

Laporan KJK - Kelompok 6

ITS Secure Network Challenge

Anggota :

1. Angga Firmansyah - 5027241062
2. Ahmad Rafi Fadhillah Dwiputra - 5027241068
3. Fika Arka Nuriyah - 5027241071
4. Dimas Muhammad Putra - 5027241076

LAPORAN PROYEK KEAMANAN JARINGAN: WEEK 9

Topik: Rancangan Konsep Keamanan Sistem Jaringan (Zone-Based Architecture)

Departemen: Teknologi Informasi ITS

1. Filosofi Keamanan: "Zero Trust & Physical Segmentation"

Dalam merancang sistem pertahanan untuk Departemen Teknologi Informasi dengan topologi baru ini, kami mengadopsi filosofi "**Physical Isolation with Centralized Control**". Kami tidak hanya memisahkan jaringan secara logis (VLAN), tetapi secara fisik menggunakan router yang berbeda untuk setiap zona risiko.

Prinsip Utama: *Never Trust, Always Verify.*

Kami menerapkan tiga pilar utama dalam desain keamanan ini:

1. **Default Deny (Tolak Secara Default):** Secara default, *Mikrotik Firewall* dikonfigurasi dengan prinsip *Drop All* pada rantai *Forward*. Izin (*Accept*) hanya diberikan secara eksplisit untuk trafik yang didefinisikan legal.
2. **Physical Network Segmentation:** Berbeda dengan desain *Router-on-a-Stick* (satu router untuk semua), kami menggunakan **Router Dedikasi** untuk setiap zona (GuestR, StudentR, ADMR, AcademicR).
 - **Tujuan:** Isolasi kegagalan dan keamanan. Serangan DDoS pada router Guest tidak akan membebani CPU router Admin atau Akademik.
3. **Least Privilege Access:** Akses antar-zona dibatasi ketat di *Choke Point* (*Mikrotik*). Contoh: Mahasiswa boleh ke Internet, tapi tidak boleh "melihat" jaringan Admin sama sekali.

2. Zona & Klasifikasi Kepercayaan

Mengacu pada topologi fisik **Multi-Router**, jaringan diklasifikasikan menjadi 5 zona fisik yang bermuara pada satu titik pusat (*Mikrotik Firewall*).

Zona Keamanan	Subnet Terkait	Interface Firewall	Router Pengelola	Tingkat Trust	Profil Risiko & Kebijakan

Zona Edge (WAN)	Internet / Public	ether1	EdgeR	 Untrusted	Jaringan luar tak terkendali. Kebijakan: <i>NAT Masquerade & Drop Invalid Packets.</i>
Zona Guest	10.20.50.0/24	ether2	GuestR	 Untrusted	Risiko Ekstrem. Publik/Tamu. Kebijakan: Isolasi total (hanya ke Internet), <i>Bandwidth Limit</i> ketat.
Zona Student	10.20.10.0/24	ether3	StudentR	 Low	Risiko Tinggi (Malware). Kebijakan: Inspeksi trafik ketat, blokir akses ke Admin.
Zona Admin	10.20.40.0/24	ether4	ADM R	 High	Risiko Kritis. Manajemen Infrastruktur. Kebijakan: Akses penuh maintenance, <i>Logging</i> aktif.
Zona Academic	10.20.20.0/24 10.20.30.0/24	ether5	AcademicR	 Medium	Data Sensitif & Riset. Kebijakan: Hanya membuka port layanan spesifik (HTTPS/API).

3. Arsitektur Alur Trafik (Zone-Based Multi-Router)

Kami menggunakan pendekatan **Distributed Routing dengan Centralized Security**.

Dalam model ini, fungsi *routing* lokal didistribusikan ke router per-zona, namun keamanan dipusatkan di Mikrotik Firewall.

