Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer e-ISSN: 2548-964X
Vol. 6, No. 6, Juni 2022, hlm. 2664-2672 http://j-ptiik.ub.ac.id

Penerapan *Elastic Stack* sebagai *Platform* Visualisasi dan Analisis Trafik pada Jaringan Riset dan Edukasi

Muhammad Rafi Fauzan Fathin[1], Achmad Basuki[2], Adhitya Bhawiyuga[3]

Program Studi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Brawijaya
Email: [1]raxerhunter@gmail.com, [2]abazh@ub.ac.id, [3]bhawiyuga@ub.ac.id

Abstrak

Monitoring jaringan merupakan salah satu bagian penting dalam jaringan komputer, dimana *monitoring* berfungsi untuk memantau status dan aktivitas pada perangkat jaringan. Untuk menjamin keamanan dan kualitas jaringan secara efektif, diperlukan *monitoring* yang dapat memberikan informasi lalu lintas jaringan dengan detail. Namun, secara umum, *monitoring* jaringan masih banyak yang menggunakan Simple Network Management Protocol (SNMP) karena telah menjadi standar industri dalam *monitoring* jaringan. Pada kasus *monitoring* jaringan dengan cakupan luas seperti IDREN, penggunaan protokol SNMP dinilai oleh pengelola kurang efektif, karena hanya memberikan visibilitas data yang minim dan mengukur penggunaan *bandwidth*. Tugas akhir ini mengusulkan *platform monitoring* atau visualisasi dan analisis lalu lintas jaringan riset dan edukasi menggunakan Elastic Stack, karena dapat menampilkan data lalu lintas jaringan secara detail dalam berbagai tampilan. Implementasi platform visualisasi dan analisis lalu lintas jaringan pada tugas akhir ini memerlukan dua komponen utama, yaitu: router dengan protokol Netflow dan server Elastic Stack. Router yang memiliki protokol Netflow digunakan sebagai *gate* atau gerbang keluar masuknya lalu lintas jaringan sekaligus mengumpulkan metadata pada jaringan IP dan mengirimkannya menuju Netflow Collector. Sedangkan Elastic Stack digunakan sebagai pengganti Netflow Collector menggunakan sistem Logstash, penyimpanan dan analisis metadata menggunakan sistem Elasticsearch, dan visualisasi dengan bantuan Kibana. Hasil pengujian menunjukkan bahwa *platform* visualisasi dan analisis yang diimplementasikan berjalan sesuai dengan fungsinya dalam memberikan data lalulintas jaringan secara detail dalam berbagai tampilan visualisasi. Berdasarkan pengujian, performa Elastic Stack sebagai platform visualisasi dan analisis trafik jaringan dapat mengelola data sejumlah 97 B hingga 110 MB per-30 menit dan menampilkan data tersebut dalam berbagai visualisasi dan analisis secara *realtime*.

Kata kunci: *Monitoring, SNMP, ELK Stack, Autonomus System, Netflow*

Abstract

Network monitoring is an essential part of a computer network, where monitoring functions monitor the status and activity of network devices. To effectively ensure the security and quality of the network, monitoring is needed to provide detailed network traffic information. However, in general, many network monitoring uses the Simple Network Management Protocol (SNMP) because it has become the industry standard in network monitoring. In the case of network monitoring with wide coverage, such as IDREN, using the SNMP protocol is considered by the manager to be less effective, because it only provides minimal data visibility and measures bandwidth usage. This final project proposes a monitoring platform or visualization and analysis of research and education network traffic using Elastic Stack because it can display detailed network traffic data in various appearance. Implementation of network traffic visualization and analysis platform in this research requires two main components: a router with the Netflow protocol and an Elastic Stack Server. Routers that already have the Netflow protocol are used as gateways for incoming and outgoing network traffic, collecting metadata on the IP network and sending it to the Netflow Collector. Meanwhile, Elastic Stack is used instead of Netflow Collector using the Logstash system, metadata storage and analysis using the Elasticsearch system, and visualization with the help of Kibana. The test results show that the visualization and analysis platform implemented runs according to its function in providing detailed network traffic data in various visualization displays. Based on the test, the performance of Elastic Stack as a network traffic visualization and analysis platform can manage data from 97 B to 110 MB per 30 minutes and display

that data in various visualizations and analyses in real-time.

Keywords: *Monitoring, SNMP, ELK Stack, Autonomus System, Netflow*

1. PENDAHULUAN

Jurnal Sistem Monitoring Jaringan merupakan sistem yang berfungsi untuk memantau aktivitas pada perangkat jaringan. Monitoring digunakan untuk mengetahui perangkat jaringan mana yang mati dan hidup (Suyadi & Wibowo, 2019). Sistem Monitoring jaringan mencakup perangkat lunak dan perangkat keras yang dapat melacak berbagai aspek jaringan dan operasinya, seperti lalu lintas, pemanfaatan bandwidth, dan waktu aktif. Sistem ini dapat mendeteksi perangkat dan elemen lain yang membentuk atau menyentuh jaringan, serta memberikan pembaruan status (CISCO, 2021).

