

Keamanan Jaringan, Segmentasi, dan Firewall

Membangun pola pikir engineering untuk mengendalikan aliran jaringan

Posisi Materi dalam RPS

Sub-CPMK 6

Mahasiswa mampu **menganalisis lalu lintas jaringan** serta **menyusun segmentasi dan aturan firewall dasar**.

Kata kunci teknis

- Network security dan trust boundary
- Segmentasi, VLAN, subnet, ACL
- Firewall stateful dan default deny
- IDS/IPS, telemetry, packet analysis
- VPN dan secure communication

Pola pikir utama

- 1 Mulai dari **kebutuhan aliran data**.
- 2 Definisikan **zona dan batas kepercayaan**.
- 3 Buat policy dengan owner dan tujuan.
- 4 Verifikasi dengan packet evidence.

Materi ini mengembangkan dokumen Minggu 6: keamanan jaringan, segmentasi, firewall, IDS/IPS, VPN, dan packet analysis.

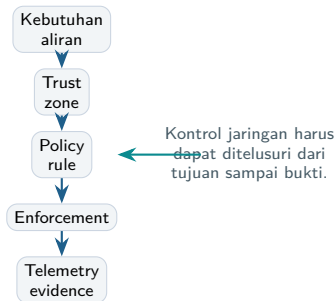
Masalah Engineering: Bukan Sekadar “Tutup Port”

Pertanyaan yang salah

- Port apa saja yang harus diblok?
- Firewall rule apa yang paling aman?
- Apakah VLAN sudah cukup?

Pertanyaan engineering yang benar

- Aliran data apa yang benar-benar dibutuhkan?
- Siapa source, destination, service, owner, dan tujuannya?
- Di mana trust boundary dan enforcement point?
- Bagaimana membuktikan allow dan deny bekerja?



Prinsip pengarah

**ALLOW rule = source + destination + service + direction
+ purpose + owner**

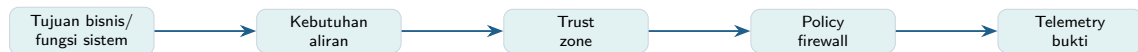
Capaian Pembelajaran Mingguan

- 1 Memetakan **aliran data** dan **trust boundary** pada arsitektur jaringan.
- 2 Menjelaskan peran **segmentasi**, **firewall**, **IDS/IPS**, **VPN**, dan protokol aman.
- 3 Menganalisis **metadata paket** pada capture yang disediakan.
- 4 Menulis aturan berbasis kebutuhan dengan prinsip **default deny**.

Target pemahaman

Mahasiswa tidak hanya dapat menjalankan tool, tetapi dapat menjelaskan **mengapa satu aliran diizinkan, mengapa aliran lain ditolak, dan bukti paket apa yang mendukung klaim tersebut.**

Model Berpikir: Dari Tujuan ke Telemetry



Jika aliran tidak memiliki tujuan, pemilik, dan bukti uji, maka rule tersebut tidak layak dianggap kontrol engineering.

Contoh buruk

Allow any dari user network ke server network karena “nanti aplikasi error”.

Contoh baik

Allow user-zone ke web:443 untuk akses portal akademik; owner: akademik; logging: enabled; negative test: user-zone ke DB ditolak.

Trust Zone dan Trust Boundary

Trust zone

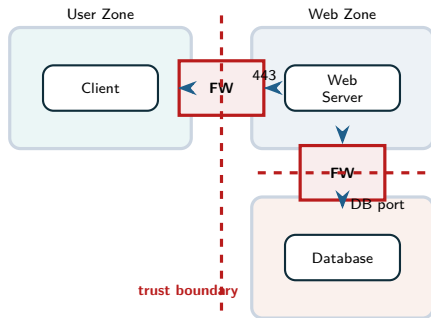
Kumpulan aset dengan tingkat kepercayaan, fungsi, sensitivitas, dan kontrol yang relatif serupa.

Trust boundary

Batas tempat asumsi keamanan berubah: dari user ke web, dari web ke aplikasi, dari aplikasi ke database, dari admin ke server.

Engineering implication

- Boundary harus punya enforcement.
- Enforcement harus punya telemetry.
- Telemetry harus punya pemilik triage.



