Analisis Performansi Remote Access VPN Berbasis IPSec dan Berbasis SSL pada Jaringan IPv6

Alex Yuasta[1], Fazmah Arif Yulianto, S.T., M.T.[2], Gandeva Bayu Satrya, S.T., M.T.[3]
Program Studi S1 Teknik Informatika, Fakultas Informatika, Universitas Telkom, Bandung
alex.yuasta@gmail.com, faz@ittelkom.ac.id, gandeva.bayu.s@ittelkom.ac.id

Abstrak

Protokol keamanan Internet Protocol Security (IPSec) dan Secure Socket Layer (SSL) merupakan protokol keamanan yang paling banyak digunakan untuk meningkatkan keamanan VPN. Hal ini dikarenakan, kedua protokol mampu memenuhi kriteria dukungan keamanan dan mememiliki tingkat keamanan yang lebih baik dari protokol-protokol keamanan lainnya.

Selain tingkat keamanan, performansi protokol keamanan juga bisa diuji dengan parameter seperti throughput dan delay. Parameter ini akan memberikan gambaran Quality of Service (QoS) protokol keamanan dari segi performansi jaringan.

Skenario pengimplementasian VPN dengan IPSec dan VPN dengan SSL adalah VPN remote access. Jenis pengimplementasian remote access memungkinkan pengguna VPN yang mobile untuk terhubung ke private network. Pada private network akan menggunakan standar pengalamatan IPv6 karena sudah banyak Local Area Network (LAN) yang mampu menjalankan standar Ipv6.

Kata Kunci: ***IPSec, SSL, IPv6, VPN, Remote Access.***

Abstract

Internet Protocol Security (IPSec) and Secure Socket Layer (SSL) are the most deployed security protocol to improve VPN security. This because both protocol fulfill security criteria and have securing capability more than any other security protocol.

Beside securing capability, security protocol performance also can be tested with other parameters such as throughput dan delay. This parameters will show security protocol's Quality of Service (QoS) from network performance capability.

The IPSec VPN and SSL VPN implementing scenario is remote access. Remote access VPN allow mobile VPN user to connect to private network. On private network will use IPv6 standard because most of Local Area Network already support IPv6 standard.

Key words : ***IPSec, SSL, IPv6, VPN, Remote Access.***

1. Pendahuluan

Virtual Private Network (VPN) merupakan suatu teknologi membangun jaringan private dalam jaringan publik [7]. Teknologi tersebut mampu meningkatkan keamanan komunikasi pada jaringan publik, karena komunikasi tersebut seolah-olah berada pada sebuah jaringan private. Karena keunggulan tersebut, VPN telah banyak diimplementasikan pada jaringan internet. Internet saat ini masih menggunakan standar pengalamatan Internet Protocol version 4 (IPv4). Standar pengalamatan IPv4 akan digantikan dengan standar pengalamatan Internet Protocol version 6 (IPv6). Hal ini mengharuskan VPN yang merupakan suatu solusi keamanan pada jaringan IPv4 agar tetap bisa mengerjakan fungsinya pada jaringan IPv6.

Proses penggantian sistem pengalamatan ini tidak berlangsung serentak. Beberapa jaringan sudah mulai menggunakan standar pengalamatan IPv6, biasanya jaringan berstatus Local Area Network (LAN) . Salah satu penyebab beberapa jaringan masih menggunakan standar pengalamatan IPv4 seperti internet dikarenakan keterbatasan perangkat keras. Dimana perangkat keras yang digunakan sekarang masih banyak yang belum mendukung jaringan yang menggunakan sistem pengalamatan IPv6.

Standar pengalamatan IPv6 memiliki beberapa perbedaan dengan standar IPv4, misalnya pada panjangnya header dan payload. Perbedaan-perbedaan tersebut diperkirakan akan memberikan perbedaan kinerja antara VPN pada jaringan IPv4 dengan VPN pada jaringan IPv6.

Saat ini banyak kantor yang menerapkan metode work-at-home yaitu mengerjakan pekerjaan kantoran di rumah. Pegawai kantor yang bekerja di rumah tetap harus terhubung dengan jaringan internal kantor. Sehingga dibutuhkan sebuah VPN berjenis

remote access agar pegawai tersebut bisa terhubung ke jaringan internal kantor melalui Internet.

Ada beberapa jenis protokol yang biasa digunakan pada VPN seperti Internet Protocol Security (IPSec), Secure Socket Layer (SSL), Point-to-Point Tunnelling (PPTP), dan Layer 2 Tunneling Protocol (L2TP). Namun dilihat dari segi dukungan keamanan protokol IPSec dan SSL merupakan protokol yang paling banyak digunakan [1].

