

FIREWALL

Konsep Firewall

- Firewall adalah sebuah sistem atau grup sistem yang menjalankan kontrol akses keamanan diantara jaringan internal yang aman dan jaringan yang untrusted seperti internet.
- Firewall didesain untuk mengijinkan trusted data lewat, menolak layanan yang mudah diserang, mencegah jaringan internal dari serangan luar yang bisa menembus firewall setiap waktu

Ilustrasi Firewall

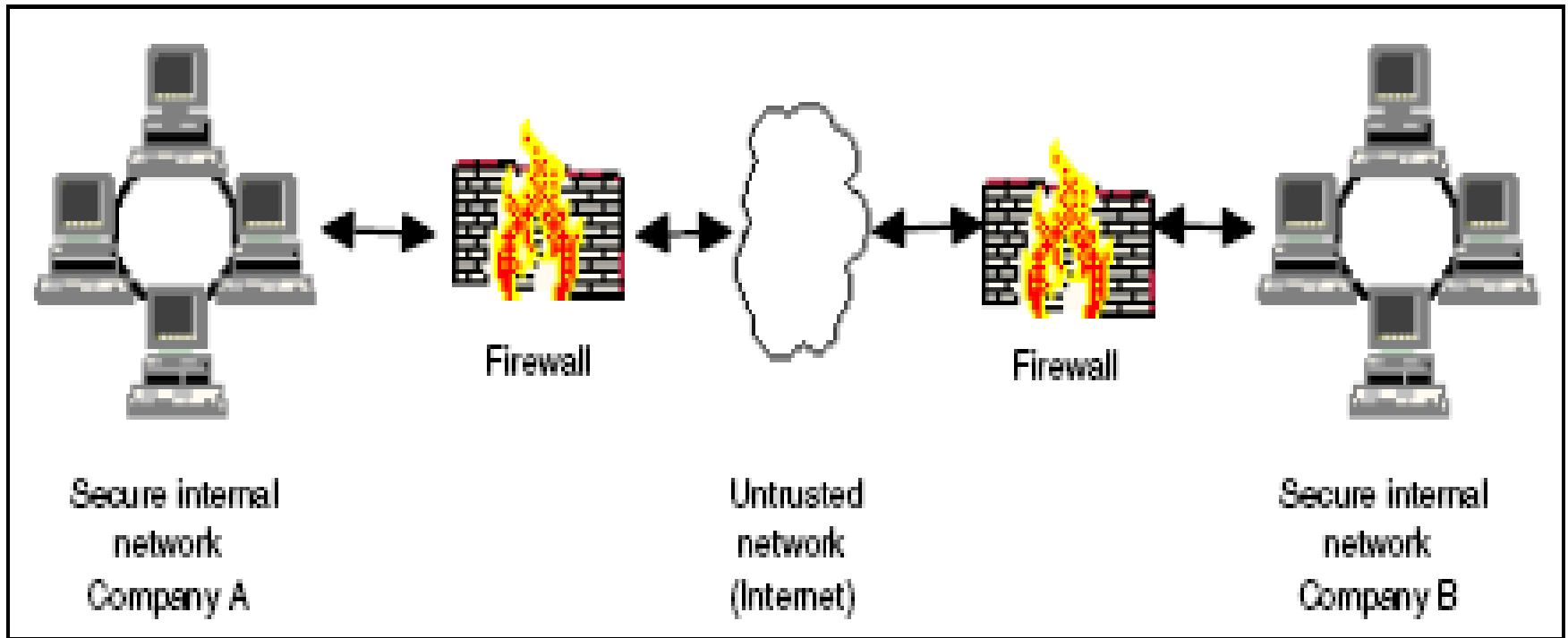


Figure 266. A firewall illustration

Komponen Sistem Firewall

- Firewall dapat berupa PC, router, midrange, mainframe, UNIX workstation, atau gabungan dari yang tersebut diatas.
- Firewall dapat terdiri dari satu atau lebih komponen fungsional sebagai berikut :
 - Packet-filtering router
 - Application level gateway (proxy)
 - Circuit level gateway

Packet-Filtering Router

- Packet-filtering diselesaikan dengan menggunakan router yang dapat meneruskan paket sesuai dengan filtering rules.
- Informasi yang dapat ditangkap dari packet header :
 - IP address sumber dan tujuan
 - Nomor port TCP/UDP sumber dan tujuan
 - Tipe ICMP message
 - Informasi encapsulated protocol (TCP, UDP, ICMP atau IP tunnel)