Diagram Logika Trafik

```
Internet((Internet)) <--> NAT1
NAT1 <--> EdgeR[Edge Router]
EdgeR <==>|ether1| Mikrotik[Mikrotik Firewall]

subgraph Zone: Guest
Mikrotik <==>|ether2| GuestR[Guest Router]
GuestR --- UserGuest((Guest User))

subgraph Zone: Student
Mikrotik <==>|ether3| StudentR[Student Router]
StudentR --- UserMhs((Mahasiswa))

subgraph Zone: Admin
Mikrotik <==>|ether4| ADMR[Admin Router]
ADMR --- UserAdm((Admin PC))

subgraph Zone: Academic
Mikrotik <==>|ether5| AcademicR[Academic Router]
AcademicR --- SrvAkad((Server/Riset))
```

Mekanisme Kontrol Trafik

1. Pusat Kontrol (Choke Point):
Mikrotik Firewall adalah satu-satunya jembatan antar-zona. Tidak ada kabel yang menghubungkan GuestR langsung ke StudentR. Semua paket harus "lapor" dulu ke Mikrotik.
2. **Alur East-West (Antar Departemen):**
 - **Skenario:** Mahasiswa akses Server Akademik.
 - **Jalur:** PC Mhs → StudentR → **Mikrotik (Filter Rule Check)** → AcademicR → Server.
 - **Keunggulan:** Jika Mikrotik memblokir, paket langsung dibuang sebelum menyentuh router Akademik.
3. **Alur North-South (Internet):**
 - Setiap Router Internal (StudentR, dll) memiliki *Default Route* (\$0.0.0.0/0\$) yang mengarah ke IP Interface Mikrotik.
 - Mikrotik meneruskan ke EdgeR, lalu EdgeR ke Internet.

4. Matriks Kebijakan Akses (Firewall Policy)

Aturan ini diimplementasikan pada menu **IP > Firewall > Filter Rules** di Mikrotik, menggunakan parameter **in-interface** (sumber) dan **out-interface** (tujuan)

No	Sumber (Source)	Tujuan (Destination)	Protokol / Port	Aksi	Justifikasi & Penyesuaian Topologi
1	Mahasiswa	Akademik	TCP 443 (HTTPS)	ALLOW	Mahasiswa mengakses portal akademik/LMS yang berada di server balik AcademicR.
2	Mahasiswa	Akademik	TCP 22, 3389, 445	DENY	Hardening: Mencegah upaya SSH/RDP dari jaringan mahasiswa ke server akademik.
3	Mahasiswa	Admin	ANY	DENY	Critical: Memastikan tidak ada paket dari StudentR yang bisa menyeberang ke ADMR.
4	Mahasiswa	Internet	TCP 80, 443, UDP 53	ALLOW	Akses internet standar. DNS diarahkan ke DNS Resolver (jika ada) atau Public.
5	Guest	Internal (All)	ANY	DENY	Isolasi Fisik & Logis: Paket dari GuestR langsung dibuang jika tujuannya bukan internet.
6	Guest	Internet	TCP 80, 443	ALLOW	Tamu hanya diizinkan browsing HTTP/HTTPS. Port lain diblokir untuk hemat bandwidth.

7	Admin	Semua Zona	SSH, RDP, ICMP	<input checked="" type="checkbox"/> ALLOW	Admin butuh akses penuh ke StudentR, AcademicR, dan GuestR untuk troubleshooting.
8*	Akademik	Riset & IoT	TCP 3306, 1883	<input checked="" type="checkbox"/> ALLOW	<i>Catatan:</i> Karena Riset & Akademik berada di balik router yang sama (AcademicR), trafik ini mungkin tidak melewati Mikrotik kecuali dikonfigurasi khusus (Hairpin NAT).
9	Riset & IoT	Internet	TCP 443, UDP 123	<input checked="" type="checkbox"/> ALLOW	IoT device mengirim data ke Cloud (API) dan sinkronisasi waktu (NTP).
10	ANY	ANY	ANY	<input type="stop"/> DENY	Implicit Deny: Rule terakhir ("Bawah") untuk menangkap dan mencatat (Log) semua trafik ilegal.

