Penerapan IP *Security* pada Jaringan VPN *Site to Site* di PT. Pertamina Ubeb Adera Pengabuan

Dedi Irawan[1], Fatoni[2]
Dosen Universitas Bina Darma
Pos-el: dedi.irawan@binadarma.ac.id [1], fatoni@binadarma.ac.id [2]

ABSTRACT

VPN (Virtual Private Network) in its implementation is divided into two types namely VPN remote access and site-to-site VPN. VPN Remote access is a VPN that is used to remotely host a server or private host through a public network. Whereas site-to-site VPN is used to connect networks that have long distances through the public network so that it seems to be on a local network, for example between Field Ubeb Adera premises Field Prabumulih. In this case the occurrence of communication or sharing of data between the two fields of surviving with field Prabumulih through VPN (Virtual Private Network) site to site technology, it requires a security (security) to maintain the confidentiality of these data. The Internet Protocol Security (IPSec) security protocol is a security protocol capable of meeting the criteria of security support and has a better security level that is most widely used to improve the security of site to site VPNs in PT. Pertamina Ubeb Adera Pengabuan.

Keywords *- IPSec; VPN; Sharing; Host Private.*

ABSTRAK

VPN (*Virtual Private Network*) dalam implementasinya terbagi dua jenis yaitu VPN remote access dan *site-to-site* VPN. VPN *Remote access* adalah VPN yang digunakan untuk meremote server atau host private dengan aman melalui jaringan publik. Sedangkan VPN *site-to-site* digunakan untuk menghubungkan jaringan yang memiliki jarak yang cukup jauh melalui jaringan publik sehingga seakan berada pada satu jaringan local, misal antara Field Ubeb Adera denga Field Prabumulih. Dalam kasus ini terjadinya komunikasi atau sharing data antara kedua Field Pengabuan dengan *Field* Prabumulih melalui teknologi VPN (*Virtual Private Network*) *site to site*, tentuhnya membutuhkan sebuah scurity(keamanan) untuk menjaga kerahasian data-data tersebut. Protokol keamanan Internet Protocol Security (IPSec) merupakan protokol keamanan mampu memenuhi kriteria dukungan keamanan dan mememiliki tingkat keamanan yang lebih baik yang paling banyak digunakan untuk meningkatkan keamanan VPN site to site yang ada di PT. Pertamina Ubeb Adera Pengabuan.

Kata Kunci - IPSec; VPN; Sharing; Host Private.

1. PENDAHULUAN

Kebutuhan bisnis dimasa sekarang didukung dengan variasi jaringan komunikasi yang luas. Para karyawan di perusahaan mengakses sumberdaya perusahaan untuk mendukung pekerjaan mereka melalaui jaringan komunikasi yang

perusahaan mereka miliki. Belum lagi rekanan bisnis perusahaan yang turut mengakses sumberdaya perusahaan dengan jaringan yang lain dalam rangka kerja sama membagi informasi bisnis, perencanaan bisnis bersama, dan lain sebagainya. Pada umumnya perusahaan menggunaakan berbasis *leased lines* atau sirkit *frame relay* untuk menghubungkan kantor pusat dengan kantor cabang yang ada, hal tersebut tidak fleksibel mengingat saat ini sebuah perusahaan biasanya ingin cepat mempunyai jaringan komunikasi dengan rekanan bisnis yang lain atau untuk mendukung karyawan yang sedang bekerja mengerjakan proyek yang bersifat lapangan dan menuntut mobilitas.[1]

