Laboratorium
Multimedia dan Internet of Things
Departemen Teknik Komputer
Institut Teknologi Sepuluh Nopember

Laporan Sementara
Praktikum Jaringan Komputer

VPN QoS

Benice Didan Al Ghifari - 5024231045

2025

1 Pendahuluan

1.1 Latar Belakang

Dalam era digital saat ini, pertukaran data melalui jaringan publik seperti internet telah menjadi kebutuhan utama bagi banyak organisasi dan perusahaan. Namun, keterbukaan jaringan publik membawa berbagai ancaman keamanan, mulai dari penyadapan, manipulasi data, hingga serangan siber yang bisa merugikan bisnis secara signifikan. Oleh karena itu, perlindungan terhadap data yang dikirim melalui jaringan tersebut menjadi sangat krusial, terutama ketika data yang ditransmisikan bersifat sensitif atau rahasia.

Internet Protocol Security (IPSec) hadir sebagai solusi keamanan jaringan yang dirancang untuk menjaga kerahasiaan, integritas, dan keaslian data yang dikirimkan melalui jaringan IP, khususnya internet. IPSec bekerja dengan cara mengenkripsi dan mengautentikasi paket data sehingga informasi yang dikirim hanya bisa dibaca dan diakses oleh pihak yang berwenang. Dengan menggunakan teknologi ini, data menjadi lebih terlindungi dari potensi ancaman seperti sniffing, spoofing, maupun man-in-the-middle attack.

Salah satu implementasi paling umum dari IPSec adalah pada jaringan Virtual Private Network (VPN). VPN memungkinkan dua titik atau lebih yang berada di lokasi geografis berbeda untuk terhubung melalui jaringan publik secara aman seolah-olah berada dalam satu jaringan privat. Misalnya, koneksi antara kantor pusat dan kantor cabang sebuah perusahaan dapat dilakukan dengan memanfaatkan VPN berbasis IPSec, sehingga komunikasi antar lokasi tetap aman, terenkripsi, dan terlindungi dari gangguan pihak luar.

Keunggulan lain dari IPSec adalah fleksibilitas dan skalabilitasnya. Protokol ini dapat diintegrasikan dengan berbagai jenis perangkat dan sistem operasi, serta dapat digunakan pada berbagai skala jaringan, mulai dari individu, organisasi kecil, hingga perusahaan besar. Dengan dukungan fitur-fitur seperti tunneling, enkripsi kuat, dan otentikasi berbasis sertifikat digital atau pre-shared key, IPSec menjadi tulang punggung dalam membangun sistem komunikasi jaringan yang aman dan handal.

Dengan semakin tingginya kebutuhan akan keamanan data di tengah maraknya serangan siber dan peningkatan mobilitas kerja jarak jauh, penggunaan IPSec dalam jaringan modern bukan lagi sebuah opsi, melainkan suatu keharusan. Implementasi IPSec yang tepat dapat memastikan bahwa data perusahaan tetap aman, operasional berjalan lancar, dan kepercayaan dari pelanggan maupun mitra tetap terjaga.

1.2 Dasar Teori

Internet Protocol Security, atau yang dikenal dengan IPSec, merupakan kumpulan protokol keamanan yang dirancang untuk melindungi komunikasi data melalui jaringan berbasis Internet Protocol (IP). IPSec bekerja pada layer jaringan (network layer) dalam model OSI dan memiliki kemampuan untuk mengenkripsi serta mengautentikasi setiap paket data yang dikirim antara dua titik komunikasi. Dengan kemampuan tersebut, IPSec menjadi salah satu komponen utama dalam pembangunan jaringan Virtual Private Network (VPN) yang aman dan andal. Penggunaan IPSec memungkinkan data dikirim secara rahasia dan utuh meskipun melewati jaringan publik seperti internet. Protokol ini menjamin tiga prinsip utama keamanan informasi, yaitu kerahasiaan (confidentiality), integritas (integrity), dan autentikasi (authentication). Kerahasiaan dicapai melalui proses enkripsi sehingga hanya pihak yang memiliki kunci sah yang dapat membaca data. Integritas memastikan bahwa data yang diki-

rim tidak mengalami perubahan selama transmisi, dan autentikasi menjamin bahwa sumber pengirim data adalah pihak yang sah.