5. Strategi Pertahanan Berlapis (Defense in Depth)

Keamanan tidak hanya bertumpu pada firewall, melainkan diterapkan di setiap lapisan infrastruktur:

Layer 1 & 2: Access Security (Switch Level)

- Dedicated Routing Infrastructure:** Kami memitigasi risiko keamanan terbesar (jaringan Guest) dengan memberikan perangkat keras terpisah (GuestR dan Switch4). Ini mencegah beban trafik tamu mengganggu performa jaringan mahasiswa (StudentR) dan mencegah akses fisik antar-jaringan di level switch.
- Port Security:** Tetap diterapkan pada switch akses untuk mencegah *MAC Flooding*.

- **DHCP Snooping:** (Opsional) Mencegah pemasangan router liar (*Rogue DHCP Server*) di jaringan akses.

Layer 3: Network Security (Internal Router Level)

- **Routing Control:** Router internal (**StudentR**, **AcademicR**) dikonfigurasi hanya untuk meneruskan trafik ke hulu (pfSense), mencegah *asymmetric routing*.
- **Local ACL (Sanity Check):** Memblokir trafik dengan *Source IP Spoofing* (misal: paket dari subnet Mahasiswa tapi dengan Source IP Admin) agar tidak membebani firewall utama.

Layer 3-7: Core Security (pfSense Firewall Level)

- **Stateful Inspection:** Memastikan hanya paket balasan yang sah dari koneksi yang diinisiasi dari dalam yang diizinkan masuk kembali.
 - **IDS/IPS (Suricata):**
 - Diaktifkan pada interface **em1** (Zona Student) dan WAN.
 - Mendeteksi *signature* serangan seperti *Nmap Scan*, *SQL Injection*, atau upaya *Brute Force*.
 - **Egress Filtering:**
 - Memblokir port SMTP (25) keluar (mencegah jaringan kampus jadi sarang spam bot).
 - Memblokir DNS (53) keluar selain ke DNS Resolver kampus (mencegah *DNS Tunneling / Malware C2*).
 - **Traffic Shaping (Limiter):** Membatasi *bandwidth* dan *connection rate* dari Zona Guest/Mahasiswa untuk mencegah serangan DoS ringan.
-

6. Adaptabilitas & Skala Sistem

Desain arsitektur *Hub-and-Spoke* fisik ini dirancang untuk mendukung pertumbuhan jaringan kampus di masa depan dengan dua pendekatan sistematis:

1. Skala Vertikal (Penambahan User/Lab dalam Zona yang Sama)

Skenario: Departemen Akademik membuka 3 Laboratorium Komputer baru.

- **Tindakan:** Cukup tambahkan *Switch Access* atau konfigurasi VLAN baru di bawah router internal yang relevan (**AcademicR**).
- **Keunggulan:**
 - **Efisiensi Konfigurasi:** Tidak perlu mengubah konfigurasi apa pun di **Mikrotik Firewall**. Mikrotik hanya perlu tahu bahwa seluruh trafik menuju subnet baru tersebut dialihkan ke **AcademicR**.
 - **Pewarisan Kebijakan:** Subnet/Lab baru tersebut secara otomatis mewarisi kebijakan keamanan Zona Akademik (misal: otomatis terblokir dari akses ke Admin) tanpa perlu pembuatan *rule* firewall baru.

2. Skala Horizontal (Penambahan Zona/Fakultas Baru)

Skenario: Kampus membuka unit baru yang butuh isolasi total, misalnya "Fakultas Kedokteran" atau "Server Data Center".

