PANDUAN PENGGUNAAN

F I R E W A L L

GOV-CSIRT (Government Computer Security Insident Response Team)

Pusat Monitoring dan Penanganan Insiden Keamanan Informasi Instansi Pemerintah

Direktorat Keamanan Informasi

Kementerian Komunikasi dan Informatika Republik Indonesia

Agenda

- Overview Teknologi Firewall
- Arsitektur jaringan komputer dan firewall
- Kebijakan Firewall
- Perencanaan & implementasi Firewall

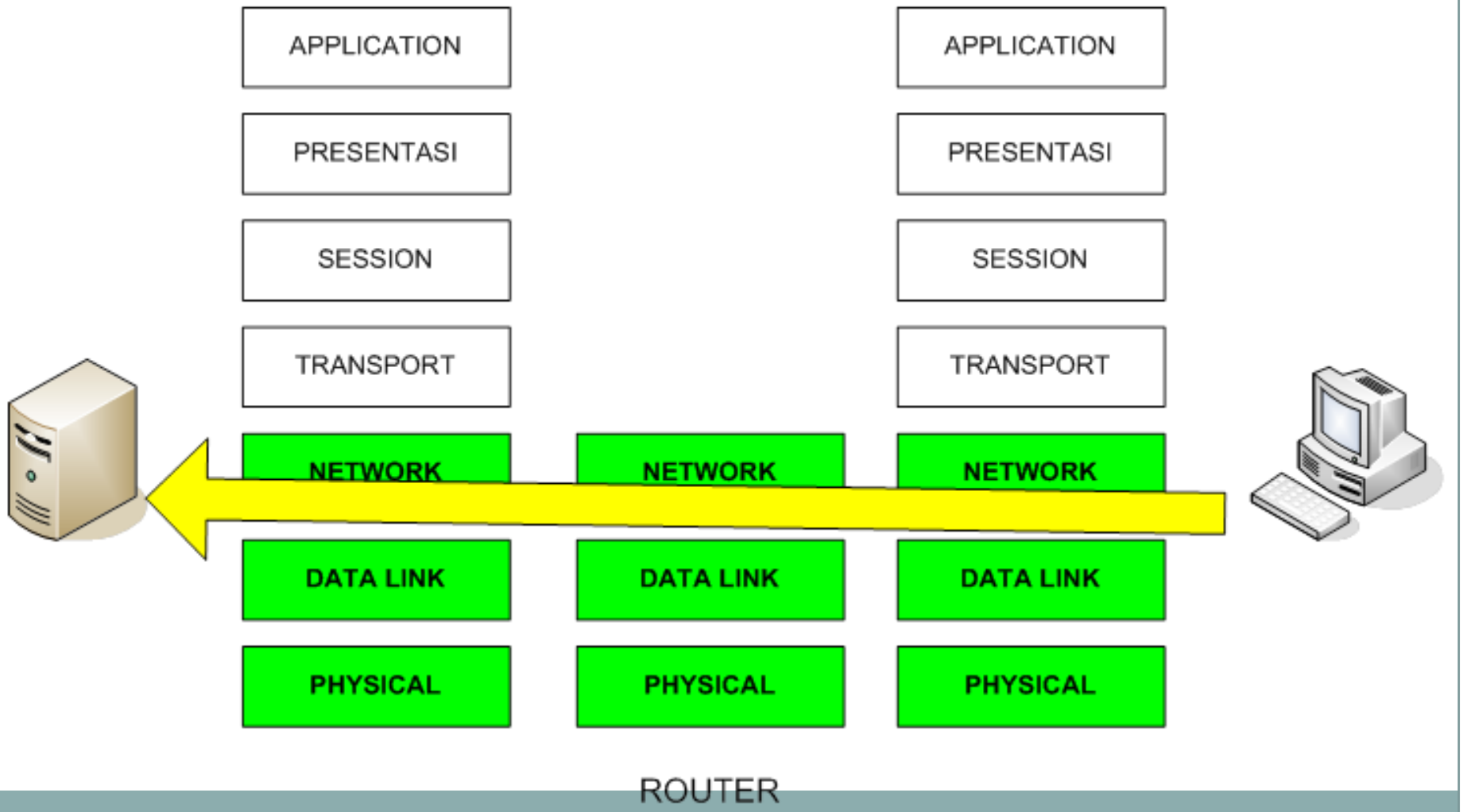
Overview Teknologi Firewall

- **Teknologi Firewall ➔ Penyaringan Paket**
- **Teknologi Firewall ➔ Application Layer Gateways**
- **Teknologi Firewall ➔ Statefull Inspection**

