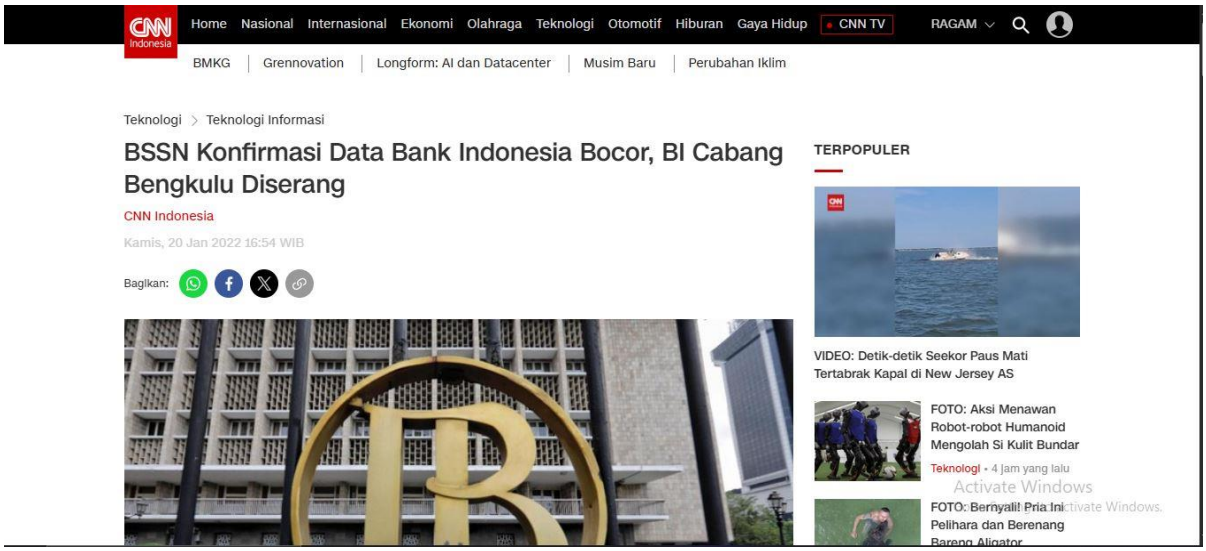
BAB 1
USULAN GAGASAN

1.1. Deskripsi Umum Masalah

Di dunia digital yang terus berkembang dengan cepat perusahaan di seluruh dunia kini dihadapkan pada masalah yang seiring waktu semakin kompleks dalam mengelola infrastruktur jaringan yang semakin canggih. Dalam hal ini keamanan adalah komponen penting yang bertindak sebagai tindakan perlindungan, maka dari itu diperlukan teknologi yang dinamis dan sederhana dalam mengamankan jaringan dari ancaman *cyber* serta teknologi yang dapat mengurangi kompleksitas dengan mengandalkan kemampuan berbasis cloud yang dapat digunakan oleh perusahaan besar maupun kecil.



Gambar 1.1 informasi dari CNN Indonesia mengenai berita bahwa "BSSN konfirmasi data Bank Indonesia bocor"

Pada tahun 2021, telah terjadi kebocoran data yang dialami oleh Bank Indonesia cabang bengkulu yang disebabkan oleh penyerangan siber yang berakibat bocornya pekerjaan-pekerjaan personal di kantor tersebut dan menyerang 16 komputer yang ada di Bank Indonesia cabang bengkulu. Sistem keamanan yang ada di perusahaan Indonesia banyak yang belum bisa untuk mencegah penyerangan siber apalagi dengan kemajuan zaman yang semakin canggih dan maju dengan bentuk penyerangan yang bermacam-macam. Tantangan seperti inilah yang menyebabkan keamanan menjadi pilar penting untuk menjaga privasi dan perlindungan di perusahaan. Penyerangan siber yang menjadi masalah utama menjadi suatu pertimbangan dalam perusahaan agar memerlukan perlindungan.

