Volume 11 Number 2 November 2021 Page. 73-84
Journal Homepage : http://teknois.stikombinaniaga.ac.id/index.php/JBS
DOI Link : http://doi.org/10.36350/jbs.v11i2

Article DOI : 10.36350/jbs.v11i2.117
Received: September; Accepted : October; Published : November

Penerapan Algoritma Rivest Shamir Adleman Untuk Meningkatkan Keamanan Virtual Private Network

Adiat Pariddudin[1*], Muhammad Syawaludin[2]
[1]Sistem Informasi/Universitas Binaniga Indonesia
Email: adiat@stikombinaniaga.ac.id
[2]Sistem Informasi/ Universitas Binaniga Indonesia
Email: syawaludi04@gmail.com

ABSTRACT

Data and information security of an organization or company is very important. Data in an organization or company has important information for the sustainability of a company, as well as PT Karya Gemilang Plasindo. In order to increase the productivity and speed of information data, a VPN (Virtual Private Network) technology was built to connect the branch company and some employees who work on a mobility. But in practice there is a gap in the VPN (Virtual Private Network) technology used, the management of devices and users is irregular because the connecting process is only a username and password. The solution is to increase security in VPN (Virtual Private Network) technology by changing the VPN (Virtual Private Network) protocol and adding a certificate to limit devices that can connect to the intranet network. Previously, VPN (Virtual Private Network) technology used the PPTP (Point-to-Point Tunneling Protocol) protocol. These deficiencies are solved by changing the protocol to SSTP (Secure Socket Tunneling Protocol) and creating a certificate as the identity of a device while limiting the devices that can connect to the intranet network. The design in this study used RnD (Research and Development) and the results were tested using the Validity Test and Reliability Test with the KR 20 technique (Kuder Richardson). This test is tested using a questionnaire about the level of security of the latest technology to users. The test results to be achieved are the increased security of VPN (Virtual Private Network) on the designed intranet network that is considered to be able to maintain data and information security at PT Karya Gemilang Plasindo.

***Keywords**: RSA; PPTP; VPN; RnD; Protocol.*

ABSTRAK

Keamanan data dan informasi dari sebuat organisasi atau perusahaan sangatlah penting. Data dalam sebuah organisasi atau perusahaan memiliki informasi dan keterangan-keterangan penting untuk keberlanjutan sebuah perusahaan, begitu juga dengan PT Karya Gemilang Plasindo. Demi meningkatkan produktifitas dan kecepatan data informasi dibangunlah sebuah teknologi VPN (Virtual Private Network) untuk menghubungkan jaringan komputer perusahaan cabang dan beberapa karyawan yang bekerja secara mobilitas. Namun pada prakteknya ada sebuah celah kekurangan pada teknologi VPN (Virtual Private Network) yang digunakan, menejemen perangkat dan pengguna tidak teratur karena pada proses menyambungkan hanya sekedar username dan password saja. Solusinya adalah meningkatakan keamanan pada teknologi VPN (Virtual Private Netwok) dengan cara merubah protokol VPN (Virtual Private Network) dan menambahkan certificate untuk membatasi perangkat yang dapat tersambung ke jaringan intranet. Pada teknologi VPN (Virtual Private Network) sebelumnya menggunakan protokol PPTP (Point-to-Point Tunneling Protocol). Kekurangan tersebut diperbaiki pada penelitian ini dengan mengganti protokol menjadi SSTP (Secure Socket Tunneling Protocol) dan membuat certificate sebagai

Volume 11 Number 2 November 2021 Page. 73-84
Journal Homepage : http://teknois.stikombinaniaga.ac.id/index.php/JBS
DOI Link : http://doi.org/10.36350/jbs.v11i2

identitas sebuah perangkat seklaigus membatasi perangkat yang dapat tersambung pada jaringan intranet. Perancangan pada penelitian ini menggunakan metode penelitian dan pengembangan RnD (Research and Development) dan hasilnya diuji menggunakan Uji Validitas dan Uji Reliabilitas dengan teknik KR 20 (Kuder Richardson). Pada pengujian ini diuji dengan menggunakan kuesioner tentang tingkat keamanan teknologi terbaru kepada pengguna. Hasil uji yang ingin dicapai adalah meningkatnya keamanan VPN (Virtual PRivate Network) pada jaringan intranet yang dirancang dinilai dapat menjaga keamanan data dan informasi di PT Karya Gemilang Plasindo.

***Keywords**: RSA; PPTP; VPN; RnD; Protokol.*

A. PENDAHULUAN

1. Latar Belakang

Perkembangan teknologi saat ini semakin hari kian meningkat dengan cepat. Hal itu tentunya dapat membawa kemudahan bagi manusia dalam melakukan kegiatan sehari-hari. Begitupun dengan jaringan komputer yang berkembang mengikuti arus teknologi yang terus berinovasi. Dalam mengikuti perkembangan teknologi, saat ini banyak bidang yang membutuhkan sebuah jaringan komputer. Jaringan komputer yang baik memberikan kemudahan pengguna untuk melakukan komunikasi data antar pengguna dan dapat dilakukan dengan mudah dan cepat. Oleh karena itu efektifitas dan efisiensi bisa dicapai dan meningkatkan produktifitas lebih tinggi.