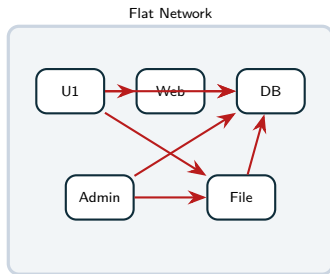
Segmentasi: Mengurangi Jalur Komunikasi dan Blast Radius

Tujuan segmentasi

- Membatasi siapa boleh berbicara dengan siapa.
- Mengurangi lateral movement.
- Melindungi aset sensitif.
- Memudahkan monitoring dan audit.

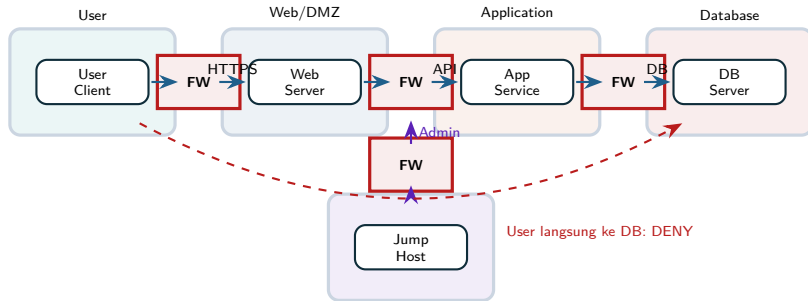
Basis segmentasi

- Fungsi: user, web, app, DB, management.
- Sensitivitas: public, internal, confidential.
- Risiko: lab, produksi, DMZ, third-party.
- Identitas: user, service account, device posture.



Terlalu banyak jalur;
blast radius besar.

Ilustrasi Segmentasi Bertingkat



Makna engineering

Setiap zona memiliki fungsi dan risiko. Setiap perpindahan zona harus melewati policy enforcement dan menghasilkan bukti yang dapat diperiksa.

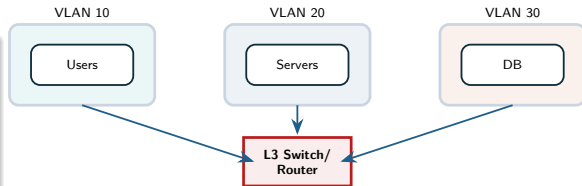
VLAN Bukan Otomatis Segmentasi Keamanan

VLAN

Membagi domain broadcast pada Layer 2. VLAN membantu organisasi jaringan, tetapi belum cukup sebagai kontrol keamanan jika routing antar-VLAN terlalu bebas.

Segmentasi keamanan

Memerlukan policy enforcement, default deny, allow rule spesifik, logging, dan uji lintas zona.



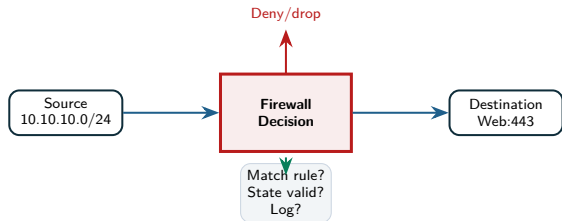
Jika inter-VLAN routing = allow any, maka segmentasi keamanan gagal.

Firewall: Policy Enforcement Point

Firewall bukan sekadar perangkat, tetapi **titik keputusan**. Ia menentukan apakah paket/aliran boleh melewati batas.

Dimensi aturan firewall

- Source dan destination.
- Service/port/protocol.
- Direction dan state.
- Purpose, owner, expiry.
- Logging dan acceptance test.



Aturan minimum yang baik

```
ALLOW user-zone -> web-zone TCP/443  
purpose=portal owner=BAAK log=enabled expiry=review-6mo
```

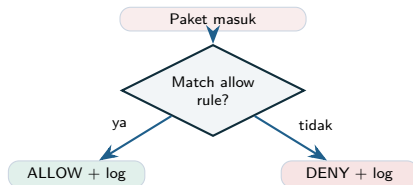
Default Deny: Aman karena Tidak Mengandalkan Keberuntungan

Default allow

Semua diizinkan kecuali yang dilarang. Masalah: kita harus tahu semua hal buruk yang mungkin terjadi.

Default deny

Semua ditolak kecuali yang dibutuhkan dan disetujui. Ini lebih sesuai dengan engineering control karena rule dapat diuji satu per satu.



Formula praktis

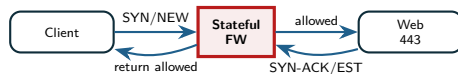
Policy yang baik bukan yang paling banyak rule, melainkan yang **paling sedikit membuka jalur** tetapi tetap memenuhi fungsi sistem.