Ilustrasi Packet-filtering Router

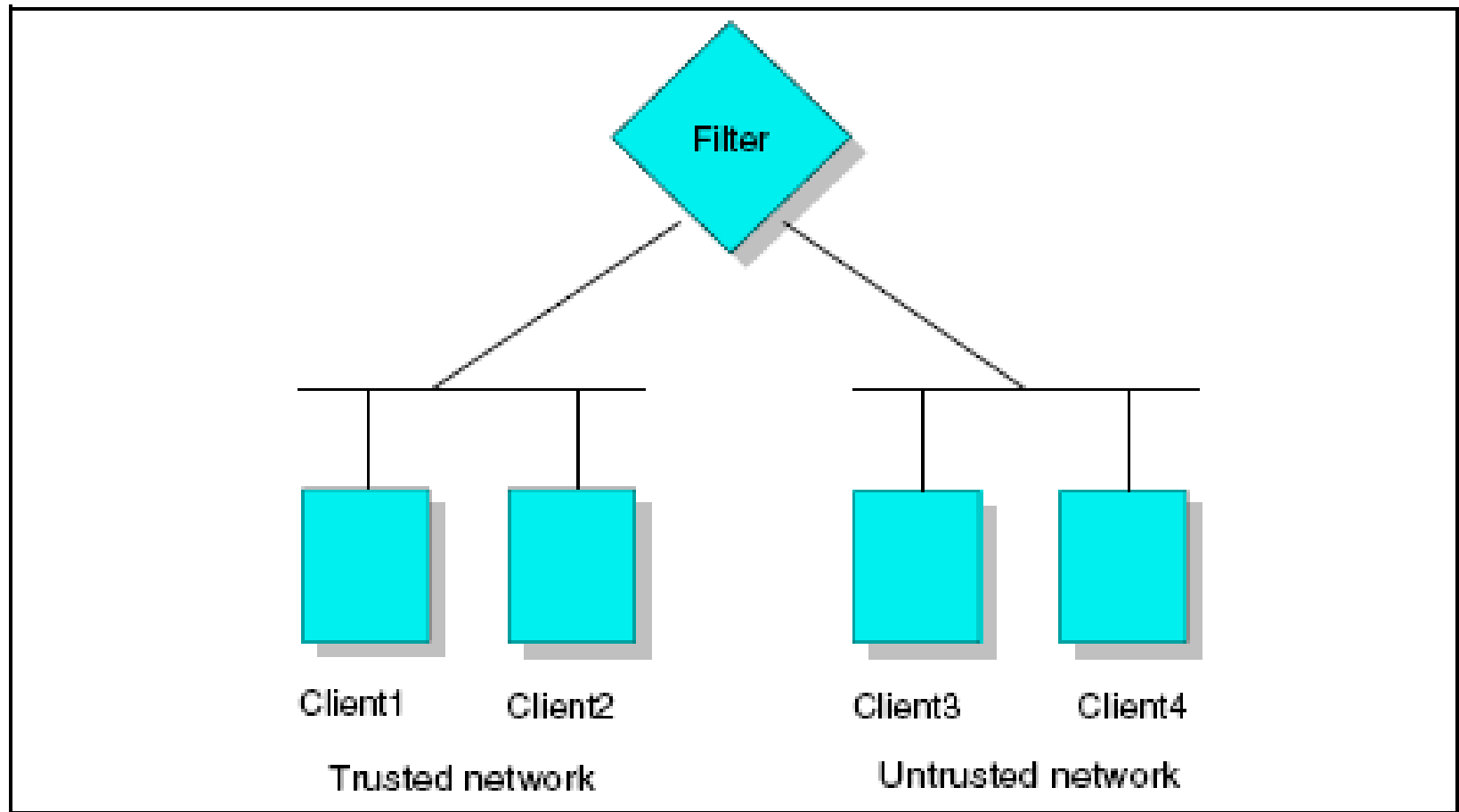


Figure 268. Packet filtering router

Contoh Rule Packet-filtering

from	to	src port	dst port	proto	rule
*	www	*	80	tcp	allow
*	mail-gw	*	25	tcp	allow
squids	proxy	*	8080, 3128	*	allow
mynet	*	*	*	*	allow
*	*	*	*	*	deny

Application Level Gateway (Proxy)

- Application level gateway bertindak sebagai “proxy”
- Application level gateway menyediakan kontrol tingkat tinggi pada traffic antara dua jaringan yang isi layanan tertentu didalamnya dapat dimonitor dan difilter sesuai dengan kebijakan keamanan jaringan.