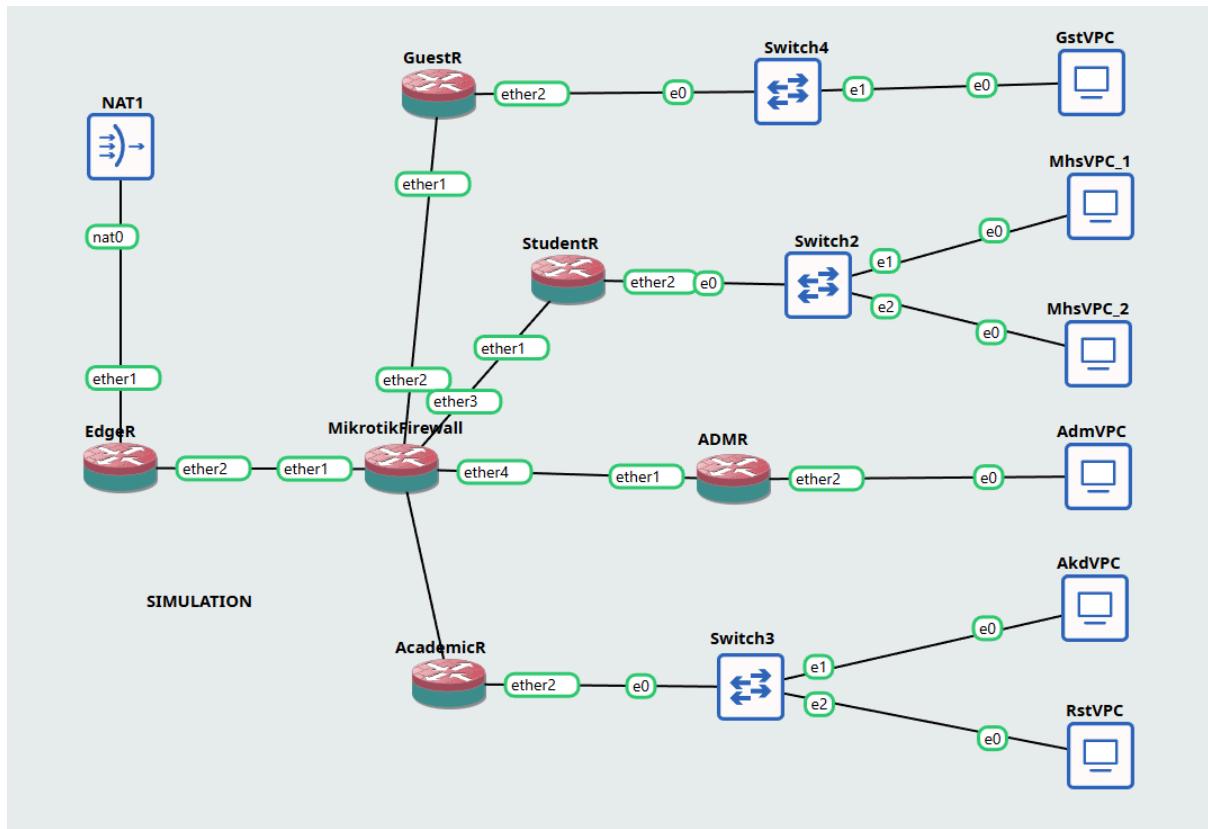
- **Prinsip Modularitas:** Kita memperlakukan setiap zona sebagai modul *plug-and-play*.
- **Tindakan:**
 1. Pasang 1 Router Internal baru (misal: **MedicalR**).
 2. Hubungkan router tersebut ke interface fisik kosong di **Mikrotik Firewall** (misal: **ether6**).
 3. Konfigurasi IP Transit (/30) antara Mikrotik dan Router baru.
- **Keunggulan:** Penambahan zona baru tidak mengganggu operasional zona lain (Student/Admin) karena perangkat kerasnya terpisah.

3. Manajemen Terpusat (Centralized Policy)

Meskipun topologi ini menggunakan banyak router (*Distributed Routing*), manajemen keamanan tetap **terpusat satu pintu**.

