ISSN 2087 2429

Implementasi Remote Desktop Melalui VPN Berbasis IPSec pada Smartphone dengan Menggunakan Vyatta OS

Kiki Agnia Maryam Larasati
Prodi Teknik Komputer
Universitas Telkom
Bandung, Indonesia
qq.agnia@gmail.com

Eddy Prasetyo Nugroho
Prodi Teknik Komputer
Universitas Telkom
Bandung, Indonesia
eddy.pn@gmail.com

Moch. Fahru Rizal
Prodi Teknik Komputer
Universitas Telkom
Bandung, Indonesia
mfrizal@tass.telkomuniversity.ac.id

Abstrak— Akses internet yang semakin baik membuat variasi aktivitas semakin beragam, termasuk untuk mengakses PC di lokasi kerja dengan *smarthone.* Salah satu kendala dari remote akses ini adalah faktor keamanan. Penelitian ini bertujuan untuk menyediakan jalur komunikasi *private* untuk terhubung dengan LAN perusahaan guna monitoring dan mengakses data perusahaan secara *ubiquituous*. Prototipe jaringan dibangun dengan aplikasi remote desktop melalui VPN (Virtual Private Network) berbasis IPSec. Pengujian yang dilakukan menghasilkan fitur remote desktop, akses data dan *resource monitoring* berhasil dijalankan melalui *smartphone* dengan baik tanpa *lag*. Pengujian pada VPN berbasis IPSec melalui Wireshark menghasilkan paket ESP (*Encapsulating Security Payload*), yang berarti konten yang dikirimkan sudah dienkripsi.

Kata Kunci— VPN, Remote Desktop, Resource Monitoring, IPSec, ESP (Encapsulating Security Payload)

Abstract— Internet access makes increasingly varied activities, including to access the PC off-site with smartphone. One of the constraints of remote access is security.This research aims to provide a private communication line connection to the company's local network to monitor and accessing corporate data ubiquitously. The prototype network is built with a remote desktop application through VPN (Virtual Private Network)-based IPSec. Tests were conducted by generating remote desktop, data and resource access monitoring with successful result which executed without lag. Tests on IPSec-based VPN via Wireshark produces an ESP (Encapsulating Security Payload) packet, which means the content is already encrypted.

Keywords— VPN, Remote Desktop, Resource Monitoring, IPSec, ESP (Encapsulating Security Payload)

I. PENDAHULUAN

Pengguna aktif dengan mobilitas tinggi membutuhkan jalur komunikasi privat untuk memonitoring, mengakses data maupun informasi penting di jaringan lokal perusahaan dimanapun mereka berada.

Remote Desktop melalui Teknologi VPN (*Virtual Private Network*) berbasis IPSec adalah solusi yang tepat untuk mengatasi permasalahan tersebut. VPN adalah sebuah koneksi virtual yang bersifat *private* di atas jaringan publik. IPSec ditambahkan untuk mendukung dan menyediakan keamanan dalam transimisi data.

Penelitian ini membahas mengenai Remote User VPN dengan Vyatta OS dan pengamanan data saat proses transmisi. Penggunaan OS Android dibahas dalam skema monitoring dan akses data.

II. DASAR TEORI

A. Virtual Network Computing (VNC)

Sistem Virtual Networking Computing (VNC) adalah *thin-client system*. VNC mengurangi jumlah proses yang ada pada terminal user. VNC viewer sangat ringan karena mereka menyimpan *unrecoverable state* pada *endpoint*. Kontras dengan sistem seperti X Windows, dan memungkinkan diskoneksi secara sembarang dan rekoneksi dari *client* tanpa efek dari sesi di server [1].

Arsitektur protokol VNC digunakan untuk komunikasi dengan model client - server. Dalam lingkup jaringan, aktivitas dirancang untuk memungkinkan terjadi secara *remote* antar perangkat. Meskipun sebagian besar arsitektur perangkat memiliki tujuan kontrol PC dari jarak jauh, sedikit inisiatif yang bertujuan untuk mengontrol melalui perangkat *mobile* [2].

