Pengertian Routing, proses menghubungkan jaringan yang berbeda. Tujuan : mengirim data dari satu jaringan ke jaringan lain secara efisien melalui perangkat router.
Cara kerja router: Melihat alamat IP tujuan, Meneruskan data ke jalur terbaik berdasarkan tabel routing.
Router, Fungsi utama : melakukan routing pada lapisan jaringan (Network Layer). Peran: Menghubungkan dua atau lebih jraingn untuk bertukar data, Meneruskan paket data dan membagi/menyatukan segmen jaringan.
Jenis2 Routing
Static Routing. Dikonfigurasi secara manual oleh administrator, Cocok untuk jaringan kecil yang stabil.
Keuntungan : Lebih aman karena tidak berubah otomatis, Menghemat sumber daya router. Kerugian : Tidak fleksibel jika jaringan bertambah besar, Harus memperbarui secara menual saat topologi berubah.
Contoh konfigurasi di router cisco:
ip route 192.168.2.0 255.255.255.0 192.168.1.2
Artinya: kriim semua paket ke jaringan 192.168.2.0/25 melalui router dengan IP 192.168.1.2
Dynamic Routing, Router otomatis menemukan jalur terbaik menggunakan protokol routing. Cocok untuk jaringan besar yang sering berubah.
Keuntungan : Fleksibel, otomatis menyesuaikan perubahan topologi, Skalabel untuk jaringan besar. Kerugian -> Mengguanakn lebih banyak sumber daya (CPU DAN RAM), Konfigurasi lebih kompleks
Contoh konfigurasi OSPF di router CISCO:
router ospf 1
network 192.168.1.0 0.0.0.255 area 0
network 192.168.2.0 0.0.0.255 area 0
Artinya: Router bertukar informasi dengan router lain dalam area OSPF
Default Routing, Digunakan saat router tidak memiliki rute spesifik untuk tujuan tertentu. Mengarahkan semua lalu lintas ke gateway utama (misalnya router ISP).
Keuntungan: Sederhana, hanya perlu satu perintah.
Kerugian: Tidak efisien jika ada jalur alternatif yang lebih baik.
Contoh Konfigurasi di Router Cisco:
ip route 0.0.0.0 0.0.0.0 192.168.1.1
Artinya: Kirim semua paket yang tidak dikenali ke gateway 192.168.1.1.
Protokol Routing
Pengertian: Digunakan untuk mencari rute tersingkat dalam mengirimkan paket data ke alamat tujuan.
Pengguna: Router, bukan host seperti laptop atau desktop.
Fungsi: Membangun dan memperbarui tabel routing. Mempelajari semua router, menempatkan rute terbaik, dan menghapus rute yang tidak valid.
Contoh Protokol: RIP, IGRP, OSPF, EIGRP, BGP, IS-IS.
Klasifikasi Protokol Routing
Distance Vector, Fokus pada jarak dan arah., Router hanya melihat router/jaringan terdekat.. Analogi: Membaca petunjuk arah.
Contoh: RIP (Routing Information Protocol)., IGRP (Interior Gateway Routing Protocol)., EIGRP (Enhanced Interior Gateway Routing Protocol).
Link-State, Membaca jaringan secara keseluruhan (jarak, arah, kecepatan)., Menentukan jalur terbaik., Analogi: Membaca peta.
Contoh:
OSPF (Open Shortest Path First):Kategori IGP, menggunakan algoritma Dijkstra. Nomor protokol 89. Berkomunikasi dengan router tetangga (neighbour router).
IS-IS (Intermediate System to Intermediate System): Protokol link-state untuk CLNP (Connectionless-mode Network Service).
Path-Vector, Menjaga informasi jalur dan memperbaruinya secara dinamis.
Contoh:
BGP (Border Gateway Protocol): Digunakan untuk pertukaran informasi antar Autonomous System (AS). Berjalan melalui protokol transport TCP. Mengatur trafik dari sumber berbeda dalam jaringan multi-home.
Interior Gateway Protocols (IGP) vs Exterior Gateway Protocols (EGP)
IGP: Digunakan dalam satu organisasi atau autonomous system.
Contoh: RIP, OSPF, EIGRP, IS-IS.
EGP: Digunakan untuk pertukaran data antar autonomous system.
Contoh: BGP.
Konfigurasi Routing Statis
Syntax Umum:ip route [destination_network] [netmask] [next-hop_address or exit interface] [adm_distance] [permanent]
Contoh: Jaringan: 10.0.0.1, 10.0.0.2, 10.0.0.3, 30.0.0.1, 30.0.0.2.
Konfigurasi: Mengatur jalur paket data secara manual.
Catatan Tambahan
Tabel Routing: Berisi informasi jaringan dan interface terkait.
Routing Algorithms: Komponen proses untuk menentukan jalur terbaik.
Konteks Jaringan: Routing digunakan baik di LAN (jaringan lokal) maupun WAN (internet).