Teknologi Firewall ➔ Penyaringan Paket

- teknologi penyaringan paket dapat memeriksa setiap paket data yang masuk maupun keluar dari suatu jaringan dan menerima ataupun menolak paket-paket data tersebut berdasarkan pada aturan yang telah ditentukan sebelumnya

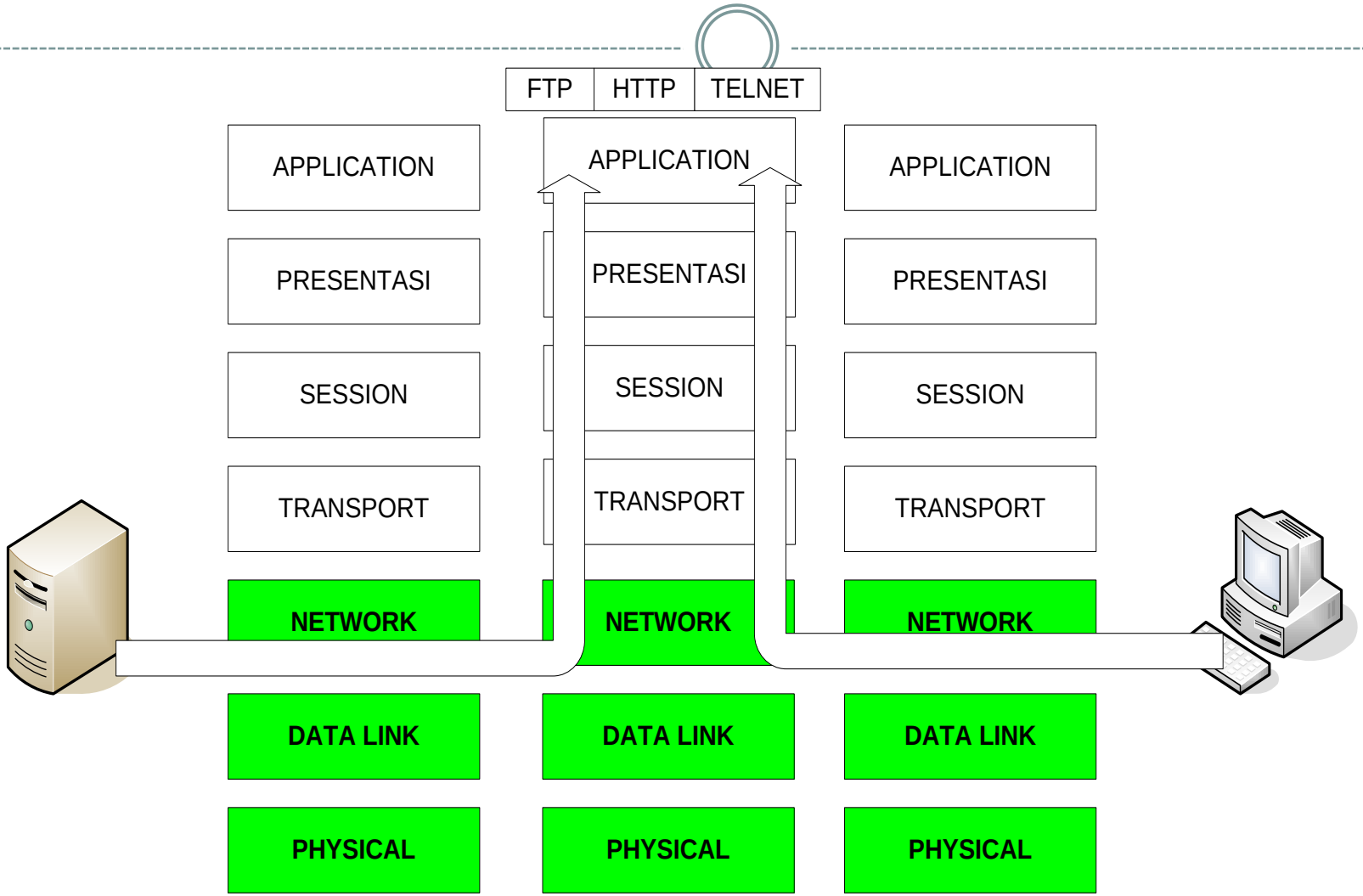
Penyaringan Paket



Teknologi Firewall ➔ Application Layer Gateways

- mengimplementasikan firewall pada layer aplikasi