Adanya manfaat dari perkembangan teknologi komunikasi dan informasi juga dapat dirasakan seiring dengan semakin berkembangnya sistem komunikasi dalam komputer. Komputer sebagai salah satu bukti adanya perkembangan teknologi pastinya sudah tidak asing lagi dalam kehidupan sehari-hari. Bahkan dengan berkembangnya literasi media dan komunikasi masa seperti internet yang dapat memudahkan mencari informasi juga menjadikan komputer sebagai sarana teknologi informasi dan komunikasi yang menjanjikan. Oleh sebab itu, pembahasan mengenai sistem komunikasi dalam komputer menarik untuk dibahas. Sistem komunikasi sendiri sebenarnya merupakan gabungan dari adanya perangkat keras dan perangkat lunak yang dicipatakan untuk menyampaikan informasi atau komunikasi dari satu lokasi ke lokasi yang lainnya. Perkembangan sistem komunikasi tersebut juga berpengaruh pada perkembangan teknologi komunikasi dalam komputer. Komputer juga dianggap menjadi suatu komponen yang penting dalam sistem komunikasi. Hal ini dikarenakan komputer memiliki peran penting dalam proses perubahan data menjadi informasi. Oleh sebab itu, jenis teknologi komunikasi dalam komputer juga beragam.

Selain itu, hal yang mendasar dari teknologi komunikasi dan informasi adalah standar. Sementara itu, perkembangan jaringan amat membutuhkan sebuah standar sistem operasional. Ketika seseorang menggunakan jaringan untuk berkomunikasi dengan orang lain, maka sesungguhnya dia secara tidak langsung membutuhkan sistem yang kompatibel antara satu dengan lainnya. Keterikatan antara standar, jaringan dan sistem ibarat perekat dalam menunjang komunikasi bersama.

Virtual Private Network (VPN) adalah cara untuk mensimulasikan jaringan private melalui jaringan publik, seperti internet. Disebut "virtual" karena bergantung pada penggunaan virtual yaitu koneksi, koneksi sementara yang tidak memiliki kehadiran fisik secara nyata, tetapi terdiri dari paket diarahkan melalui variasi mesin di internet secara ad-hoc. Koneksi virtual yang aman yang dibuat antara dua mesin, mesin dan jaringan, atau dua jaringan. Teknologi Virtual Private Network (VPN) memiliki kemampuan untuk melakukan autentikasi terhadap sumber pengirim data yang akan diterima. Virtual Private Network (VPN) akan melakukan pemeriksaan terhadap semua data yang masuk dan mengambil informasi source datanya. Alamat source data ini akan disetujui jika proses autentikasinya berhasil. Dengan demikian, Virtual Private Network (VPN) menjamin semua data yang dikirim dan diterima oleh client berasal dari sumber yang semestinya. Tidak ada data yang dipalsukan atau dikirimkan oleh pihak-pihak lain.

Seiring dengan maraknya penggunaan internet, banyak perusahaan yang kemudian beralih menggunakan internet sebagai bagian dari jaringan mereka untuk menghemat biaya. Akan tetapi permasalahan keamanan masih menjadi faktor utama dalam relabilitas suatu jaringan. Virtual Private Network (VPN) merupakan salah satu cara yang dapat digunakan untuk membuat jaringan yang bersifat private dan koneksi jarak jauh (remote access) dengan tingkat keamanan yang tinggi diatas jaringan publik dan internet.

Layanan VPN didukung oleh beberapa protokol komunikasi data, yang mana tiap protokol tersebut memiliki konsep keamanan yang berbeda-beda. Berikut jenis setiap VPN. Point to Point Transfer Protocol (PPTP), Layer 2 Transfer Protocol (L2TP), Internet Protocol Security (IPSec), Internet Key Exchange (IKEv2), Secure Socket Tunneling Protocol (SSTP).

Dalam merancang dan implemntasi VPN pada sebuah jaringan nirkabel karyawan dapat dengan mudah memperoleh data ataupun informasi dari internet dengan tetap memastikan bahwa kerahasiaan dari data yang sensitif dapat terjaga pada saat transmisi. Sehingga dibangun sebuah sistem baru dengan mempertimbangkan beberapa aspek keamanan dan hak akses. Sistem tersebut yaitu Virtual Private Network (VPN) yang memberikan fungsi dalam menjaga kerahasiaan data (Confidentiality), keutuhan data (Data Integrity) serta otentikasi sumber (Origin Authentication).