B. Virtual Private Network (VPN)

VPN adalah sebuah jaringan virtual yang dapat menyediakan mekanisme komunikasi aman untuk data dan informasi IP yang ditransmisikan antar jaringan. VPN dapat dibangun dalam jaringan tunggal untuk melindungi komunikasi yang sensitif dari pihak lain di jaringan yang sama [3].

Protokol yang biasa dan sering digunakan dalam implementasi VPN (Virtual Private Network), yaitu:

- Ipsec (Ip Security Protocol)
- Layer-2 Forwarding
- Layer-2 Tunneling Protocol (L2TP)
- Point to Point Tunneling Protocol

C. *Internet Protocol Security*

IPSec menggunakan dua protokol untuk menyediakan layanan keamanan lalulintas yaitu Authentication Header (AH) and Encapsulating Security Payload (ESP). Implementasi IPSec harus mendukung ESP dan juga AH.

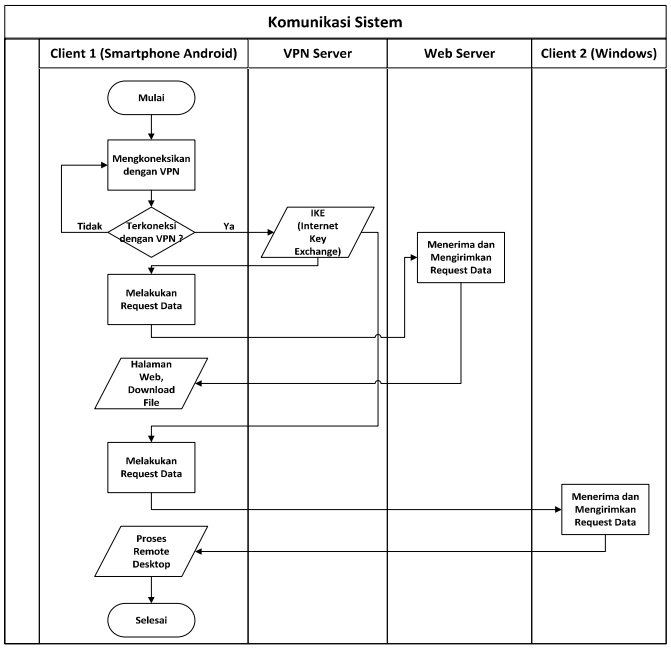
Protokol-protokol ini dapat diterapkan secara sendiri-sendiri atau dikombinasikan antara keduanya untuk menyediakan layanan keamanan yang diinginkan dalam IPv4 dan IPv6. Masing-masing protokol mendukung dua mode penggunaan: mode transport dan mode x. Dalam mode transport protokol menyediakan proteksi terutama untuk layer protokol berikutnya. Sedangkan dalam mode tunnel protokol diterapkan untuk meneruskan paket IP [3].

IPSec via VPN tidak dapat menangani user dalam jumlah signifikan. Performasi system secara gradual menurun ketika trafik dibebani lebih dari satu user. Demikian pula faktor *delay* transmisi dan enkripsi (AES) [4].

III. ANALISIS DAN PERANCANGAN

A. *Flow Map* Sistem

Gambar 1 merupakan flow chart sistem yang dibuat.



Gambar 1. Flow Map Sistem

B. *Konfigurasi IP*

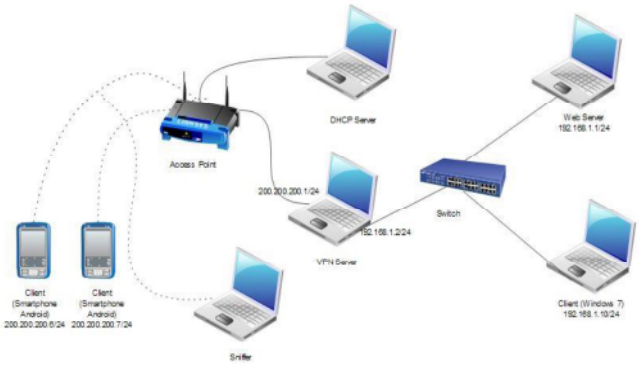
Tabel 1 merupakan konfigurasi IP yang digunakan;

TABEL 1 KEBUTUHAN ANTARMUKA IP

Router	Net ID	Eth0	Eth1	Note
Vyatta Router OS	192.168.1.0/ 24	-	192.168.1.2/ 24	Workstation (IP Private)
	200.200.200. 0/24	200.200.200.1/ 24	-	Internet (IP Publik)

C. *Arsitektur Sistem*

Gambar 2 adalah arsitektur dan rancangan sistem yang dibangun.