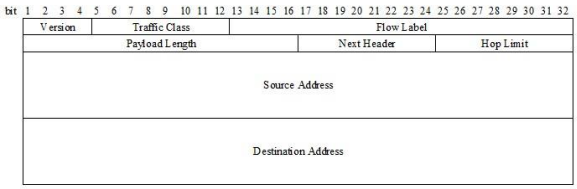
Karena telah mampu memenuhi kriteria dukungan keamanan [8], maka akan digunakan kriteria Quality of service (QoS) dalam menetukan mana protokol keamanan yang lebih baik. Dimana dalam menganalisa QoS, akan digunakan parameter throughput dan delay.

2. Dasar Teori

2.1. IPv6

Internet Engineering Task Force (IETF) telah mengembangkan standar pengalamatan baru yang dikenal dengan Internet Protocol version 6 (IPv6). IPv6 menggunakan 128 bit dalam memberikan suatu alamat IP [7]. IPv6 mampu mengalokasikan alamat IP sebanyak 2128 yaitu sekitar 3,4 x 1038. Jumlah alamat IP yang mampu dialokasikan oleh IPv6 jauh lebih banyak dibandingkan dengan jumlah yang mampu dialokasikan oleh IPv4. Sehingga akan lebih banyak pengguna yang akan bisa terhubung ke jaringan internet.

Paket IPv6 terdiri dari header dan payload. Header IPv6 memiliki panjang 320 bit atau 40 octet. Header IPv6 terdiri dari delapan field. Payload memiliki panjang 65.535 octet. Payload IPv6 terdiri dari Extension Headers dan Upper Layer Protocol



Data Unit [7].

Extension Header merupakan header-header yang mengikuti header IPv6, bersifat opsional dan berfungsi untuk memberikan perluasan fungsionalitas dari IP datagram. Panjang dari Extension Header bervariasi dan tidak memiliki ukuran maksimum agar nantinya bisa ditambah dengan extension yang dibutuhkan. IPv6 setidaknya memiliki enam Extension Header dengan urutan [6]:

1. Hop-by-Hop Option header
2. Destination Option header
3. Routing header
4. Fragment header
5. Authentication header
6. Encapsulating Security Payload header

Upper Layer Protocol Data Unit (PDU) memiliki panjang normal mencapai 65.535 octet. Dengan menggunakan tambahan opsi Jumbo Payload pada extension Hop-by-Hop option, PDU bisa memiliki panjang lebih dari 65.535 octet. PDU biasanya disusun dari header protokol upper-layer dan payload-nya.

2.2. VPN

Virtual Private Network (VPN) merupakan teknologi dalam jaringan komputer yang membangun suatu jaringan pribadi didalam jaringan publik agar pengguna jaringan pribadi bisa berkomunikasi dengan aman. Beberapa fungsi yang harus dimiliki oleh VPN agar mampu menyediakan jaringan yang aman adalah [9]:

1. Data confidentiality

Memproteksi informasi yang ada selama berkomunikasi dengan cara mengenkripsi informasi dari si pengirim sebelum dikirim melalui jaringan publik.

2. Data integrity

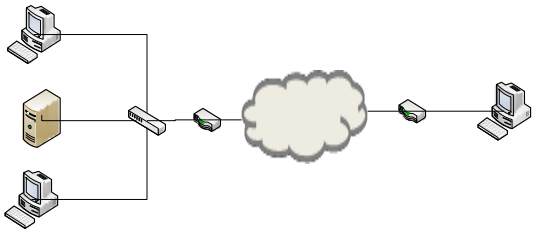
Informasi yang diterima oleh si penerima harus dapat dipastikan bahwa informasi tersebut bersifat utuh sebagaimana informasi tersebut dikirm oleh si pengirim.

3. Authentication

Memastikan pihak-pihak yang berkomunikasi adalah pihak-pihak otentik.

2.2.1 Jenis Implementasi VPN

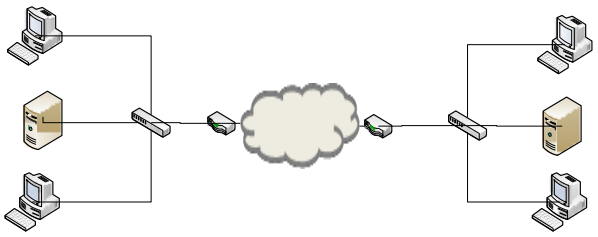
VPN diimplementasikan dalam dua jenis, yaitu: remote access dan site-to-site. VPN remote access memungkinkan suatu client untuk terhubung ke jaringan private dari remote location. VPN client dan VPN server akan melakukan otentikasi sebelum keduanya bisa terhubung.