PT. Pertamina Ubeb Adera Pengabuan adalah salah satu perusaan BUMN yang bertugas mengelola penambangan minyak dan gas bumi cabang Pertamina Prabumulih EP, dalam proses komunikasi atau *sharing* data kedua perusahaan tersebut menggunakan teknologi jaringan VPN *site to site*, sebagai media komunikasi dan *sharing* data. Mengingat jarak antara *field* Adera dengan *field* Prabumulih memiliki jarak yang cukup jauh yaitu 30 kilometer dimana kedua *field* tersebut sudah memiliki layanan ISP (*Internet Service Provider*) tersendiri dan sudah memanfaatkan VPN sebagai media komunikasi dan *sharing*. VPN (*Virtual Private Network*) merupakan suatu cara untuk membuat sebuah jaringan bersifat *private* dan aman dengan menggunakan jaringan *publik* misalnya internet. Jaringan *publik* yang digunakan saat ini sangat rentan terhadap ancaman keamanan seperti pencurian data, dan memberikan kerugian yang besar apabila data yang dicuri adalah data penting transaksi bisnis suatu perusahaan. Oleh karena itu, dibutuhkan jaringan yang tidak bisa diakses oleh *publik*. Data yang dilewatkan *dienkapsulasi* terlebih dahulu kemudian di *enkripsi* agar tidak terbaca ketika melewati jaringan *publik* karena harus melewati *proses dekripsi*. Dikenal tiga jenis VPN dalam implementasinya, yaitu *trusted, secure*, dan *hybrid* VPN *Secure* VPN adalah perpaduan teknologi *tunneling* dan *enkripsi*. Penggunaan *enkripsi* dalam teknologi VPN membuat VPN tidak dapat dibaca oleh pihak-pihak yang tidak berkepentingan karena harus melewati *proses dekripsi* terlebih dahulu. Implementasi jaringan VPN

berbasis IPSec (*Internet Protocol Security*) dan GRE (*Generic Routing Encapsulation*) merupakan jenis VPN yang sering digunakan untuk membentuk jaringan yang bersifat *private* dan aman.[2]

Dalam penelitian ini penulis berupaya untuk menghindari hal tersebut maka penulis berinisiatif melakukan penerepan IP *Scurity* pada jaringan VPN PT. Pertamina Ubeb Adera Pengabuan sebagai *scurity* saat komunikasi data melalui jaringan VPN tersebut.

2. METODOLOGI PENELITIAN

2.1 Metode Penelitian

Metode penelitian yang digunakan adalah metode *eksperimen*, Metode *Eksperimen*, adalah penelitian untuk menguji apakah *variabel-variabel eksperimen efektif* atau tidak. Untuk menguji *efektif* tidaknya harus digunakan variabel kontrol. Penelitian *eksperimen* adalah untuk menguji *hipotesis* yang dirumuskan secara ketat. Penelitian *eksperimen* biasanya dilakukan untuk bidang yang bersifat eksak. Sedangkan untuk bidang sosial biasanya digunakan metode *survey eksplanatory*, metode *deskriptif*, dan *historis*.[3] Adapun tahapan atau siklus dari metode *eksperimen* ialah sebagai berikut:

1. Pencobaan awal dalam tahapan berikut penulis melakukan analisis terhadap topologi dan konfigurasi jaringan VPN *Site to Site* yang ada pada PT. Pertamina Ubeb Adera Pengabuan dan PT. Pertamina EP Prabumulih untuk mengetahui apa saja yang dibutuhkan dalam proses penerapan IP *Security* di jaringan tersebut.
2. Pengamatan, merupakan kegiatan saat melakukan percobaan untuk melihat proses kerja VPN *site to site* yang di gunakan di PT tersebut sehingga penulis mendapatkan sebuah hipotesis.
3. *Hipotesis* awal, dalam proses ini penulis mendapatkan hasil sementara sehingga penulis dapat melihat kekurangan dan kelebihan kemanan/ scurity yang ada pada jaringan VPN tersebut.
4. *Verifikasi*, dalam tahapan ini untuk membuktikan kebenaran dari dugaan awal, penulis menggunakan *software wireshak* untuk memonitoring proses terjadinya komunikasi dan sharing data sehingga penulis dapat melihat sejauh mana tingkat keamanan yang ada sebelum

dilakukannya konfigurasi IP*Security* pada jaringan tersebut.

5. *Evaluasi*, Merupakan proses konfigurasi IPSecurity dan melakukan kembali monitoring menggunakan *software wireshak* untuk melihat hasil konfigurasi IPSecurity apakah hasil konfigurasinya dapat berjalan dengan baik pada jaringan VPN tersebut.

