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

Laporan Sementara Praktikum Jaringan Komputer

Firewall dan NAT

Nur Rahman Fauzan - 5024231069

Sabtu, 31 Mei 2025

1 Latar Belakang

Seiring meluasnya penggunaan jaringan komputer dalam lingkungan kampus, perusahaan, dan institusi publik, perlindungan terhadap akses jaringan menjadi semakin krusial. Internet memberikan kemudahan akses informasi, tetapi sekaligus membuka celah bagi serangan siber seperti hacking, malware, dan akses tidak sah. Tanpa mekanisme proteksi yang memadai, setiap perangkat di dalam jaringan internal rentan terhadap ancaman eksternal.

Firewall adalah komponen utama yang bertindak sebagai *satpam digital*, memastikan bahwa hanya lalu lintas yang diizinkan oleh kebijakan organisasi yang boleh melintas di antara jaringan internal dan dunia luar. Selain itu, keterbatasan ruang alamat IPv4 memaksa hampir semua jaringan modern menerapkan *Network Address Translation* (NAT) agar banyak perangkat lokal dapat berbagi satu alamat publik. Untuk mendukung kedua fungsi tersebutkeamanan dan translasi alamatfitur *Connection Tracking* diperlukan agar firewall mengetahui status setiap koneksi dan NAT dapat menerjemahkan alamat dengan benar.

Modul ini membahas tiga topik utama:

1. **Firewall:** Definisi, jenis-jenis (Packet Filtering, Stateful Inspection, Application Layer, Next-Generation, Circuit Level, Software, Hardware, dan Cloud), serta cara kerjanya (kebijakan *Accept*, *Reject*, dan *Drop*).

2. **Network Address Translation (NAT):** Prinsip NAT sebagai solusi kekurangan alamat IPv4, tipe-tipe NAT (*Static*, *Dynamic*, dan *Port Address Translation/PAT*), serta istilah-istilah penting (Inside Local, Inside Global, Outside Local, Outside Global).

3. **Connection Tracking:** Konsep pelacakan koneksi yang memungkinkan firewall mempertahankan status koneksi (STATE), sehingga paket balasan dapat dikenali dan diterima secara otomatis, serta manfaatnya dalam meningkatkan keamanan dan efisiensi NAT.

Dengan memahami ketiga topik ini secara mendalam, diharapkan mahasiswa mampu merancang kebijakan keamanan yang tepat, melakukan konfigurasi NAT dengan benar, serta memastikan router atau firewall dapat mengelola koneksi jaringan secara cerdas.

2 Dasar Teori

2.1 Firewall

2.1.1 Definisi

Firewall adalah *perangkat lunak* atau *perangkat keras* yang bertindak sebagai penjaga gerbang (*gatekeeper*) di antara jaringan internal dan jaringan eksternal (internet). Setiap paket data yang berusaha masuk atau keluar jaringan diperiksa terhadap sekumpulan

aturan (policy). Jika paket memenuhi aturan, maka diizinkan lewat, sebaliknya paket diblokir. Aturan tersebut dapat berupa alamat IP sumber/destinasi, port TCP/UDP, dan protokol yang digunakan.

Sebelum adanya firewall, keamanan jaringan umumnya hanya mengandalkan *Access Control List* (ACL) pada router, yang hanya melakukan filter berbasis IP/port tanpa mengetahui konteks koneksi. Dengan ledakan penggunaan internet dan kompleksitas serangan siber, diperlukan firewall yang lebih canggih untuk melindungi jaringan internal.