Ilustrasi Proxy

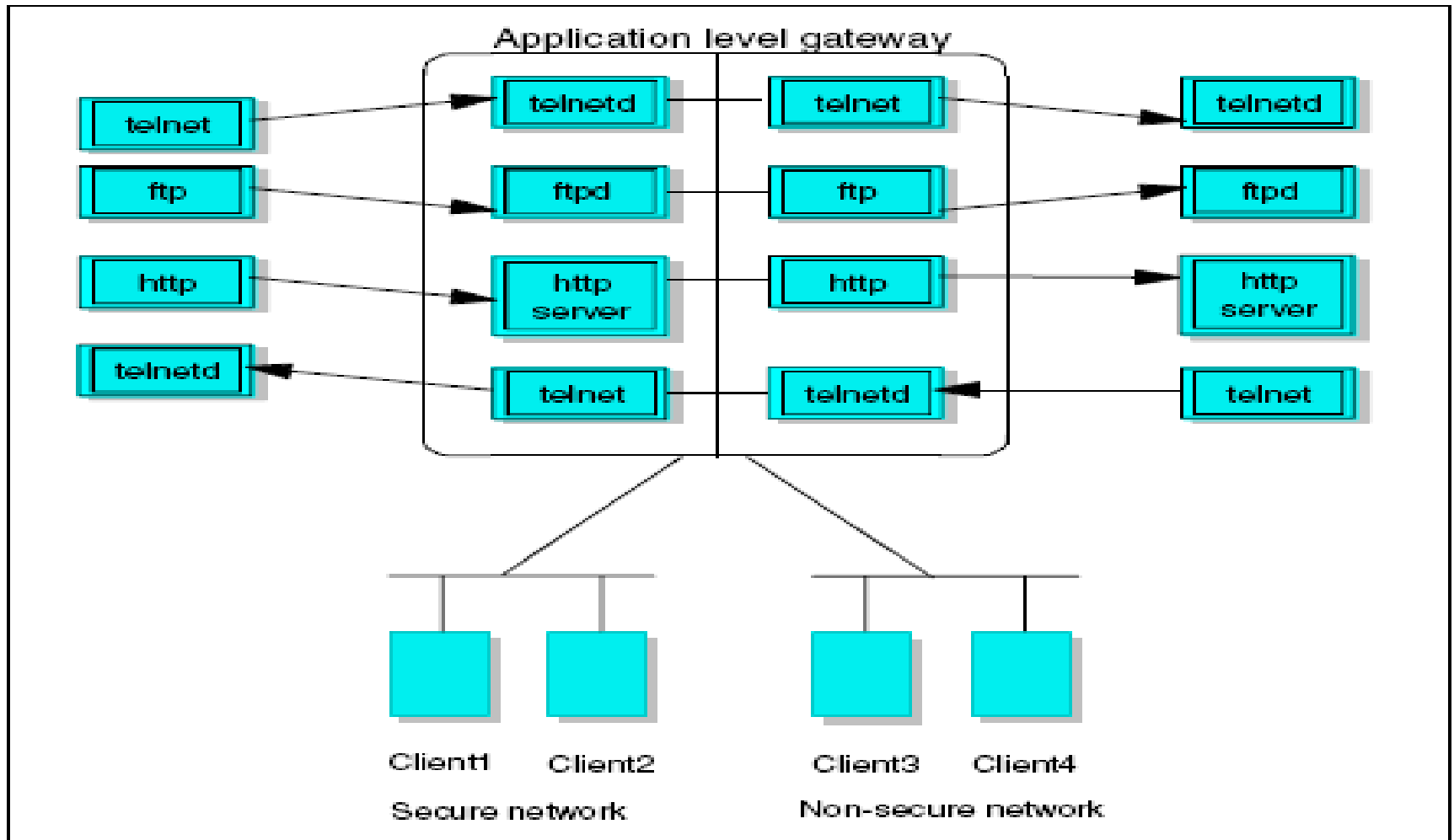


Figure 269. Application level gateway

Circuit Level Gateway

- Circuit level gateway menghandle koneksi TCP dan tidak menyediakan paket tambahan seperti processing atau filtering.
- Circuit level gateway dapat dikatakan sebagai tipe khusus dari proxy karena proxy dapat dikonfigurasi untuk melewati semua informasi user yang sudah diauthentifikasi sebagai circuit level gateway.