2.2 Metode Pengumpulan Data

Metode pengumpulan data yang digunakan dalam melakukan penelitian ini :

1. Studi Kepustakaan (*Literature*)
   Yaitu data yang diperoleh melalui *literature*, melakukan studi kepustakaan dalam mencari bahan dari *internet* dan membaca buku yang sesuai dengan objek yang akan diteliti ;
2. Penelitian (*Observation*)
   Metode pengumpulan data dengan cara melakukan penelitian secara langsung pada objek penelitian yaitu pada PT. Pertamina Ubep Adera Pengabuan dimana

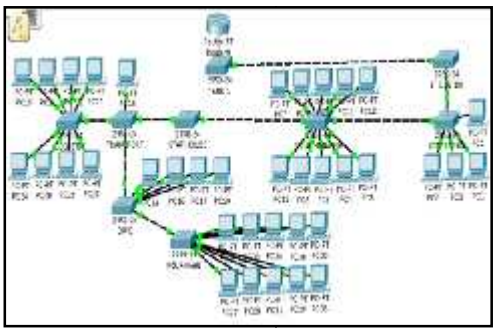
2.3 Prinsip Kerja Simulasi

Pada penelitian ini telah dirancang sebuah topologi menggunakan router mikrotik RB750 yang telah dilakukan konfigurasi VPN (*Virtual Private Network*) dan IPSec *Tunnel* pada router tersebut, dan dua unit laptop satu sebagai sumber, satu lagi sebagai tujuan dalam proses pengiriman data. Saat proses pengiriman data tersebut sedang berlangsung secara bersamaan penulis melakukan monitoring lalulintas data untuk melihat hasil penerapan IP*Sec* pada VPN *Tunnel* menggunakan *software wireshak*.

2.4 Topologi Jaringan

Adapun bentuk jaringan atau topologi jaringan pada PT. Pertamina Ubep Adera pengabuan ini yaitu topologi *star* yang menghubungkan setiap switch yang berjumlah 9 buah switch yang terhubung secara *peer to peer* sehingga sistem kerjanya pun untuk setiap *stafnya* saling terhubung satu sama lain dengan demikian secara tidak langsung dapat mengakibatkan sedikit pemborosan *bandwith* saat melakukan pengiriman data untuk alamat tertentu yang secara otomatis menyebar kepada alamat-alamat *host* yang lainnya. Adapun jumlah Komputer yang digunakan dalam setiap aktivitas pekerjaan pada PT tersebut yaitu

berjumlah 37 *Unit* Komputer dengan *Spesifikasi* sebagai berikut :



Gambar 3.1 Topologi PT. Pertamina Ubep Adera Pengabuan

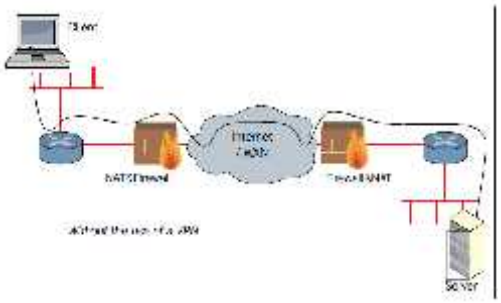
2.5 Parameter Kinerja VPN

2.5.1 *VPN (Virtual Private Network)*

Put simply, a VPN allows an administrator to create a "local" network between multiple computers on varying network segments. In some instances, those machines can be on the same LAN, they can be distant from each other across the vast Internet, or they can even be connected across a multitude of connection media such as wireless uplinks, satellite, dial-up-networking, and so on. The P in VPN comes from the added protection to make that virtual network private. Network traffic that is flowing over a VPN is often referred to as inside the (VPN) tunnel, compared to all the other traffic that is outside the tunnel.

In the following figure, network traffic is shown as it traditionally traverses across multiple network segments and the general Internet. Here, this traffic is relatively open to inspection and analysis. Though protected protocols such as HTTPS and SSH are less vulnerable, they are still identifiable; if an attacker is snooping network traffic, they can still see what type of connection is made from which computer to which server.

