Implementasi DMZ dan Firewall pada Cisco Packet Tracer

Perancangan Keamanan Sistem dan Jaringan

Dosen Pengampu : Ferdi Chahyadi, S. Kom., M.Cs

Oleh :

2201020052 Ade Latifia

2201020111 Mardita Rindi

2201020133 Meylin

2201020135 Annisya Awari

PROGRAM STUDI TEKNIK INFORMATIKA

FAKULTAS TEKNIK DAN TEKNOLOGI KEMARITIMAN

UNIVERSITAS MARITIM RAJA ALI HAJI

TANJUNGPINANG

2026

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

BAB I

PENDAHULUAN

1.1 Latar Belakang

Keamanan jaringan merupakan aspek penting dalam menjaga kerahasiaan, integritas, dan ketersediaan data di sebuah sistem informasi. Dalam lingkungan jaringan modern yang terhubung dengan internet, ancaman seperti peretasan, malware, dan akses tidak sah dapat terjadi kapan saja. Oleh karena itu, diperlukan strategi keamanan yang efektif untuk melindungi jaringan internal dari ancaman eksternal.

Salah satu konsep yang banyak digunakan dalam keamanan jaringan adalah Demilitarized Zone (DMZ). DMZ berfungsi sebagai area penyangga antara jaringan internal dan jaringan public (internet), dimana server yang bersifat public seperti web server, DNS server, atau mail server ditempatkan. Dengan adanya DMZ, lalu lintas antara jaringan internal dan eksternal dapat dikontrol dengan lebih aman menggunakan firewall yang mengatur aturan sukses (access rules) antar zona.

Dalam proyek ini, penerapan konsep DMZ dan firewall dilakukan menggunakan Cisco Packet Tracer, yaitu perangkat lunak simulasi jaringan yang umum digunakan dalam pembelajaran dan perancangan jaringan komputer. Melalui simulasi ini, mahasiswa dapat memahami bagaimana segmentasi jaringan, pembuatan aturan firewall, dan pengamanan layanan public dilakukan secara terstruktur dan efisien.

1.2 Tujuan Proyek

Tujuan dari proyek ini adalah:

1. Memahami konsep segmentasi jaringan menggunakan tiga zona: internal, DMZ, dan internet.

2. Membangun topologi jaringan yang menerapkan DMZ dengan menggunakan Cisco Packet Tracer.
3. Mengimplementasikan dan mengkonfigurasi firewall untuk mengatur akses antar zona.
4. Meningkatkan pemahaman mahasiswa terhadap mekanisme perlindungan jaringan melalui penggunaan firewall dan DMZ.

1.3. Ruang Lingkup Pekerjaan

Ruang lingkup proyek ini meliputi:

1. Perancangan topologi jaringan dengan tiga zona: internal, DMZ, dan internet.
2. Pembagian Alamat IP (IP addressing) untuk setiap zona dan perangkat jaringan.
3. Konfigurasi dasar perangkat jaringan seperti router, switch, server, dan PC.
4. Penerapan aturan firewall (Access Control List / ACL) untuk mengatur lalu lintas antar zona.
5. Pengujian konektivitas antara jaringan internal, DMZ, dan internet.

Hal-hal yang tidak meliputi dalam ruang lingkup proyek ini antara lain:

1. Implementasi sistem keamanan lanjutan seperti IDS/IPS atau VPN.
2. Pengujian performa jaringan secara real-time di lingkungan fisik.
3. Integrasi dengan sistem keamanan eksternal lainnya.

BAB II

DASAR TEORI

2.1 Keamanan Jaringan

Keamanan jaringan merupakan langkah-langkah yang dilakukan untuk menjaga sistem, perangkat, dan layanan jaringan tetap aman dari berbagai ancaman yang dapat mengganggu kerahasiaan, keutuhan, dan ketersediaan data. Dalam praktiknya, keamanan jaringan tidak hanya sekadar memblokir akses, tetapi juga memastikan bahwa sistem mampu bertahan dari serangan dan tetap berjalan dengan stabil (Stallings, 2020).

- Confidentiality, berarti data tidak boleh diakses oleh pihak yang tidak berwenang.
- Integrity, menegaskan bahwa data tidak berubah secara sembarangan.
- Availability, memastikan bahwa layanan dan sumber daya jaringan selalu dapat diakses ketika dibutuhkan (Kurose & Ross, 2017).

Di lingkungan jaringan, ancaman yang sering muncul mencakup malware, sniffing, DDoS, spoofing, dan serangan Man-in-the-Middle. Karena ancaman bisa datang dari banyak titik, sistem keamanan biasanya dirancang berlapis (defense-in-depth) supaya ketika satu lapisan ditembus, masih ada lapisan lain yang melindungi.

2.1.1. CIA Triad

CIA Triad merupakan model keamanan yang paling sering digunakan sebagai dasar dalam perancangan sistem keamanan jaringan. Model ini terdiri dari tiga pilar (Kurose & Ross, 2017):

1. **Confidentiality**

   Confidentiality menekankan perlindungan data dari akses yang tidak sah. Mekanisme umum yang digunakan meliputi autentikasi, enkripsi, dan kontrol akses. Pengamanan semacam ini membantu memastikan

bahwa hanya pengguna yang memiliki izin yang dapat mengakses informasi tertentu (Kurose & Ross, 2017)

2. **Integrity**

   Integrity memastikan bahwa data tidak mengalami perubahan tanpa izin. Mekanisme seperti hashing, digital signature, dan checksum digunakan untuk menjaga konsistensi data (Stallings, 2020).