Perubahan zaman yang terus berkembang telah mendorong suatu perusahaan agar merubah cara kerja dan struktur perusahaan. Saat ini, model kerja yang fleksibel, penggunaan aplikasi berbasis cloud serta konektivitas antar-cabang dan lokasi remote menuntut sistem jaringan yang aman, efisien dan mudah dikelola. Teknologi keamanan jaringan tradisional yang berpusat pada perimeter tidak lagi efektif dalam menghadapi tantangan era digital seperti akses pengguna dari berbagai lokasi, mobilitas perangkat, serta serangan siber yang semakin kompleks. Adapun beberapa masalah yang dihadapi seperti kompleksitas dalam mengintegrasikan suatu keamanan memiliki tantangan, perancanaan yang cermat dan dan ancaman yang semakin canggih dan bervariasi.

Untuk itu, Secure Access Service Edge (SASE) muncul sebagai solusi jaringan modern yang menyatukan fungsi keamanan dan konektivitas dalam satu platform yang berbasis opensource dan dikelola secara terpusat. Dalam usulan ini, penulis merancang dan mengimplementasikan arsitektur Secure Access Service Edge (SASE) berbasis cloud yang mengintegrasikan 3 komponen inti yaitu;

- VyOs sebagai SD-WAN
- OpenDaylight sebagai alat monitoring dan manajemen berbasis SDN,
- OPNsense sebagai Firewall as a Service (FWaaS).

Ketiga komponen ini dikombinasikan untuk membangun sistem jaringan yang aman, fleksibel, mudah di monitoring dan lebih efisien secara biaya. Sistem ini juga diharapkan dapat mendukung keamanan perusahaan di Indonesia, khususnya yang memiliki infrastruktur terdistribusi dan memerlukan solusi keamanan yang efisien.

1.2. Analisis Masalah

Keamanan saat ini sudah mulai menjadi peran penting untuk menjaga hal yang penting bagi perusahaan, namun perlu peninjauan aspek agar keamanannya dapat di implementasikan dengan benar. Diantaranya sebagai berikut;

1.2.1. Aspek Teknis

Integrasi komponen untuk SASE menjadi tantangan dikarenakan setiap *software* VyOs, OpenDaylight dan OPNsense memiliki konfigurasi dan fungsi yang berbeda, dan membutuhkan pemahaman yang cukup agar dapat diintegrasikan secara efektif. Meskipun SASE dirancang untuk menyederhanakan pengelolaan jaringan, meningkatkan dan memberikan perlindungan agar dapat menjaga keamanan di perusahaan, jika tidak dikelola dan di monitoring dengan baik dapat mengurangi efektivitas SASE secara keseluruhan. Tantangan

lain muncul dalam manajemen akses dan identitas dimana untuk mencegah akses dari suatu entitas yang tidak diketahui, perlu menerapkan metode autentikasi multi-faktor (MFA) secara efektif.

1.2.2. Aspek Ekonomi

Dalam menerapkan SASE, tantangan yang dihadapi adalah biaya awal penerapan karena investasi dalam infrastruktur, perangkat keras, dan pelatihan karyawan yang membutuhkan anggaran yang signifikan. Selain itu perusahaan akan mempertimbangkan potensi pengembalian investasi (ROI) dan memikirkan tentang waktu yang diperlukan untuk menerapkan hal ini dan harus diperhitungkan dengan teliti. Dengan SASE yang mulai dikenal di Indonesia, perusahaan memiliki peluang besar untuk meningkatkan keamanan dengan biaya terjangkau, namun juga perlu bersiap untuk bersaing dengan penyedia layanan yang menawarkan solusi serupa.

1.2.3. Aspek Hukum

Penerapan SASE harus mengikuti regulasi keamanan data dan privasi yang berlaku di Indonesia, seperti yang telah diatur di Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi[8]. Selain itu, perusahaan wajib membuat sistem pencatatan aktivitas (log) agar dapat memonitoring serta pengelolaan yang sudah sesuai dan mengikuti standar internasional seperti ISO/IEC 27001.

1.2.4. Aspek Industri

Aspek Industri spesifiknya industri ritel adalah industri yang memiliki pengaruh kuat dalam penerapan SASE. Perusahaan retail memiliki profil keamanan yang sensitif dikarenakan mengumpulkan dan memproses sejumlah data pribadi dan finansial yang menjadi target utama bagi pelaku serangan siber. Ada beberapa serangan/ancaman yang beragam seperti malware yang menyerang point-of-sale fisik[6].