When a VPN is used, the traffic inside the tunnel is no longer identifiable.



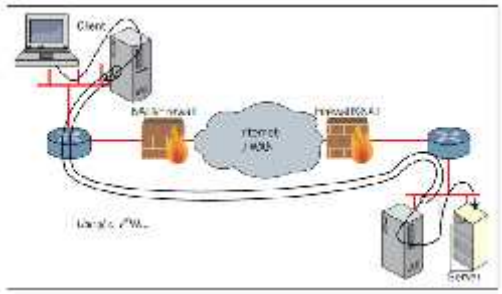
Gambar 1. VPN *Client Server*

The traffic within a VPN can be anything you would send over a local or wide-area network: web traffic, e-mail, text, graphics, and so on. Examples of some applications include the following:

1. *Automated Teller Machines: ATMs may use a VPN to connect more securely to banking systems.*
2. *Open / Free Wi-Fi: With the proliferation of free or open wireless networks, everyday users can utilize a VPN to protect the entirety of their Internet browsing.*

3. *Corporate networks: Corporations and other organizations may use a VPN to connect multiple office locations or even entire data centers.*
4. *GeoIP / Location-based services: Some websites serve data based on geographic location by using GeoIP databases and other records. A VPN can allow you to "bounce" through another machine in a location closer to the content you really want. Internet video services such as Hulu, YouTube, and Netflix are common examples of this.*
5. *Bypassing censorship / Political freedom: Some regimes, such as North Korea or China, have extraordinarily restrictive censorship rules. The "Great Firewall of China" is one extreme example. The lockdowns of Internet access during political uprisings such as the "Arab Spring" attempt to contain and control reports outside the conflict. VPNs can aid in getting outside those restrictive rules to the greater Internet.*

Here is an example of the traffic within a VPN. While the VPN itself is routed across the Internet like in the preceding figure, devices along the network path only see VPN traffic; those devices are completely unaware of what is being transmitted inside the private tunnel. Protected protocols, such as HTTPS and SSH, will still be protected inside the tunnel from other VPN users, but will be additionally unidentifiable from outside the tunnel. A VPN not only encrypts the traffic within, it hides and protects individual data streams from those outside the tunnel.



Gambar 2. *Tunnel* VPN

It should be noted that the preceding figure shows both the strengths and one of the greatest threats of VPN technologies. The VPN tunnel is dug through routers and firewalls on both sides. Thus, all the network traffic that is flowing via the VPN tunnel is bypassing the regular network defenses, unless special measures are taken to police the VPN traffic. Most VPN implementations utilize some form of encryption and, additionally, authentication. The encryption of the VPN ensures that other parties that

may be monitoring traffic between systems cannot decode and further analyze otherwise sensitive data. Authentication has two components, each in a different context. First, there is user or system authentication that ensures those connecting to the service are authorized. This type of authentication may be in the form of per-user certificates, or a username/password combination. Further, rules specific to a given user can be negotiated such as specific routes, firewall rules, or other scripts and utilities. Typically, these are unique to a single instance, though even that can be configurable (when OpenVPN is used, see --duplicate-cn). The second component of authentication is added protection to the communication stream. In this case, a method of signing each packet sent is established. Each system verifies the VPN packets it receives are properly signed before decrypting the payload. By authenticating packets that are already encrypted, a system can save processing time by not even decrypting packets that do not meet the authentication rules. In the end, this prevents a very real potential Denial of Service (DoS) attack, as well as thwarting Man in the Middle (MITM) attacks, assuming the signing keys are kept secure!