3. **Availability**

   Availability memastikan bahwa layanan tetap bisa diakses ketika diperlukan. Ancaman seperti DDoS, kerusakan jaringan, atau kesalahan konfigurasi dapat mempengaruhi ketersediaan.

2.1.2 Zero Trust Architecture (ZTA)

Zero Trust adalah model keamanan yang dikembangkan berdasarkan prinsip “never trust, always verify”. Menurut NIST SP 800-207, Zero Trust menekankan bahwa:

- Setiap permintaan akses harus divalidasi.
- Pengguna harus diberikan hak akses paling minim (least privilege).
- Akses harus terus dievaluasi berdasarkan konteks, misalnya lokasi, perangkat, dan tingkat risiko (Rose et al., 2020).

Zero Trust sangat relevan dalam penerapan DMZ karena server yang berada di DMZ dianggap berisiko tinggi, sehingga aturan akses harus sangat ketat dan terisolasi..

2.1.3 Access Control List (ACL)

ACL adalah mekanisme kontrol lalu lintas jaringan yang digunakan pada router dan firewall untuk menentukan apakah suatu paket diizinkan (permit) atau ditolak (deny).

Menurut Cisco IOS Security Guide, ACL dibagi menjadi:

- Standard ACL – menyaring lalu lintas hanya berdasarkan alamat IP sumber.

- Extended ACL – dapat menyaring berdasarkan IP sumber, IP tujuan, protokol, dan port (Cisco, 2023).

ACL diterapkan pada interface router menggunakan rule top-down, di mana rule pertama yang cocok langsung dieksekusi (first match rule). ACL adalah pondasi utama firewall di Cisco Packet Tracer.

2.1.4 Encryption

Enkripsi merupakan teknik untuk mengubah data menjadi bentuk yang tidak dapat dibaca oleh pihak yang tidak memiliki kunci dekripsi. Menurut dokumentasi OpenSSL, enkripsi dibagi menjadi dua:

1. Symmetric Encryption (AES, DES)
2. Asymmetric Encryption (misalnya RSA, ECC) (OpenSSL Foundation, 2022)

Penerapan enkripsi penting pada server DMZ seperti:

1. HTTPS (TLS) untuk web server
2. SSH untuk remote administration
3. VPN untuk akses jaringan internal

Enkripsi menjaga confidentiality dan integrity.

2.2 Tools dan Protokol Keamanan yang Digunakan

2.2.1 Cisco Packet Tracer

Cisco Packet Tracer adalah simulator jaringan yang dikembangkan oleh Cisco Networking Academy untuk membantu pembelajaran dan pengujian topologi jaringan. Aplikasi ini menyediakan dukungan untuk konfigurasi firewall berbasis ACL, NAT, routing, VLAN, dan berbagai skenario keamanan jaringan (Cisco Networking Academy, 2023).

Dalam konteks implementasi DMZ, Cisco Packet Tracer sangat ideal karena memungkinkan pengguna membuat jaringan inside–DMZ–outside secara virtual tanpa perangkat fisik.

2.3 Arsitektur dan Logika Teoretis DMZ

DMZ atau *Demilitarized Zone* adalah area khusus di jaringan yang digunakan untuk menempatkan server yang dapat diakses dari internet. Tujuannya adalah memisahkan server publik dari jaringan internal agar risiko serangan tidak langsung berdampak pada LAN. Menurut *Cisco Press – Network Security*, DMZ biasanya terdiri dari tiga segmen:

1. **Internet (Outside Network)**
   Berisi pengguna eksternal yang ingin mengakses layanan.
2. **DMZ Network**
   Tempat server publik (misalnya web server, DNS server, mail server).
   Server pada DMZ memiliki batasan akses sangat ketat.
3. **Internal Network (LAN)**
   Jaringan sensitif seperti database dan komputer internal perusahaan (Oppenheimer, 2020).

Alur Keamanan:

1. Lalu lintas dari internet masuk melalui firewall dan diarahkan ke DMZ.
2. Server yang berada di DMZ hanya diberikan akses terbatas.
3. Server DMZ tidak boleh mengakses LAN tanpa aturan khusus.
4. LAN dapat mengakses DMZ untuk keperluan maintenance.
5. NAT digunakan untuk mempublikasikan server ke internet.

Tujuan Arsitektur DMZ:

1. Mengurangi risiko jika server publik diserang
2. Mencegah penyerang masuk ke jaringan internal
3. Memisahkan trafik publik dan privat
4. Mempermudah monitoring dan logging keamanan

Dalam implementasi di Cisco Packet Tracer, DMZ biasanya dibuat menggunakan router dengan tiga interface (inside–DMZ–outside) dan ACL sebagai firewall.

BAB III

PERANCANGAN SISTEM / ARSITEKTUR

3.1 Gambaran Umum Perancangan Sistem

Perancangan sistem keamanan jaringan pada project ini bertujuan untuk membangun arsitektur yang mampu melindungi jaringan internal dari ancaman eksternal melalui implementasi Demilitarized Zone (DMZ) dan Firewall menggunakan aplikasi Cisco Packet Tracer. Perancangan dilakukan dengan mempertimbangkan aspek keamanan utama, yaitu kerahasiaan (confidentiality), integritas (integrity), dan ketersediaan (availability). Firewall digunakan untuk mengontrol lalu lintas data antar zona berdasarkan aturan keamanan (firewall rule) yang telah ditentukan.