Teknologi Firewall ➔ Application Layer Gateways

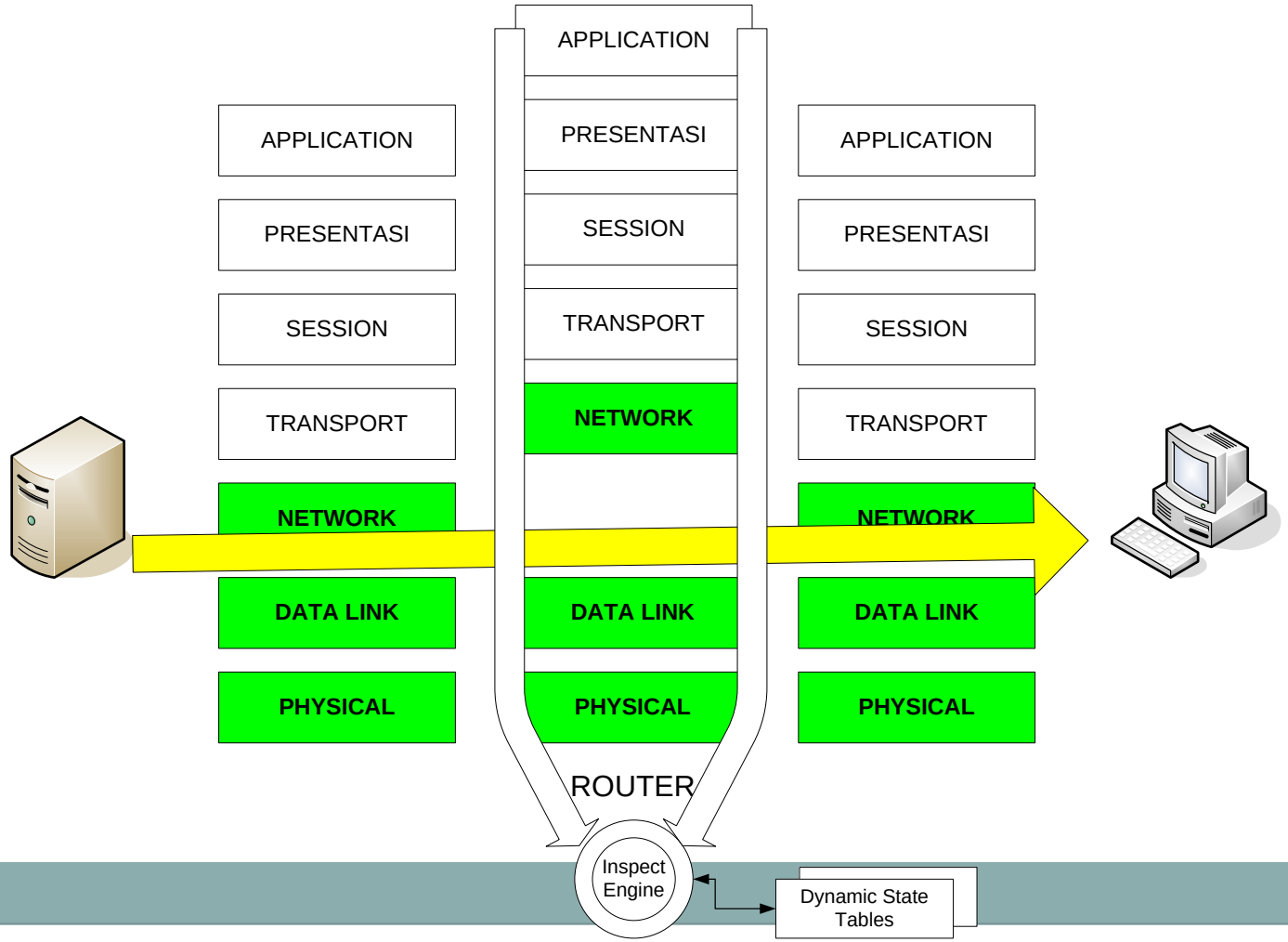


ROUTER

Teknologi Firewall ➔ Statefull Inspection

- Teknologi stateful inspection dapat melihat keseluruhan paket dan membuat suatu keputusan terhadap kebijakan keamanan berdasarkan isi dari paket tersebut. Teknologi ini juga akan menjaga jejak perjalanan setiap koneksi aktif ke dalam suatu tabel kondisi.