Gambar 2.2 VPN Remote Access

VPN site-to-site memungkinkan terhubung ke jaringan private dari remote location, dimana remote location-nya juga sebuah jaringan private. VPN site-to-site seolah-olah membentuk jaringan

Wide Area Network (WAN) antar beberapa jaringan private. Masing-masing VPN server yang terhubung akan saling melakukan otentikasi. [7]



Gambar 2.3 VPN Site-to-site

2.3. IPSec

Internet Protocol Security (IPSec) merupakan suatu protokol keamanan yang berada pada layer internet. IPSec disusun dari protokol keamanan Authentication Header (AH) dan/atau Encapsulating Security Payload (ESP) [2].

2.2.2 Aunthentication Header (AH)

Protokol AH mendukung otentikasi host yang berkomunikasi dan integritas data. Protokol AH memiliki panjang sebesar 24 byte.

2.2.3 Encapsulating Security Payload

Protokol ESP mendukung confidentiality dan host authentication. ESP menengkripsi data yang berada diantara ESP Header dan ESP Auth.

2.4. SSL

Secure Socket Layer (SSL) merupakan protokol keamanan layer transpor [4]. Protokol SSL berada diantara connection-oriented network layer protocol dan application protocol layer. Untuk SSL versi 3 lebih dikenal dengan Transport Layer Security (TLS). SSL menggunakan konsep kriptografi kunci publik. Pihak yang berkomunikasi mengirimkan data yang telah disamarkan dengan teknologi kriptografi.

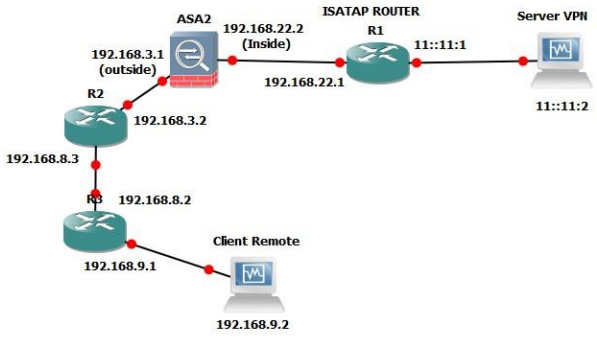
Protokol SSL disusun dari dua layer yaitu: protokol SSL Record Protocol dan SSL Handshake Sequence Protocol. SSL Record Protocol berada pada layer terbawah. SSL record Protocol digunakan untuk mengenkapsulasi protokol layer diatasnya. SSL Handshake Sequence Protocol memungkinkan pihak-pihak yang berkomunikasi untuk mengotentikasi satu sama lain dan menegosiasikan algoritma enkripsi dan kunci kriptografi sebelum protokol aplikasi mengririmkan atau menerima byte pertama dari data.[3]

3. Perancangan dan Implementasi Sistem

Pada tugas akhir ini akan mengimplementasikan topologi remote access VPN, topologi remote access dipilih karena topologi ini banyak digunakan oleh para karyawan yang yang bekerja secara mobile di luar perusahaan, sehingga tetap dapat mengakses data di perusahaannya dari manapun. Secara umum untuk implementasi simulasi ini semua router baik di sisi jaringan publik dan jaringan private menggunakan router IOS Cisco pada GNS3 sebagai emulator. Perangkat keamanan pada gateway jaringan private menggunakan Cisco Adaptive Security Appliance (ASA) pada GNS3. Topologi remote access VPN didukung dua jenis protocol keamanan yaitu IPSec dan SSL dalam pengamanan data dari perusahaan ke clien dan sebaliknya.

Jaringan publik menggunakan standar pengalamatan IPv4 yaitu pada sisi client hingga gateway jaringan private, sedangkan untuk jaringan private menggunakan standar pengalamatan IPv6. Pemilihan topologi jaringan ini dipilih karena untuk VPN remote access, client bisa mengakses VPN dari jaringan manasaja sehingga digunakan standar pengalamatan IPv4.