Topologi yang dirancang bertujuan untuk:

1. Memisahkan jaringan internal dengan jaringan publik.
2. Menyediakan area netral (DMZ) untuk server yang diakses pengguna luar.
3. Menerapkan firewall sebagai pengontrol lalu lintas jaringan berdasarkan aturan keamanan yang ditentukan.

3.2 Arsitektur Jaringan yang digunakan

Arsitektur sistem keamanan jaringan dirancang menggunakan tiga lapisan utama:

3.2.1. Jaringan Eksternal (Public Network / Internet)

Merupakan area yang tidak terpercaya (untrusted network). Semua trafik dari jaringan ini akan melewati firewall sebelum mencapai DMZ atau jaringan internal.

3.2.2. Zona DMZ

Zona DMZ ditempatkan di antara Firewall dan Router, berisi server yang memang harus diakses oleh publik. Contoh layanan yang ditempatkan di DMZ:

a. Web Server
b. DNS Server

a. Mail Server
b. FTP Server

DMZ berfungsi untuk membatasi akses langsung ke jaringan internal.

3.2.3. Jaringan Internal (Private Network)

Berisi perangkat komputer user, printer, database server, atau sistem penting yang hanya boleh diakses oleh internal perusahaan.

Firewall akan memblokir semua akses dari luar menuju jaringan internal kecuali yang memiliki izin.

3.3 Firewall Rules

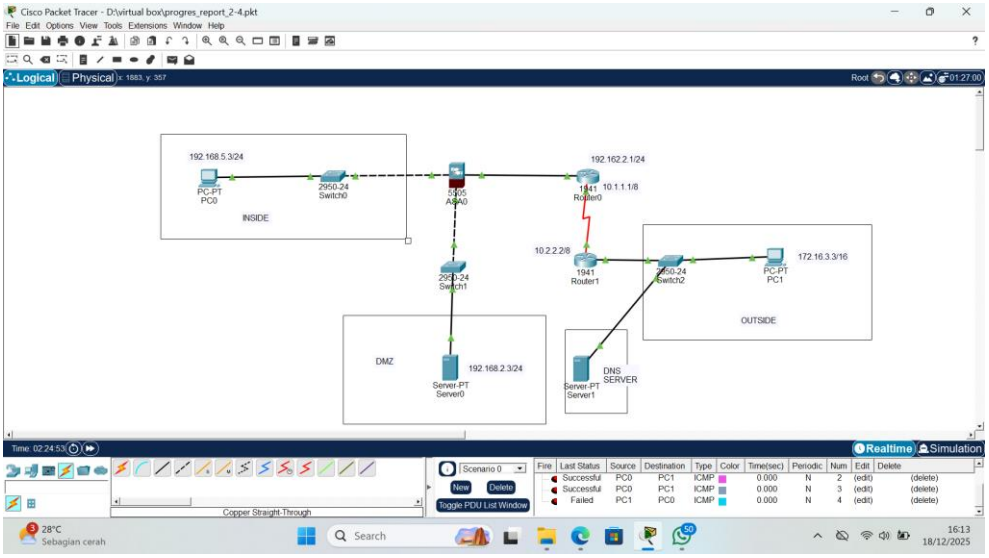
Firewall dikonfigurasi menggunakan **Access Control List (ACL)** untuk membatasi lalu lintas jaringan antar zona.

No	Source	Destination	Protocol	Port	Action	Keterangan
1	Any	Web Server (DMZ)	TCP	80	Allow	Publik Akses HTTP
2	LAN	Web Server (DMZ)	TCP	22	Allow	Admin SSH
3	LAN	Internet	TCP	80, 443	Allow	Akses browsing