Gambar 2. Arsitektur Sistem

IV. IMPLEMENTASI SISTEM

Berikut langkah-langkah implementasi sistem :

A. *Konfigurasi Interfaces*

Setting IP Address 200.200.200.1/24 pada *interface* eth1. Interface ini yang berhubungan dengan internet. Setting IP Address 192.168.1.2/24 pada *interface* eth2. Interface ini yang akan menjadi *interface* untuk jaringan lokal.

B. *Konfigurasi IPSec Interfaces*

Menjadikan *interface* ethernet eth1 sebagai *interface* ipsec.

C. *Konfigurasi Outside Address*

Mengatur IP Address keluar pada interface *vpn remote access*. Client akan terkoneksi dengan IP Address 200.200.200.1 pada saat mengakses VPN.

D. *Konfigurasi Outside Nexthop*

Mengatur IP Address untuk *nexthop* pada *vpn remote access*.

E. *Konfigurasi Client IP Pool*

Konfigurasi untuk menentukan range IP Address remote pada jaringan lokal. Range IP Address dimulai dari 192.168.1.5 sampai 192.168.1.15. Client yang terkoneksi dengan VPN akan mendapatkan IP Address tersebut secara otomatis, sehingga pada *client* akan terdapat dua IP yaitu IP yang digunakan untuk berhubungan dengan internet, dan IP yang didapat dari hasil tunneling ke VPN Server.

F. *Konfigurasi Username dan Password*

Menambahkan *username* dan *password* untuk *client* agar bisa mengakses VPN Server.

G. *Konfigurasi Mode Autentikasi IPSec*

Menentukan mode otentikasi IPSec yaitu *Pre-Shared-Secret* (*Pre-shared key*). Untuk mode otentikasi ini terdapat manajemen pertukaran kunci antara VPN Server dengan Client.

H. *Konfigurasi Kunci Pre-shared key IPSec*

Menentukan Pre-shared key.

I. *Konfigurasi NAT*

Konfigurasi NAT agar *client* yang mengakses VPN Server dapat mengakses internet. Network yang diizinkan yaitu 200.200.200.0/24 dan 192.168.1.0/24.

J. *Konfigurasi DNS Forwarding*

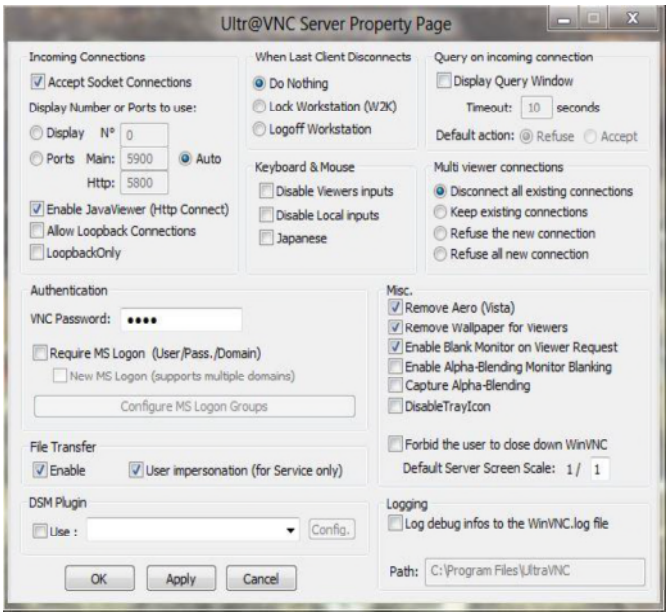
Jika terdapat memiliki DNS server di tempat lain, maka dapat dilakukan forwarding ke IP DNS server tersebut. DNS berada dalam jaringan lokal dengan IP Address 192.168.1.1.