2.5.2. Types of VPNs

Types of VPNs There are many VPN products available on the market, both commercial and open source. Almost all of these VPN products can be separated into the following four categories:

1. *PPTP-protocol based VPNs*

   PPTP One of the oldest VPN protocols is the Point-to-Point Tunneling Protocol (PPTP) developed by Microsoft and Ascend in 1999. The PPTP client has been included in Windows ever since 1995 and is still included in most operating systems. Nowadays, the PPTP protocol is considered fundamentally insecure, as the strength of the security of the connection is directly related to the strength of the authentication mechanism chosen (for example, the password). Thus, an insecure password leads to an insecure VPN connection. Most PPTP setups use the MS-CHAPv2 protocol for encrypting passwords, and it is this protocol which is fundamentally broken. The security of the PPTP

protocol, including the Microsoft MS-CHAPv2 extensions. It is also possible to use X.509 certificates for securing a PPTP connection, which does lead to a fairly secure connection. However, not all PPTP clients support EAP-TLS, which is needed to allow the use of X.509 certificates. PPTP uses two channels, a control channel for setting up the connection and another channel for data transport. The control channel is initiated over TCP port 1723. The data channel uses the General Routing Encapsulation (GRE) protocol, which is IP protocol 47. For comparison, "regular" TCP/IP traffic is done using IP protocol 6 (TCP) and 17 (UDP). PPTP clients are available on almost all operating systems, ranging from Windows to Linux and Unix derivatives to iOS and Android devices.

2. *IPSec-protocol based VPNs*

   The IPSec standard is the official IEEE/IETF standard for IP security. IPSec is also built into the IPv6 standard. IPSec operates at layer 2 and 3 of the OSI model of the network stack. It introduces the concept of security policies, which makes it extremely flexible and powerful, but also notoriously hard to configure and troubleshoot. Security policies allow an administrator to encrypt traffic between two endpoints based on many parameters, such as the source and destination IP address, as well as the source and destination TCP or UDP ports. IPSec can be configured to use pre-shared keys or X.509 certificates to secure the VPN connection. Additionally, it uses either X.509 certificates, one-time passwords, or username/password protocols to authenticate the VPN connection. There are two modes of operation in IPSec: tunneling mode and transport mode. Transport mode is used most often in combination with the Level 2 Tunneling Protocol (L2TP). This L2TP protocol performs the user authentication as described in the preceding section. The IPSec clients built into most operating systems usually perform IPSec+L2TP, although it is also possible to set up an IPSec-only connection. The IPSec VPN client built into Microsoft Windows uses IPSec+L2TP by default, but it is possible to disable or bypass it. However, this involves cryptic

commands and security policy changes. Like PPTP, IPSec also uses two channels: a control channel for setting up the connection and one for data transport. The control channel is initiated over UDP port 500 or 4500. The data channel uses the Encapsulated Security Payload (ESP) protocol, which is IP protocol 50. For comparison, "regular" TCP/IP traffic is done using IP protocol 6 (TCP) and 17 (UDP). The integrity of IPSec packets is ensured using Hash-based Message Authentication Code (HMAC), which is the same method that OpenVPN uses. One of the main disadvantages of IPSec is that many vendors have implemented extensions to the standard, which makes it hard (if not impossible) to connect two IPSec endpoints from different vendors. IPSec software is included in almost all operating systems, as well as firewall, router, and switch firmware.

3. *SSL-based VPNs*

   SSL-based VPNs The most commonly used VPNs nowadays are SSL-based VPNs, which are based on the SSL/TLS protocol. SSL-based VPNs are often called client-less VPNs or webbased VPNs, although there are some vendors that provide separate client software, such as Cisco AnyConnect and Microsoft SSTP. Most SSL-based VPNs use the same network protocol as is used for secure website (HTTPS), while OpenVPN uses a custom format for encrypting and signing data traffic. This is the main reason why OpenVPN is listed as a separate VPN category. There is no well-defined standard for SSL-based VPNs, but most use the SSL/TLS protocol to set up and secure the connection. The connection is secured in most cases by using X.509 certificates, with one-time password or username/password protocols for authenticating the connection. SSL-based VPNs are very similar to the connections used to secure websites (HTTPS) and the same protocol and channel (TCP and port 443) is often used.