Stateful Firewall: Memahami Status Koneksi

Firewall stateful mengingat status koneksi. Ini penting agar return traffic dari sesi sah diizinkan tanpa membuka rule dua arah secara kasar.

Contoh HTTPS

- Client memulai koneksi ke web:443.
- Firewall mencatat state: NEW -> ESTABLISHED.
- Paket balasan diterima karena bagian dari sesi yang valid.



State table:

source, destination, port, protocol, sequence, timeout

Kesalahan umum

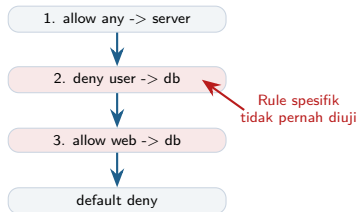
Membuat allow dua arah tanpa memahami state dapat memperbesar attack surface secara tidak perlu.

Rule Order dan Shadowed Rule

Firewall mengevaluasi rule secara berurutan. Rule umum yang diletakkan terlalu awal dapat menutupi rule spesifik di bawahnya.

No	Rule	Efek
1	allow any -> server	Terlalu luas
2	deny user -> db	Tidak pernah kena
3	allow web -> db	Tidak berarti

Rule 2 dan 3 menjadi **shadowed** oleh Rule 1.



Merancang Policy: Dari Data Flow ke Rule

Aliran	Policy	Bukti uji
User ke portal	Allow user-zone ke web:443	TLS handshake dan HTTP request sukses
Web ke aplikasi	Allow web identity ke app API	Request aplikasi sah berhasil
Aplikasi ke DB	Allow app identity ke DB port	Query sah berhasil; user langsung ditolak
Admin ke server	Allow jump host + MFA	Sesi admin tercatat
Antarzona lain	Default deny	Paket uji ditolak dan dilog

Acceptance test

Setiap rule harus punya dua jenis pengujian: **positive test** untuk aliran yang boleh dan **negative test** untuk aliran yang harus ditolak.

Positive Test dan Negative Test

Positive test

Membuktikan fungsi yang sah tetap berjalan.

- User bisa akses web:443.
- Web bisa akses app API.
- App bisa akses database.
- Admin bisa lewat jump host.

Negative test

Membuktikan jalur yang tidak sah ditolak.

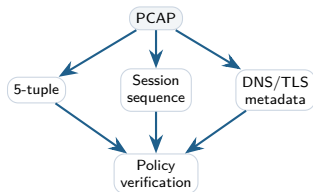
- User langsung ke DB ditolak.
- Web ke management ditolak.
- Third-party ke internal subnet ditolak.
- Admin tanpa jump host ditolak.

Kontrol yang tidak diuji belum layak disebut kontrol.

Packet Analysis: Apa yang Kita Cari?

Metadata penting pada packet capture

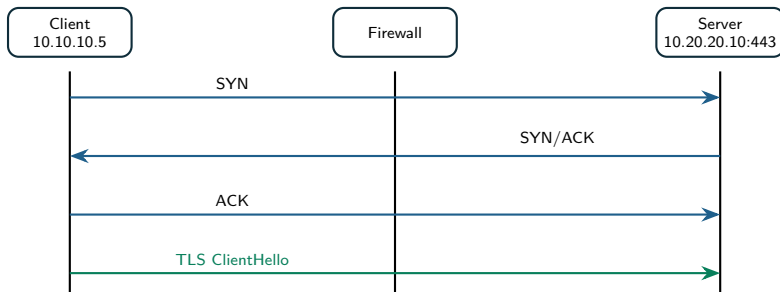
- 5-tuple: source IP, source port, destination IP, destination port, protocol.
- Urutan sesi: SYN, SYN/ACK, ACK, FIN/RST.
- DNS query dan response.
- TLS handshake metadata.
- Retransmission, reset, latency, packet loss.



Tujuan

Bukan membaca semua paket, melainkan mencari bukti apakah aliran sesuai dengan policy.

Ilustrasi TCP Handshake dan Bukti Koneksi



Jika policy allow benar, terlihat handshake sukses. Jika default deny bekerja, terlihat drop/timeout atau reset sesuai desain.

Apa yang Masih Tampak Saat Payload Terenkripsi?