2.1.2 Jenis-Jenis Firewall

1. **Packet Filtering** Melakukan pemeriksaan satu per satu paket data berdasarkan alamat IP sumber/tujuan, port sumber/tujuan, dan protokol. Karena tidak memahami konteks koneksi, jenis ini bersifat *stateless* dan cukup kaku.
    - Kelebihan: Sederhana, kinerja tinggi, implementasi di layer jaringan (layer 3/4).
    - Kekurangan: Tidak mengenali apakah paket termasuk balasan dari koneksi sah atau bukan.
2. **Stateful Inspection** Lebih canggih, firewall ini memelihara *state table*rekaman detail setiap koneksi yang sah (state). Ketika paket datang, firewall memeriksa tabel koneksi untuk menentukan apakah paket tersebut bagian dari koneksi yang sudah diizinkan. Jika cocok, paket diizinkan; jika tidak, diblokir.
    - Kelebihan: Mampu mengikuti status koneksi, menolak paket tampungan (spoofing).
    - Kekurangan: Memerlukan lebih banyak memori untuk menyimpan *state table*.
3. **Application Layer Firewall** Bekerja hingga lapisan aplikasi (layer 7). Firewall jenis ini dapat *memeriksa isi* paket sampai ke konten aplikasi seperti HTTP, FTP, SMTP, dan bahkan memblokir URL atau pola tertentu. Biasanya diimplementasikan sebagai proxy yang menerima permintaan dari klien, memprosesnya, lalu meneruskan ke server sebenarnya.
    - Kelebihan: Kontrol granular hingga konten aplikasi, mampu deteksi serangan aplikasi (misalnya SQL injection).
    - Kekurangan: Overhead tinggi, memerlukan sumber daya CPU/memori besar.
4. **Next-Generation Firewall (NGFW)** Paduan antara stateful inspection dan kemampuan *deep packet inspection* (DPI). NGFW tidak hanya memeriksa header, tetapi juga payload, termasuk analisis enkripsi SSL/TLS. Fitur tambahan meliputi pencegahan intrusi (IPS), kontrol aplikasi, dan integrasi layanan keamanan (misalnya threat intelligence).
    - Kelebihan: Proteksi multi-lapisan, deteksi malware/serangan canggih, segmentasi lalu lintas aplikasi.

- Kekurangan: Harga tinggi, konfigurasi kompleks, memerlukan hardware kelas atas.

5. **Circuit Level Gateway** Bekerja pada lapisan koneksi (session). Firewall jenis ini memeriksa apakah koneksi TCP/UDP sah, tetapi tidak memeriksa isi paket secara mendalam. Circuit level gateway mencatat sesi koneksi (misalnya handshake TCP), kemudian mengizinkan aliran data pada sesi tersebut tanpa inspeksi lebih lanjut.
    - Kelebihan: Lebih cepat daripada application layer, memberikan sedikit konteks sesi.
    - Kekurangan: Tidak dapat mendeteksi konten berbahaya di dalam sesi; malware masih bisa lolos.
6. **Software Firewall** Firewall yang dipasang di level host (komputer atau server). Biasanya berupa aplikasi yang berjalan di sistem operasi, memeriksa lalu lintas yang masuk/keluar melalui host tersebut. Cocok untuk perlindungan endpoint, tetapi memerlukan instalasi dan konfigurasi di tiap perangkat.
    - Kelebihan: Fleksibel, kontrol per-application, pembaruan mudah.
    - Kekurangan: Mengonsumsi sumber daya host (CPU/RAM), potensi konflik dengan aplikasi lain.
7. **Hardware Firewall** Perangkat fisik khusus yang dipasang di antara jaringan internal dan internet. Berfungsi sebagai barikade pertama untuk menahan serangan sebelum mencapai perangkat internal. Sering kali terintegrasi dengan switch/router enterprise.
    - Kelebihan: Kinerja tinggi, isolasi fisik, hemat beban pada server.
    - Kekurangan: Biaya investasi awal tinggi, konfigurasi dan pemeliharaan memerlukan keahlian khusus.
8. **Cloud Firewall** Firewall yang dioperasikan di lingkungan cloud (misalnya *Firewall as a Service*). Cocok untuk organisasi yang banyak memanfaatkan layanan cloud publik/privat. Cloud firewall melindungi beban kerja virtual di cloud dan dapat diintegrasikan dengan kebijakan keamanan terpusat.
    - Kelebihan: Mudah skalasi, integrasi dengan infrastruktur cloud, tidak memerlukan perangkat fisik.
    - Kekurangan: Bergantung pada koneksi internet, mungkin biaya operasional berkelanjutan.