- Seluruh keputusan "Siapa boleh akses ke mana" (Filtering & NAT) dilakukan di **Mikrotik Firewall**.
- Router internal (**StudentR**, **ADM**, dll) hanya fokus pada distribusi paket lokal, sehingga memudahkan tim IT dalam melakukan audit keamanan dan *monitoring* trafik global.

LAPORAN TOPOLOGI KEAMANAN JARINGAN: WEEK 10



1. Deskripsi Perangkat

Topologi simulasi GNS3 telah diperbarui dari desain *router-on-a-stick* menjadi desain *multi-router* fisik untuk memenuhi kebutuhan segmentasi zona yang lebih ketat. Berikut adalah komponen yang digunakan:la

2. Konfigurasi Perangkat & Pengalamatan IP

Topologi ini mepresentasikan evolusi dari arsitektur *Zone-Based Security*. Jika sebelumnya segmentasi hanya mengandalkan VLAN (Logis), kini kami menerapkan **Segmentasi Fisik (Physical Segmentation)** menggunakan router yang berdedikasi per zona.

A. Subnet Pengguna (LAN)

Zona	Subnet Network	Gateway (Router Internal)	VLAN/Switch Fisik
Mahasiswa	10.20.10.0/24	10.20.10.1 (StudentR)	Switch2
Akademik	10.20.20.0/24	10.20.20.1 (AcademicR)	Switch3

Riset & IoT	10.20.30.0/24	10.20.30.1 (AcademicR)	Switch3
Admin	10.20.40.0/24	10.20.40.1 (ADM)R	Direct / Switch Dedicated
Guest	10.20.50.0/24	10.20.50.1 (GuestR)	Switch4

B. Subnet Transit (Interkoneksi Router ke Firewall)

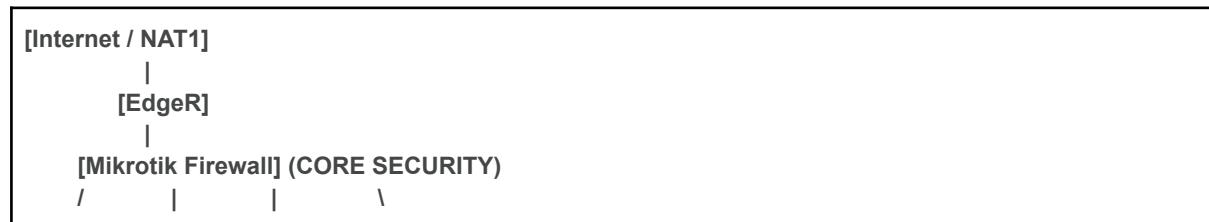
Jaringan kecil (/30) untuk menghubungkan interface fisik pfSense dengan router internal.

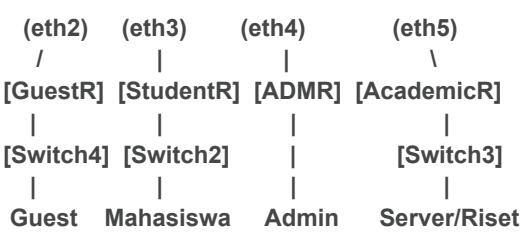
Link Koneksi	Network Transit	IP Firewall (Interface)	IP Router Tetangga
Firewall ↔ GuestR	192.168.50.0/30	192.168.50.1 (ether2)	192.168.50.2
Firewall ↔ StudentR	192.168.10.0/30	192.168.10.1 (ether3)	192.168.10.2
Firewall ↔ ADMR	192.168.40.0/30	192.168.40.1 (ether4)	192.168.40.2
Firewall ↔ AcademicR	192.168.20.0/30	192.168.20.1 (ether5)*	192.168.20.2

3. Penjelasan Topologi

Topologi ini merepresentasikan arsitektur **Zone-Based Security**. Alih-alih menumpuk semua VLAN dalam satu trunk switch, kami memisahkan zona secara fisik menggunakan router yang berdedikasi.