Namun, semakin tingginya penggunaan teknologi informasi di era globalisasi komunikasi ini, semakin meningkat pula risiko yang dihadapi, terutama dari sisi kualitas dan keamanannya. Berbagai ancaman terhadap suatu data atau informasi yang dipertukarkan melalui jaringan internet menuntut suatu solusi keamanan salah satunya dengan menggunakan sertifikat elektronik yang dikeluarkan dan dikelola oleh pihak ketiga terpercaya (Trusted Third Party) atau lazim disebut CA (Certification Authority). CA atau dikenal juga dengan istilah sertifikat elektronik menjamin 4 (empat) aspek dalam interaksi data, yaitu kerahasiaan (confidentiality), menyangkut kerahasiaan dari data atau informasi, dan perlindungan bagi informasi tersebut dari pihak yang tidak berwenang, Keotentikan (authenticity), menyangkut kemampuan seseorang, organisasi, atau komputer untuk membuktikan identitas dari pemilik yang sesungguhnya dari informasi tersebut, integritas (integrity), menyangkut perlindungan data terhadap upaya perubahan oleh pihak-pihak yang tidak bertanggung jawab, baik selama data itu disimpan maupun selama data itu dikirimkan kepada pihak lain, dan nir sangkal (non repudiation), menyangkut perlindungan terhadap suatu pihak yang terlibat dalam suatu transaksi.

CRT (Chinese Remainder Theorem) merupakan suatu algoritma untuk mengurangi perhitungan aritmatika modular dengan modulus besar untuk perhitungan yang sama untuk masing-masing faktor dari modulus. CRT dapat memperpendek ukuran bit eksponen dekripsi d (merupakan kunci publik RSA atau RSA-CRT) dengan cara menyembunyikan d pada sistem kongruen sehingga mempercepat waktu dekripsi serta dapat digunakan bersama algoritma RSA yang disebut RSA-CRT.

Algoritma RSA menggunakan 2 angka (e dan d) sebagai kunci publik dan kunci private. Pada algoritma RSA e dan n diumumkan untuk umum sedangkan d dirahasiakan. Meskipun RSA dapat digunakan untuk mengenkripsi dan mendekripsi pesan, sangat lambat jika pesan tersebut panjang. Oleh karena itu, algoritma RSA berguna untuk pesan singkat. Sejak algoritma menggunakan 2 kunci untuk enkripsi dan dekripsi, algoritma RSA dianggap sebagai contoh kunci asimetrik kriptografi. Sistem kriptografi RSA dapat dimodifikasi dengan menggunakan teorema CRT disebut dengan RSA-CRT. Terbukti sistem kriptografi RSA-CRT memiliki waktu komputasi yang lebih singkat dari pada sistem kriptografi RSA biasa, yaitu sekitar empat kali lebih cepat.

2. Permasalahan

Dalam menghubungkan jaringan intranet disetiap perusahaan memiliki kelemahan keamanan pada VPN dalam mengautentikasi username dan perangkat VPN client yang akan tersambung ke dalam jaringan intranet

Volume 11 Number 2 November 2021 Page. 73-84
Journal Homepage : http://teknois.stikombinaniaga.ac.id/index.php/JBS
DOI Link : http://doi.org/10.36350/jbs.v11i2

3. Tujuan

Menerapkan Algoritma Rivest Shamir Adleman (RSA) untuk perangkat Virtual Private Network (VPN) client dalam meningkatkan keamanan jaringan intranet

4. Tinjauan Pustaka

Algoritma RSA adalah algoritma yang sangat maju dalam bidang kriptografi kunci public (kriptografi public key) yang sangat popular dan masih digunakan sampai saat ini. RSA merupakan algoritma yang paling cocok untuk digital signature seperti halnya enkripsi. Algoritma RSA masih digunakan secara luas dalam protocol electronic commerce dan dipercaya dalam pengamanan dengan kunci yang sangat panjang. Algoritma RSA disebut sebagai kunci publik karena kunci enkripsi dapat dibuat public yang berarti semua orang dapat mengetahuinya. Walaupun dibuat public key, keamanan algoritma RSA sangat terjaga. Hal itu dikarenakan kunci yang digunakan untuk enkripsi pada algoritma RSA berbeda dengan kunci yang digunakan untuk dekripsinya. Keamanan enkripsi dan dekripsi algoritma RSA terletak pada kesulitan untuk memfaktorkan modulus n yang sangat besar. Penamaan algoritma RSA diambil dari nama penemunya, yaitu Rivest, Shamir dan Adleman yang diplubikasikan pada tahun 1977 di MIT yang bertujuan untuk menjawab tantangan dari Algoritma Pertukaran Kunci Diffie Helman.

B. METODE

Metode penelitian yang digunakan dalam penelitian ini adalah penelitian dan pengembangan (Research and Development). Metode penelitian pengembangan atau dalam bahasa Inggrisnya Research and Development adalah metode penelitian yang digunakan untuk menghasilkan produk tertentu, dan menguji keefektifan produk tersebut. Untuk menghasilkan produk tertentu digunakan penelitian yang bersifat analisis kebutuhan dan untuk menguji keefektifan produk tersebut supaya dapat berfungsi di masyarakat luas, maka diperlukan penelitian untuk menguji keefektifan produk tersebut (Sugiyono, 2012,p.297). Secara skematik langkah-langkah tersebut dapat ditunjukkan seperti pada gambar 3.