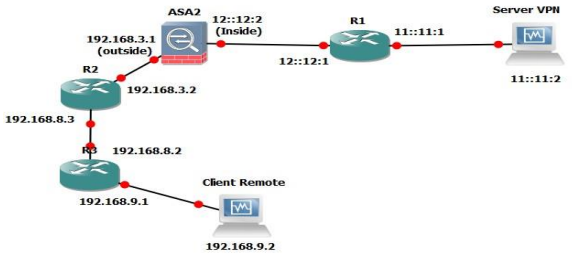
3.1 Topologi IPSec VPN Remote Access



Gambar 3.2 Topologi jaringan remote access IPSec VPN

Awalnya client melakukan koneksi ke gateway ASA (outside), dengan memasukkan username dan password pada cisco VPN client. hanya saja karena keterbatasan pada ASA, dimana ASA hanya belum mendukung pemberian IPv6 untuk client yang masuk menggunakan protokol IPSec, dan mendukung pemberian IPv4. Sehingga karena server yang digunakan menggunakan IPv6 maka setelah autentikasi IPSec berhasil di ASA dan client mendapatkan IPv4 jaringan private lalu IPv4 tersebut ditranslasikan ke IPv6 menggunakan Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) pada router. Setelah keluar dari router ISATAP, client akan mendapatkan IPv6 yang digunakan untuk terhubung ke server FTP yang ada di dalam jaringan internal perusahaan.

3.2 Topologi SSL VPN Remote Access



Gambar 3.3 Topologi jaringan remote Access SSL VPN

Pada koneksi VPN dengan SSL ini secara umum proses koneksinya sama dengan koneksi VPN pada protokol IPSec. Awalnya client melakukan koneksi ke gateway ASA (outside), dengan memasukkan username dan password pada cisco anyconnect. ASA akan membuat tunnel dengan protokol keamanan SSL dari client ke jaringan private (inside). Lalu client akan diberikan alamat IPv6 yang satu subnet dengan jaringan private (LAN), sehingga seolah-olah client berada di jaringan LAN dan dapat mengakses server File Transfer Protocol (FTP).

4. Pengujian

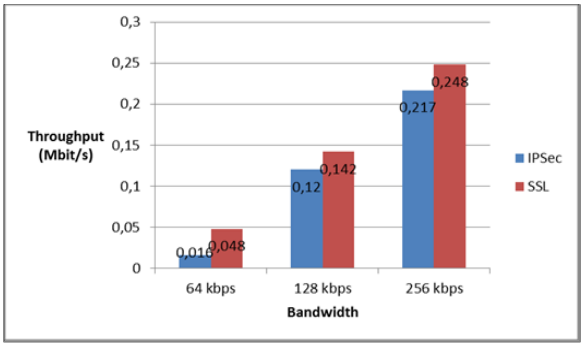
Pada pengujian terhadap perbandingan performansi, akan dilakukan pengujian terhadap performansi IPSec dan SSL dengan parameter delay, throughput.

4.1 Throughput

Hasil pengujian throughput merupakan hasil dari 6 skenario yang dilakukan dimana nilai throughput adalah MBit/sec yang merupakan rata-rata throughput dari setiap pengujian yang dilakukan. Pengambilan data throughput menggunakan aplikasi Wireshark. Pada pengujian menggunkan FTP, nilai throughput yang dihasilkan oleh SSL jauh lebih besar dibandingkan dengan IPSec.

Tabel 4.1 perbandingan nilai Throughput FTP (Mbit/s)

Bandwidth	IPSec	SSL
64 kbps	0,016	0,048
128 kbps	0,12	0,142
256 kbps	0,217	0,248



Gambar 4.9 Throughput FTP hasil pengujian SSL & IPSec

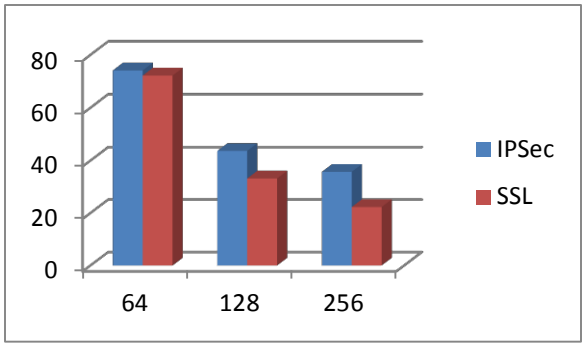
Throughput yang sangat kecil dihasilkan oleh IPSec dibandingkan dengan SSL memiliki perbedaan sangat jauh. Hal tersebut diakibatkan oleh IPSec yang memiliki performansi yang lebih buruk ketika mengirimkan paket TCP. Hal tersebut mengakibatkan adanya kemungkinan paket yang hilang ketika koneksi fail dan juga RTO, sehingga nilai throughput yang dihasilkan menjadi sangat kecil. Jika dibandingkan dengan SSL yang mengirimkan paket TCP dengan metode handshaking seperti pada penukaran kunci sertifikat yang dilakukan oleh SSL, maka kemungkinan pengiriman yang gagal menjadi lebih sedikit sehingga nilai rata-rata throughput yang dihasilkan menjadi lebih besar.