Pada umumnya monitoring jaringan menggunakan Simple Network Management Protocol (SNMP) karena telah menjadi standar industri dalam monitoring jaringan. Standar industri ini terdiri dari Network Management System (NMS) dan SNMP Agent. NMS bertugas untuk mendapatkan dan pengolahan data dari perangkat jaringan yang dipantau. SNMP Agent terimplementasi pada router, server dan perangkat jaringan lainnya. Hasil monitoring akan disajikan dalam bentuk grafik fluktuasi dari tiap agen SNMPT yang dipantau (Asmunin & Wahyu Khamdani, 2016). SNMP bekerja sangat baik dalam mendapatkan visibilitas jaringan dan mengukur penggunaan bandwidth jaringan. Namun protocol ini tidak terlalu baik dalam memberikan detail yang dapat membantu admin jaringan untuk memahami apa yang terjadi dengan jaringan mereka.

Hingga saat ini monitoring jaringan yang ada pada IDREN masih menggunakan protocol SNMP dan sistem CACTI, yaitu aplikasi berbasis website untuk melakukan monitoring jaringan. CACTI merupakan solusi pembuatan grafik network yang lengkap yang didesain untuk memanfaatkan kemampuan fungsi RRDTool sebagai penyimpanan data dan pembuatan grafik (Biznetgio, 2020). Sayangnya karena hanya dapat membuat grafik dari lalu lintas jaringan, CACTI dirasa kurang tepat untuk pengelolaan jaringan sebesar IDREN. Maka dari itu, IDREN membutuhkan sistem monitoring modern yang dapat memudahkan administrator jaringan untuk mengawasi serta mengelola jaringan dengan efektif.

Infrastruktur pada tingkat perbankan, perusahaan, ISP dan lembaga Pendidikan seperti IDREN, memerlukan monitoring jaringan yang besar. Karena monitoring data dari sumber IP sangat sulit dilakukan, maka kita dapat menggantinya dengan memantau data lalu lintas AS (Autonomus) menggunakan Netflow. Netflow adalah fitur yang diperkenalkan pada router Cisco yang memberikan kemampuan untuk mengumpulkan lalu lintas jaringan IP. Dengan menganalisis data yang disediakan oleh Netflow, administrator jaringan dapat menentukan hal-hal seperti sumber dan tujuan lalu lintas, kelas layanan, dan penyebab terjadinya kemacetan. Netflow terdiri dari tiga komponen: Flow Caching, Flow Collector, dan Data Analyzer. Keuntungan Netflow dibandingkan metode pemantauan lain seperti SNMP adalah ada banyak paket perangkat lunak analisis lalu lintas (penganalisis data) yang ada untuk menarik data dari paket Netflow dan menyajikannya dengan cara yang lebih ramah pengguna (Cecil, A Summary of Network Traffic Monitoring and Analysis Techniques, n.d.).

Pada penelitian berjudul Operational Security, Threat Intelligence & Distributed Computing: The WLCG Security Operations Center Working Group, Davids Croocks dkk. melakukan monitoring jaringan menggunakan ELK Elasticsearch, Logstash, Kibana) dan Elastiflow. Monitoring jaringan dilakukan dengan mengubah konfigurasi default Logstah ke Elastiflow, membuat Logstah supaya dapat meneriman dan mengelola data dari Netflow, serta mengirimkannya dalam bentuk file ke Elasticsearch agar kumpulan data tesebut dapat dianalisis (Crooks, et al., 2019).

Hal tersebut dapat dilakukan dengan mudah menggunakan bantuan Kibana yang berfungsi untuk menampilkan hasil analisis data dari Netflow pada index file menjadi berbagai macam visualisasi, seperti: diagram lingkaran untuk menunjukkan 10 Traffic Autonomous System dan IP tertinggi, Sankey Visualization untuk menampilkan alur lalu lintas antar Autonomous System dan IP, pemetaan Client/Server dan Source/Destination berdasarkan Geo IP, daftar protocol yang sering digunakan, resiko keamanan, dll.

Penelitian ini bertujuan untuk mengimplementasikan teknologi Netflow dan ELK Stack, untuk mengembangkan sebuah sistem platform visualisasi dan analisis yang dapat memberikan data secara detail, baik dari dari inbound ataupun outbound lalu lintas jaringan. Data tersebut harus dapat digunakan untuk menciptakan visualisasi yang bisa dimanfaatkan dan dikelola oleh administrasi jaringan.

Berdasarkan permasalahan pada monitoring jaringan IDREN yang masih menggunakan protocol SNMP dan sistem Cacti, dapat diidentifikasi bahwa informasi tampilan data lalu lintas jaringan tidak memiliki informasi detail yang dapat membantu admin jaringan dalam kegiatan monitoring.