4. *OpenVPN*

   OpenVPN is often called an SSL-based VPN, as it uses the SSL/TLS protocol to secure the connection. However, OpenVPN also uses HMAC in combination with a digest (or hashing) algorithm for

ensuring the integrity of the packets delivered. It can be configured to use pre-shared keys as well as X.509 certificates. These features are not typically offered by other SSL-based VPNs. Furthermore, OpenVPN uses a virtual network adapter (a tun or tap device) as an interface between the user-level OpenVPN software and the operating system. In general, any operating system that has support for a tun/tap device can run OpenVPN. This currently includes Linux, Free/Open/NetBSD, Solaris, AIX, Windows, and Mac OS, as well as iOS/Android devices. For all these platforms, client software needs to be installed, which sets OpenVPN apart from client-less or web-based VPNs. The OpenVPN protocol is not defined in an RFC standard, but the protocol is publicly available because OpenVPN is a piece of open source software. The fact that it is open source actually makes OpenVPN more secure than closed-source VPNs, as the code is continually inspected by different people. Also, there is very little chance of secret backdoors being built into OpenVPN. OpenVPN has the notion of a control channel and a data channel, both of which are encrypted and secured differently. However, all traffic passes over a single UDP or TCP connection. The control channel is encrypted and secured using SSL/TLS, the data channel is encrypted using a custom encryption protocol. The default protocol and port for OpenVPN is UDP and port 1194. Before IANA granted OpenVPN an official port assignment, older clients (2.0-beta16 and older) defaulted to port 5000.[4]

2.5.3. Komponen Keamanan VPN

Untuk keamanan VPN terdiri dari 4 komponen, yakni: *Autentikasi User, Kendali Akses, Enkripsi*, dan *Public Key Infrastructure* (PKI).

1. *Autentikasi User, Autentikasi* adalah proses dalam rangka *validasi user* pada saat memasuki sistem. nama dan *password* dari pengguna diperiksa melalui proses yang memeriksa langsung daftar para *user,* yang diberikan hak untuk memasuki sistem.
2. Kendali akses (*access control*), memliki kemampuan untuk memberikan akses (seperti hak terhadap *server, direktori*, dan

file) yang berbeda kepada setiap *user* atau *group* tertentu dalam jaringan komputer lokal (*private network*) atau *remote access*.

3. *Enkripsi*, merupakan proses untuk mengubah, menyandikan atau mengkodekan sebuah pesan (informasi), sehingga tidak dapat dilihat atau dibaca tanpa menggunakan kunci pembuka.
4. *Public Key Infrastructure* (PKI) adalah teknologi lanjutan, yang pada akhirnya menjadi standar IETF (*Internet Engineering Task Force*). Sasaran PKI adalah menyediakan dasar untuk sistem yang akan mendukung berbagai layanan keamanan, sepeti *integritas* data, kerahasiaan data, dan *autentikasi user*.
5. *Tunneling* adalah dasar dari VPN untuk membuat suatu jaringan *private* melalui jaringan internet yang merupakan proses pengambilan semua paket data, dan mengenkapsulasinya dengan paket lain sebelum mengirimnya melalui sebuah jaringan.[5]

2.5.4. Kriptografi pada VPN

VPN menggunakan dua bentuk kriptografi, yaitu kriptografi kunci simetris dan kriptografi kunci *publik*. Kriptografi kunci simetris biasanya lebih *efisien* dan membutuhkan biaya pemrosesan yang lebih murah bila dibandingkan dengan kriptografi kunci *publik*. Oleh karena itu, kriptografi kunci *simetri* lebih sering digunakan untuk mengenkripsi bagian terpenting dari data yang akan dikirimkan melalui VPN. Algoritma yang umumnya digunakan untuk implementasi kriptografi kunci simetris meliputi *Digital Encryption Standard* (DES), *Triple* DES (3DES), *Advanced Encryption Standard* (AES), *Blowfish*, RC4, *International Data Encryption Algorithm* (IDEA), dan *Hash Message Authentication Code* (HMAC) *versi Message Digest* 5 (MD5) dan *Secure Hash Algorithm* (SHA-1). *Algoritma* yang umumnya digunakan untuk algoritma kunci publik adalah meliputi RSA, *Digital Signature Algorithm* (DSA), dan *Elliptic Curve* DSA (EDBSA) (Frankel, 2005). *Arsitektur Protokol* IPSec, IPSec protokol yang dikombinasikan dengan algoritma *default*-nya didesain untuk menyediakan keamanan lalu lintas internet yang baik. Bagaimanapun juga keamanan yang diberikan oleh protokol ini sebenarnya bergantung pada kualitas dari implementasi. Perkembangan arsitektur IPsec