Ilustrasi Circuit Level Gateway

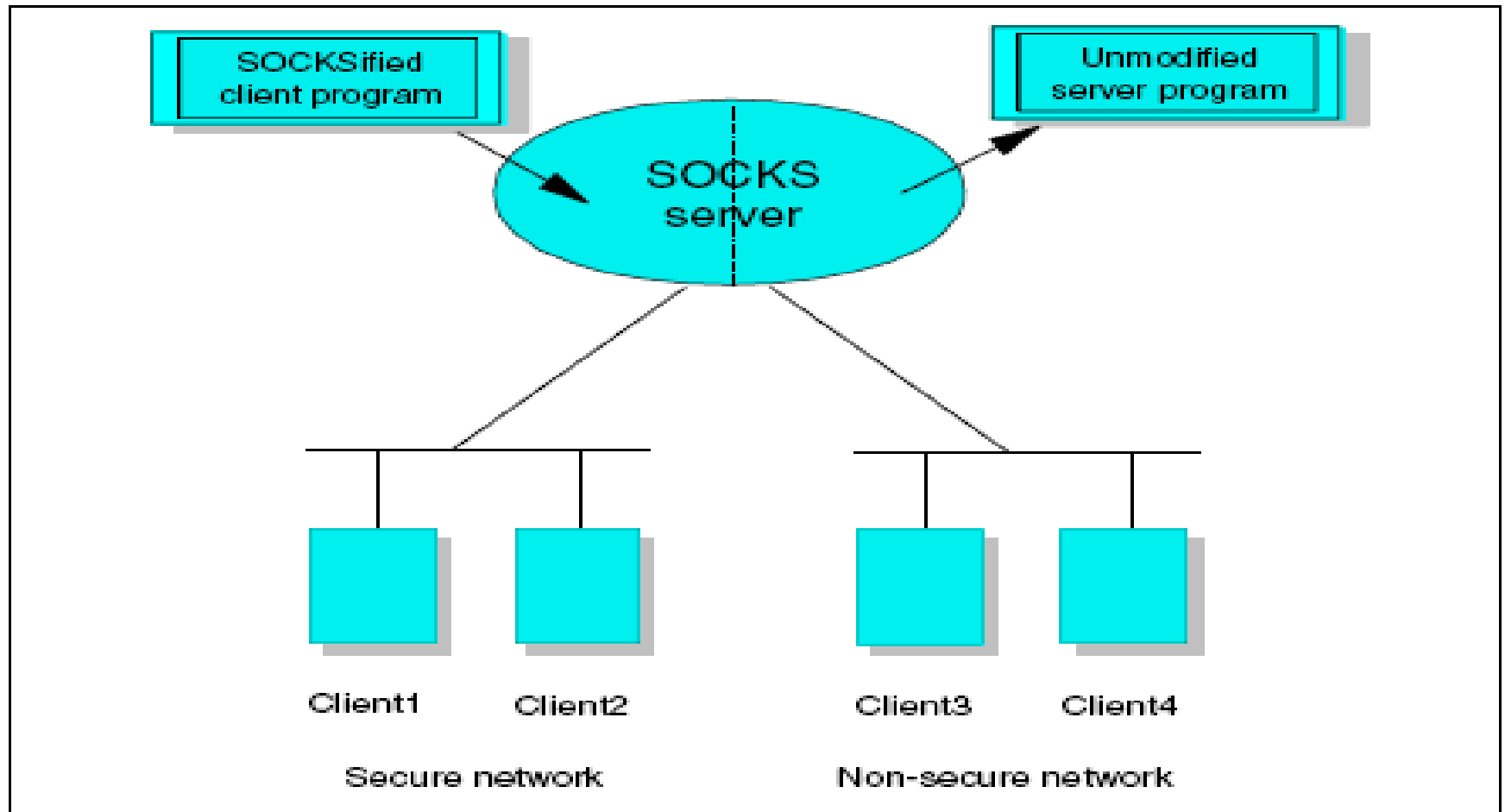


Figure 274. Circuit level gateway

Contoh Tipe Firewall

- Firewall terdiri dari satu atau lebih elemen software yang berjalan pada satu atau lebih host.
- Tipe-tipe firewall adalah sebagai berikut:
 - Packet-filtering Firewall
 - Dual-homed Gateway Firewall
 - Screened Host Firewall
 - Screened Subnet Firewall

Packet-Filtering Firewall

- Terdiri dari sebuah router yang diletakkan diantara jaringan eksternal dan jaringan internal yang aman.
- Rule Packet Filtering didefinisikan untuk mengijinkan atau menolak traffic.

