JURNAL ELEKTRO & INFORMATIKA
SWADHARMA (JEIS)
VOLUME 01 NOMOR 01 JANUARI 2021
ISSN 2774 – 5775 | eISSN 2774-5767

PENERAPAN TEKNOLOGI FORTIGATE DALAM PEMBANGUNAN JARINGAN VPN-IP BERBASIS IPSEC

Hari Suryantoro[1)], Adi Sopian[2)], Dartono[3)]
[1]Prodi Teknik Informatika, Fakultas Teknologi, ITB Swadharma
[2]Prodi Manajemen Informatika, Fakultas Teknologi, ITB Swadharma
[3]Prodi Sistem Informasi, Fakultas Teknologi, ITB Swadharma

Correspondence author: Hari Suryantoro, akoehari@gmail.com, Jakarta, Indonesia

Abstract

IPSec based VPN (Virtual Private Network) is a standard that provides data confidentiality, data integrity, and source authentication on public communication such as the internet. IPSec VPN is a secure technology and reliable (secure and reliable) which can connect private networks between campuses using internet public communications. The availability of data and services in real-time is very much needed by the main campus to ensure that operational and business activities at branch campus and main campus run smoothly. FortiGate is the best choice for system security that provides high protection against threats dynamic security and simplifies the IT security infrastructure company. This study aims to build a VPN (Virtual Private Network) based on IPSec. The research was conducted on a Wide Area Network using two FortiGate devices as a firewall and gateways are connected to each other and form a tunnel as a special path connect private networks between campuses securely. The results showed that clients at branch campus can access servers located at the main campus in real-time, and data transfer performance between branch campus and main campus was successfully accepted, and getting bigger packets sent, the file transfer process time will also be longer.

Keywords: VPN, IPSec, fortigate

Abstrak

VPN (Virtual Private Network) berbasis IPSec merupakan standar yang menyediakan kerahasiaan data, keutuhan data dan autentikasi sumber pada komunikasi publik seperti internet. VPN IPSec merupakan teknologi yang aman dan terpercaya (secure and reliable) yang dapat menghubungkan jaringan private antar kampus dengan menggunakan komunikasi publik internet. Ketersediaan data dan layanan secara real time sangat dibutuhkan pimpinan untuk menjamin kegiatan operasional dan bisnis pada kampus cabang dan kampus pusat berjalan dengan lancar. FortiGate sebuah pilihan terbaik untuk sistem keamanan yang menyediakan perlindungan tinggi terhadap ancaman keamanan yang dinamis dan menyederhanakan infrastruktur keamanan IT organisasi. Penelitian ini bertujuan untuk membangun VPN (Virtual Private Network) berbasis IPSec. Penelitian dilakukan pada jaringan Wide Area Network menggunakan dua buah

perangkat FortiGate sebagai firewall dan gateway yang saling terhubung dan membentuk tunnel sebagai jalur khusus yang menghubungkan jaringan private antar kampus secara aman. Hasil penelitian menunjukan bahwa komputer pengguna pada kampus cabang dapat mengakses server yang berada pada kampus pusat secara real time, dan kinerja transfer data antara kampus cabang dengan kampus pusat sukses diterima, dan semakin besar paket yang dikirim maka waktu proses transfer file juga akan semakin lama.

Kata Kunci: VPN, IPSec, fortigate

A. PENDAHULUAN

Perkembangan teknologi saat ini menjadikan masalah keamanan, kemudahan dan kecepatan transfer (pertukaran data) sebagai salah satu aspek penting dari sebuah jaringan komunikasi pada perusahaan-perusahaan skala menengah ke atas. Jaringan komputer merupakan solusi yang digunakan perusahaan untuk mempercepat dan memperlancar arus informasi di perusahaan. Pada perusahaan yang hanya memiliki satu lokasi kantor akan lebih mudah dalam membangun jaringannya karena hanya akan menggunakan satu jaringan lokal, disebut LAN (*Local Area Network*), pada jaringan ini kecepatan dan kehandalan jaringan masih aman, dan juga administrator jaringan perusahaan tidak terlalu sulit dalam membangun jaringan LAN. Namun, apabila suatu perusahaan atau institusi memiliki kantor cabang dimana lokasinya terpisah secara geografis maka untuk menghubungkannya harus menggunakan WAN (Wide Area Network), disini mulai terdapat banyak masalah yang terjadi mulai dari *speed*, *bandwidth* dan *delay*.