Gambar 3. Model RnD

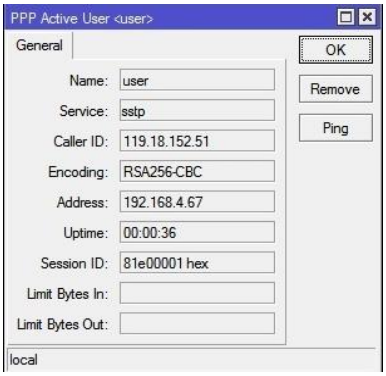
C. HASIL DAN PEMBAHASAN

1. Hasil

Hasil dari penerepan Algoritma Rivest Shamir Adleman (RSA) dalam meningkatkan untuk Virtual Private Network (VPN) yaitu, terhubungnya koneksi setelah pengguna berhasil tersambung ke dalam jaringan intranet menggunakan SSTP disajikan pada Gambar 2. Dan Status pengguna yang terekam pada router disajikan pada Gambar 3.

Volume 11 Number 2 November 2021 Page. 73-84
Journal Homepage : http://teknois.stikombinaniaga.ac.id/index.php/JBS
DOI Link : http://doi.org/10.36350/jbs.v11i2

Gambar 2. Status Koneksi Pada Client



Gambar 3. Status Koneksi Pada Router

2. Pembahasan

Komunikasi jaringan Virtual Private Network (VPN) dikembangkan menggunakan SSTP dan RSA yang terintegrasi pada Router Mikrotik. Pengguna harus menghubungkan laptopnya ke internet kemudian memasukan username dan password pada koneksi VPN yang telah dibuat. Sebelum SSTP mengenali username dan password, SSTP memeriksa certifcate authority pada client yang sudah dipasang sebelumnya.

a. Membuat Certificate Authority (CA) Private Key dan Certificate Authority (CA) Pair menggunakan perintah **# openssl genrsa –des3 –out ca.key 4096**

```
root@ubuntu:/home/syawal/syawal/key# openssl genrsa -des3 -out ca.key 4096
Generating RSA private key, 4096 bit long modulus
.....................................................................++
...........................++
e is 65537 (0x10001)
Enter pass phrase for ca.key:
Verifying - Enter pass phrase for ca.key:
root@ubuntu:/home/syawal/syawal/key#
```

Gambar 4 Proses Membuat Certificate Authority (CA)

b. Generate file Certificate Authority (CA Certificate) menggunakan perintah **# openssl req –new –x509 –days 3650 –key –out ca.crt**

Volume 11 Number 2 November 2021 Page. 73-84
Journal Homepage : http://teknois.stikombinaniaga.ac.id/index.php/JBS
DOI Link : http://doi.org/10.36350/jbs.v11i2

```
root@ubuntu:/home/syawal/syawal/key# openssl req -new -x509 -days 3650 -key ca.k
ey -out ca.crt
Enter pass phrase for ca.key:
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:ID
State or Province Name (full name) [Some-State]:Jawa Barat
Locality Name (eg, city) []:Bogor
Organization Name (eg, company) [Internet Widgits Pty Ltd]:cahayabuana
Organizational Unit Name (eg, section) []:IT
Common Name (e.g. server FQDN or YOUR name) []:www.cahayabuana.co.id
Email Address []:it@cahayabuana.co.id
root@ubuntu:/home/syawal/syawal/key#
```

Gambar 5 Generate Certificate Authority (CA)

c. Membuat Certificate Pair / Server key untuk server SSTP dengan perintah **# openssl genrsa –des3 –out server.key 4096**

```
root@ubuntu:/home/syawal/syawal/key# openssl genrsa -des3 -out server.key 4096
Generating RSA private key, 4096 bit long modulus
.....................................................................................
.....................................................................++
.....................................................................................
.....................................................................................
........++
e is 65537 (0x10001)
Enter pass phrase for server.key:
Verifying - Enter pass phrase for server.key:
root@ubuntu:/home/syawal/syawal/key#
```

Gambar 6. Membuat Server Key

d. Membuat Server Certificate dengan perintah **# openssl req –new –key server.key –out server.csr**

```
root@ubuntu:/home/syawal/syawal/key# openssl req -new -key server.key -out serve
r.csr
Enter pass phrase for server.key:
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:ID
State or Province Name (full name) [Some-State]:Jawa Barat
Locality Name (eg, city) []:Bogor
Organization Name (eg, company) [Internet Widgits Pty Ltd]:cahayabuana
Organizational Unit Name (eg, section) []:it
Common Name (e.g. server FQDN or YOUR name) []:7c2608d9e0af.sn.mynetname.net
Email Address []:it@cahayabuana.co.id

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:mikrotik123
An optional company name []:cahayabuana
root@ubuntu:/home/syawal/syawal/key#
```

Gambar 7. Membuat Server Csr

e. Generate Server Certificate dengan perintah **# openssl x509 –req –days 3650 –in server.csr –CA ca.crt –Cakey ca.key –set_serial 01 –out server.crt**

```
root@ubuntu:/home/syawal/syawal/key# openssl x509 -req -days 3650 -in server.csr
 -CA ca.crt -CAkey ca.key -set_serial 01 -out server.crt
Signature ok
subject=/C=ID/ST=Jawa Barat/L=Bogor/O=cahayabuana/OU=it/CN=7c2608d9e0af.sn.mynet
name.net/emailAddress=it@cahayabuana.co.id
Getting CA Private Key
Enter pass phrase for ca.key:
root@ubuntu:/home/syawal/syawal/key#
```