Ilustrasi Packet-Filtering Firewall

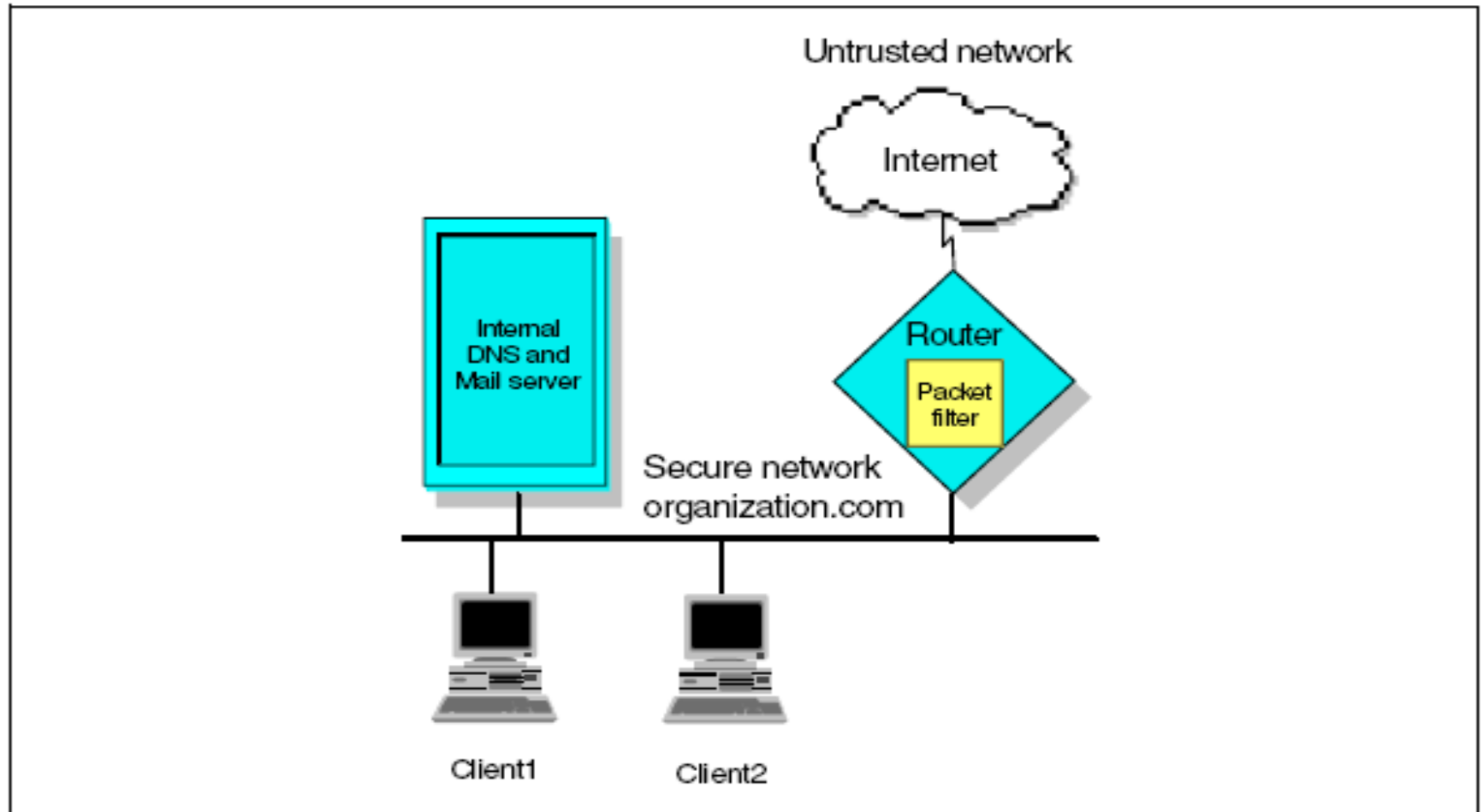


Figure 275. Packet-filtering firewall

Dual-Homed Gateway Firewall

- Dual-home host sedikitnya mempunyai dua interface jaringan dan dua IP address.
- IP forwarding dinonaktifkan pada firewall, akibatnya trafik IP pada kedua interface tersebut kacau di firewall karena tidak ada jalan lain bagi IP melewati firewall kecuali melalui proxy atau SOCKS.
- Serangan yang datang dari layanan yang tidak dikenal akan diblok.