Teknologi yang mendukung WAN antara lain VPN (*Virtual Private Network*), VSAT (*Very Small Aperture Terminal*), Frame Relay, ATM (*Asynchronus Transfer Mode*). Dari banyak teknologi WAN, VPN paling banyak digunakan karena kehandalannya dalam menjamin keamanan data. VPN sebagai teknologi alternatif untuk menghubungkan jaringan lokal yang luas dengan biaya yang relatif kecil, dan juga transmisi data teknologi VPN menggunakan media jaringan publik yang sudah ada (internet).

VPN atau *Virtual Private Network* adalah teknologi jaringan komputer yang memanfaatkan media komunikasi public (open connection atau virtual circuits), seperti Internet, untuk menghubungkan beberapa jaringan lokal (Sofana, 2012). Informasi yang berasal dari node-node VPN akan “dibungkus” (tunneled) dan kemudian mengalir melalui jaringan publik. Sehingga informasi menjadi aman dan tidak mudah dibaca oleh orang lain. Untuk implementasi jaringan VPN dapat dilakukan dengan menggunakan FortiGate. FortiGate adalah sebuah sistem keamanan jaringan berupa firewall yang dikeluarkan oleh perusahaan Fortinet sebagai pemimpin pasar untuk Unified Threat Management (UTM).

Untuk mengamankan informasi yang berasal dari jaringan internal, VPN menggunakan beberapa metode security yaitu *firewall*, enkripsi dan IPSec (Sofana, 2012). IPSec (*Internet Protocol Security Protocol*) merupakan suatu protokol yang digunakan untuk melakukan pertukaran paket pada layer IP secara aman dan menyediakan fitur *security* yang lebih baik. Seperti algoritma enkripsi yang lebih bagus dan *comprehensive authentication*. IPSec menggunakan dua buah mode enkripsi, yaitu *tunnel* dan *transport*.

Penggunaan FortiGate dikarenakan FortiGate merupakan produk UTM (*Unified Threat Management*) dimana dalam satu perangkat sudah terdapat fitur-fitur keamanan jaringan penting tanpa harus

JURNAL ELEKTRO & INFORMATIKA
SWADHARMA (JEIS)
VOLUME 01 NOMOR 01 JANUARI 2021
ISSN 2774 – 5775 | eISSN 2774-5767

membeli perangkat lainnya secara terpisah, dan FortiGate bisa diandalkan untuk menanganani kompleksitas dari sebuah jaringan perusahaan menengah ke atas, serta FortiGate merupakan investasi perusahaan pada bidang *security* untuk melindungi data-data penting agar tetap aman.

B. METODE PENELITIAN

Lokasi penelitian pada Kampus ITB Swadharma Jakarta yang beralamat di Jalan Malaka No.3 Jakarta Barat (Kampus Pusat) dan Jl. Raya Pondok Cabe Tangerang Selatan (Kampus Cabang). Waktu penelitian dilakukan selama 4 (empat) bulan yang dilaksanakan antara bulan Agustus sampai dengan Desember 2020.

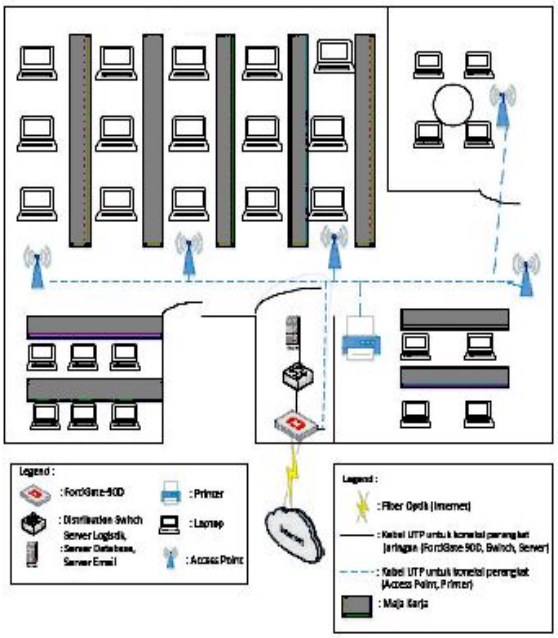
Dalam pelaksanaan penelitian ini, tahapan yang dilakukan yaitu :