K. *Konfigurasi Web Caching*

Konfigurasi jika web server yang ada akan difungsikan sebagai web caching.

L. *Instalasi Aplikasi pada Client (Windows)*

Pada *client* yaitu PC yang di*remote* diharuskan menginstal UltraVNC. Hal ini bertujuan untuk mengaktifkan fitur remote desktop. Gambar 3 menunjukkan setting UltraVNC Server pada *client* (windows):

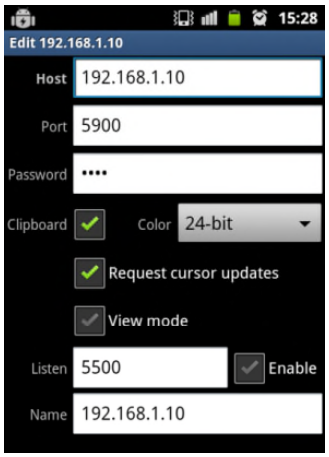


Gambar 3. Setting UltraVNC Server

IP Address client adalah 192.168.1.10 dengan subnet mask 255.255.255.0. Default Gateway 192.168.1.2 adalah gateway yang terhubung dengan VPN Server.

M. *Instalasi RemoteVNC (Android)*

Pada *client* (Smartphone Android) dilakukan instalasi RemoteVNC untuk melakukan koneksi ke PC yang diremote. Langkah-langkah instalasi RemoteVNC ditunjukkan pada Gambar 4.



Gambar 4. Setting IP Address RemoteVNC

IP Address pada host adalah IP Address PC *client* yang akan di remote. Port 5900 disamakan dengan port pada *setting* UltraVNC Server di PC *client* yang diremote. Password disamakan dengan setting password pada UltraVNC Server di PC client yang diremote.

V. PENGUJIAN SISTEM

A. *Pengujian Status IPSec*

Interface ini menunjukan status tunnel ipsec yang sedang aktif ketika kedua client (Smartphone Android) terkoneksi dengan VPN Server. Pengujian dapat dilakukan dengan perintah: "`show vpn ipsec ipsec status`". Jika terdapat respon sistem berupa PID IPSec maka IPSec sudah aktif.

B. *Pengujian Status Remote Access*

Interface ini menunjukkan status sesi *remote access* yang sedang aktif. Sesi remote access aktif ketika *client* terkoneksi dengan VPN Server. Parameter yang diukur: Status aktif remote access, Username *client* yang terkoneksi dan Remote IP client. Berikut capture sesi remote access:

```
vyatta@vyatta:~$ show vpn remote-access
Active remote access VPN sessions :

User     Time        Proto  Iface    Remote IP    TX
pkt/byte   RX pkt/byte
-------- ---------  -----  -----    ----------- ---
--- -----  ------ ----
kikosshi 00h01m56s  L2TP   l2tp1   192.168.1.6     91
24.7K    107    6.3K
manager   00h29m22s   L2TP    l2tp0    192.168.1.5
10.4K 12.1M   6.1K 330.3K
```

C. *Pengujian IKE Secrets*

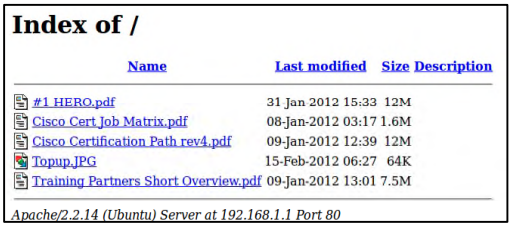
Tujuan pengujian untuk menunjukan IKE (Internet Key Exchange) yang telah terkonfigurasi yaitu *pre-shared key*. Berikut *capture* IKE:

```
vyatta@vyatta# show vpn ike secrets
Local            Peer       Secret
--------         -------    -------
200.200.200.1    %any       "l4r4s4t1"
```

Dapat disimpulkan bahwa IKE (pre-shared key) telah terkonfigurasi pada interface ipsec yaitu "l4r4s4t1".

D. *Pengujian Akses Data*

Client (Smartphone Android) yang terkoneksi dengan VPN Server dapat mengakses data pada web server yang tersedia dalam jaringan lokal. Hasil pengujian ini dapat dilihat pada Gambar 5.