2.1.3 Cara Kerja Firewall

Setiap firewall menjalankan sekumpulan aturan (rule base) yang diurutkan menurut prioritas. Ketika sebuah paket data (baik masuk maupun keluar) tiba di firewall, maka proses pemeriksaannya mengikuti langkah-langkah berikut:

1. **Periksa Header:** Firewall membaca IP sumber, IP tujuan, port sumber, port tujuan, dan protokol (TCP/UDP/ICMP).

2. **Cek State (pada firewall stateful):** Jika paket adalah bagian dari koneksi yang sudah tercatat di *state table* (misalnya *established* atau *related*), maka paket diizinkan langsung (Accept). Jika tidak, firewall akan lanjut ke langkah berikutnya.

3. **Bandingkan dengan Rule Base:** Paket dibandingkan satu per satu dengan aturan di daftar kebijakan. Tiga tindakan umum yang dapat diambil:

    - **Accept:** Izinkan paket melewati firewall.
    - **Reject:** Blokir paket, tetapi kirim balasan ICMP *unreachable* atau TCP RST kepada pengirim.
    - **Drop:** Blokir paket tanpa memberi respons apa pun (silent drop).

4. **Log dan Audit (opsional):** Jika aturan mengharuskan pencatatan (*logging*), maka firewall akan menyimpan detail paket yang match ke sistem log untuk keperluan audit atau analisis.

5. **Forward atau Block:** Berdasarkan hasil evaluasi, paket diarahkan ke jaringan internal (jika *Accept*) atau langsung dibuang (jika *Reject/Drop*).

Dengan mekanisme di atas, firewall dapat menegakkan kebijakan keamanan yang telah ditetapkan oleh organisasi, misalnya memblokir akses dari subnet tertentu, mengizinkan layanan tertentu saja (misal HTTP/HTTPS), atau menolak semua koneksi masuk kecuali yang secara eksplisit diizinkan.

2.2 Network Address Translation (NAT)

2.2.1 Definisi dan Motivasi

Alamat IPv4 publik di internet bersifat terbatas (kira-kira 4,3 miliar). Namun, jumlah perangkat yang terhubung ke internet jauh melampaui angka tersebut. Untuk mengatasi keterbatasan tersebut, digunakan *Network Address Translation* (NAT), yaitu mekanisme yang memungkinkan banyak perangkat di jaringan lokal (yang memiliki alamat IP privat) dapat mengakses internet menggunakan satu (atau sekelompok) alamat IP publik.

Dengan NAT, router atau firewall yang menghubungkan jaringan internal ke internet akan menerjemahkan alamat IP lokal (private) menjadi alamat IP publik saat paket keluar, dan sebaliknya saat paket balasan dikembalikan dari internet.

2.2.2 Jenis-Jenis NAT

1. **Static NAT (One-to-One)** Setiap alamat IP privat dipetakan ke satu alamat IP publik yang sama secara tetap. Cocok untuk melayani server yang harus dapat dijangkau dari internet (misal web server atau VPN server).

- *Kelebihan:* Alamat tetap, mudah melakukan konfigurasi DNS publik.
- *Kekurangan:* Membutuhkan banyak alamat IP publik, kurang efisien bila jumlah perangkat privat banyak.

2. **Dynamic NAT** Alamat IP privat dipetakan ke alamat IP publik dari sebuah *pool* yang tersedia, secara dinamis. Ketika perangkat privat melakukan koneksi ke internet, NAT memilih sebuah IP publik yang masih bebas dari *pool*. Jika semua IP publik di pool telah terpakai, perangkat baru tidak dapat melakukan koneksi keluar hingga ada IP publik yang dilepas.