1. Perancangan dan Implementasi
   Perancangan dan implementasi, tahapan ini digunakan unuk melakukan analisis kebutuhan, desain atau perancangan, setting, dan konfigurasi software dan hardware yang dibutuhkan dalam membuat virtual private network berbasis IPSec yang meliputi perangkat FortiGate dan perangkat pendukung lainnya. Tahapan yang dilakukan adalah sebagai berikut :
   a. Merancang topologi jaringan yang ingin dibangun.
   b. Konfigurasi perangkat FortiGate untuk membangun jaringan dasar sebagai pendukung membangun virtual private network berbasis IPSec
   c. Konfigurasi perangkat FortiGate untuk membangun virtual private network berbasis IPSec
2. Pengujian dan Evaluasi Jaringan VPN
   Setelah proses perancangan dan implementasi telah selesai dilakukan seperti instalasi dan konfigurasi FortiGate, maka dilakukan pengujian berupa tes koneksi dari komputer ke komputer menggunakan jaringan VPN. Setelah terkoneksi dengan baik, pengujian berikutnya dilakukan pada client untuk transfer data ke server menggunakan FTP Server.
3. Analisa Hasil Pengujian
   Tahap ini dilakukan dengan menguji virtual private network berbasis IPSec yang sudah dilakukan konfigurasi pada FortiGate sebagai tolak ukur meminimalisirkan kehilangan data disaat komputer melakukan transfer data ke server menggunakan jaringan VPN IPSec.

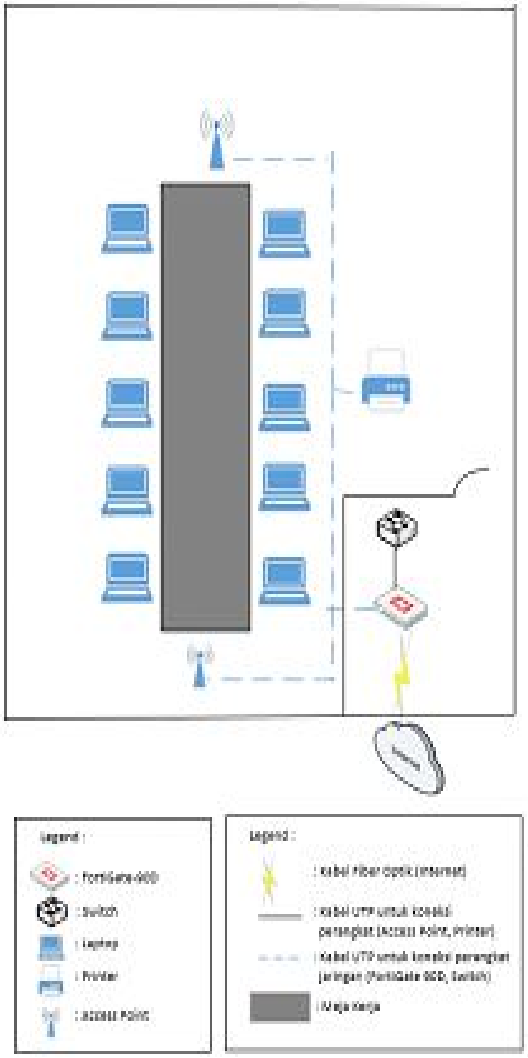
C. HASIL DAN PEMBAHASAN

Analisa Kondisi Jaringan Saat Ini

Pada topologi jaringan untuk kampus pusat dengan kampus cabang terpisah letaknya secara geografis, sehingga pada kampus pusat dan kampus cabang menggunakan koneksi jaringan internet sendiri-sendiri untuk kegiatan operasional jaringannya. Namun ketika kampus cabang ingin menggunakan layanan *server* Keuangan, SDM, dan lain-lain yang berada pada kampus pusat, maka kampus cabang harus terhubung dengan jaringan pada kampus pusat dikarenakan aplikasi yang digunakan masih berbasis *client-server* atas pertimbangan masalah keamanan data.