Pada penelitian ini penulis menggunakan Netflow untuk mengumpulkan lalu lintas jaringan dari gerbang jaringan IDREN di berapa universitas di Indonesia. Data yang disediakan oleh Netflow akan memberikan informasi yang cukup detail seperti sumber dan tujuan lalu lintas, kelas layanan, dan penyebab terjadinya kemacetan. Data lalu lintas jaringan tersebut kemudian dianalisis dan dikirimkan pada ELK Stack untuk dikelola dan divisualisasi agar dapat membantu admin jaringan untuk memahami apa yang terjadi dengan jaringan mereka.

2. LANDASAN KEPUSTAKAAN

2.1 Monitoring Jaringan

Gambar 2.1 Contoh Monitoring Jaringan

Monitoring jaringan adalah proses penting dalam dunia teknologi informasi yang berfungsi untuk melacak komponen dan endpoints jaringan, dan menyediakan monitoring kesalahan, kinerja, dan lalu lintas jaringan. Hal ini meliputi monitoring masalah kritis suatu jaringan, menyediakan deteksi kesalahan, dan monitoring kesehatan berbagai elemen jaringan dari tingkat perangkat ke tingkat protokol dan antarmuka (site24x7, n.d.).

2.2 ELK Stack

Gambar 2.2 Elastic Stack

ELK Stack adalah salah satu solusi log manajemen, dimana solusi ini berbasis *open source* yang dapat mencatat seluruh log dari perangkat infrastruktur IT secara real-time. Adapun ELK Stack terdiri dari empat komponen berbeda, yaitu: Beats/Netflow, Logstash, Elasticsearch, dan Kibana.

Keempat komponen di atas saling bekerjasama untuk memonitor dan mengamankan infrastruktur IT secara real-time. Melihat Gambar 2.2 ELK Stack di atas, dapat disimpulkan bahwa log dari seluruh perangkat yang ada di infrastruktur IT dikumpulkan oleh Filebeat atau Netflow untuk dikirim ke Logstash. Kemudian, Logstash akan memproses dan mengindeks log ke Elasticsearch agar dapat disimpan dan dicari oleh user, yang kemudian dapat divisualisasikan melalui Kibana (i-3, 2020).

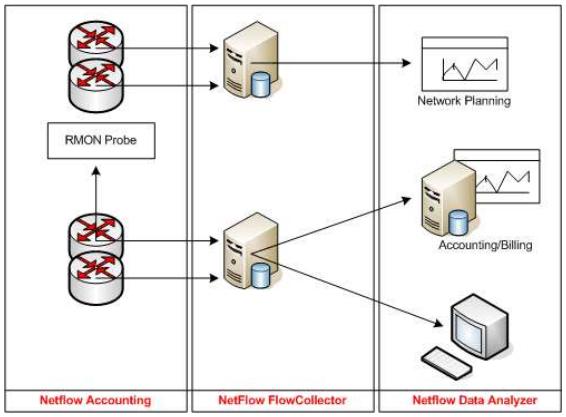
2.3 Elastiflow

Gambar 2.3 Elastiflow

ElastiFlow adalah alat untuk menganalisis NetFlow yang bekerja dengan ELK Stack. Alat ini menyediakan pengumpulan dan visualisasi data lalu lintas jaringan dengan menggunakan bantuan Elastic Stack. ElastiFlow Unified Flow Collector menerima, menakukan dekode, mengubah, menormalkan, menerjemahkan, dan memperkaya catatan lalu lintas jaringan dan telemetri yang dikirim dari perangkat jaringan

dan aplikasi menggunakan IPFIX, Netflow, dan sFlow. Catatan yang dihasilkan dapat dikirim ke berbagai distribusi dan layanan Elasticsearch (Elastiflow, n.d.). Selain itu, Elastiflow Analyzer menyediakan sejumlah dasbor siap pakai yang membuat analisis aliran data menjadi lebih mudah (NetEye, 2021). Untuk menginstal dan mengkonfigurasi ElastiFlow, pertama-tama kita harus terlebih dahulu memiliki environment ELK Stack yang telah berjalan dengan normal. Kemudian baru kita dapat menghubungkan data dari Elasticflow ke dalam environment ELK Stack untuk dianalisa dan divisualisasi.

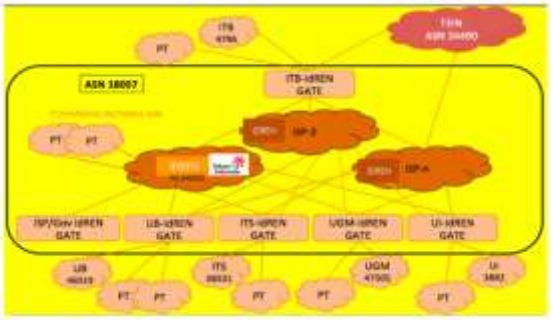
2.4 Netflow



Gambar 2.4 Netflow

Netflow adalah fitur yang diperkenalkan pada router Cisco yang memberikan kemampuan untuk mengumpulkan lalu lintas jaringan IP dari berbagai router. Dengan menganalisis data yang disediakan oleh Netflow, administrator jaringan dapat menentukan hal-hal seperti sumber dan tujuan lalu lintas, kelas layanan, dan penyebab terjadinya kemacetan. (Cecil, A Summary of Network Traffic Monitoring and Analysis Techniques, n.d.).