mengacu pada pokok persoalan yang terdapat pada RFC.[6]

3. HASIL DAN PEMBAHASAN

A. *Verifikasi dan Evaluasi*

Merupakan kegiatan yang dilakukan sebagai pembuktian dari hasil percobaan awal yang telah dilakukan sebelumnya. Dalam hal ini ada beberapa tahapan yang dilakukan penulis sebagai berikut:

1. Langkah pertama, penulis menggunakan terminal dari *client* pada setiap router dan mengetikkan perintah *Tracert* ditambah IP *Address* sebagai alamat tujuan guna melihat proses aliran data serta pembuktian bahwa konfigurasi IPsec yang telah dilakukan sebelumnya berjalan dengan baik. Berikut IP *Address* yang digunakan penulis pada penelitian ini dapat terlihat pada tabel dibawah ini :

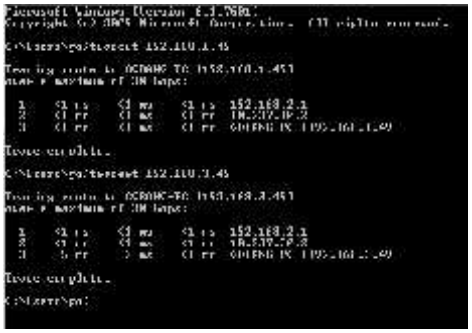
Tabel 2. IP *Address*

	Lokasi	*Public*	*Local*
1	Pertamina Ubeb Adera	10.237.10.2/24	192.168.1.1/24
2	Pertamina EP Prabumulih	10.237.20.2/24	192.168.2.1/24

Proses *tracert* dilakukan dari *site* jaringan *field* Adera ke *site* jaringan *field* Prabumulih;

Gambar 3. Hasil *proses Tracert*

Proses *tracert* dari *site* jaringan *field* Prabumulih ke *site* jaringan *field* Adira;



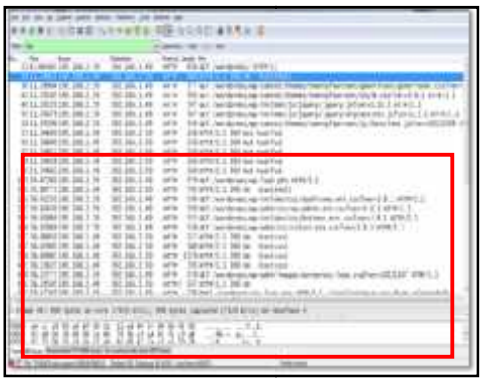
Gambar 4. Hasil Proses *Tracert*

Dari hasil diatas maka dapat dilihat route paket yang dikirim melalui router Ubeb Adera menujuh router Prabumulih begitupun sebaliknya.

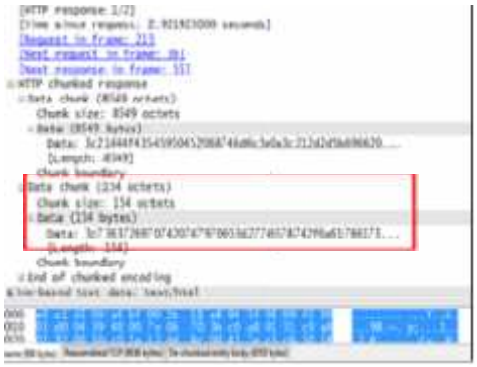
2. Berikut hasil *testing* konfigurasi IPsec dalam jaringan VPN *Site to Site* Mikrotik Router untuk melihat apakah proses komunikasih data antar *site* telah terenkripsi dengan baik sesuai dengan fungsi kerja IPsec sebagai keamanan dalam proses komunikasih data. Adapun kegiatan yang dilakukan penulis instal *web server* pada *client site router field* Ubeb Adira Pengabuan yang akan dijadikan *server wordpress* kemudian *setting* IP *address* 192.168.1.49, *username* dediirawan dan *password* “123Dedi” kemudian jalankan *software wireshark* pada