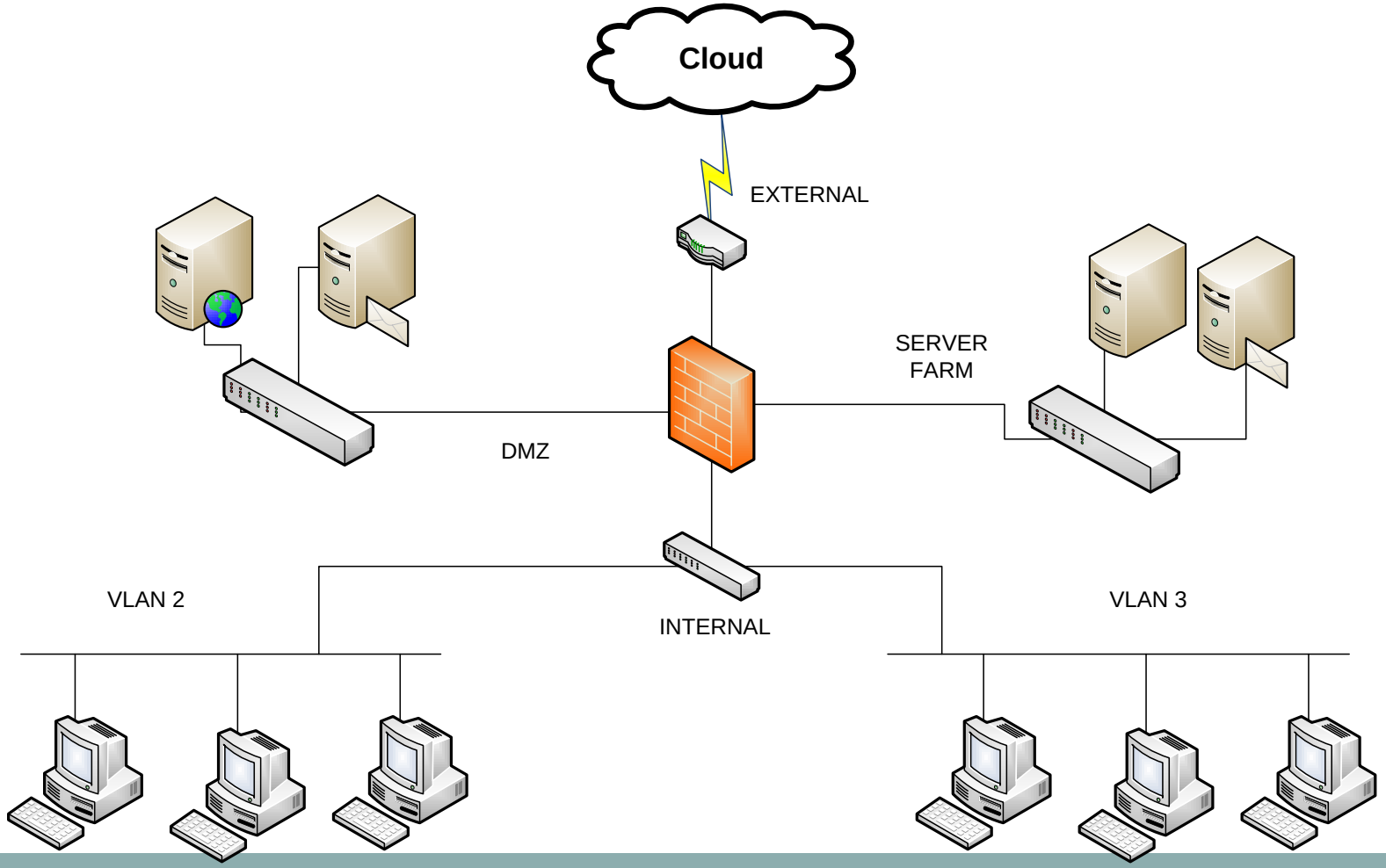
Teknologi Firewall ➔ Statefull Inspection