Gambar 8. Generate Server Crt

f. Membuat Client key denga perintah **# openssl genrsa –des3 –out client.key 4096**

Volume 11 Number 2 November 2021 Page. 73-84
Journal Homepage : http://teknois.stikombinaniaga.ac.id/index.php/JBS
DOI Link : http://doi.org/10.36350/jbs.v11i2

```
root@ubuntu:/home/syawal/syawal/key# openssl genrsa -des3 -out client.key 4096
Generating RSA private key, 4096 bit long modulus
......++
.....................................................................................
.++
e is 65537 (0x10001)
Enter pass phrase for client.key:
Verifying - Enter pass phrase for client.key:
root@ubuntu:/home/syawal/syawal/key#
```

Gambar 9. Membuat Client Key

g. Membuat Client Certificate dengan perintah **# openssl req –new –key client.key –out client.csr**

```
root@ubuntu:/home/syawal/syawal/key# openssl req -new -key client.key -out clien
t.csr
Enter pass phrase for client.key:
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:ID
State or Province Name (full name) [Some-State]:Jawa Barat
Locality Name (eg, city) []:Bogor
Organization Name (eg, company) [Internet Widgits Pty Ltd]:cahayabuana
Organizational Unit Name (eg, section) []:it
Common Name (e.g. server FQDN or YOUR name) []:7c2608d9e0af.sn.mynetname.net
Email Address []:it@cahayabuana.co.id

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:mikrotik123
An optional company name []:cahayabuana
root@ubuntu:/home/syawal/syawal/key#
```

Gambar 10. Membuat Client Csr

h. Generate Client Certificate dengan perintah **# openssl x509 -req -days 3650 -in client.csr -CA ca.crt -CAkey ca.key -set_serial 01 -out client.crt**

```
root@ubuntu:/home/syawal/syawal/key# openssl x509 -req -days 3650 -in client.csr
 -CA ca.crt -CAkey ca.key -set_serial 01 -out client.crt
Signature ok
subject=/C=ID/ST=Jawa Barat/L=Bogor/O=cahayabuana/OU=it/CN=7c2608d9e0af.sn.mynet
name.net/emailAddress=it@cahayabuana.co.id
Getting CA Private Key
Enter pass phrase for ca.key:
root@ubuntu:/home/syawal/syawal/key#
```

Gambar 11. Generate Client Crt

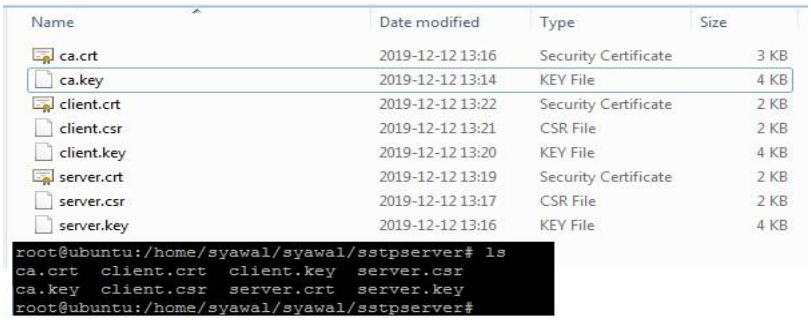
i. Memeriksa sertifikat dengan perintah **# openssl x509 -noout -text -in server.crt –purpose**

```
Certificate purposes:
SSL client : Yes
SSL client CA : No
SSL server : Yes
SSL server CA : No
Netscape SSL server : Yes
Netscape SSL server CA : No
S/MIME signing : Yes
S/MIME signing CA : No
S/MIME encryption : Yes
S/MIME encryption CA : No
CRL signing : Yes
CRL signing CA : No
Any Purpose : Yes
Any Purpose CA : Yes
OCSP helper : Yes
OCSP helper CA : No
Time Stamp signing : No
Time Stamp signing CA : No
root@ubuntu:/home/syawal/syawal/key#
```