Ilustrasi Dual-Home Firewall

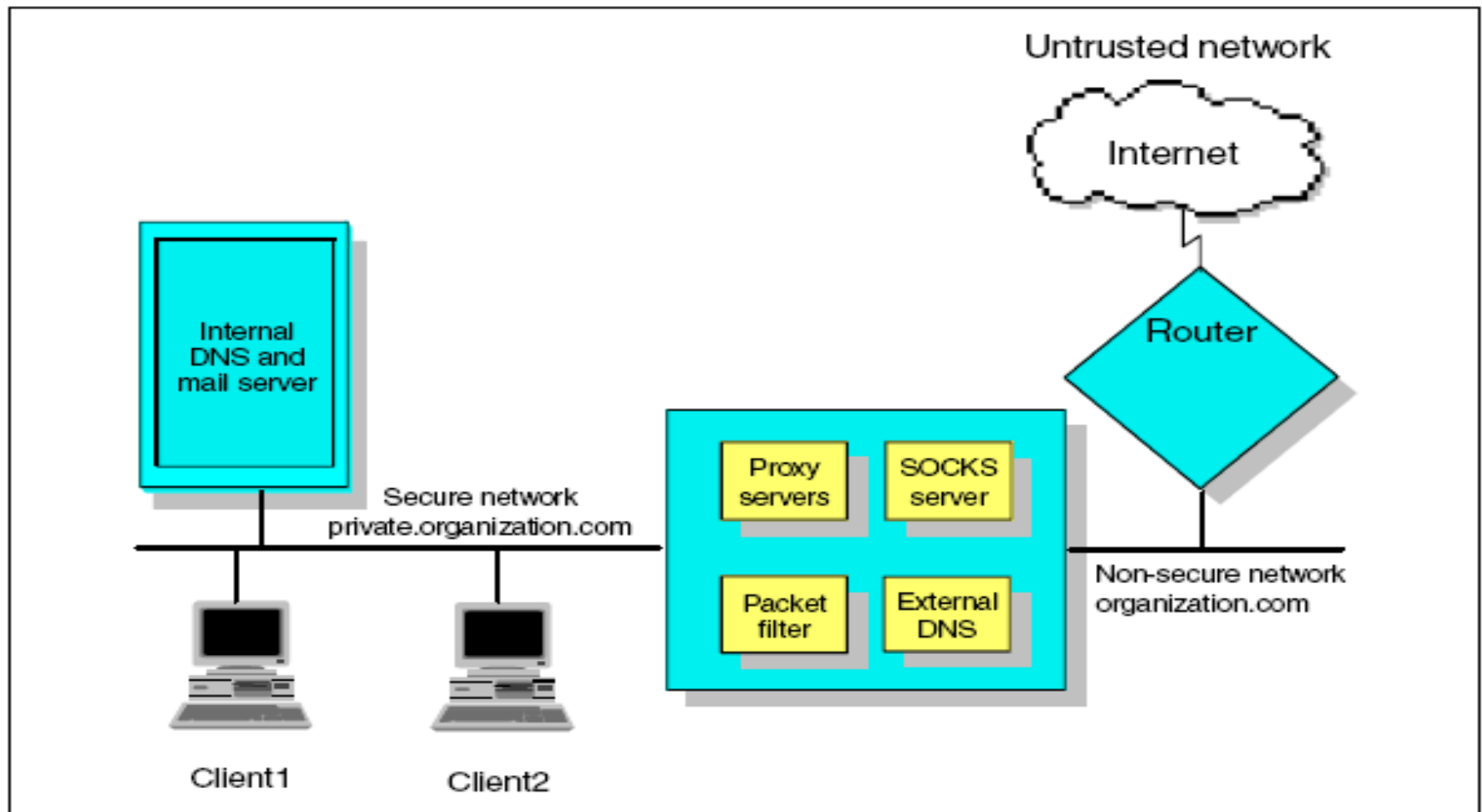


Figure 276. Dual-homed firewall

Screened Host Firewall

- Terdiri dari sebuah packet-filtering router dan application level gateway
- Host berupa application level gateway yang dikenal sebagai “bastion host”
- Router dikonfigurasi untuk meneruskan semua untrusted traffic ke bastion host dan pada kasus yang sama juga ke information server.