1.3. Analisis Solusi yang Ada

SASE (Secure Access Service Edge) adalah pendekatan baru yang menggabungkan layanan jaringan dan teknologi keamanan menjadi satu infrastruktur berbasis opensource dalam satu kerangka kerja. Ini diimplementasikan untuk memenuhi kebutuhan perusahaan yang bekerja secara tersebar dan digital, seperti memiliki karyawan jarak jauh atau ingin mengakses hal penting diperusahaan dengan aman dan efektif[5].

Gambar 2.1 Ilustrasi Topologi SASE

SASE juga memungkinkan untuk dapat memberikan perlindungan lebih kepada keamanan perusahaan, meningkatkan skalabilitias dan fleksibilitas serta menjadi lebih efektif dalam segi biaya. Berikut adalah komponen-komponen yang umum pada platform SASE;

1.3.1. SD-WAN

SD-WAN adalah teknologi baru yang lebih mengandalkan perangkat lunak untuk memungkinkan kontrol dan kapabilitas manajemen[1]. SD-WAN dapat melakukan hal seperti, mengoptimalkan traffic, meningkatkan kinerja dengan memastikan tiap aplikasi mendapatkan yang dibutuhkan dan dapat menggunakan berbagai jenis koneksi seperti MPLS yang dapat menghubungkan pengguna ke aplikasi dengan aman.

SD-WAN memiliki kelebihan yaitu dapat mengoptimalkan koneksi jaringan area luas (WAN), mengarahkan traffic secara dinamis, meningkatkan kinerja[1]. SD-WAN juga memiliki kekurangan seperti membutuhkan keahlian konfigurasi dan optimalisasi, berpotensi mengalami masalah kompatibilitas dengan infrastruktur yang ada dan bergantung pada koneksi internet yang cepat dan handal untuk kinerja optimal.

1.3.2. FWaaS

FWaaS adalah sebuah jenis pengaturan firewall yang menggunakan infrastruktur cloud dan memiliki kemampuan untuk keamanan jaringan[1]. FWaaS tidak seperti firewall tradisional yang hanya dirancang untuk jaringan statis dan lokal. Tetapi FWaaS muncul sebagai teknologi modern yang memiliki banyak fitur seperti, menyediakan alternatif yang scalable, fleksibel, dan biaya yang terjangkau untuk firewall lokal memungkinkan perusahaan melindungi jaringan dan aplikasi dari ancaman[1].

FWaaS memiliki kelebihan yaitu, menyaring dan memeriksa traffic untuk mencegah akses dari luar, menjalankan kebijakan keamanan secara konsisten di jaringan dan memberikan efisiensi dengan cara mengurangi kebutuhan perangkat keras dan pemeliharaannya. FWaaS memiliki kekurangan diantaranya, dapat menyebabkan latensi dan beban tambahan dalam inspeksi traffic, membutuhkan pemantauan dan pembaharuan secara terus menerus dan berpotensi mempengaruhi kinerja jaringan.

1.3.3 ZTNA

ZTNA adalah sebuah teknologi yang memungkinkan akses aman ke aplikasi internal bagi pengguna jarak jauh. ZTNA memastikan bahwa pengguna diautentikasi dan diotorisasi sebelum mereka mendapatkan akses aplikasi di tertentu[2]. ZTNA memperlakukan semua pengguna, perangkat, dan aplikasi sebagai hal luar hingga mereka di verifikasi secara jelas. Dan ZTNA juga memberikan keamanan kepada pengguna jarak jauh ke aplikasi internal tanpa mengekspos aplikasi tersebut ke luar.

Seperti komponen yang lain, ZTNA memiliki kelebihan yaitu, dapat mengadopsi keamanan zero-trust untuk memastikan akses yang aman ke berbagai sumber daya, mengurangi potensi area serangan dan meminimalisir resiko[2], dan menjamin akses yang aman ke aplikasi dan sumber daya manapun. Kekurangannya adalah membutuhkan konektivitas jaringan yang stabil, berisiko mengalami kendala latensi khususnya dalam proses autentikasi dan otorisasi.