2.5 IDREN



Gambar 2.5 Konsep Arsitektur dari IDREN

Jaringan Riset dan Edukasi Nasional (NREN) merupakan sebuah infrastruktur jaringan khusus yang menghubungkan institusi riset dan edukasi pada suatu negara. NREN di Indonesia diinisiasi oleh projek INHERENT (Indonesian HighER Education NeTwork) pada 2006. Pemerintah mendukung pendanaan jaringan INHERENT hingga 2012. Pada tahun 2012-2015, NREN di Indonesia tidak beroperasi yang mengakibatkan terhambatnya riset menggunakan jaringan nasional. Konsep NREN kemudian dikembangkan dengan kolaborasi antar industri telekomunikasi, institusi pendidikan tinggi, dan Kementerian Pendidikan, Kebudayaan, Riset dan Teknologi. NREN yang baru ini kemudian dinamakan IDREN (Indonesia Research and Education Network). Operator jaringan akan mendukung jaringan IDREN pada layer 2 untuk koneksi antar operator jaringan dan universitas atau institusi riset. Sedangkan untuk dukungan layer 3 ke atas akan dikelola oleh tim IDREN. Sedangkan untuk Kementerian Pendidikan, Kebudayaan, Riset dan Teknologi akan mendukung anggaran untuk menghubungkan IDREN dengan TEIN (Trans European Information Network) sebagai tulang punggung REN global (Affandi, Achmad Basuki, & Widyawan, 2019). Konsep arsitektur dari IDREN dapat dilihat pada Gambar 2.5.

3. METODOLOGI PENELITIAN

3.1 Tipe Penelitian

Tipe penelitian yang dilakukan yaitu implementatif pengembangan. Implementatif yaitu penelitian yang menitikberatkan pada luaran penelitian yang berupa produk baik software atau hardware, sebagai solusi terhadap permasalahan yang diangkat dalam penelitian, dalam hal ini yaitu monitoring lalu lintas jaringan dari Netflow. Pengembangan yaitu merancang pengelolaan dan visualisasi data agar lebih human friendly dengan menggunakan Elastiflow dan ELK Stack.

3.2 Studi Literatur

Pada tahap ini akan dilakukan pengumpulan beberapa referensi dan dasar teori, yang dapat digunakan untuk melakukan dan mendukung pelaksanaan penelitian. Referensi dan dasar teori bersumber dan berkaitan dengan penelitian yang telah dilakukan.

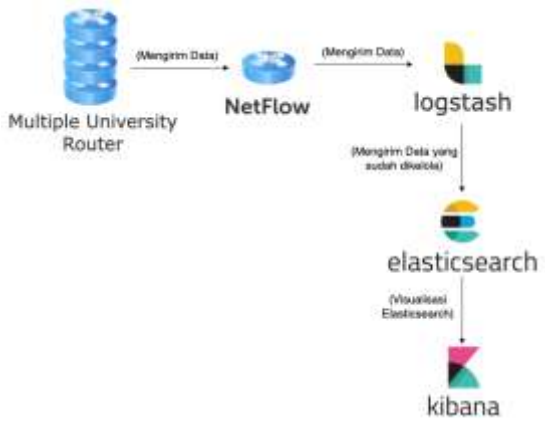
3.3 Perancangan Sistem

Perancangan sistem merupakan tahapan untuk

dapat mendefinisikan sistem yang selanjutnya akan diimplementasikan untuk dapat mencapai tujuan dan menjawab permasalahan dari penelitian yang dilakukan. Perancangan sistem diawali dengan mendefinisikan deskripsi umum sistem. Kemudian dilakukan analisis kebutuhan untuk mendefinisikan kebutuhan-kebutuhan yang harus dicapai oleh sistem yang diimplementasikan nantinya.

3.3.1 Deskripsi Umum Sistem

Berikut merupakan kebutuhan pada perangkat keras dalam penelitian ini:



Gambar 3.1 Deskripsi Umum Sistem

Penelitian ini menerapkan suatu sistem monitoring menggunakan Elastic Stack sebagai platform visualisasi dan analisis trafik jaringan IDREN. Alur kerja dari sistem monitoring secara umum yang digunakan dalam penelitian ini dapat dilihat pada Gambar 3.1.