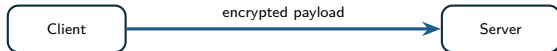
Tidak tampak

- Isi password/form.
- Isi file yang dikirim.
- Detail HTTP payload pada HTTPS.

Masih tampak

- Source dan destination IP.
- Port dan protokol.
- Waktu, ukuran paket, durasi sesi.
- DNS metadata, jika tidak dienkripsi.
- TLS handshake metadata tertentu.

Payload tidak dibaca, tetapi pola komunikasi masih dapat dianalisis.



Observer melihat metadata:
IP, port, timing, size, flow direction, handshake

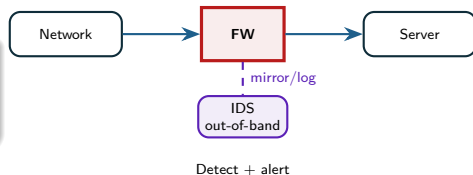
IDS dan IPS: Deteksi vs Tindakan Inline

IDS - Intrusion Detection System

Mendeteksi pola atau anomali, menghasilkan alert, tetapi tidak otomatis memblok traffic.

IPS - Intrusion Prevention System

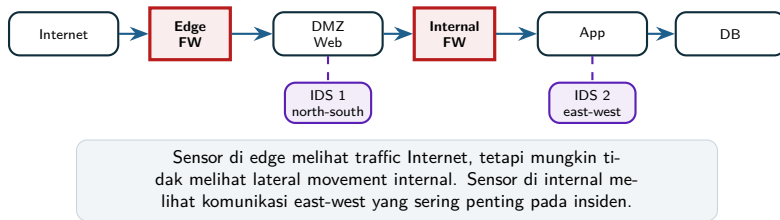
Berada inline dan dapat melakukan drop, reset, rate limit, atau block.



Masalah operasional

Alert tanpa konteks aset, tuning, sinkronisasi waktu, owner, dan playbook akan berubah menjadi noise.

Penempatan Sensor: Di Mana IDS/IPS Berguna?

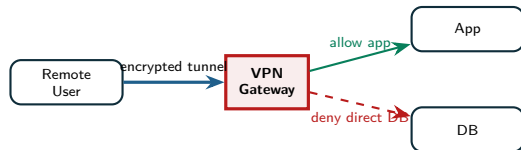


VPN: Tunnel Aman Bukan Izin Total

VPN melindungi jalur komunikasi, tetapi tidak otomatis membuat endpoint atau user menjadi terpercaya.

VPN tetap membutuhkan:

- Autentikasi kuat dan MFA.
- Otorisasi berbasis role.
- Posture check endpoint.
- Segmentasi setelah masuk VPN.
- Key management dan monitoring.



Kesalahan umum

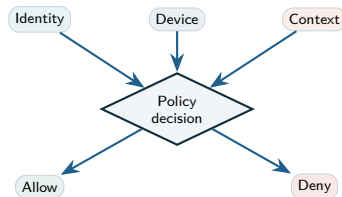
Memberikan akses VPN ke seluruh subnet internal sama saja memindahkan perimeter ke laptop pengguna.

Zero Trust sebagai Cara Berpikir, Bukan Produk

Zero Trust berarti akses tidak diberikan hanya karena user berada di jaringan internal.

Pertanyaan inti

- Siapa user atau service identity?
- Apakah device sehat dan dikelola?
- Aplikasi apa yang dibutuhkan?
- Apakah request sesuai konteks?
- Apakah telemetry mencukupi?



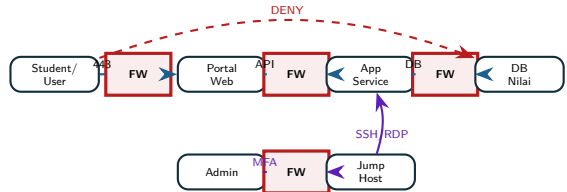
Contoh Terpandu: Kampus dengan Portal Akademik

Kebutuhan sistem

- Mahasiswa mengakses portal akademik via HTTPS.
- Web server memanggil app service.
- App service mengakses database nilai.
- Admin mengelola server lewat jump host.

Risiko utama

- User langsung mencoba akses database.
- Kompromi web bergerak ke jaringan internal.
- Admin credential disalahgunakan.



Checklist Policy Engineering

Sebelum membuat rule

- Apa fungsi bisnis/operasionalnya?
- Siapa owner aplikasi dan owner rule?
- Source dan destination tepat?
- Service/port/protocol tepat?
- Perlu waktu berlaku/expiry?