Tabel 1. Tabel Konfigurasi Firewall

BAB IV
IMPLEMENTASI

4.1 Perancangan Topologi dan Pembagian IP

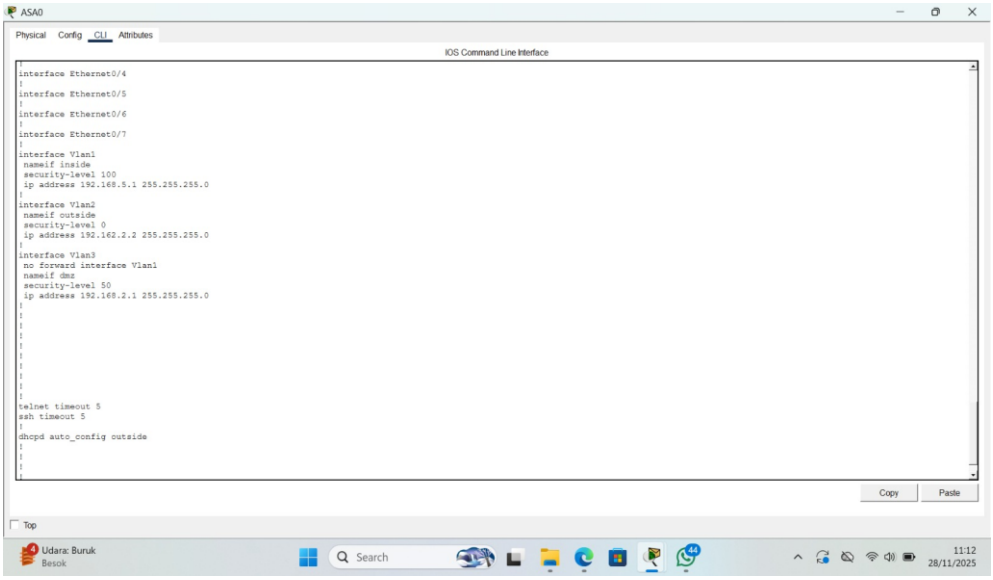


Gambar 1. Perancangan Topologi dan Pembagian IP

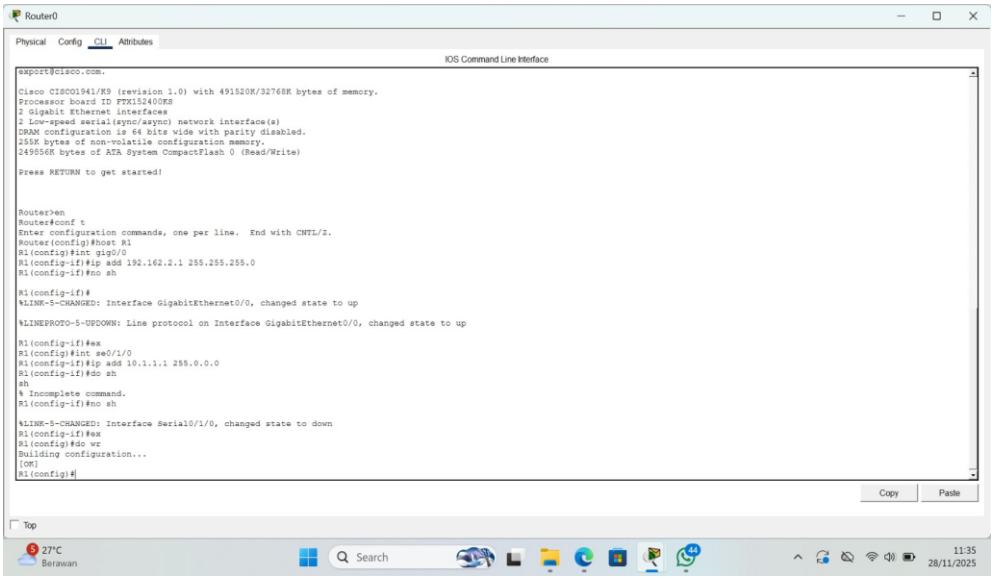
Implementasi jaringan dilakukan dengan membagi jaringan menjadi tiga zona utama: Inside, DMZ, dan Outside. Jaringan Inside digunakan untuk klien internal, Jaringan DMZ digunakan untuk menghosting server web, dan Jaringan Outside digunakan sebagai jaringan publik. Tujuan pembangunan zona ini adalah untuk meningkatkan keamanan jaringan dengan mencegah akses tidak sah ke jaringan internal.

Setiap perangkat memiliki alamat IP sesuai dengan zona jaringannya. Sementara jaringan DMZ dan Inside menggunakan alamat IP pribadi, jaringan Outside menggunakan alamat IP publik. Server web di DMZ memiliki alamat IP pribadi yang diubah menjadi alamat IP publik menggunakan mekanisme static NAT pada firewall ASA.