3.3.2 Analisis Kebutuhan

3.3.2.1 Kebutuhan perangkat keras

1. sPerangkat Router yang digunakan untuk gate utama trafik IDREN. Router tersebut haruslah bermerek Cisco yang telah terintegrasi dengan software Netflow
2. Beberapa Router yang digunakan sebagai sub-gate. Router tersebut akan dipasang ke beberapa universitas di Indonesia (ITB, ITS, UB, dan UGM) dan dapat menjangkau sebagian besar universitas di sekitarnya.
3. Server IDREN, dengan spesifikasi 8 core CPU, 24 GB RAM, dan OS Ubuntu Server 18.04 LTS. Digunakan sebagai tempat penerapan Elastic Stack, sebagai platform visualisasi dan analisis trafik IDREN

3.3.2.2 Kebutuhan Perangkat Lunak

1. Netflow, digunakan untuk mengumpulkan metadata pada jaringan IP dalam switch maupun router.
2. Elasticsearch, bagian sistem Elastic Stack yang berfungsi sebagai penyimpanan, analisis dan pencarian kumpulan data lalu lintas yang terdistribusi pada file index pada.
3. Kibana, bagian sistem Elastic Stack yang berfungsi sebagai visualisasi Elasticsearch.
4. Logstash, bagian sistem Elastic Stack yang berfungsi untuk mem-parsing log data, serta membuat indeks log yang nantinya dapat disimpan dan dikelola oleh Elasticsearch.
5. Elastiflow, digunakan untuk memodifikasi Logstash agar dapat mengumpulkan dan mem-parsing data yang berasal dari Netflow.
6. Docker, perangkat lunak yang digunakan untuk membungkus ELK (ElasticSearch, Logstash, Kibana) dan Elastiflow menjadi image agar nantinya dapat dijalankan dengan mudah pada server.

3.3.2.3 Kebutuhan Visualisasi

No	Visualisasi	Deskripsi
1	Flow AS	Visualisasi yang dapat menampilkan besar bandwidth dan hubungan antar AS
2	Top Service	Visualisasi yang dapat memberikan informasi tentang Service yang paling banyak digunakan dalam jaringan IDREN
3	Top AS	Visualisasi yang dapat memberikan informasi tentang AS yang paling banyak menggunakan jaringan IDREN
4	Inbound & Outbound Traffic	Visualisasi yang dapat memberikan informasi tentang berapa banyak lalulintas data yang masuk dan keluar dari jaringan IDREN
5	GeoIP	Visualisasi yang dapat memberikan gambaran mengenai wilayah mana pada peta yang paling banyak terkoneksi dengan jaringan IDREN

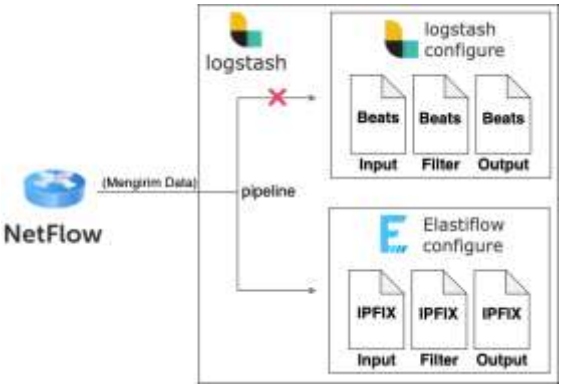
3.3.3 Rancangan Sistem

3.3.3.1 Perancangan Netflow

Gambar 3.2 Konfigurasi Netflow

Perancangan pada Netflow dilakukan dengan menghubungkan jaringan REN dan Universitas di Indonesia melalui satu router utama IDREN. Pada router tersebut kemudian akan diberi instalasi Netflow yang berfungsi untuk mengirimkan lalu lintas jaringan yang terhubung dengan router IDREN menuju Logstash. Logstash sendiri akan dibantu dengan Elasticsearch agar dapat berfungsi sebagai pengganti Netflow collector, karena Elasticsearch sendiri memiliki fungsi untuk menyimpan seluruh data yang dikirimkan oleh Logstash pada sistem ELK Stack

3.3.3.2 Konfigurasi Logstash



Gambar 3.3 Konfigurasi Pipeline Logstash

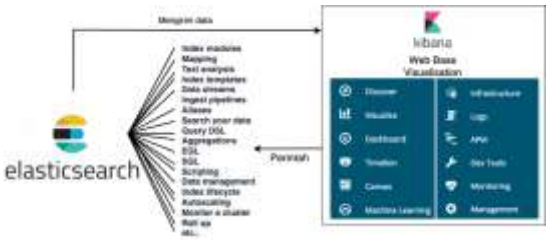
Perancangan pada Logstast dilakukan dengan menambahkan konfigurasi Elastiflow ke dalam folder Logstash. Kemudian memodifikasi pipeline Logstash dengan menghapus alamat default konfigurasi dan menggantinya dengan alamat konfigurasi Elastiflow. Hal tersebut dilakukan agar setiap data dari Netfow yang masuk dapat dikelola dengan mudah oleh Logstash.