Gambar 1. Skema Jaringan Kampus Pusat



Gambar 2. Skema Jaringan Kampus Cabang

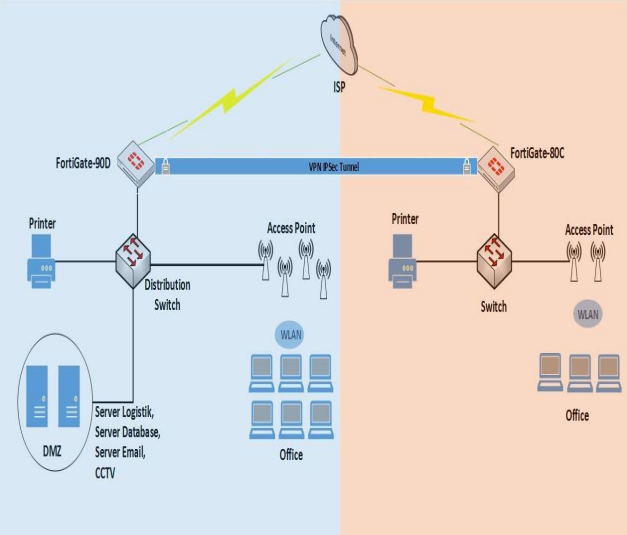
Permasalahan Jaringan Saat Ini

Kebutuhan teknologi yang dibutukan adalah teknologi yang memungkinkan kampus pusat dengan kampus cabang yang berbeda letak geografis saling terhubung meskipun tidak satu area/gedung namun masih tetap berkomunikasi langsung secara jaringan komputer. Karena kampus pusat dan cabang letaknya berjauhan, sehingga kampus cabang tidak dapat terkoneksi jaringan secara langsung dengan kampus pusat yang mengakibatkan tidak dapat mengakses layanan server yang berada di kampus pusat. Untuk permasalahan yang dialami tersebut, saat ini digunakan karyawan tambahan untuk mengakses data di server, baik untuk mengambil atau memasukkan data di server dengan cara pihak yang akan memasukan atau membutuhkan data akan mengemail ke karyawan tersebut yang menjadi operator server. Masalah ini akan membuat biaya operasional membengkak karena harus mengakomodasi gaji tambahan bagi operator tersebut. Tingkat kesalahan atau *human error* juga akan menjadi masalah yang cukup penting. Masalah tersebut akan terjadi ketika operator tersebut memasukkan data secara manual satu per satu ke dalam server.

Rancangan Jaringan Usulan

Rancangan yang diusulkan menggunakan teknologi VPN IPSec yang menghubungkan antara kampus pusat dengan kampus cabang dengan menggunakan infrastruktur jaringan yang sudah ada di ITB Swadharma, karena jaringan yang sudah ada sangat mendukung untuk implementasi rancangan jaringan yang baru, peneliti hanya menambah konfigurasi VPN IPSec pada FortiGate yang berada pada kampus pusat dan kampus cabang yang diharapkan dengan topologi baru ini dapat meningkatkan kinerja dan konektifitas jaringan antar kedua kampus.

JURNAL ELEKTRO & INFORMATIKA
SWADHARMA (JEIS)
VOLUME 01 NOMOR 01 JANUARI 2021
ISSN 2774 – 5775 | eISSN 2774-5767



Gambar 3. Topologi Jaringan Usulan

Topologi jaringan menggunakan teknologi VPN IPSec dengan rincian sebagai berikut:

1. ISP pada kampus pusat menggunakan Fibernet dengan bandwidth 50Mbps dedicated;
2. ISP yang digunakan pada kampus cabang menggunakan Telkom Indihome dengan bandwidth 40Mbps;
3. Kemudian paket data internet dialirkan ke FortiGate-90D pada masing-masing kampus yang berfungsi sebagai router, yang bertugas meneruskan dan mengatur paket data kepada client melalui switch.
4. Selanjutnya paket data tersebut melewati switch, dan switch mendistribusikan paket paket tersebut ke access point, server – server, dan printer agar dapat terhubung dengan baik;
5. Setelah semua perangkat yang sudah terkonfigurasi dapat terkoneksi satu sama lain, maka selanjutnya client mengkoneksikan laptop ke wireless agar bisa terkoneksi ke jaringan lokal dan juga internet.
6. Untuk tahap koneksi antara kampus cabang ke kampus pusat dilakukan konfigurasi VPN pada perangkat FortiGate-90D di kampus cabang maupun di kampus pusat.
7. Konfigurasi VPN berbasis IPSec dan menggunakan mode tunnel mode.