Firewall, merupakan sistem keamanan jaringan yang berfungsi sebagai "tembok pengaman" untuk mengontrol lalu lintas data yang masuk dan keluar berdasarkan aturan keamanan yang telah ditentukan
Contoh: Software: Windows Firewall, Zone Alarm, pfSense.
Hardware: Cisco ASA, FortiGate, Palo Alto
Jenis-jenis firewall:
Packet Filtering Firewall – menyaring lalu lintas berdasarkan alamat IP, port, dan protokol
Stateful Inspection Firewall – Menganalisis koneksi jaringan lebih dalam, bukan hanya berdasarkan paket individu
Proxy Firewall – Bertindak sebagai perantara antara pengguna dan sumber daya internet, menyembunyikan identitas pengguna
Next-Generation Firewall (NGFW) – Firewall modern yang menggabungkan berbagai fitur keamnaan seperti IDS (Instrusion Detection System) dan IPS (Intrusion Prevention System).
Virtual Private Network (vpn), VPN adalah teknologi yang mengenkripsi koneksi internet pengguna dengan mengarahkannya melalui server aman, untuk menjaga privasi dan keamanan data.
VPN : Mengenkripsi data sehingga tidak bisa disadap, Menyembunyikan alamat IP asli pengguna, Menakses konten yang diblokir di wilayah tertentu, Mengamankan koneksi saat memakai WIFI publik.
Jenis VPN: Remote Access Vpn – digunakan oleh pengguna individu untuk mengakses jaringan pribadi dari lokasi jauh. Site-to-site vpn – Menghubungkan dua jaringan perusahaan di lokasi berbeda. SSL VPN – Menggunakan enskripsi ssl/tls untuk keamanan tingkat tinggi
Contoh VPN : nordvpn, expressvpn, openvpn
Enkripsi data, adalah teknik mengubah data menjadi kode rahasia, agar hanya bisa dibaca oleh pihak yang memiliki kunci deskripsi.
Jenis2 enkripsi: Enkripsi simetrsi – menggunakan satu kunci untuk enkripsi dan dekripsi. Contoh algoritma : aes (advanced encryption standard), des (data encryption standard).

Enkripsi asimetris – Menggunakan dua kunci: kunci publik untuk enkripsi dan kunci privat untuk dekripsi. Contoh algoritma : RSA, ECC (elliptic Curve Cryptography).

Penerapan Enkripsi:

HTTPS (SSL/TLS) - Mengamankan komunikasi web.

Email (PGP, S/MIME) - Melindungi isi email dari penyadapan.

Disk Encryption (BitLocker, VeraCrypt) - Mengamankan data pada hard drive.

Serangan Siber (Cyber Attacks)

Serangan siber adalah upaya untuk mengganggu, merusak, atau mencuri data dari sistem komputer atau jaringan. Jenis jenisnya (Malware, phising, DDOS, sql injection)

Cara Mencegah Serangan Siber: Gunakan antivirus dan firewall yang kuat. Jangan klik tautan atau unduhan dari sumber yang tidak dikenal. Gunakan autentikasi dua faktor (2FA).

Kesimpulan

Keamanan jaringan sangat penting untuk melindungi sistem dan data dari ancaman atau serangan siber. Penerapan firewall, VPN, enkripsi, dan langkah pencegahan serangan siber dapat membantu mengamankan jaringan dari berbagai ancaman.

Demilitarized Zone (DMZ)

Pengertian DMZ, Area jaringan yang berada di antara jaringan internal (trusted) & internet (untrusted). DMZ dipakai untuk menempatkan server publik (seperti) web server, email server, & DNS server, agar bisa diakses dari internet, tanpa membahayakan jaringan internal.

Fungsi & Tujuan DMZ

Menambah Lapisan Keamanan → Melindungi jaringan internal dari serangan siber, dengan menempatkan server publik di zona terpisah.