3.3.3.3 Konfigurasi Elasticsearch

Gambar 3.4 Konfigurasi Elasticsearch

Pada Elasticsearch data-data yang memiliki index dari Logstash, akan dikumpulkan berdasarkan nama index yang sama pada satu file json. Data-data tersebut kemudian dapat dikumpulkan pada satu format index yang sama, misal dari index dengan nama Elastiflow dengan format bulan yang sama. Setelah dibuat dalam satu Index template data bisa dimanfaatkan untuk menggunakan beberapa fitur Elasticsearch lain, seperti pada Gambar 3.4 antara lain search data, mapping, text analyst, dll.

3.3.3.4 Konfigurasi Kibana



Gambar 3.5 Konfigurasi Kibana

Fungsi utama Kibana adalah untuk memvisualisasikan Elasticsearch. Melalui penghubungan Kibana dengan Elasticsearch, admin jaringan dapat menggunakan tools yang ada pada Elasticsearch menggunakan tombol pada website Kibana yang telah dibuat. Misal jika kita menekan navigasi management kemudian index pada browser visualisasi Kibana, maka Kibana akan meminta data-data pada Elasticsearch berupa list seluruh index yang ada, beserta detail setiap data tersebut. Jika kita mengubah atau menghapus data index melalui Kibana makan data tersebut juga berubah di Elasticsearch.

3.3.4 Metode Evaluasi

Metode evaluasi bertujuan untuk mendefinisikan parameter dan skenario pengujian setelah melakukan implementasi. Hal tersebut diperlukan untuk mengetahui apakah sistem yang direalisasikan telah sesuai dengan tujuan dan rumusan masalah. Parameter yang akan diuji

meliputi pengujian performa lama waktu loading page, pengujian sumber daya, dan pengujian ketersediaan data masuk di Logstash pada visualisasi tertentu.

- **Pengumpulan Data Traffic** dilakukan untuk mengetahui berapa besar data yang dapat disimpan dan diproses oleh server ELK Stack IDREN.
- **Pengujian Visualisasi** dilakukan untuk membandingkan kecepatan penampilan data pada tiap dashboard visualisasi.
- **Pengujian Sumber Daya** dilakukan untuk mengetahui berapakah sumber daya seperti CPU dan RAM yang sebenarnya dibutuhkan untuk melakukan penelitian ini.

4. HASIL DAN PEMBAHASAN

4.1 Pengumpulan Data Traffic

Hasil dari pengumpulan data traffic pada penelitian ini menunjukan besar data lalu lintas yang dapat diproses waktu tertentu oleh ELK Stack IDREN. Hasil ini dapat dilihat pada Table 4.1

Table 4.1 Jumlah data Pengujian Traffic per 30 Menit

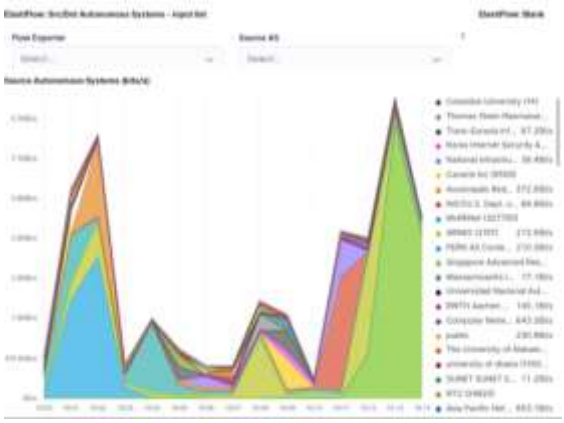
Traffic	MIN	MAX	AVERAGE
Inbound	25.5 b	94.6 Mb	52.5 Mb
Outbound	71.8 b	15.4 Mb	2.9 Mb
Total	97.3 b	110.0 Mb	45.4 Mb

Dari Table 4.1 dapat diketahui bahwa dalam satu hari, lalu lintas data yang di proses oleh ELK Stack IDREN berjumlah 97.28 b hingga 110 Mb, dengan rata-rata 45.4 MB data per-30 menit. Selanjutnya untuk total data yang di proses oleh ELK Stack IDREN dalam satu hari dapat dilihat dalam bentuk tabel pada Table 4.2

Table 4.2 Jumlah data Pengujian Traffic per Hari

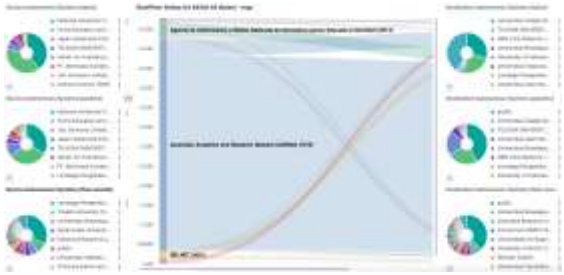
Traffic	Total
Inbound	2.5 Gb
Outbound	138.4 Mb