Ilustrasi Screened Host Firewall

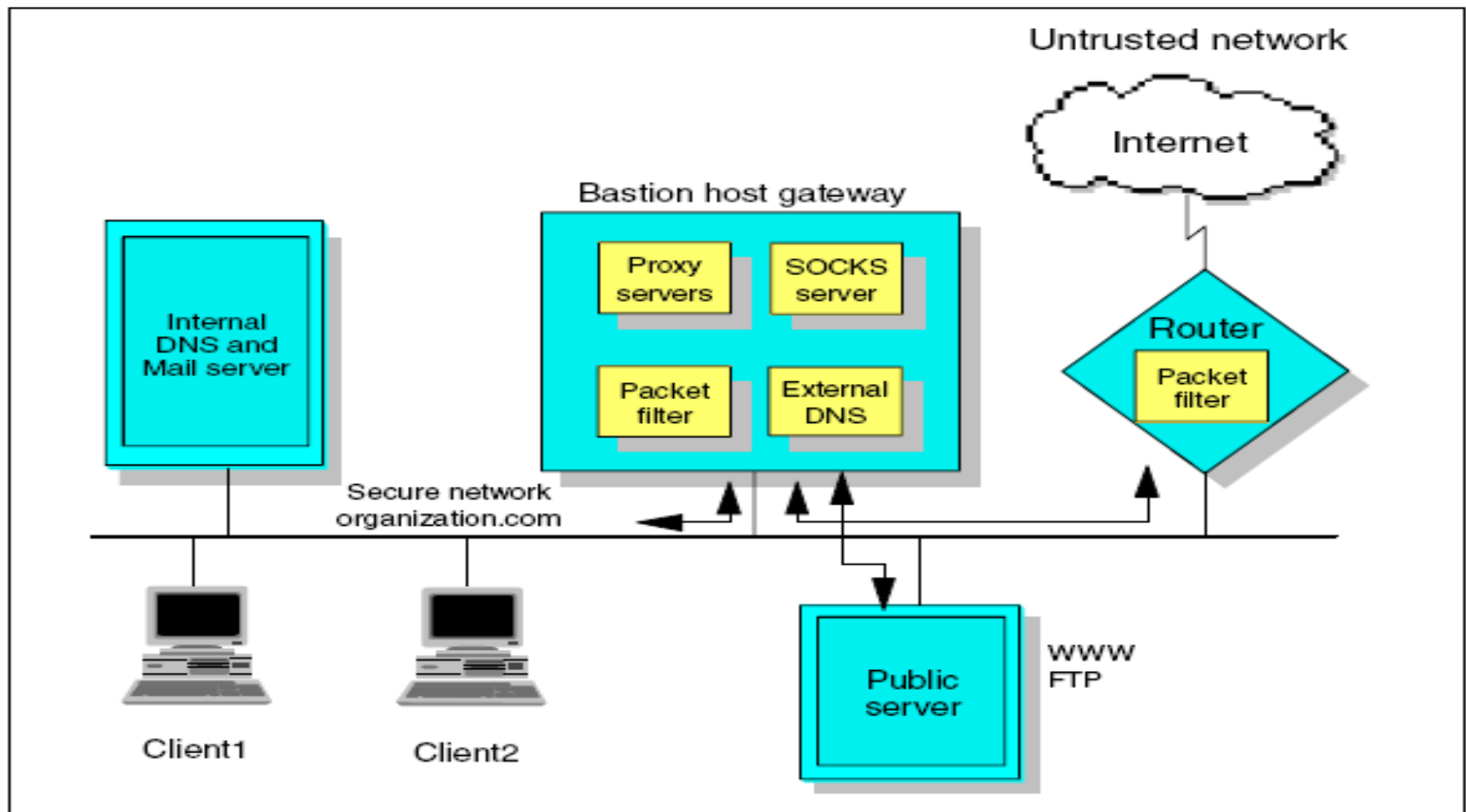


Figure 277. Screened host firewall

Screened Subnet Firewall

- Terdiri dari dua router packet filtering dan sebuah bastion host
- Menyediakan tingkat keamanan yang tinggi daripada tipe firewall yang lain
- Membuat DMZ(Demilitarized Zone) diantara jaringan internal dan eksternal,sehingga router luar hanya mengijinkan akses dari luar bastion host ke information server dan router dalam hanya mengijinkan akses dari jaringan internal ke bastion host