4.2 Delay

Pengujian untuk parameter delay (ms) dilakukan pada total 6 skenario simulasi pengujian dimana pengujian dibagi menjadi tiga bagian berdasarkan Bandwidth dan dengan dua kali pengujian masing-masing download file pada server FTP. Pada pengujian ini dilakukan perhitungan delay berdasarkan persamaan 2.3 yang telah dijelaskan pada bab sebelumnya. Pengambilan data delay menggunakan software Wire Shark sebagai alat bantu pengambilan data traffic.

Tabel 4.2 perbandingan nilai Delay FTP (millisecond)

Bandwidth	IPSec	SSL
64 kbps	74,103	72,185
128 kbps	43,679	33,2
256 kbps	35,72	22,302



Gambar 4.10 Delay FTP pada SSL & IPSec

Pada gambar 4.8 dapat dilihat delay tertinggi pada SSL terjadi ketika melakukan download file FTP dengan bandwidth 64 Kbps yang hanya mencapai 38.827 ms. Jika dibandingkan dengan IPSec yang dari keseluruhan percobaan menghasilkan nilai lebih dari 100 ms menunjukkan SSL memilki keunggulan yang sangat jauh dibandingkan dengan IPSec dalam hal pengiriman paket TCP yang pada tugas akhir ini adalah file dari server FTP.

Hasil delay dari pengujian menggunakan FTP menunjukkan IPSec memiliki performansi yang buruk ketika mengirimkan file TCP yang dalam tugas akhir ini menggunakan FTP.

Perbedaan delay diakibatkan karena IPSec yang melakukan penambahan header pada paket yang dikirim. Untuk paket yang sama, header IPSec berukuran 94 byte sedangkan header SSL hanya 74 byte. Selain itu, delay IPSec juga diperburuk oleh proses-proses yang ada pada ISATAP. Proses translasi IPv4 ke IPv6 menggunakan ISATAP jauh lebih kompleks dari proses transalasi yang dilakukan ASA untuk VPN SSL.

5. Kesimpulan dan Saran

5.1. Kesimpulan

Berdasarkan analisis dan pengujian terhadap analisis performansi remote access VPN berbasis IPSec dan SSL dapat disimpulkan:

1. IPSec remote access VPN dan SSL remote access VPN dapat di implementasikan pada jaringan private IPv6 dan dengan jaringan publik IPv4 menggunakan Cisco ASA.
2. Pada parameter delay, IPSec memiliki performansi lebih buruk daripada SSL.
3. Pada paremeter throughput, IPSec memiliki performansi lebih buruk lebih buruk daripada SSL.

5.2. Saran

1. Untuk pengembangan tugas akhir di masa mendatang, penulis menyarankan bebrapa hal berikut:
2. Pengujian perbandingan IPSec dan SSL dilakukan dengan menggunakan jaringan murni IPv6.
3. Penggunaan protokol keamanan lain disamping IPSec dan SSL.
4. Menggunakan router sebenarnya untuk mengetahui lebih lanjut tentang delay dan throughput berdasarkan keadaan nyata.

Daftar Pustaka

[1] Alshamsi, A. N.and Saito, T. 2005. A Technical Comparison of IPSec and SSL. Taipei: 19th International Conference on Advanced Information Networking and Applications (AINA'05) Volume 2 (INA,, USW,, WAMIS,, and IPv6 papers).

[2] Haeni, R. E. 1997. IPV6 vs. SSL - Comparing Apples with Oranges. Washington DC: The Goerge Washington University

[3] Dierks, T and Allen, C. 1999 The TLS Protocol Version 1.0 , RFC 2246. https://www.ietf.org/rfc/rfc2246.txt

[4] Haeni, R. E. 1997. IPV6 vs. SSL - Comparing Apples with Oranges. Washington DC: The Goerge Washington University.

[6] Miller, M. A. 2000. Implementing IPv6, Second Edition : Supporting the Next Generation Protocol. M&T Books.

[7] Rafiudin, R. 2005. IPv6 Addressing. Jakarta: Elex Media Komputindo.

[8] VPN Security. 2008. The Government of the Hong Kong Special Administrative Region

[9] Wijaya, H. 2006 . Belajar Sendiri Cisco ADSL Router, PIX Firewall, dan VPN. Jakarta: Elex Media Komputindo