   - *Kelebihan:* Lebih efisien daripada static NAT karena alamat publik hanya dialokasikan saat dibutuhkan.
   - *Kekurangan:* Masih memerlukan beberapa IP publik, tidak cocok jika jumlah host yang simultan tinggi lebih banyak daripada jumlah IP publik di pool.

3. **Port Address Translation (PAT) atau NAT Overloading** Banyak alamat IP privat dapat berbagi satu alamat IP publik dengan membedakan nomor port TCP/UDP. PAT menambahkan port unik (misal port 61000, 61001, dst.) di sisi publik untuk setiap koneksi dari host privat. Server di internet tetap mengirim balasan ke alamat publik dan port tersebut, yang kemudian diterjemahkan kembali ke alamat IP dan port lokal yang sesuai.

   - *Kelebihan:* Sangat hemat alamat IP publik, biasa disebut NAT tipe Many-to-One.
   - *Kekurangan:* Ketika terlalu banyak koneksi simultan, NAT table dapat menjadi penuh; juga ada batas jumlah port (sekitar 65.000) per alamat publik.

2.2.3 Cara Kerja NAT

1. Ketika sebuah perangkat di jaringan lokal (misal IP privat 192.168.1.10) mengirim paket ke server di internet (misal 8.8.8.8:80), NAT router mengubah:

   - *Source IP* dari `192.168.1.10` menjadi `[IP_Publik_Router]`.
   - Jika menggunakan PAT, *Source Port* juga diubah menjadi nomor port unik (misal 62000).

2. Router mencatat mapping (tabel NAT) yang mencatat:

   $$(\text{Inside Local}, \text{Inside Global}, \text{Source Port}, \text{Translated Port})$$

   agar paket balasan dapat diteruskan ke perangkat privat yang benar.

3. Saat paket balasan dari server (8.8.8.8:80) kembali ke alamat `[IP_Publik_Router]:62000`, router melihat tabel NAT dan mengetahui bahwa paket ini harus diterjemahkan kembali menjadi:

$$(\text{Address: } 192.168.1.10, \text{ Port: } < portasal >)$$

kemudian diteruskan ke perangkat 192.168.1.10.

4. Jika dua perangkat di jaringan lokal (misalnya 192.168.1.10 dan 192.168.1.11) mengakses situs yang sama pada saat bersamaan dengan port yang sama (80), PAT membedakan koneksi dengan menambahkan port berbeda (misal 62000 untuk .10 dan 62001 untuk .11), sehingga paket balasan dapat diteruskan ke host yang tepat.

2.2.4 Istilah Penting di NAT

- **Inside Local Address:** Alamat IP yang digunakan perangkat di jaringan internal (biasanya alamat privat seperti 192.168.x.x).
- **Inside Global Address:** Alamat IP publik yang mewakili perangkat lokal saat berkomunikasi dengan internet.
- **Outside Local Address:** Alamat IP tujuan di luar jaringan, yang telah diterjemahkan oleh NAT agar sesuai konteks internal (jarang dipakai dalam deskripsi umum).
- **Outside Global Address:** Alamat IP asli dari tujuan di internet (misal alamat server 8.8.8.8).

2.3 Connection Tracking

2.3.1 Definisi

Connection Tracking adalah fitur yang mencatat setiap koneksi IP yang terjadi melalui router atau firewall. Setiap koneksitermasuk detail seperti alamat sumber, alamat tujuan, port sumber, port tujuan, protokol, dan status koneksi (*state*)ditelusuri dan disimpan dalam *state table*. Dengan demikian, ketika paket balasan tiba, sistem dapat mengenali bahwa paket tersebut termasuk dalam koneksi yang sah dan langsung mengizinkannya melewati firewall atau NAT tanpa evaluasi aturan yang sama sekali baru.

Fitur ini menjadikan firewall bersifat *stateful*, sehingga dapat membedakan paket baru, paket yang bagian dari koneksi yang sudah ada (*established/related*), dan paket yang tidak valid (*invalid*).