4.2 Pengujian Visualisasi



Gambar 4.1 Dashboard Traffic-AS Time

Gambar 4.2 Dashboard Top-Service_Time



Gambar 4.3 Dashboard Flow-AS Page

Hasil dari pengujian visualisasi pada penelitian ini menunjukan perbedaan waktu respon yang dapat dilihat pada Table 4.3

Table 4.3 Waktu Tiap Skenario Pengujian

Kode	Waktu menyelesaikan request/ *loading time*
Dashboard Traffic-AS	7.30 s
Dashboard Top-Service	6.41 s
Dashboard Flow-AS	18.18 s

Dari Table 4.3 yang berisi data waktu tiap skenario, diketahui bahwa dashboard Traffic-AS dan dashboard Top-Service memerlukan waktu yang cukup cepat untuk menampilkan seluruh visualisasi jika dibandingkan dashboard Flow-AS. Hal ini terjadi karena dashboard Flow-AS

menghasilkan visualisasi berupa diagram Sankey yang membutuhkan resource komputasi yang tinggi, sehingga membutuhkan waktu yang cukup lama. Sedangkan visualisasi pada dashboard Traffic-AS dan dashboard Top-Service membutuhkan waktu yang cukup cepat karena visualisasi grafik dan tabel tidak membutuhkan komputasi yang tinggi.

4.3 Pengujian Sumber Daya

Hasil pengujian tersebut penulis ubah dalam bentuk tabel untuk memudahkan pembacaan dan proses analisis. Hasil pengujian tersebut dapat dilihat pada Table 4.4 dan Table 4.5.

Table 4.4 Pengujian Sumber Daya

NAME	CPU %	RAM USAGE / LIMIT	RAM %
docker-elk_Logstash_1	20.41 %	3.359 GiB / 23.49GiB	14.31 %
docker-elk_kibana_1	0.63 %	423.4MiB/ 23.49GiB	1.76 %
docker-elk_*Elasticsearch*_1	00.08 %	15.71GiB / 23.49GiB	66.80 %
Total	20.49 %	19,48 GiB / 23.49GiB	82.87 %

Table 4.5 Pengujian Sumber Daya berdasarkan Logstash

NAME	AverageCPU %	RAM USAGE / LIMIT
Dengan Logstack	46.0 %	20,0 GiB / 23.49GiB
Tanpa Logstack	7.0 %	16,3 GiB / 23.49GiB
Selisih	39.0 %	3,7GiB / 23.49GiB

Dari Table 5.7 dan Table 5.8 diketahui bahwa pada penelitian ini ELK Stack yang telah dimodifikasi berdasarkan Elastiflow menggunakan 38.64 % dari 8 vCPU dan 21,096 GiB atau sekitar 82.87 % dari 23.49 GiB RAM yang disediakan untuk menerima data lalu lintas jaringan dari Netflow IDREN.

5. KESIMPULAN DAN SARAN

5.1 Kesimpulan

Kesimpulan yang didapat dalam keseluruhan proses penelitian ini antara lain:

1. Implementasi platform visualisasi dan analisis trafik IDREN pada penelitian ini membutuhkan empat buah router dan sebuah server. Tiga router sebagai sub-gate untuk masuk ke jaringan IDREN dan satu router sebagai gate. Gate digunakan untuk melakukan monitoring lalu lintas jaringan dengan bantuan Netflow, serta sebagai penghubung antar sub-gate. Satu server yang digunakan pada percobaan ini, telah dikonfigurasi menggunakan sistem ELK Stack agar dapat berfungsi sebagai Netflow Collector, platform visualisasi, dan analisis untuk jaringan IDREN.
2. Seluruh pengguna yang masuk ke jaringan IDREN harus melewati beberapa jaringan seperti: jaringan universitas di Indonesia, sub-gate IDREN (router IDREN di ITS, UB, dan UGM), dan gate IDREN (router IDREN yang telah memiliki Netflow). Sebagai gate, router Netflow mendapatkan data dari seluruh lalu lintas jaringan yang melewati sub-gate atau yang melalui sistem IDREN. Sebagai tahap awal seluruh data lalu lintas jaringan IDREN yang dimiliki oleh Netflow, dikirimkan menuju ELK Stack yang dapat berfungsi sebagai Netflow Collector pada sistem Logstash. Data tersebut disimpan dan dapat dianalisis menggunakan sistem Elasticsearch, kemudian divisualisasikan dan dikelola pada website dengan bantuan Kibana. Di dalam Kibana, admin jaringan dapat membuat visualisasi dan dashboard secara custom untuk menampilkan data dan analisis yang diinginkan, seperti contoh pada pengujian visualisasi.
3. Performa platform visualisasi, dan analisis yang dikembangkan diukur berdasarkan waktu penyediaan lab dan sumber daya yang digunakan untuk menjalankan server ELK Stack IDREN. Dari hasil pengujian, didapatkan informasi bahwa server ELK Stack IDREN rata-rata dapat mengelola 2,9MB hingga 52.5MB data per-30 menit dengan total 2.5 GB per-hari. Membutuhkan 7% hingga 46% dari 8 thread CPU, dan 16,3GB hingga 20GB RAM hanya untuk memastikan bahwa seluruh data lalu lintas jaringan IDREN dapat diterima dan disimpan oleh ELK Stack. Sedangkan ketika melakukan analisis dan visualisasi pada dashboard tertentu website Kibana memerlukan rentang waktu berbeda untuk menampilkan sebuah visualisasi, karena bergantung pada berapa besar komputasi yang dibutuhkan.