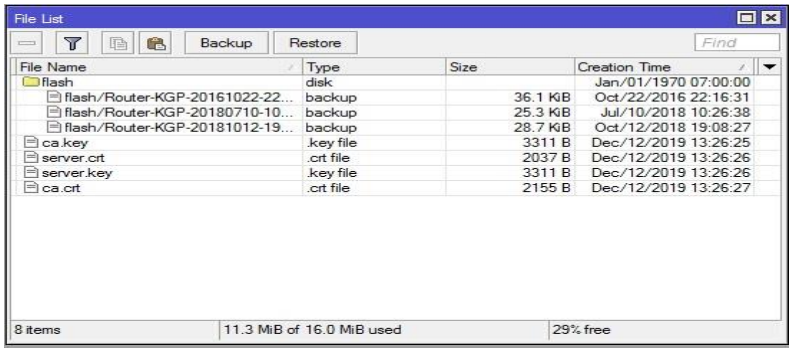
Gambar 12. Memeriksa file Sertfikat

j. Melihat sertifikat

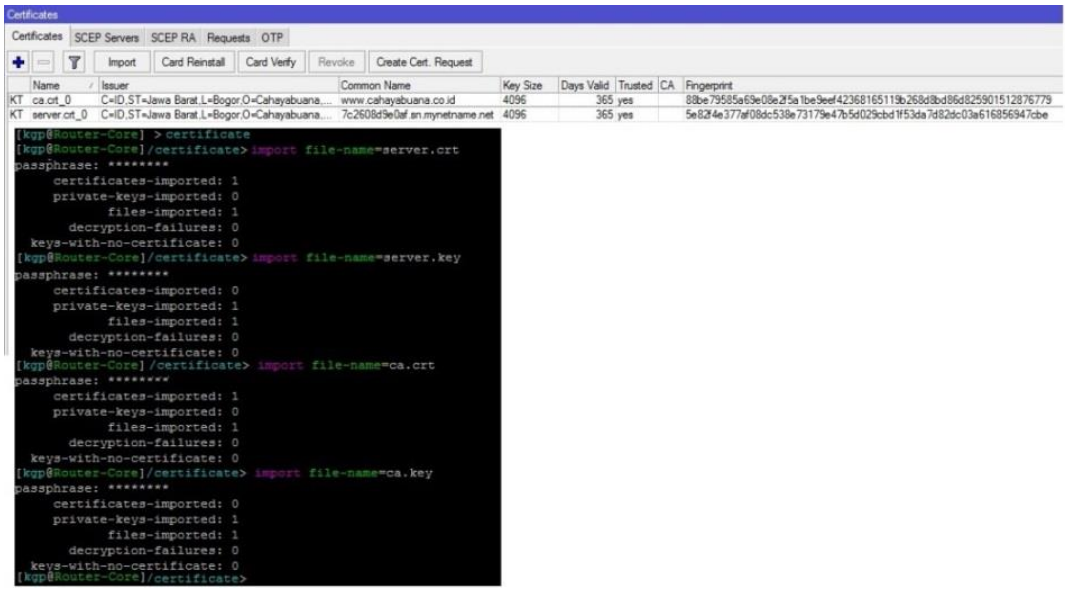
Volume 11 Number 2 November 2021 Page. 73-84
Journal Homepage : http://teknois.stikombinaniaga.ac.id/index.php/JBS
DOI Link : http://doi.org/10.36350/jbs.v11i2



Gambar 13 Melihat file Sertifikat dan *Export* file Sertifikat

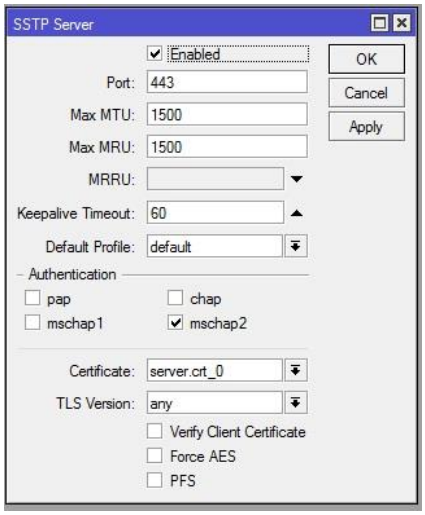


Gambar 14 Upload File ke Router Mikrotik

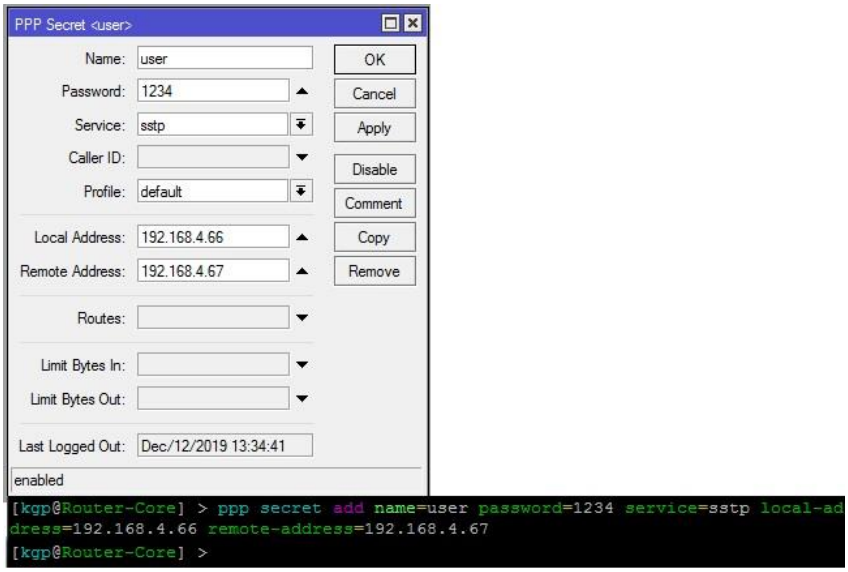


Gambar 15 Import File ke Router Mikrotik

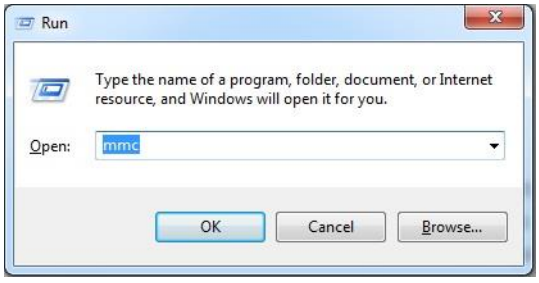
Volume 11 Number 2 November 2021 Page. 73-84
Journal Homepage : http://teknois.stikombinaniaga.ac.id/index.php/JBS
DOI Link : http://doi.org/10.36350/jbs.v11i2