Membatasi Akses Langsung ke Jaringan Internal → Jika ada serangan ke server di DMZ, jaringan internal tetap aman.

Memisahkan Layanan Publik & Privat → Layanan (seperti) web server atau email server, agar dapat diakses publik tanpa membuka akses ke sistem internal.

Layanan yang Biasanya Ada di DMZ

Web Server - Agar situs web bisa diakses oleh pengguna internet.

Mail Server - Untuk mengelola email yang masuk dari luar jaringan.

DNS Server - Menerjemahkan domain ke alamat IP agar bisa diakses oleh publik.

Reverse Proxy - Menerjemahkan permintaan ke server internal tanpa mengeksposnya langsung ke internet.

Cara Kerja DMZ

DMZ biasanya memakai 1 (satu) firewall atau 2 (dua) firewall, dengan konfigurasi tertentu untuk mengontrol lalu lintas antara internet, DMZ, & jaringan internal.

Single Firewall Strategy

Menggunakan satu firewall untuk mengatur lalu lintas antara internet, DMZ, dan jaringan internal (Private LAN).

Keuntungan: Lebih murah & mudah dikelola dibandingkan dengan 2 (dua) firewall.

Arsitektur 2 Firewall (Lebih Aman)

Firewall Eksternal → Mengontrol lalu lintas antara internet & DMZ.

Firewall Internal → Mengontrol lalu lintas antara DMZ & jaringan internal.

Keuntungan: Jika hacker menembus firewall pertama, hacker hanya bisa mengakses DMZ, bukan jaringan internal.

Jika hacker menyerang Web Server di DMZ, hacker tetap tidak bisa langsung mengakses jaringan internal, karena masih ada firewall kedua.

Zona dalam Jaringan

1, Internet (Untrusted Zone)

2, DMZ (Semi-Trusted Zone)

3, Jaringan Internal (Trusted Zone)

Menjaga Keamanan DMZ

Aturan Firewall yang Ketat - Hanya mengizinkan lalu lintas tertentu yang diperlukan.

Segmentasi Jaringan - Memisahkan DMZ dari jaringan internal dengan firewall.

Intrusion Detection System (IDS) - Mendeteksi ancaman yang masuk ke DMZ.

Monitoring & Logging - Mengawasi aktivitas mencurigakan di DMZ.

Kesimpulan

DMZ melindungi jaringan internal dengan menempatkan server publik di zona aman.

Layanan seperti web server, DNS, & email biasanya ditempatkan di DMZ untuk akses publik yang aman.

Menggunakan firewall untuk mengontrol lalu lintas antara internet, DMZ, & jaringan internal.

Tunneling dalam Jaringan, Tunneling adalah teknik mengirim data secara aman melalui jaringan publik dengan membungkus data dalam protokol lain, digunakan di VPN, SSH, GRE, dan IPsec untuk meningkatkan keamanan dan efisiensi.

Cara Kerja

Data asli dienkapsulasi, dikirim melalui tunnel, lalu diekstrak di tujuan, menjaga keamanan data di jaringan publik.

Jenis Tunneling

VPN Tunneling: Mengenkripsi komunikasi melalui jaringan publik.

Protokol: PPTP (kurang aman), L2TP/IPSec (lebih aman), OpenVPN (fleksibel, aman), WireGuard (ringan, performa tinggi).

SSH Tunneling: Mengamankan koneksi via protokol SSH.

Jenis: Local, Remote, dan Dynamic Port Forwarding.

Contoh: ssh -L 8080:example.com:80 user@server.com.

GRE Tunneling: Mengemas paket untuk protokol yang tidak didukung, seperti IPv6 di jaringan IPv4.

IPsec Tunneling: Mengamankan komunikasi antar jaringan.

Mode: Transport (enkripsi payload) dan Tunnel (enkripsi seluruh paket).

Keuntungan

Keamanan data terenkripsi.

Melewati firewall/sensor internet.

Menghubungkan jaringan terpisah.

Anonimitas dengan menyembunyikan IP.

Implementasi Sehari-hari

VPN untuk akses jaringan kantor dari rumah.

VPN/SSH Tunnel untuk bypass pemblokiran situs.

IPsec untuk koneksi antar kantor cabang.

SSH Tunnel untuk gaming dengan ping rendah.

Kesimpulan

Tunneling meningkatkan privasi, keamanan, dan fleksibilitas koneksi jaringan, digunakan untuk melewati sensor, menghubungkan jaringan, atau melindungi data.