IPSec memiliki dua mode operasional, yaitu Transport Mode dan Tunnel Mode. Transport Mode mengenkripsi hanya bagian isi (payload) dari paket IP, sedangkan Tunnel Mode mengenkripsi seluruh paket IP dan membungkusnya dalam paket IP baru. Tunnel Mode sering digunakan dalam koneksi VPN antar jaringan (site-to-site), sementara Transport Mode lebih umum digunakan dalam komunikasi antar perangkat (end-to-end). Proses negosiasi dan pertukaran parameter keamanan dalam IPSec dilakukan melalui dua tahap yang disebut sebagai IKE (Internet Key Exchange) Phase 1 dan Phase 2. Pada IKE Phase 1, dua titik komunikasi melakukan pertukaran informasi untuk membentuk saluran yang aman dan terenkripsi, disebut IKE Security Association (IKE SA). Di fase ini juga dilakukan autentikasi antara kedua pihak serta pembentukan kunci enkripsi menggunakan metode seperti Diffie-Hellman.

Setelah saluran aman terbentuk, proses dilanjutkan ke IKE Phase 2. Pada fase ini, kedua pihak menyepakati parameter keamanan yang digunakan untuk melindungi lalu lintas data aktual. Parameter tersebut meliputi algoritma enkripsi seperti AES atau 3DES, metode autentikasi seperti SHA-256, waktu hidup Security Association (SA), serta protokol IPSec yang akan digunakan, yaitu Authentication Header (AH) atau Encapsulating Security Payload (ESP). Protokol AH menyediakan autentikasi dan integritas tetapi tidak mengenkripsi data, sedangkan ESP menyediakan layanan enkripsi serta dapat dilengkapi dengan autentikasi dan integritas, menjadikannya lebih umum digunakan dalam implementasi VPN.

Sebagai protokol yang bersifat agnostik terhadap jenis data dan aplikasi, IPSec dapat digunakan untuk mengamankan berbagai jenis lalu lintas IP, seperti TCP, UDP, atau ICMP. Fleksibilitas ini membuat IPSec menjadi solusi yang kuat dan efisien untuk pengamanan komunikasi jaringan dalam berbagai skenario, baik untuk keperluan perusahaan, pemerintahan, maupun individu. Dengan penerapan yang tepat, IPSec dapat menjamin bahwa transmisi data sensitif melalui jaringan tetap aman dari penyadapan, pemalsuan, maupun serangan dari pihak yang tidak berwenang.

2 Tugas Pendahuluan

1 Konfigurasi IPSec (IKE Phase 1 dan Phase 2)

- Pada IKE Phase 1, tujuannya adalah untuk membentuk saluran yang aman dan terautentikasi antara dua gateway VPN (router), yang dikenal sebagai ISAKMP SA atau IKE SA. Saluran ini digunakan untuk negosiasi IPSec SA pada Phase 2. Parameter utama yang dinegosiasikan meliputi metode autentikasi, algoritma enkripsi, algoritma hashing, grup Diffie-Hellman (DH), dan masa berlaku (lifetime) SA. Autentikasi bisa menggunakan pre-shared key (PSK) atau sertifikat digital (PKI). PSK lebih sederhana tapi kurang skalabel dibandingkan PKI yang lebih aman dan cocok untuk banyak situs. Untuk algoritma enkripsi, disarankan menggunakan AES-256, sedangkan untuk hashing disarankan SHA-256 atau yang lebih tinggi. Grup DH yang direkomendasikan minimal adalah Group 14 (2048-bit), atau lebih tinggi seperti Group 19 dan 21. Umumnya, masa berlaku IKE SA diset selama 86400 detik (24 jam). Negosiasi dilakukan melalui Main Mode (lebih aman) atau Aggressive Mode (lebih cepat tapi kurang aman, digunakan bila salah satu router memiliki IP dinamis).