Gambar 16 Aktifkan SSTP Server

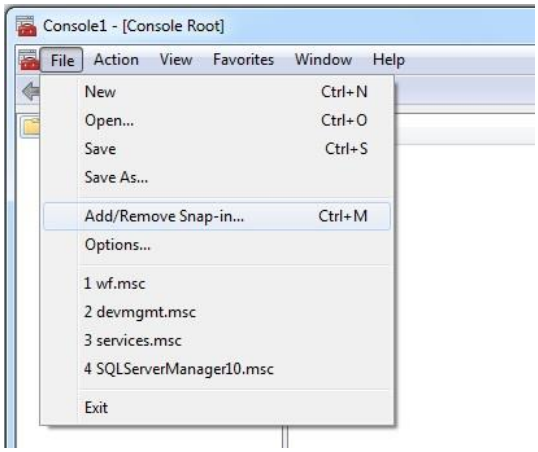


Gambar 17 Membuat User VPN

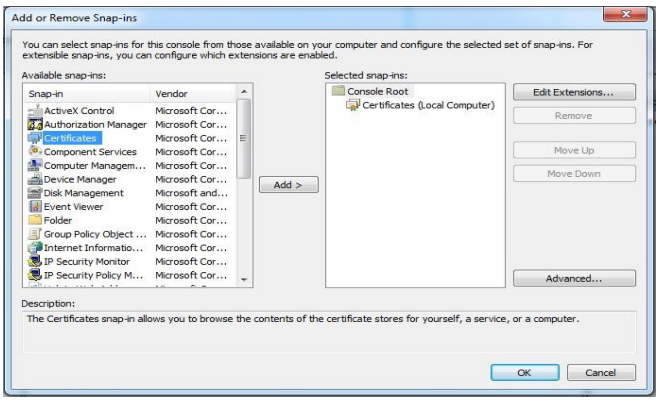


Gambar 18 Membuka Console

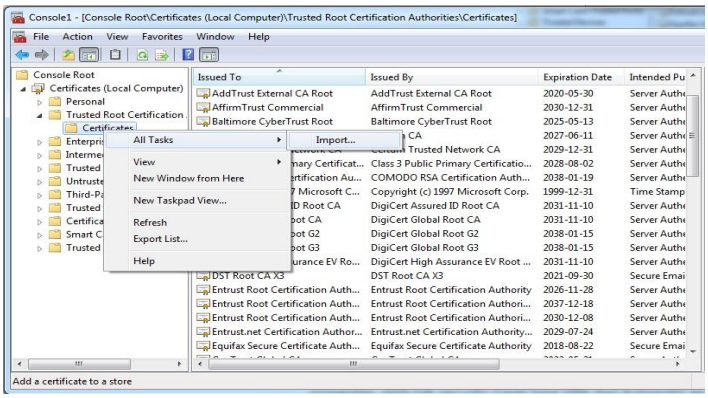
Volume 11 Number 2 November 2021 Page. 73-84
Journal Homepage : http://teknois.stikombinaniaga.ac.id/index.php/JBS
DOI Link : http://doi.org/10.36350/jbs.v11i2