5.2 Saran

Saran peneliti terhadap penelitian kedepannya yaitu:

1. 1Berdasarkan konsumsi penyimpanan yang memakan 4,31 GiB perhari dari 1 TB storage. Penerapan penghapusan berkala (retention) dari data index pattern pada Kibana untuk menjamin ketersediaan storage dalam jangka panjang, karena storage akan penuh dalam 7-8 Bulan.
2. Seperti pada LAMPIRAN C, bahwa visualisasi dari monitoring Cacti dapat diakses secara public sedangkan monitoring

Elastic Stack tidak. Dapat ditambahkan pembuatan web untuk mengakses dashboard atau visualisasi tertentu secara public menggunakan iframe untuk menggantikan fitur tersebut.

6. CONTOH DAFTAR PUSTAKA

Affandi, A., Achmad Basuki, & Widyawan. (2019). Network Architecture Design of Indonesia Research and Education Network (IDREN). 1-6.

Asmunin, & Wahyu Khamdani. (2016). Sistem Monitoring Resource pada Jaringan FMIPA Unesa dengan Protocol SNMP. *MULTINETICS, 2*, 8-12.

Biznetgio. (2020). *Cara Install & Konfigurasi Monitoring Cacti Serta Mengetahui Fungsi Fitur Pada Cacti*. Retrieved September 2021, from https://kb.biznetgio.com/id_ID/monitoring/cara-install-konfigurasi-monitoring-cacti-serta-mengetahui-fungsi-fitur-pada-cacti

Cecil, A. (n.d.). *A Summary of Network Traffic Monitoring and Analysis Techniques*. Retrieved September 2021, from https://www.cse.wustl.edu/~jain/cse567-06/ftp/net_monitoring/

Cecil, A. (n.d.). *A Summary of Network Traffic Monitoring and Analysis Techniques* . Retrieved October 2021, from https://www.cse.wustl.edu/~jain/cse567-06/ftp/net_monitoring/

CISCO. (2021). *What Is Network Monitoring?* Retrieved December 2021, from https://www.cisco.com/c/en/us/solutions/automation/what-is-network-monitoring.html

Crooks, D., Liviu Vâlsan, Kashif Mohammad, Shawn McKee, Paul Clark, Adam Boutcher, . . . Bas Kreukniet. (2019). Operational security, threat intelligence & distributed computing: the WLCG Security Operations Center Working Group. 1-8.

elastic. (n.d.). *Elasticsearch The heart of the free and open Elastic Stack*. Retrieved August 2021, from https://www.elastic.co/elasticsearch/

elastic. (n.d.). *Kibana Your window into the Elastic Stack*. Retrieved October 2021, from https://www.elastic.co/kibana/

elastic. (n.d.). *Logstash Centralize, transform & stash your data*. Retrieved August 2021, from https://www.elastic.co/logstash/

Elastiflow. (n.d.). *ElastiFlow Unified Flow Collector*. Retrieved October 2021, from https://docs.Elastiflow.com/docs

i-3. (2020). *Monitor Infrastruktur IT Anda Secara Real-Time dengan ELK Stack*. Retrieved October 2021, from https://i-3.co.id/monitor-infrastruktur-it-anda-secara-real-time-dengan-elk-stack

NetEye. (2021). *Installing Elastiflow on NetEye SIEM* . Retrieved October 2021, from https://www.neteye-blog.com/2021/05/installing-Elastiflow-on-neteye-siem/

site24x7. (n.d.). *What is Network Monitoring?* Retrieved September 2021, from https://www.site24x7.com/network-monitoring.html

site24x7. (n.d.). *Why are network monitoring tools important?* . Retrieved September 2021, from https://www.site24x7.com/network-monitoring.html

Solarwinds. (n.d.). *What is NetFlow?* Retrieved September 2021, from https://www.solarwinds.com/Netflow-traffic-analyzer/use-cases/what-is-Netflow

Suyadi, S., & Wibowo, S. H. (2019). *Monitoring Jaringan? Bisa*. Retrieved Desember 2021, from https://bti.ums.ac.id/monitoring-jaringan-bisa/