Setelah membuat rule

- Positive test berhasil?
- Negative test berhasil?
- Log muncul di tempat yang benar?
- Tidak ada rule shadowing?
- Ada review berkala?

Kriteria rule yang buruk

allow any any tanpa tujuan, owner, masa berlaku, logging, dan bukti uji.

Lab: Analisis PCAP dan Policy Violation

Aktivitas

Analisis file PCAP sintetis yang disediakan dosen menggunakan Wireshark. Identifikasi lima tuple, urutan sesi, DNS/TLS metadata, retransmission, dan satu aliran yang melanggar policy fiktif.

Langkah kerja

- 1 Buka PCAP dan identifikasi endpoint.
- 2 Filter per IP, port, dan protokol.
- 3 Rekonstruksi flow utama.
- 4 Cocokkan flow dengan policy.
- 5 Tandai evidence packet number.

Contoh filter Wireshark

```
ip.addr == 10.200.1.20
tcp.port == 443
dns
_tls || tcp.port == 443
tcp.analysis.retransmission
```

Capture hanya dilakukan pada sistem/data laboratorium yang memiliki izin eksplisit. Jangan melakukan capture pada jaringan publik atau pihak lain.

Bukti Minimum yang Harus Dipertahankan

- Scope, otorisasi, topologi, dan versi konfigurasi.
- Raw log atau observasi dengan identifier dan timestamp.
- Tabel analisis yang memisahkan bukti, asumsi, dan interpretasi.
- Hasil uji positif dan negatif terkait acceptance criterion.
- Anomali, keterbatasan, perubahan, rollback, dan residual risk.

Standar profesional

Jika klaim tidak dapat ditelusuri ke bukti, maka klaim tersebut lemah. Security engineering menuntut audit trail.

Tugas Mingguan

Deliverable

Serahkan dokumen singkat yang memuat:

- 1 Diagram zona jaringan.
- 2 Daftar aliran data yang dibutuhkan.
- 3 Enam aturan firewall tingkat kebijakan.
- 4 Dua negative test untuk membuktikan default deny.
- 5 Ringkasan bukti PCAP.
- 6 Penjelasan keterbatasan metadata terenkripsi.

Catatan mutu

Jangan hanya menggambar kotak dan panah. Setiap panah harus punya source, destination, service, direction, purpose, owner, dan acceptance test.

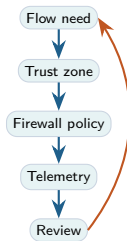
Pertanyaan Diskusi di Kelas

- ➊ Mengapa VLAN belum tentu segmentasi keamanan?
- ➋ Apa fungsi default deny pada desain jaringan?
- ➌ Bagaimana aturan firewall ditelusuri ke kebutuhan aplikasi?
- ➍ Apa perbedaan IDS dan IPS dari sisi posisi dan konsekuensi operasional?
- ➎ Data apa yang masih dapat dianalisis ketika payload terenkripsi?
- ➏ Dalam kasus kompromi web server, bagaimana segmentasi membatasi lateral movement?

Ringkasan Konsep

Yang harus diingat

- Mulai dari kebutuhan aliran, bukan daftar port.
- Segmentasi perlu enforcement dan uji lintas zona.
- Firewall rule harus spesifik, teruji, dan punya owner.
- IDS/IPS membutuhkan konteks, tuning, dan proses triage.
- VPN bukan izin bebas ke seluruh jaringan internal.



Referensi dan Bacaan Lanjutan

- 1 William Stallings, *Cryptography and Network Security: Principles and Practice*. Pearson.
- 2 Chuck Easttom, *Computer Security Fundamentals*. Pearson.
- 3 NIST Cybersecurity Framework (CSF) 2.0. <https://www.nist.gov/cyberframework>
- 4 NIST SP 800-41 Rev. 1, *Guidelines on Firewalls and Firewall Policy*.
<https://csrc.nist.gov/pubs/sp/800/41/r1/final>
- 5 Wireshark Foundation, *Wireshark User's Guide*.
https://www.wireshark.org/docs/wsug_html_chunked/

Pesan akhir

Keamanan jaringan yang matang adalah kombinasi desain arsitektur, policy yang eksplisit, enforcement yang benar, telemetry yang cukup, dan verifikasi berkala.