Gambar 19. Masuk ke Directory Certificate

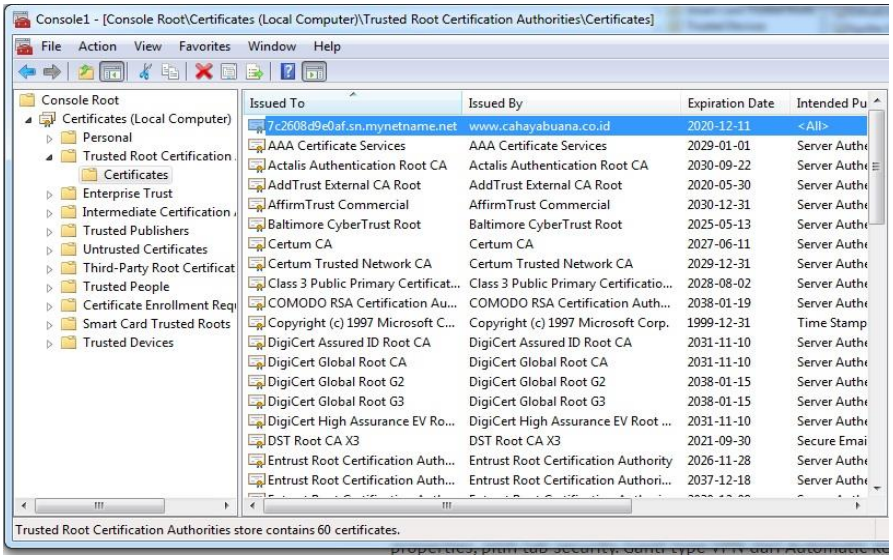


Gambar 20. Masuk ke Management Certificate

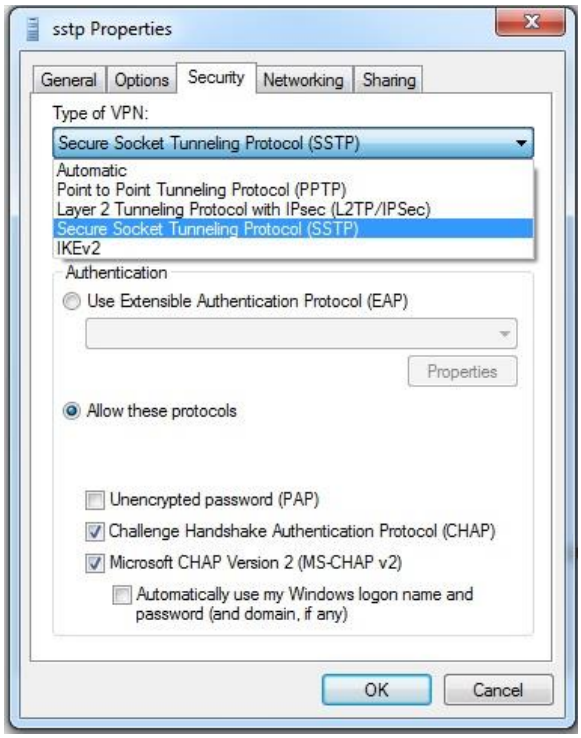


Gambar 21. Import Certificate ke End Device

Volume 11 Number 2 November 2021 Page. 73-84
Journal Homepage : http://teknois.stikombinaniaga.ac.id/index.php/JBS
DOI Link : http://doi.org/10.36350/jbs.v11i2



Gambar 22. Memeriksa Certificate



Gambar 23. Konfigurasi SSTP Client

D. KESIMPULAN

Berdasarkan hasil penelitian yang telah diuraikan, maka kesimpulan yaitu:

1. Dengan menggunakan SSTP dan Algoritma RSA pada jarigan VPN yang menggunakan jaringan internet menjadi lebih aman, jangkauan jaringan lokal yang dimiliki perusahaan akan menjadi luas. Waktu yang dibutuhkan untuk menghubungkan jaringan intranet semakin cepat. Selama bisa mendapatkan akses internet, pengguna tetap dapat melakukan koneksi dengan jaringan lokal.
2. Teknologi VPN yang menggunakan SSTP menggunakan cetificate RSA untuk menjamin keamanan lalu lintas data. SSTP dapat membuat sambungan dan mengidentifikasi VPN client yang diberi wewenang untuk tersambung ke jaringan intranet. Resiko tidak menggunakan certificate RSA akan mempermudah peretas untuk tersambung ke jaringan intranet dan mengakses informasi maupun data perusahaan yang sensitif dan disalah gunakan.

E. DAFTAR PUSTAKA

[1] Ahmad Budi Setiawan. 2015. Ekosistem Penyelenggaraan Sertifikat Elektronik Dalam Sistem Perdagangan Elektronik, Vol.6, No.2, Puslitbang Aplikasi Informatika dan Informasi Komunikasi, hal 15-27.

[2] Ahmad, Amar. 2012. Perkembangan Teknologi Komunikasi dan Informasi: Akar Revolusi dan Berbagai Standarnya, Jurnal Dakwah Tabligh, Vol.13, No.1, Universitas Indonesia Jakarta, hal 137-149.

[3] Arikunto, Suharsimi. 1998. Prosedur Penelitian, Rineka Cipta, Jakarta.

[4] Guilford, J.P. 1956. Fundamental Statistic in Psychology and Education. McGraw-Hill Book Company, Inc. New York.

[5] Harbani, Arif, and Muhamad A. Fahreza. "Aplikasi Keamanan Data Gambar Menggunakan Algoritma RSA (Rivest Shamir Adleman) Berbasis Desktop." Teknois, vol. 9, no. 1, May. 2019, pp. 1-9, doi:10.36350/jbs.v9i1.1.

[6] Nasution. 2009. Metode Research (Penelitian Ilmiah). Bumi Aksara. Jakarta.

[7] Sahari. 2008. Perancangan dan Implementasi Virtual Private Network (VPN) Pada Jaringan Nirkabel, Poli Rekayasa, Vol.4, No.1, UPI-YPTK Padang, hal 48-55.

[8] Singarimbun, Masri & Effendi, Sofian. 1999. Metode Penelitian Survay. PT Pustaka LP3ES Indonesia. Jakarta.

[9] Sugiyono. 2009. Metode Penelitian Kualitatif, Alfabeta, Bandung.

[10] Sugiyono. 2012. Metode Penelitian Kuantitatif, Kualitatif, dan R & D, Alfabeta, Bandung.