Ilustrasi Screened Subnet Firewall

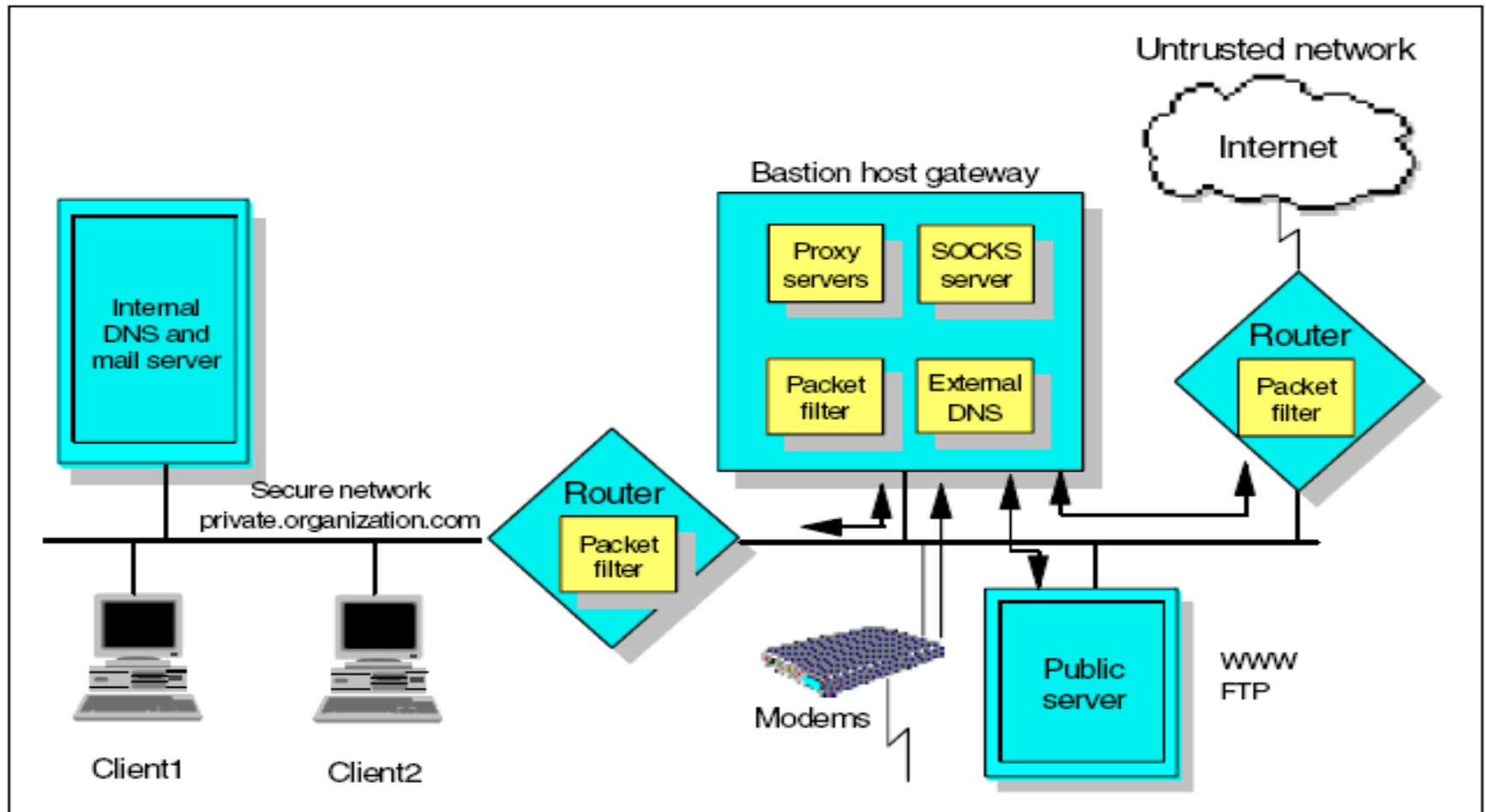


Figure 278. Screened subnet firewall

TERIMA KASIH