2.3.2 Cara Kerja Connection Tracking

1. Ketika sebuah perangkat (misal 192.168.1.10) mengakses website (misal server 8.8.8.8:80), router/firewall mencatat koneksi baru:

   Source: $192.168.1.10 : \langle porta \rangle$, Destination: $8.8.8.8 : 80$, Protocol: TCP, State: NEW.

2. Saat server 8.8.8.8 membalas (paket RETURN), maka koneksi tersebut dikenali sebagai *ESTABLISHED*. Firewall atau NAT langsung mengizinkan paket balasan tanpa memeriksa ulang aturan filtering yang berat.

3. Jika ada paket yang datang dari luar tanpa ada catatan koneksi yang cocok, maka paket tersebut dianggap *INVALID* dan dapat diblokir otomatis (Drop) tanpa pengecekan lanjutan.

4. Tabel koneksi (*state table*) terus diperbarui: koneksi yang sudah selesai atau tidak aktif akan dihapus setelah timeout tertentu, sehingga memori tidak terus membengkak.

2.3.3 Manfaat Connection Tracking

1. **Keamanan yang Lebih Baik:** Dengan mengenali status koneksi, firewall dapat memblokir paket yang tidak termasuk koneksi sah (misalnya paket spoofing atau scanning) lebih efisien.

2. **Dukungan NAT yang Efisien:** Karena NAT membutuhkan *mapping* alamat dan port untuk setiap koneksi, connection tracking membantu menjaga konsistensi tabel NAT sehingga paket balasan dapat diterjemahkan dengan benar.

3. **Pengurangan Beban Router:** Setelah koneksi dicatat, paket balasan cukup dicek pada state table tanpa perlu menyaring ulang aturan lengkap, sehingga proses filtering menjadi lebih cepat.

4. **Kontrol Detail Lalu Lintas:** Administrator dapat membuat aturan firewall yang bergantung pada status koneksi (NEW, ESTABLISHED, RELATED, INVALID), sehingga dapat memberikan izin lebih spesifik (misalnya hanya izinkan trafik ESTABLISHED ke dalam jaringan).

5. **Deteksi dan Pencegahan Koneksi Tidak Sah:** Paket yang tidak cocok dengan koneksi manapun (state = INVALID) dapat langsung dibuang, membantu mengurangi risiko serangan atau traffic anomali.

3 Tugas Pendahuluan

1. **Konfigurasi NAT pada Cisco agar Web Server Lokal (192.168.1.10:80) Dapat Diakses dari Internet.** Untuk memungkinkan server web ber-IP `192.168.1.10` (port 80) di jaringan lokal diakses dari internet, diperlukan konfigurasi *static NAT* (port forwarding) pada router Cisco. Pertama, tentukan interface mana yang menghadap lokal (diberi perintah `ip nat inside`) dan mana yang menghadap publik (`ip nat outside`). Misalnya, interface LAN (mengarah ke 192.168.1.0/24) diset sebagai *inside*, dan interface WAN (mengarah ke internet, memiliki IP publik) diset sebagai *outside*. Berikut contoh sintaks konfigurasi NAT untuk scenario ini:

```
interface FastEthernet0/1
ip address 192.168.1.1 255.255.255.0
ip nat inside
!
interface FastEthernet0/0
ip address 20.20.20.1 255.255.255.0
ip nat outside
!
ip nat inside source static tcp 192.168.1.10 80 20.20.20.1 80
```

cisco.com

. Komponen sintaks di atas adalah sebagai berikut:

- `ip nat inside source static tcp` Perintah untuk membuat translasi statis NAT untuk protokol TCP.
- `192.168.1.10 80` Alamat IP dan port *inside local*, yaitu IP privat server internal (192.168.1.10) dan port lokal 80 (HTTP) yang digunakan server tersebut.
- `20.20.20.1 80` Alamat IP dan port *inside global*, yaitu alamat IP publik dan port yang akan dipakai dari sisi luar. Dalam contoh ini menggunakan IP publik router (20.20.20.1) pada port 80. (Alternatifnya, dapat pula menggunakan kata kunci `interface` jika ingin menggunakan IP interface luar secara dinamis).