Diagram Topologi Akhir:





Filosofi Desain Baru:

1. **Physical Isolation (Isolasi Fisik):**
 - Kami memisahkan jalur **Guest** (via **GuestR** & **Switch4**) dari jalur **Mahasiswa** (via **StudentR** & **Switch2**).
 - **Keuntungan:** Serangan *bandwidth flooding* atau DDoS di jaringan Guest tidak akan mematikan CPU router mahasiswa, menjaga stabilitas kegiatan belajar mengajar.
2. **Enforced Choke Point:**
 - Tidak ada kabel yang menghubungkan antar-router zona secara langsung (misal: tidak ada kabel dari **StudentR** ke **AcademicR**).
 - Satu-satunya jalan komunikasi antar departemen adalah melalui **Mikrotik Firewall**. Ini menjamin 100% trafik lalu lintas internal dapat diinspeksi oleh **Firewall Filter Rules**.
3. **Dedicated Management Lane:**
 - Router **ADMR** dikhkususkan untuk manajemen. Jika jaringan mahasiswa atau guest *down* karena serangan, admin tetap memiliki jalur belakang (*backdoor*) yang aman untuk memperbaiki sistem.

4. Alur Traffic (Traffic Flow)

Dalam topologi *Multi-Router* ini, alur lalu lintas menjadi lebih terstruktur dengan pola *Hub-and-Spoke*.

A. Internal → Internet (North-South)

Semua subnet internal mengakses Internet melalui jalur hierarkis bertingkat:

1. **Host** mengirim paket ke Gateway lokalnya (misal: **10.20.10.1** di **StudentR**).
2. **Router Zona** meneruskan paket via *Default Route* ke IP Transit Firewall (misal: **192.168.10.1**).
3. **Mikrotik Firewall** melakukan *Source NAT (Masquerade)* agar IP privat bisa keluar, lalu meneruskan ke **EdgeR**.
4. **EdgeR** meneruskan ke Internet (NAT1).

B. Antar Subnet (East-West) — Zero Trust

Ini adalah implementasi utama keamanan. Komunikasi antar departemen tidak terjadi secara langsung.

- **Skenario:** Mahasiswa (10.20.10.2) ingin mengakses Website Akademik (10.20.20.2).
 1. **MhsVPC** mengirim request ke **StudentR**.
 2. **StudentR** melihat tujuan ada di network lain, meneruskan paket ke **Mikrotik Firewall**.
 3. **Firewall (Decision Point):** Mengecek *Filter Rules*.
 - "Apakah Source: 10.20.10.0/24 boleh ke Destination: 10.20.20.0/24 dengan Port 80/443?"
 4. **Action:**
 - Jika **MATCH/ALLOW**: Paket diteruskan ke **ether5** menuju **AcademicR**.
 - Jika **NO MATCH**: Paket terkena aturan *Implicit Deny* (Drop).

C. Guest → Internet (Jalur Isolasi)

Pengisolasian jalur akses melalui Guest dengan role *untrusted*.

1. Trafik dari **GstVPC** masuk ke **Switch4**, lalu ke **GuestR**.
2. **GuestR** melempar trafik ke Firewall via interface **ether2**.
3. **Firewall Policy:**
 - **Dst-Address != 10.20.0.0/16** (Bukan IP Lokal) → **ALLOW** (Internet).
 - **Dst-Address == 10.20.0.0/16** (IP Lokal) → **DROP**.
 - **Hasil:** Guest bisa browsing, tapi tidak bisa *ping* atau *scan* jaringan Mahasiswa/Admin.

D. Admin → Semua Subnet

Jalur ini digunakan untuk *maintenance*.

1. **AdmVPC** terhubung ke **ADM**.
2. Trafik masuk ke Firewall via interface **ether4** (Zona High Trust).
3. **Firewall Policy:** Mengizinkan protokol manajemen (SSH, Winbox, ICMP) dari **Src : Admin** ke semua interface lain.

LAPORAN KONFIGURASI TOPOLOGI KJK : WEEK 11