  Setelah Phase 1 selesai, dilanjutkan dengan IKE Phase 2 yang berfokus pada pembentukan

IPSec SA, yaitu saluran data yang akan digunakan untuk mengenkripsi dan mengautentikasi lalu lintas antar situs. Proses ini disebut Quick Mode. Parameter yang dinegosiasikan pada fase ini mencakup protokol IPSec yang digunakan (ESP lebih umum karena menyediakan enkripsi dan autentikasi), algoritma enkripsi (misalnya AES-256), algoritma integritas (misalnya SHA-256), serta masa berlaku SA (misalnya 3600 detik atau 1 jam). Perfect Forward Secrecy (PFS) juga dapat diaktifkan untuk meningkatkan keamanan dengan menggunakan DH Group baru setiap kali IPSec SA dinegosiasikan.

Dalam konfigurasi router Cisco, beberapa komponen penting meliputi: Access Control List (ACL) yang menentukan lalu lintas yang akan dienkripsi; transform set yang menyatakan kombinasi protokol, algoritma enkripsi, dan hashing; serta crypto map yang menggabungkan semua parameter tersebut, termasuk peer IP, transform set, PFS, dan ACL. Crypto map ini kemudian diterapkan pada antarmuka publik router, misalnya GigabitEthernet0/0.

Sebagai alternatif dari crypto map, dapat digunakan Tunnel Interface seperti VTI (Virtual Tunnel Interface), yang lebih cocok untuk VPN berbasis routing. VTI mempermudah penerapan protokol routing dinamis melalui VPN dan menggantikan ACL dengan kebijakan routing. Pada konfigurasi VTI, setiap router memiliki antarmuka tunnel yang saling terhubung melalui IP publik masing-masing, dan lalu lintas antar jaringan lokal diarahkan melalui tunnel ini menggunakan routing statis atau dinamis.

Dalam memilih parameter keamanan, AES-256 dipilih karena kekuatannya terhadap serangan brute-force, SHA-256 untuk menjaga integritas data, dan PFS agar kunci sesi sebelumnya tidak bisa diretas meskipun kunci jangka panjang bocor. Waktu hidup SA yang pendek meningkatkan keamanan tetapi juga menambah beban kerja karena seringnya pembaruan kunci. Oleh karena itu, kombinasi umum adalah 24 jam untuk IKE Phase 1 dan 1 jam untuk IKE Phase 2.

2 Implementasi QoS untuk Alokasi Bandwidth Sekolah (100 Mbps)

- Tujuan dari skenario ini adalah membagi koneksi internet sebesar 100 Mbps di lingkungan sekolah ke dalam empat kategori penggunaan, yaitu: 40 Mbps untuk e-learning, 30 Mbps untuk akses staf (seperti email dan penyimpanan cloud), 20 Mbps untuk browsing siswa, dan 10 Mbps untuk CCTV serta pembaruan sistem. Untuk memastikan tiap jenis lalu lintas mendapatkan bandwidth dan prioritas sesuai kebutuhan, diterapkan Quality of Service (QoS) melalui beberapa langkah: klasifikasi lalu lintas, penandaan DSCP, pengalokasian bandwidth, dan pengendalian kemacetan.

  Langkah pertama adalah klasifikasi lalu lintas dan penandaan DSCP (Differentiated Services Code Point). Tujuannya adalah mengidentifikasi jenis lalu lintas agar bisa diprioritaskan. Lalu lintas e-learning ditandai dengan DSCP EF (Expedited Forwarding) karena bersifat sensitif terhadap delay. Akses staf diberi tanda AF31 (Assured Forwarding prioritas tinggi), browsing siswa dengan AF21 (prioritas sedang), dan CCTV serta pembaruan sistem dengan AF11 (prioritas rendah). Penandaan ini membantu router dalam mengatur prioritas lalu lintas berdasarkan tingkat kepentingannya.

  Langkah kedua adalah pengaturan alokasi bandwidth menggunakan Class-Based Weighted Fair Queuing (CBWFQ). Mekanisme ini memastikan setiap jenis lalu lintas mendapatkan jatah bandwidth sesuai yang direncanakan. Selain itu, lalu lintas e-learning juga diberikan prioritas

lebih tinggi melalui priority queuing, untuk mengurangi latency dan menjamin kualitas koneksi real-time.