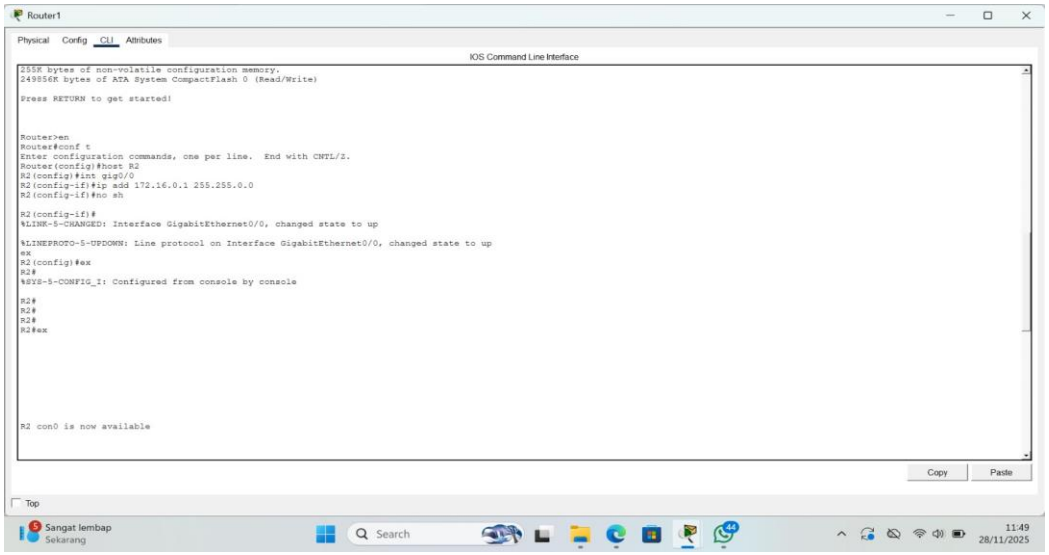
4.2 Konfigurasi Router dan VLAN



Gambar 2. Konfigurasi Router dan VLAN



Gambar 3. Konfigurasi Router dan VLAN

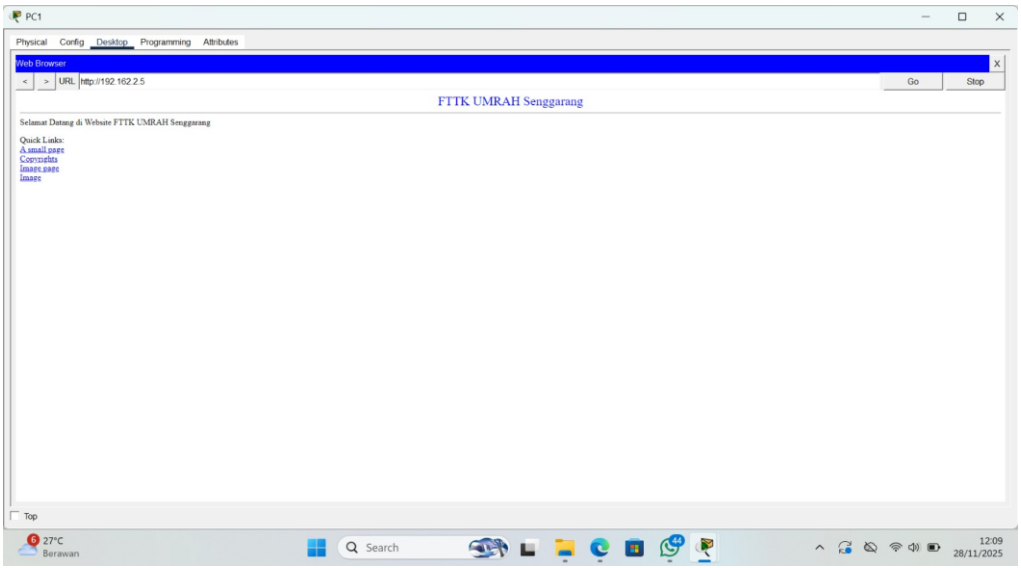


Gambar 4. Proses Konfigurasi

Berdasarkan tiga gambar di atas, konfigurasi routing dan VLAN dilakukan pada firewall ASA dan dua router yang terdapat dalam topologi pada fase ini. Firewall ASA dikonfigurasi dengan tiga antarmuka: inner (192.168.5.1/24), dmz (192.168.2.1/24), dan outside (192.162.2.2/24) untuk mengakses DMZ, zona internal, dan router eksternal.

Dua router lainnya dikonfigurasi dengan gateway IP di berbagai jaringan: router kiri, yang terhubung ke jaringan internal 192.168.5.0/24, router kanan, yang terhubung ke jaringan 172.16.3.0/16, dan jalur antar-router (10.1.1.0/8 dan 10.2.2.0/8). Dengan konfigurasi ini, semua perangkat saat ini telah terhubung melalui routing dasar, dan jalur antara zona (di dalam dan di luar DMZ) telah ditetapkan sehingga masing-masing dapat digunakan untuk langkah selanjutnya, yaitu deployment aturan server dan firewall.

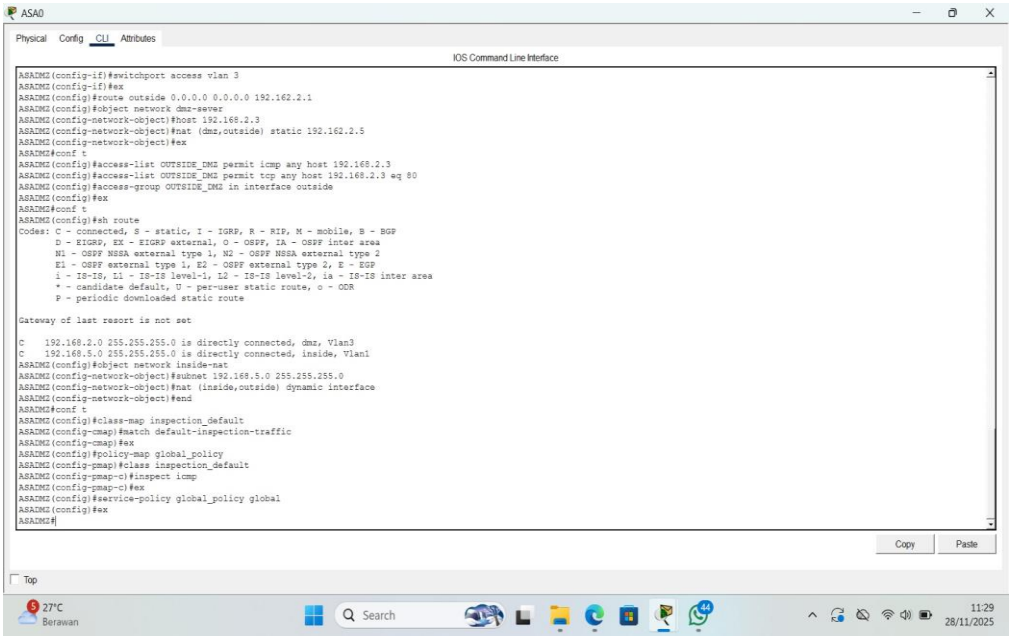
4.3 Deploy Web Server di DMZ



Gambar 5. Proses Deploy Web Server di DMZ

Pemasangan dan pengujian server web yang terletak di jaringan DMZ dilakukan pada fase ini. Server DMZ dikonfigurasi sebagai layanan publik menggunakan alamat IP 192.162.2.5 dan berhasil menampilkan halaman website bertuliskan “FTTK UMRAH Senggarang”, yang merupakan simulasi dari Fakultas Teknologi dan Teknologi UMRAH. Pengujian dilakukan melalui PC yang terhubung ke jaringan internal menggunakan URL http://192.162.2.5, dan hasil halaman web ditampilkan secara normal. Dengan demikian, fungsi DMZ dan server web dinyatakan beroperasi dengan lancar dan siap digunakan untuk fase berikutnya.