Dengan konfigurasi di atas, router akan selalu menerjemahkan alamat tujuan paket yang datang ke `20.20.20.1:80` menjadi `192.168.1.10:80`, sehingga pengguna dari internet dapat mengakses web server internal tersebut seolah-olah menggunakan IP publik cisco.com . Tentunya, selain NAT, pastikan juga terdapat rute menuju jaringan 192.168.1.0/24 di router, dan apabila ada mekanisme keamanan (ACL/firewall) di router, bukalah akses TCP port 80 ke server tersebut sesuai kebutuhan.

2. **Urutan Penerapan: Mana Lebih Dahulu, NAT atau Firewall?** Secara prinsip, **firewall sebaiknya diterapkan lebih dahulu** (atau setidaknya bersamaan) dibanding NAT dalam desain jaringan. Alasan teknisnya adalah bahwa NAT dan firewall memiliki fungsi berbeda: NAT bertugas menerjemahkan alamat IP (utama untuk mengatasi keterbatasan IPv4), sedangkan firewall bertugas menyaring/mengontrol lalu lintas berdasarkan kebijakan keamanan. NAT *bukan* fitur keamanan, dan tidak melakukan inspeksi paket atau penegakan policy seperti firewall networkengineering.stackexchange.com . Meskipun NAT dapat memberikan efek samping berupa tersembunyinya IP privat internal (karena dari luar hanya terlihat satu IP publik), hal ini tidak boleh menggantikan peran firewall dalam melindungi jaringan. Best practice jaringan menyarankan bahwa perangkat perbatasan (misal router gateway) seharusnya dipasangi aturan firewall/ACL pada interface yang menghadap internet untuk memblokir trafik yang tidak diinginkan, alih-alih mengandalkan NAT semata untuk

keamanan. Dengan kata lain, firewall lah yang menjadi garis pertahanan pertama terhadap serangan luar, sedangkan NAT hanyalah mekanisme translasi alamat networkengineering.stackexchange.com . Dari sisi urutan pemrosesan paket, firewall (misalnya implementasi ACL atau inspeksi stateful) biasanya akan memeriksa paket sesuai aturan keamanan, dan NAT akan menerjemahkan alamat/port jika aturan NAT terpenuhi. Menempatkan firewall logikanya sebelum NAT memastikan bahwa hanya trafik yang diperbolehkan yang akan diterjemahkan dan diteruskan. Sebagai ilustrasi, jika NAT diaktifkan tanpa firewall, semua koneksi yang menuju port yang di-NAT akan langsung diteruskan ke host internal, berpotensi membuka celah. Sebaliknya, jika firewall diterapkan lebih dulu, maka meskipun suatu alamat privat dipetakan melalui NAT, akses dari luar dapat dibatasi hanya untuk sumber dan jenis trafik yang diizinkan. Karena itu, penerapan firewall sebaiknya diprioritaskan. Singkatnya, NAT tidak boleh dianggap sebagai pengganti firewall NAT only adds complexity without increasing security (NAT justru menambah kompleksitas tanpa meningkatkan keamanan) networkengineering.stackexchange.com . Praktik terbaiknya adalah menerapkan kebijakan firewall terlebih dahulu untuk mengamankan jaringan, kemudian menerapkan NAT untuk keperluan alokasi/alamat IP publik sesuai kebutuhan.