Langkah ketiga melibatkan pengendalian kemacetan (congestion control) menggunakan metode Random Early Detection (RED). RED bekerja dengan menjatuhkan paket lebih awal sebelum antrean penuh, untuk mencegah kemacetan. Dengan pendekatan ini, sistem dapat menjaga performa lalu lintas berprioritas tinggi, sehingga pengalaman pengguna tetap optimal meskipun terjadi kepadatan jaringan.

Secara keseluruhan, kombinasi DSCP, CBWFQ, dan RED memastikan setiap jenis layanan di sekolah menerima bandwidth sesuai kebutuhan dan berjalan dengan efisien, terutama pada kondisi jaringan yang padat.

3 Queue Trees

- Sistem Hierarchical Queue Tree pada MikroTik RouterOS digunakan untuk mengelola alokasi bandwidth secara efisien, mengatur prioritas lalu lintas, dan memungkinkan penanganan burst serta skalabilitas jaringan. Dalam contoh ini, diasumsikan bahwa total bandwidth adalah 100 Mbps untuk upload dan download, dengan interface WAN di ether1 dan LAN di bridge-local.

  Pertama-tama, dilakukan packet marking menggunakan aturan mangle di firewall. Masing-masing jenis trafik seperti e-learning, staf, siswa, CCTV, dan update sistem ditandai berdasarkan daftar alamat IP. Penandaan dilakukan dalam dua tahap: penandaan koneksi di chain prerouting dan penandaan paket di chain prerouting (untuk download) serta postrouting (untuk upload). Ini memungkinkan antrian (queue tree) mengenali dan memproses paket sesuai kategori trafik.

  Setelah itu, dibuat dua antrian induk, yaitu GLOBAL_UPLOAD dan GLOBAL_DOWNLOAD, masing-masing dengan batas maksimum 100 Mbps. Antrian anak untuk setiap jenis trafik dikaitkan dengan antrian induk, menggunakan tanda paket dari tahap mangle. Masing-masing antrian anak memiliki parameter limit-at sebagai bandwidth minimum terjamin, dan max-limit sebagai batas maksimum yang bisa digunakan saat tidak ada kontensi.

  Prioritas diatur dari 1 (tertinggi) sampai 8 (terendah). Trafik e-learning diberi prioritas tertinggi (1), diikuti oleh staf (2), siswa (3), dan CCTV/update (4). Trafik tak terklasifikasi diberi prioritas terendah (8). Jenis antrian yang digunakan meliputi fq_codel untuk trafik sensitif terhadap delay seperti e-learning dan staf, serta pcq (Per Connection Queuing) untuk siswa, yang membagi bandwidth secara adil antar pengguna berdasarkan alamat IP. Antrian default menggunakan sfq untuk memastikan keadilan dasar bagi lalu lintas tak terklasifikasi.

  RouterOS juga mendukung burst, yaitu kemampuan sementara untuk melebihi max-limit saat bandwidth tersedia. Hal ini memungkinkan antrian dengan prioritas tinggi memanfaatkan sisa kapasitas saat trafik lainnya sedang rendah. Sistem ini bersifat modular dan mudah diskalakan. Penambahan trafik baru cukup dengan menambah aturan mangle dan entri queue baru. Dengan mengatur ulang limit-at dan max-limit, sistem bisa disesuaikan dengan peningkatan bandwidth atau kebutuhan baru di masa depan.

  Konfigurasi ini memberikan kontrol granular terhadap penggunaan bandwidth, memastikan aplikasi penting selalu mendapatkan prioritas, sambil tetap adil dan fleksibel terhadap trafik lainnya.

Pemantauan melalui fitur seperti /queue tree print stats, Torch, dan Graphing juga sangat disarankan untuk memastikan performa optimal dan penyesuaian konfigurasi bila diperlukan.

Referensi:

- https://jurnal.umko.ac.id/index.php/sienna/article