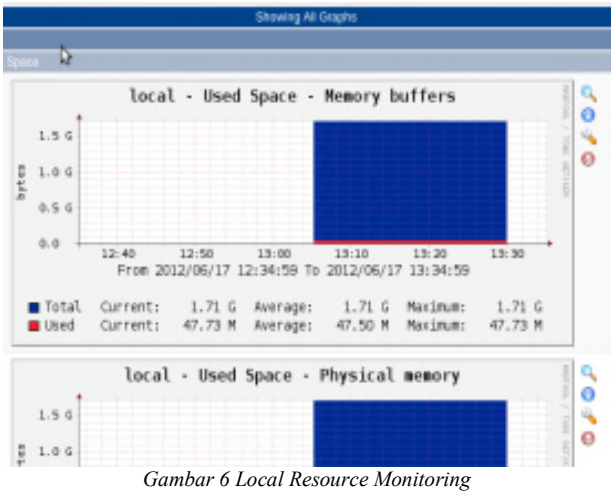


Gambar 5. Uji Akses Data

E. *Pengujian Monitoring Resource dan Trafik*

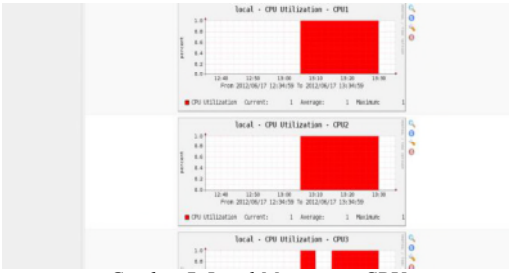
Client (*Smartphone* Android) yang terkoneksi dengan VPN Server dapat melakukan *resource monitoring* dan trafik pada PC yang di-*remote* dalam jaringan lokal. Langkah-langkah pengujian sebagai berikut;

1. Client terkoneksi dengan VPN Server
2. Mengakses 192.168.1.1/cacti melalui browser
3. Login dengan username dan password yang tersedia :
   a. username : guest
      password : guest
      (hanya dapat melihat grafik penggunaan resource dan trafik)
   b. username : admin
      password : admin
      (hak akses administrator : menambah, merubah, modifikasi, maintenance)



Gambar 6 Local Resource Monitoring

Gambar 6 merupakan grafik penggunaan *resource memory* pada web server.



Gambar 7. Local Monitoring CPU

Gambar 7 adalah grafik penggunaan resource CPU pada web server.

Gambar 8. Monitoring Traffic Client

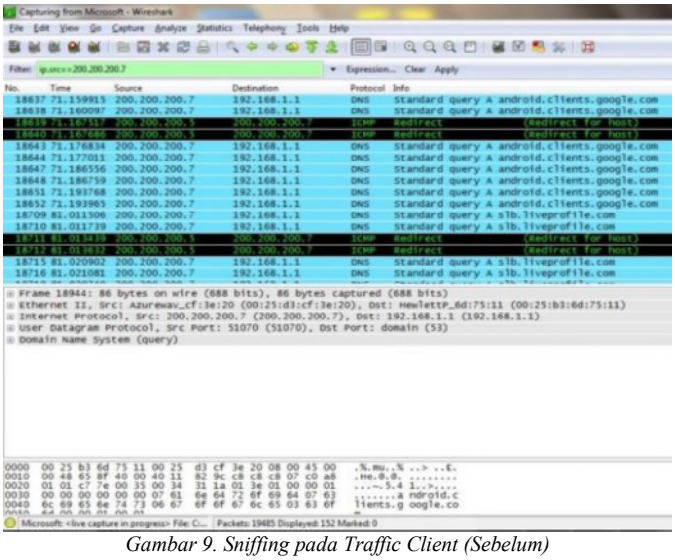
Gambar 8 adalah grafik penggunaan *resource* CPU dan penggunaan internet pada *client* (Windows).

F. *Pengujian Remote Desktop*

Client (*Smartphone* Android) yang terkoneksi dengan VPN Server dapat melakukan remote desktop pada PC yang diremote dalam jaringan lokal. Langkah-langkah : *Client* terkoneksi dengan VPN Server, gunakan Aplikasi RemoteVNC untuk melakukan *remote desktop*.

