168.10.250	28
	192.168.30.4	162
IHDN Ratna	10.88.88.2	4
	10.51.88.113	2
	10.51.89.182	1
	10.51.89.170	1
	10.51.89.250	7
	10.51.89.97	1
	192.168.44.44	1
IHDN Brahma	10.5.50.166	3
	10.5.50.38	3
Sanjaya	192.168.1.63	20
	192.168.1.131	2
Dapurku Supratman	192.168.1.101	4
	172.16.46.4	3

Pelanggan	Src IP Pelanggan	Total Flow
Bawaslu Selatan	192.168.1.250	20
	192.168.1.44	10
	192.168.10.35	3
Bawaslu Utara	192.168.20.62	27
	192.168.20.6	3

Deteksi trafik botnet menggunakan *port* SSH dan Telnet pada penelitian ini didasarkan untuk mengetahui pola yang terjadi pada *anomaly* jaringan pada pelanggan yang dilakukan oleh *bot* SSH dan Telnet. Aktifitas *bot* yang menggunakan *port* SSH dan Telnet yang terhubung antara komputer target dengan *bot* untuk mengontrol perangkat target secara *remote* atau dari jarak jauh. Pendekatan menggunakan *port* ssh dan telnet mampu mengetahui komunikasi atau pengiriman data antara *botnet* dengan target. Pemeriksaan *port* SSH dan Telnet dengan menggunakan filter aplikasi NfSen "((*source* net IP local and (destination port 22 or destination port 23) or ((destination net IP local and (*source* port 22 or *source* port 23))" akan menampilkan alamat IP *public* yang berkomunikasi dengan IP jaringan lokal.

Table 6. Hasil Identifikasi Botnet Port SSH dan Telnet

Pelanggan	Src IP Pelanggan	Total Flow
Dapurku Supratman	192.168.1.101	98
	192.168.30.4	8
STIKes Bali	192.168.26.18	5
	192.168.26.10	1
IHDN Ratna	10.88.88.2	146

5. Kesimpulan

Berdasarkan analisis kualitas jaringan yang menggunakan aplikasi Cacti dengan parameter *thorugput*, *latency*, dan *packet loss*. Terdapat 13 pelanggan PT Jaya Kartha Solusindo dibagi berdasarkan intansi yaitu sekolah atau universitas (STIKes Bali, SMA Dwijendra Bualu, IHDN Brahma, IHDN Pasca, dan IHDN Ratna Dedi), hotel (Munahome dan Megajaya), toko (Dapurku Hangtuah, Dapurku Siulan, Dapurku Supratman, dan Sanjaya), dan perkantoran (Gedung Utara Badan Pengawas Pemilu dan Gedung Selatan Badan Pengawas Pemilu). Hasil analisa kualitas jaringan berdasarkan TIPHON bernilai Sangat Efektif.

Sistem identifikasi berbasis *Netflow* mampu mengidentifikasi trafik jaringan yang tidak normal pada jaringan pelanggan. Pemanfaatan aplikasi NfSen pada penelitian ini mampu mendapatkan trafik pelanggan yang teridentifikasi menggunakan *port – port* yang umum digunakan *botnet* dalam melakukan penyerangan. Sehingga data jaringan pelanggan dapat dilakukan investigasi oleh *network administrator* dalam menentukan kebijakan dalam penanganan jaringan pelanggan.

Daftar Pustaka

[1] Agustina, R. M., Purnama, I., & Anwar, M. (2013). Monitoring Jaringan Menggunakan Mikrotik OS dan The Dude. *Jurnal Teknologi Universitas Kanjuruhan Malang*, Vol.6. No.2. pp.124-130.

[2] Asmunin, A., & Khamdani, W. (2016). Sistem Monitoring Resource pada Jaringan FMIPA Unesa dengan Protocol SNMP. *MULTINETICS*, Vol.2, No.1, pp.8-12

[3] Beneš, M. (2015). *Botnet Detection Based on Network.* Brno: Masaryk university.

[4] Farma, I. U., Affandi, A., & Setijadi, E. (2013). Performansi Parameter Throughput Pada Aplikasi DIAMON. *JURNAL TEKNIK POMITS*, Vol. 2, No. 1, page 39-41.

[5] Geges, S., & Wibisono, W. (2015). Pengembangan Pencegahan Serangan Distributed Denial Of Service (Ddos) Pada Sumber Daya Jaringan Dengan Integrasi Network Behavior Analysis Dan Client Puzzle. *JUTI*, Vol. 13, No.1.

[6] Iftikhar, U., Asrar, K., Waqas, M., & Ali, S. A. (2020). BOTNETs: A Network Security Issue From Definition to Detection and Prevention. *IJACSA*, Vol. 11, No. 11.

[7] Pramecwari, K. T., Sastra, N. P., & Wiharta, D. M. (2017). NetFlow dalam Monitoring Penggunaan Internet . *Teknologi Elektro*, Vol. 16, No. 03.
[8] Safrial , A., Triyono, J., & Rr, Y. R. (2017). Analisis Kinerja Wireless Access Point (Wap) Dan Virtual Access Point (VAP) Pad. *Jurnal JARKOM* , Vol. 3, No. 2, page 22-34.
[9] Saitović, E., & I. I. (2011). *Network Monitoring and Management.* Belgrade: AMRES.
[10] Saputra, R. (2016). *Perancangan Dan Implementasi Aplikasi Sistem Monitoring Jaringan Berbasis Web (Studi Kasus Telkom University).* Bandung: Universitas Telkom, D3 Teknik Telekomunikasi.

.