Implementasi Jaringan Usulan

Implementasi topologi jaringan yang diusulkan dilakukan dengan tahapan berikut:

1. Konfigurasi VPN IPSec di kampus pusat dengan melakukan konfigurasi *interfaces* dan IP *address*. Langkah selanjutnya dengan membuat *firewall policy* yang dipergunakan untuk membuka jalur *traffic* dan melakukan *scanning* terhadap *antivirus, antispam, web filtering* dan IPS. Setelah membuat *interfaces* dan pengaturan *IP address* beserta *firewall policy*, langkah selanjutnya adalah membuat *routing*. *Routing* digunakan untuk meneruskan paket-paket jaringan dari satu jaringan ke jaringan lainnya melalui sebuah *internetwork*. *Routing* yang dipakai adalah *static route*. Tahapan selanjutnya yaitu konfigurasi VPN IPSec. Dalam tahap konfigurasi VPN IPSec, FortiGate pada kampus pusat dan kampus cabang menggunakan mode NAT, dan mempunyai IP Publik Statis yang sebelumnya sudah dikonfigurasi. Konfigurasi lanjutan yang diperlukan dalam membuat VPN IPSec pada kampus pusat yaitu membuat *tunneling* IPSec menggunakan *Internet Key Exchange* (IKE). Selanjutnya membuat *Firewall address* untuk mendefinisikan IP *address* yang diperbolehkan melewati *Firewall policy* dilanjutkan dengan membuat *Firewall policy* untuk *outbound* dan *inbound traffic* VPN IPSec. Setelah konfigurasi *Internet Key Exchange* (IKE), *Firewall address*, dan *Firewall policy*, langkah terakhir yaitu membuat konfigurasi *routing static* untuk VPN IPSec.
2. Setelah melakukan konfigurasi VPN IPSec pada kampus pusat, langkah-

langkah yang sama dilakukan untuk melakukan konfigurasi pada VPN IPSec di kampus cabang agar dapat terkoneksi dengan VPN kampus pusat.

Pengujian Jaringan Usulan

Untuk memastikan jaringan yang baru dapat bekerja sesuai dengan yang direncanakan maka dilakukan serangkaian pengujian sebagai berikut :

Pengujian pertama yaitu memastikan tunneling VPN IPSec aktif dan dapat membentuk jalur VPN antara kampus cabang dengan kampus pusat. Hasil pengujian menunjukan tampilan pada IPSec monitor sesudah tunnel antara kampus cabang dengan kampus pusat terhubung terlihat pada status yang sebelumnya "Bring Up" menjadi "Bring Down" dan berwarna hijau.

Pengujian IPSec, pengujian ini akan melihat bagaimana cara kerja IPSec saat koneksi VPN terhubung. Pengujian ini dilakukan dengan melihat *log* melalui *console* di FortiGate untuk melihat paket apa saja yang melintas ketika jalur VPN terbentuk untuk menghubungkan antara kampus cabang dengan kampus pusat.

Uji Konektivitas, pengujian ini dilakukan setelah tunnel VPN IPSec antara kampus cabang dengan kampus pusat terhubung. Pengujian di sisi komputer pengguna menggunakan sistem operasi windows. Hasil pengujian terlihat dari kondisi *ipconfig* pada laptop pengguna yang berada di kampus cabang yang membuktikan *rule policy* dari VPN IPSec berjalan sesuai dengan perencanaan sebelumnya.

Pengujian *packet loss* digunakan untuk memantau rata–rata, minimum, dan maksimum *packet loss* yang melalui tunnel VPN. Pengujian ini dilakukan dengan cara 3 kali pengiriman yaitu 1000, 5000, dan 10000 bytes data dengan 100 kali tes. Tes ini menggunakan *free tools* PsPing dari Microsoft untuk tes ping, latency, dan bandwidth. Hasil pengujian terlihat pada tabel berikut :

Tabel 1. *Packet Loss Tunnel VPN*

Lokasi Pengujian Kampus Cabang					
IP Sumber	IP Tujuan	*Bytes*	*Packet*		*Packet Loss* (%)
			Dikirim	Diterima	
192.168.65.100	192.168.21.100	1000	100	100	0
192.168.65.100	192.168.21.100	5000	100	100	0
192.168.65.100	192.168.21.100	10000	100	100	0

Pengujian *round trip time* digunakan untuk menghitung rata-rata dan maksimum waktu *round trip* pada tunnel *VPN* dengan menggunakan *ping*. Hasil dari pengujian ini sama dengan hasil *packet loss* karena *packet loss* dan *round trip* merupakan satu kesatuan tes pada perintah *ping*.