3. **Dampak Negatif Jika Router Tidak Memiliki Aturan Firewall Sama Sekali.** Tanpa filter firewall, sebuah router akan memperbolehkan *nyaris seluruh* trafik melewati atau menuju ke jaringan internal secara bebas. Hal ini sangat berbahaya dari sisi keamanan. Ibaratnya, tidak memasang firewall sama dengan membiarkan pintu depan terbuka lebar semua orang dari internet bisa masuk ke jaringan tanpa halangan dan tanpa terdeteksi itsasap.com . Konsekuensi konkretnya antara lain: Rentan terhadap akses liar dan pembobolan: Sistem internal menjadi easy pickings bagi peretas itsasap.com . Penyerang dapat dengan mudah memindai IP publik dan menemukan layanan apapun yang berjalan di dalam jaringan (misal server web, database, RDP, dll.), lalu mencoba mengeksploitasinya. Tanpa firewall, tidak ada pembatas yang mencegah atau memonitor upaya tersebut. Hal ini dapat berujung pada pencurian data sensitif, penyusupan malware, ransomware, atau pengambilalihan kendali sistem internal oleh pihak tak berwenang itsasap.com itsasap.com . Tidak ada pembatasan terhadap trafik berbahaya: Router tanpa aturan ACL/firewall tidak akan memblokir trafik berbahaya seperti serangan DoS/DDoS, port scanning massal, dan paket-paket eksploit. Akibatnya, layanan di dalam jaringan dapat dengan mudah terganggu. Misalnya, serangan Denial of Service dari luar dapat menyedot bandwidth atau membanjiri router/host, menyebabkan kinerja jaringan turun drastis atau lumpuh. Meskipun NAT dinamis pada router secara default hanya mengizinkan balasan untuk koneksi outbound, penyerang masih bisa membanjiri koneksi (DDoS) ke IP publik tersebut, membuat layanan penting (seperti VoIP, server online) tidak dapat diakses security.stackexchange.com . Selain itu, tanpa egress filtering, malware di dalam jaringan bebas berkomunikasi ke luar (misal mengirim data curian) karena tidak ada aturan yang menahannya. Potensi kerusakan menyeluruh pada

jaringan: Ketiadaan firewall bisa berujung pada kolapsnya jaringan secara total apabila terjadi serangan besar. Misalnya, sebuah worm/virus dapat menyebar ke seluruh segmen internal tanpa terhalang, atau penjahat siber bisa mematikan seluruh operasi jaringan. Laporan menyebutkan bahwa salah satu skenario terburuk tanpa firewall adalah *total network collapse* di mana jaringan lumpuh dan bisnis terhenti secara katastropik itsasap.com . Selain downtime yang merugikan, biaya pemulihan dan kerugian data dapat sangat besar. Singkatnya, router tanpa firewall ibarat benteng tanpa gerbang. Dari sisi keamanan, ini jelas tidak layak. Semua trafik masuk maupun keluar dibiarkan begitu saja, sehingga jaringan rentan terhadap segala macam ancaman dari internet. Praktik ini melanggar prinsip keamanan dasar (*default deny*) dan membuka peluang eksploitasi terhadap setiap kelemahan yang ada. Oleh karena itu, memasang dan mengonfigurasi firewall (atau minimal ACL pada router) adalah keharusan untuk melindungi jaringan dari akses yang tidak sah dan serangan yang dapat terjadi kapan saja.

Pustaka

[1] Cisco Systems, *Configuring Network Address Translation and Static Port Address Translation to Support an Internal Web Server*. Cisco Support Document ID 12905, Updated April 9, 2007. [Online]. Available: `https://www.cisco.com/c/en/us/support/docs/long-reach-ethernet-lre-digital-subscriber-line-xdsl/asymmetric-digital-subscriber-line-adsl/12905-827spat.html`.

[2] JFL, Answer to “Do I get any security benefits by NATing a network that’s already behind a firewall?”, Network Engineering StackExchange, Nov.ă8ă2022. [Online]. Available: `https://networkengineering.stackexchange.com/a/80458`.

[3] Intelligent Technical Solutions, *3 Top Risks of Not Having a Firewall*, Blog Post, Oct.ă12ă2021. [Online]. Available: `https://www.itsasap.com/blog/3-top-risks-of-not-having-a-firewall`.