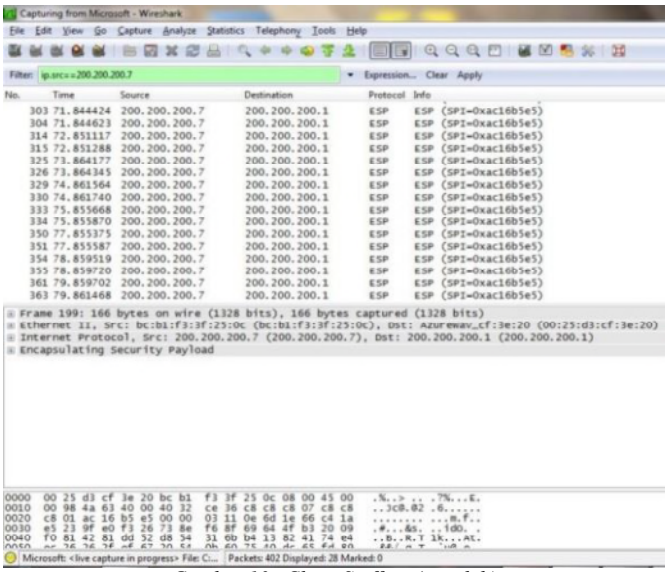
G. *Pengujian Protokol dengan Sniffing*

Gambar 9 dan Gambar 10 menampilkan hasil *sniffing* trafik jaringan antara *client* (Smartphone Android) dengan jaringan lokal menggunakan wireshark sebelum dan sesudah terkoneksi dengan VPN.



Gambar 9. Sniffing pada Traffic Client (Sebelum)

Client dengan IP Address 200.200.200.7 mengakses web server (*request*) dengan IP Address 192.168.1.1, terlihat protokol-protokol yang berjalan pada saat client me-request permintaan ke web server, diantaranya DNS dan ICMP. Dalam hal ini proses komunikasi antara client dan web server tidak aman dikarenakan protokol-protokol dan IP Address/host tujuan terbaca oleh sniffer.



Gambar 10. Client Sniffing (sesudah)

Client dengan IP Address 200.200.200.7 mengakses web server (request) dengan IP Address 192.168.1.1, akan tetapi IP Address tujuan pada hasil sniffing tidak menunjukkan IP Address web server yang diakses melainkan IP Address dari VPN Server yaitu 200.200.200.1. IP Address 200.200..200.1 merupakan interface keluar (interface IPSec) yang berhububungan dengan internet. Protokol-protokol yang berjalan antara client dan web server tidak dapat terlihat dikarenakan protokol-protokol tersebut telah dienkripsi dan dienkapsulasi oleh ESP (*Encapsulating Security Payload*).

VI. SIMPULAN

Teknologi VPN berbasis IPSec yang dibangun berhasil menyediakan layanan akses data, *resource monitoring* dan trafik, dan *remote desktop* yang aman. Protokol keamanan IPSec berfungsi dengan baik dalam mengenkripsi data yang dikirim, sehingga sniffer tidak dapat membaca trafik protokol-protokol yang berjalan antara *client* dan *web server* maupun pada saat proses *remote desktop*.

VIII. DAFTAR PUSTAKA

[1] T. Richardson, Q. Stafford-fraser, K. R. Wood, and A. Hopper, "Virtual Network Computing," 1998.

[2] A. Jadhav, V. Oswal, S. Madane, H. Zope, and V. Hatmode, "Vnc Architecture Based Remote Desktop," vol. 1, no. 2, pp. 98–103, 2012.

[3] S. Frankel, K. Kent, R. Lewkowski, A. Orebaugh, R. W. Ritchey, and S. R. Sharma, "NIST SP 800-77: Guide to IPsec VPNs," *Nist*, vol. SP 800-77, p. 126, 2005.

[4] O. Adeyinka, "Analysis of IPsec VPNs performance in a multimedia environment," *Int. Conf. Intell. Environ.*, pp. 1–5, 2008.