client site field Prabumulih EP dan buka *browser* untuk mengakses *server wordpress* yang berada pada *site field* Ubeb Adira Pengabuan dengan memasukan *username* dan *password* yang di*setting* pada *server wordpress* sebelumnya. Berikut hasil yang didapat dari percobaan yang dilakukan dari proses diatas, adapun data yang didapat merupakan data yang telah terenkripsi oleh protokol IPsec.

Gambar 5. *Proses Access Web Server Wordpress*



Gambar 6. Hasil *Enkripsi Ipsec*



Gambar 7. Hasil *Enkripsi IPSec*

Dari hasil *testing* diatas maka dapat dilihat hasil *Enkripsi Protocol IPsec* pada gambar 6. diatas merupakan *enkripsi* data saat mengakses *web server router field* adira dari *client site router field* prabumulih. Untuk gambar 7. merupakan hasil dari data *enkripsi* saat melakukan *remote router* dari *site* yang berbeda dengan menggunakan *software PuTTY* pada *SSH Protocol* terlihat data yang *terenkripsi* yaitu data *payload* merupakan sebuah data aktual yang dikirim melalui internet. Setiap unit ditranmisikan mencakup informasi *header* dan data aktual yang dikirim. *Header* mengidentifikasi sumber ke tujuan.

4. KESIMPULAN

Dalam penelitian ini dapat bahwa dengan menerapkan IP *Security* pada VPN *Site to Site* di PT. Pertamina Ubeb Adera Pengabuan dan PT. Pertamina EP Prabumulih dapat disimpulkan bahwa IP *Security* dapat mengamankan proses komunikasi dan *sharing* data dalam proses pekerjaan di PT tersebut. menjadi solusi yang baik dalam mengamankan data dalam komunikasi jaringan jarak jauh.

DAFTAR RUJUKAN

[1] RMDikshie Fauzie, *Tinjauan Mekanisme dan Aplikasi IPSEC: Studi Kasus VPN*, 14th ed. Surabaya, 2010.

[2] A. A. S, A. Mulyana, and Iikmal, "Analisis Sistem Keamanan Jaringan VPN Berbasis IPSEC (IP *Security*) dan GRE (*Generic Routing Encapsulation*) *Security System Analisys of* IPSEC (IP *Security*) *and* GRE (*Generic Routing Encapsulation*) *Based* VPN," 2011.

[3] M. S. Prof.Dr. Suryana, *Metodologi Penelitian*. Bandung: Universitas Pendidikan Indonesia, 2010.

[4] E. F. Crist and J. J. Keijser, *Mastering OpenVPN*. Birmingham: *Packt Publishing*, 2015.

[5] S. Trihadi, F. Budianto, and W. Arifin, "Perancangan V*irtual Private Network Dengan Server Linux* Pada Pt Dharma Guna Sakti," *CommIT*, vol. 2, no. 1, 2008.

[6] Y. Hendriana, "Evaluasi Implementasi Keamanan Jaringan *Virtual Private Network* VPN (Studi Kasus Pada Cv. Pangestu Jaya)," *J. Teknol. Vol. 5 Nomor 2*, vol. 5 No 2, pp. 132–142, 2012.

[7] I. Nugroho, B. Widada, and Kustanto, "Perbandingan Performansi Jaringan *Virtual Private Network Metode Point To Point Tunneling Protocol* (PPTP) Dengan *Metode Internet Protocol Security*," *TIKomSiN*, pp. 1–9, 2015.