Tabel 2. *RTT* pada *Tunnel VPN IPSec*

Lokasi Pengujian Kampus Cabang					
IP Sumber	IP Tujuan	*Bytes*	RTT *Packet* dalam *Milisecond*		
			Min.	Max.	Average
192.168.65.100	192.168.21.100	1000	1.18	11.95	2.40
192.168.65.100	192.168.21.100	5000	1.90	21.84	4.72
192.168.65.100	192.168.21.100	10000	2.72	22.20	7.84

Pengujian akses server ini akan dilakukan pada server yang berada pada kampus pusat yang sudah terhubung dengan VPN berbasis IPSec sebelumnya. Dari pengujian akses ke server maka dibuktikan bahwa *remote* akses VPN dari kampus cabang berhasil masuk ke jaringan lokal yang berada di kampus pusat dan dapat mengakses server accurate yang dibutuhkan oleh bagian keuangan untuk mengentry data keuangan kampus cabang.

D. PENUTUP

Berdasarkan dari hasil perancangan dan pengujian dapat ditarik kesimpulan bahwa telah dihasilkan sebuah jalur lintas komunikasi proses pertukaran data yang aman dan terpercaya (*secure and reliable*)

JURNAL ELEKTRO & INFORMATIKA
SWADHARMA (JEIS)
VOLUME 01 NOMOR 01 JANUARI 2021
ISSN 2774 – 5775 | eISSN 2774-5767

antara kampus cabang dengan kampus pusat ITB Swadharma Jakarta. Dengan adanya jalur VPN IPSec, ITB Swadharma Jakarta dapat menghemat biaya pengeluaran dan antara kampus cabang dengan kampus pusat dapat terhubung secara real time.

Hasil pengujian konektivitas jaringan VPN IPSec :

1. *Packet Loss* : Konektivitas jaringan VPN IPSec antara kampus cabang dengan kampus pusat selama pengujian stabil dengan tidak adanya paket yang *loss*, dengan persentase *packet loss* 0%.
2. *Round trip time* : Dilakukan 3 kali pengetesan *round trip time* dengan besar ukuran paket 1000 bytes, 5000 bytes, dan 10000 bytes dengan 100 kali tes. *Round trip* minimum 1000 bytes yaitu 1.18 millisecond dengan maksimum 11.95 bytes, *round trip times* minimum 5000 bytes yaitu 1.90 ms dengan maksimum 21.84 ms, *round trip time minimum* 10000 bytes yaitu 2.72 ms dengan maksimum 22.20 ms, dapat ditarik kesimpulan semakin besar paket membuat *round trip time* tiba ke tujuan lebih lama.
3. Transfer File : Dilakukan pengetesan transfer file dari kampus pusat menuju kampus cabang dengan besar size paket 10,1 MB, 20,2 MB, dan 24, 9 MB. Untuk transfer file 10,1 MB dibutuhkan waktu 8 detik, lalu transfer file 20,2 MB dibutuhkan waktu 17 detik, dan transfer file 24,9 MB dibutuhkan waktu 20 detik. Dapat ditarik kesimpulan bahwa transfer file antar kampus cabang dengan kampus pusat sukses diterima, dan semakin besar paket yang dikirim maka waktu proses transfer file juga akan semakin lama.

Untuk pengembangan dan perbaikan jaringan kedepannya disarankan untuk :

1. Sebelum membuat policy pada security jaringan, sebaiknya perlu merumuskan terlebih dahulu dengan jelas fungsi dan tujuan keamanan data yang ingin dicapai, agar penggunaan VPN IPSec dapat berjalan sesuai keinginan.
2. Perlu adanya manajemen *bandwidth* yang mengatur bagian mana saja yang dapat menggunakan tunneling VPN dan yang hanya membutuhkan koneksi internet untuk memaksimalkan konektivitas kinerja jaringan.
3. Untuk kelancaran konektivitas VPN IPSec pada kampus cabang dan kampus pusat, diperlukan server monitoring yang dapat memantau kinerja dari VPN bila terjadi gangguan.

E. DAFTAR PUSTAKA

Pratama, I Putu Agus Eka. 2013. Jaringan Komputer : Teori dan Praktik Berbasiskan Open Source. Bandung : Informatika

Sofana, Iwan. 2012. Cisco CCNA & Jaringan Komputer. Bandung : Informatika

Towidjojo, Rendra. 2014. Mikrotik Kungfu. Jakarta : Jasakom