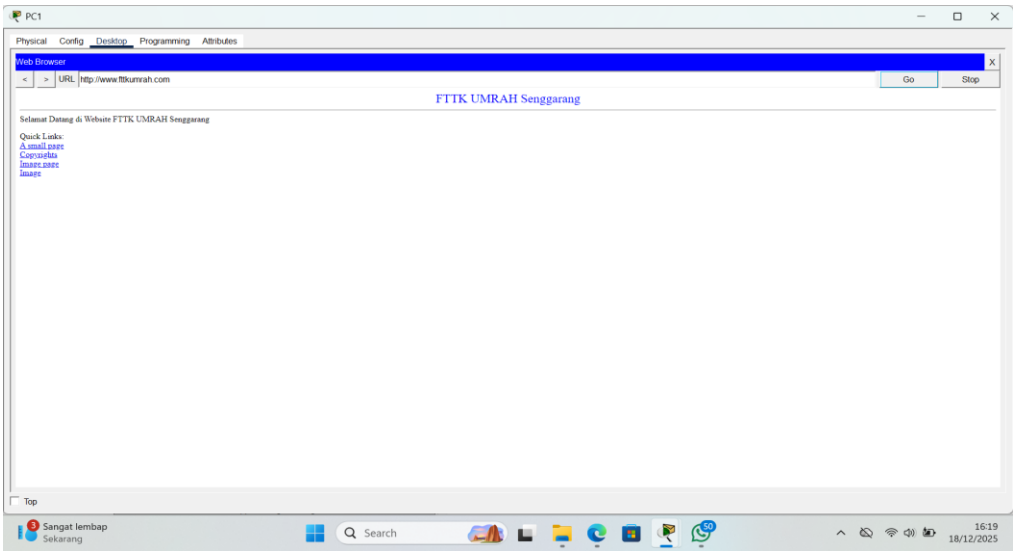
4.4 Konfigurasi Firewall ACL + NAT



Gambar 6. Konfigurasi Firewall ACL + NAT

Gambar tersebut menunjukkan konfigurasi Cisco ASA Firewall untuk mempublikasikan server internal ke internet melalui pengaturan Static NAT (memetakan IP 192.168.2.3 ke 192.162.2.5) dan Dynamic NAT untuk akses internet jaringan lokal. Konfigurasi ini dilengkapi dengan Access Control List (ACL) yang secara spesifik membuka Port 80 (HTTP) agar layanan web server dapat diakses publik, serta aktivasi ICMP Inspection untuk mengizinkan fungsi pengujian jaringan (*ping*).

4.5 Tambahan DNS Server

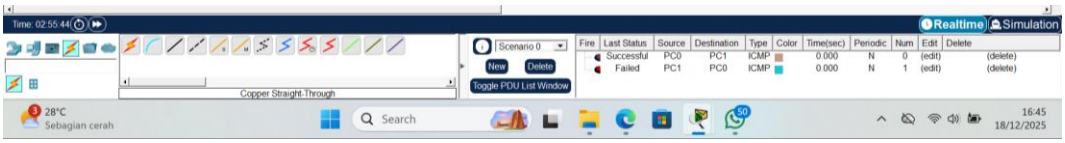


Gambar 7. Proses DNS Server

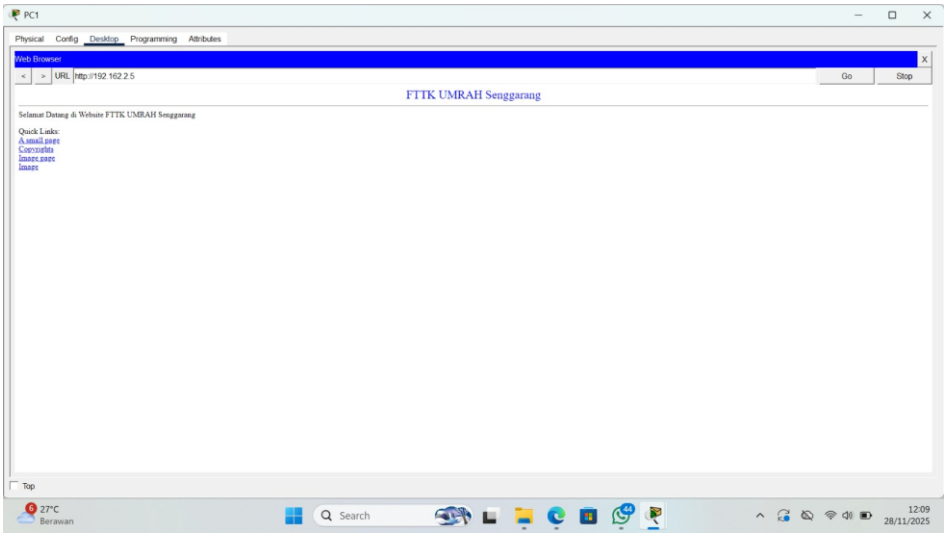
Server DNS ditempatkan di jaringan luar agar resolusi nama domain dapat dilakukan tanpa harus melewati firewall untuk mencapai DMZ. Server DNS dikonfigurasi untuk memetakan domain www.fttkumrah.com ke alamat IP publik yang dihasilkan dari NAT pada server web. Setiap klien, baik dari jaringan internal maupun eksternal, diarahkan ke server DNS ini untuk melakukan resolusi nama.