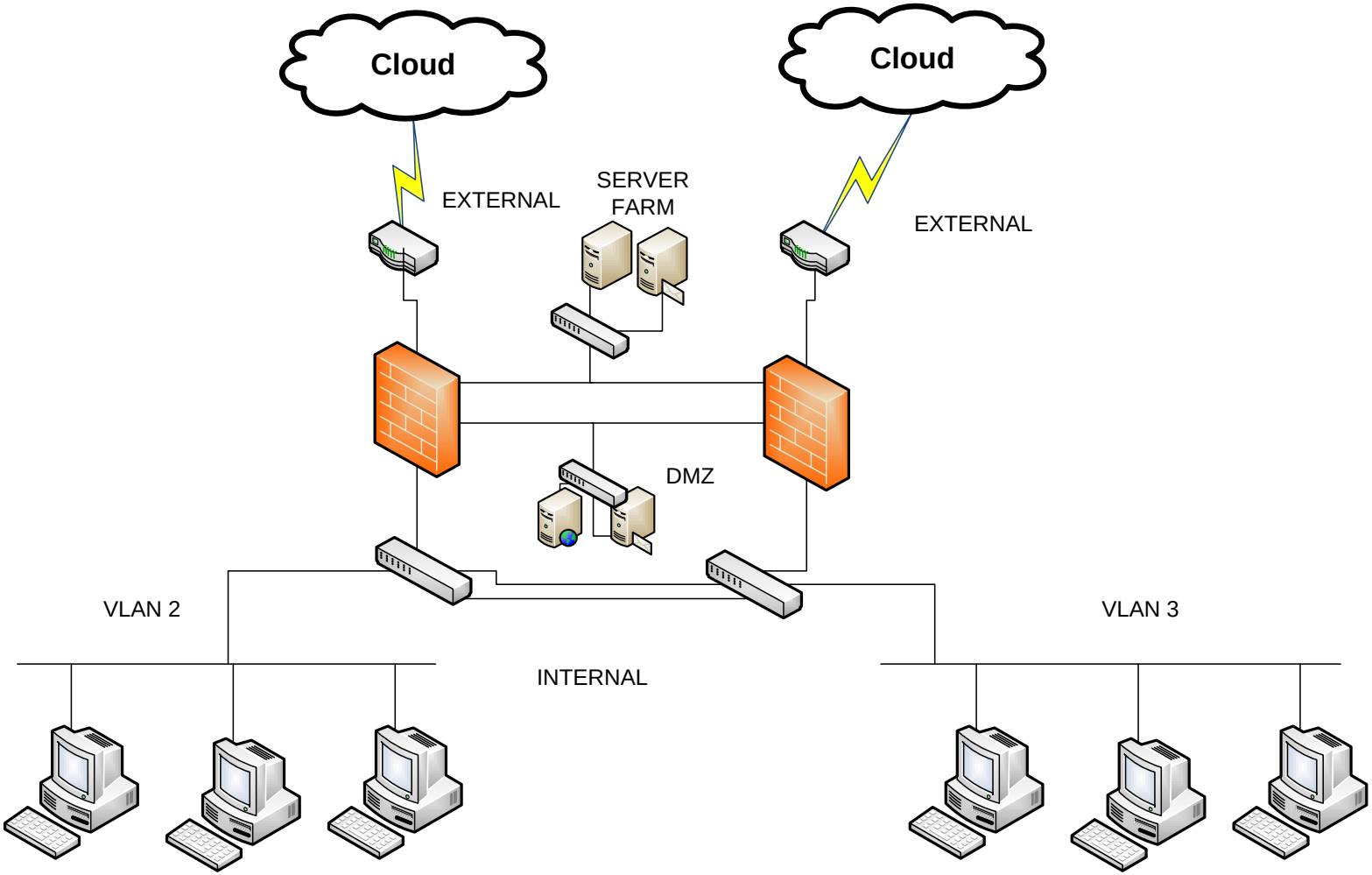
Arsitektur jaringan komputer dan firewall

- Single firewall
- Multiple firewall

Topologi single firewall



Topologi multiple firewall



Penerapan Kebijakan Firewall

- **Kebijakan berbasis hubungan antar zone**
- **Kebijakan berbasis IP & Protokol**
- **Kebijakan berbasis pada aplikasi**
- **Kebijakan berbasis pada identitas user**

Kebijakan berbasis hubungan antar zone

	Eksternal	Internal	DMZ	Server Farm
Eksternal		x	NAT/Routing	x
Internal	NAT		Routing	Routing
DMZ	NAT/Routing	Routing		Routing
Server Farm	x	Routing	Routing	

Kebijakan berbasis hubungan antar zone

- Pemasangan Access Rule antara Internal ➔ Eksternal (outgoing traffic)
- Pemasangan Access Rule antara Eksternal ➔ Internal (inbound traffic)
- Pemasangan Access Rule antara Internal ➔➔ Server Farm
- dsb

Kebijakan berbasis IP & Protokol

- Trafik yang berasal dari alamat-alamat sumber atau tujuan yang tidak sah seharusnya di block.
- Trafik arah masuk dengan alamat tujuan IP Private seharusnya di block.
- Trafik ke arah luar bagi alamat sumber yang tidak sah seharusnya di block.
- Trafik yang masuk dengan alamat tujuannya adalah alamat firewall seharusnya di block, kecuali firewall mengaktifkan layanan proxy.
- Trafik yang berisi informasi routing yang mengijinkan sistem untuk menetapkan rute yang akan paket lewati dari alamat sumber ke tujuan.
- Trafik dari arah luar jaringan yang berisi alamat broadcast yang mengarah ke jaringan internal seharusnya diblock.

Perencanaan dan implementasi Firewall

- Perencanaan
- Konfigurasi
- Pengujian
- Deployment
- Pengelolaan