1.3.4 CASB

CASB adalah sebuah jenis keamanan berbasis cloud antara konsumen layanan cloud dan penyedia layanan cloud yang memiliki fungsi untuk memblokir atau mengizinkan aplikasi tertentu[3], menjaga aplikasi perangkat lunak, dan infrastruktur agar aman dari serangan dan kebocoran data. CASB dapat melakukan verifikasi identitas, kontrol akses, dan mendukung penggunaan layanan cloud, mengontrol akses ke sumber daya internal perusahaan yang mencakup autentikasi (enkripsi, kebijakan otorisasi, pencatatan keamanan)[4].

Kelebihan CASB adalah dapat memastikan transparasi dan pengendalian dalam penggunaan aplikasi cloud, mengidentifikasi serta mengurangi ancaman dan kerentanan yang terjadi pada lingkungan cloud, dan dapat melakukan integrasi dengan infrastruktur keamanan dan kebijakan yang telah ada. Dan kekurangannya seperti berisiko terjadi latensi yang dapat mempengaruhi performa aplikasi cloud, menyulitkan pengelolaan akses dan izin di berbagai lingkungan cloud dan memerlukan integrasi yang banyak dengan beragam platform layanan cloud.

1.3.5 SWG

SWG adalah sebuah jenis keamanan yang melindungi perangkat penjelajah web dari malware dan menegakkan kebijakan penggunaan[3]. SWG bekerja sebagai garis pertahanan pertama terhadap situs web berbahaya, upaya phising dan serangan berbasis web lainnya. SWG memiliki kemampuan seperti penyaringan konten, mengontrol aplikasi, dan pencegahan kehilangan data untuk memastikan kepatuhan terhadap kebijakan/peraturan perusahaan. SWG memiliki kelebihan seperti, kemudahan dalam pengelolaan, deteksi dan pencegahan ancaman real time, memungkinkan kontrol detail atas penggunaan web dan akses aplikasi, menyediakan akses internet yang aman bagi pengguna jarak jauh, menyediakan kemampuan pencegahan kehilangan data, memastikan kepatuhan terhadap peraturan privasi data[3] dan terdistribusi serta memberikan kebijakan terhadap persyaratan regulasi. Kekurangannya adalah memerlukan pembaharuan dan pemantauan berkala, dan berpotensi menimbulkan latensi yang mempengaruhi kenyamanan pengguna.

1.4. Tujuan Capstone Design

Tujuan dari *Capstone Design* ini adalah untuk merancang dan mengimplementasikan SASE yang terdiri dari komponen SD-WAN dan FWaaS berguna untuk memberikan perlindungan dan keamanan kepada sebuah perusahaan agar lebih aman. SASE dapat dirancang dengan menggabungkan VyOs sebagai SD-WAN, OPNSense sebagai FWaaS serta OpenDaylight (ODL) yang dapat memonitoring.

Dengan perancangan dan implementasi SASE, SASE diharapkan dapat menjadi platform yang memberikan perlindungan dari serangan dan keamanan kompleks yang efisien dengan biaya yang terjangkau.

Tujuan yang ingin dicapai oleh implementasi SASE adalah;

- Dapat memberikan perlindungan dan keamanan kompleks dengan biaya terjangkau dan efisien.
- Menerapkan komponen SD-WAN, FWaaS dan ZTNA sederhana didalam SASE yang menjadi inti dari SASE.
- Memberikan solusi jaringan dan keamanan terintegrasi berbasis open-source dan dan pengelolaan traffic secara dinamis dan terpusat.

1.5. Batasan *Capstone Design*

Pada pengerjaan proyek *Capstone Design,* terdapat batasan yang ditetapkan agar perancangan dan implementasi terarah dan jelas. Batasan tersebut adalah;

- SASE dirancang sederhana dengan biaya terjangkau mungkin dan memiliki akses terbatas yang tidak terlalu kompleks dan efisiensi jaringan.
- Dapat memonitoring traffic yang lewat dan mengatur rules di OPNSense.
- Menunjukkan komponen SD-WAN, FWaaS didalam SASE.
- SASE harus sesuai dengan prinsip SASE.