BAB V
PENGUJIAN DAN ANALISIS

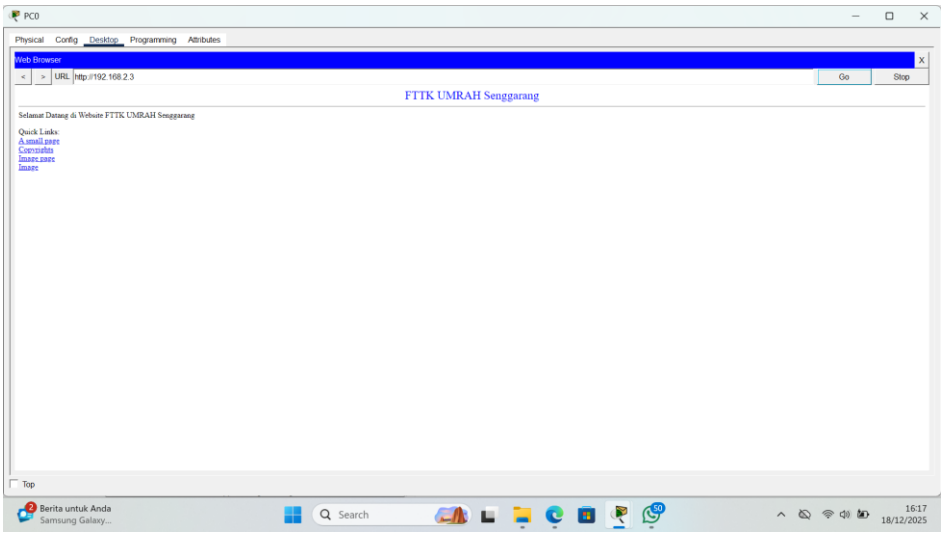
5.1 Pengujian



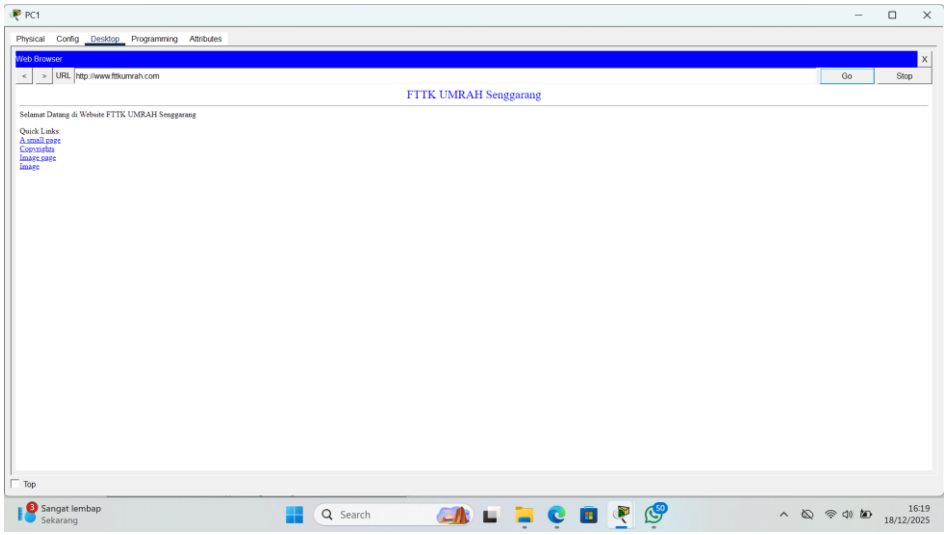
Gambar 8. Keterangan Analisis Proses Pengujian



Gambar 9. Tampilan Hasil Pengujian



Gambar 10. Hasil



Gambar 11. Hasil Konfigurasi

Konfigurasi ini menggunakan sistem Tingkat Keamanan Cisco ASA, yang secara otomatis mengizinkan jaringan Internal terhubung ke jaringan Eksternal sambil memblokir akses ke area lain, seperti Port 80, yang dibuka melalui ACL untuk mengizinkan akses publik ke situs web (HTTP) di server DMZ. Dalam hal ini, Port 80 berfungsi sebagai saluran komunikasi web yang tidak terenkripsi, yang diperkuat oleh server DNS untuk memungkinkan pengguna mengakses server menggunakan nama domain daripada hasil IP publik dari NAT.

5.2 Analisis

Berdasarkan hasil pengujian yang telah dilakukan, sistem jaringan yang dibangun menggunakan Cisco ASA Firewall ini telah berjalan sepenuhnya sesuai dengan tujuan fungsional dan keamanan yang direncanakan. Keberhasilan ini dapat dianalisis melalui tiga aspek utama:

1. **Keberhasilan Publikasi Layanan (Layanan Web DMZ)**

   Tujuan utama sistem ini adalah untuk mempublikasikan server web agar dapat diakses dari luar jaringan. Hal ini dicapai melalui penggunaan Static NAT, yang memetakan alamat IP pribadi 192.168.2.3 ke alamat IP publik 192.162.2.5. Penggunaan Port 80 (HTTP) sebagai titik masuk

utama dalam aturan Daftar Kontrol Akses (ACL) telah terbukti efektif karena protokol ini merupakan standar komunikasi web yang memungkinkan browser klien meminta data dari server. Dengan hanya membuka port 80, firewall menjalankan fungsi hak akses minimal, yaitu hanya membuka akses yang benar-benar diperlukan dan menutup celah serangan pada port lain.

2. **Efisiensi Routing Internal dan Resolusi Nama**

   Pengujian menunjukkan bahwa komputer di dalam jaringan (Inside PCs) dapat mengakses server web menggunakan alamat IP pribadi. Hal ini membuktikan bahwa konfigurasi routing internal benar, di mana lalu lintas antara zona lokal (Inside ke DMZ) tidak perlu diproses melalui NAT publik, sehingga mengurangi latensi dan beban kerja firewall. Integrasi server DNS sangat penting untuk kenyamanan pengguna; sistem berhasil mengarahkan nama domain ke alamat IP yang relevan secara kontekstual, sehingga pengguna tidak perlu mengetahui kompleksitas perubahan alamat IP di latar belakang.

3. Keamanan dan Integritas Jaringan (Security Levels)

Analisis keamanan menunjukkan bahwa sistem pertahanan berfungsi secara asimetris sesuai dengan desainnya. Melalui penerapan Tingkat Keamanan, PC Inside (tingkat tinggi) memiliki fleksibilitas untuk mengakses internet (Outside), namun sebaliknya, jaringan Outside (tingkat rendah) secara otomatis ditolak oleh firewall saat mencoba masuk ke jaringan Inside. Satu-satunya “celah” yang diizinkan adalah jalur ke DMZ melalui port 80. Selain itu, aktivasi Inspeksi ICMP memungkinkan fungsi pengujian jaringan (ping) berjalan secara dua arah secara cerdas tanpa mengorbankan keamanan, karena firewall mampu mengenali paket balasan sebagai bagian dari koneksi yang sah.

BAB VI
KESIMPULAN DAN SARAN

6.1 Kesimpulan

Berdasarkan hasil perancangan, implementasi, dan pengujian yang telah dilakukan, dapat disimpulkan bahwa penerapan Demilitarized Zone (DMZ) dan Firewall menggunakan Cisco Packet Tracer berhasil diterapkan sesuai dengan tujuan yang direncanakan. Pembagian jaringan ke dalam tiga zona, yaitu jaringan internal, DMZ, dan jaringan eksternal, mampu meningkatkan keamanan dengan memisahkan layanan publik dari jaringan internal.

Server web yang ditempatkan pada zona DMZ dapat diakses oleh pengguna luar tanpa memberikan akses langsung ke jaringan internal. Konfigurasi Cisco ASA Firewall dengan Access Control List (ACL) dan Network Address Translation (NAT) terbukti efektif dalam mengatur lalu lintas jaringan, di mana hanya port yang diperlukan saja yang dibuka. Hasil pengujian menunjukkan bahwa jaringan internal dapat mengakses internet, sementara akses dari luar ke jaringan internal berhasil diblokir, sehingga aspek keamanan jaringan dapat terjaga dengan baik.

6.2 Saran

Untuk pengembangan selanjutnya, sistem keamanan jaringan yang telah dibangun dapat ditingkatkan dengan menambahkan mekanisme keamanan lanjutan seperti Intrusion Detection System (IDS) atau Intrusion Prevention System (IPS) agar mampu mendeteksi dan mencegah serangan jaringan secara lebih optimal. Selain itu, layanan web pada server DMZ disarankan menggunakan protokol HTTPS guna meningkatkan keamanan data selama proses komunikasi. Pengujian sistem pada perangkat jaringan fisik serta penerapan monitoring lalu lintas jaringan juga dapat dilakukan agar sistem keamanan yang diterapkan lebih mendekati kondisi implementasi di dunia nyata.

DAFTAR PUSTAKA

Stallings, W. (2020). *Cryptography and Network Security: Principles and Practices.*

Kurose, J. F., & Ross, K. W. (2017). *Computer Networking: A Top-Down Approach*

Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). *Zero Trust Architecture (NIST Special Publication 800-207).* National Institute of Standards and Technology (NIST).

Ernawati, T., Kholid, I., Dahlan, & Rohmayani, D. (2024). *Case Study in Network Security System Using Random Port Knocking Method on The Principles of Availability, Confidentiality and Integrity.* Jurnal Online Informatika, 9(1), 2024.

Hasibuan, et al. (2021) *Penggunaan Cisco Packet Tracer sebagai Media Simulasi Pembelajaran Jaringan Komputer.* Jurnal Ilmiah Teknologi Informasi Terapan, 5(2), 2021.

Sari, A. M., & Gunawan, T. (2024). *Analisis Pengamanan Jaringan Menggunakan Zona Demiliterisasi (DMZ).* Jurnal Sistem & Teknologi Informasi, 12(1), 2024.

Putra, R., & Prasetyo, E. (2023). *Implementasi Firewall dan NAT pada Jaringan Komputer untuk Keamanan Sistem Informasi.* Jurnal Teknologi Informasi dan Keamanan Komputer, 4(2), 2023.