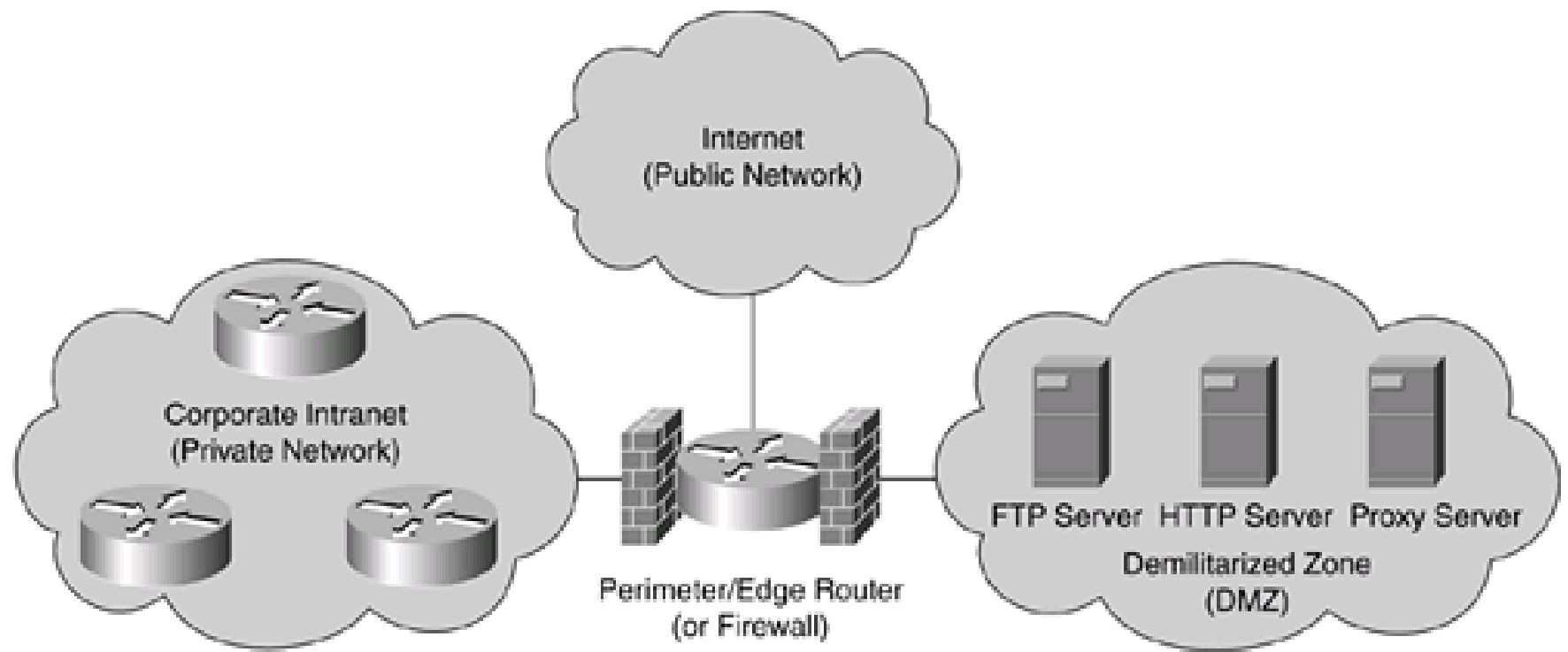


# Network Security FIREWALL

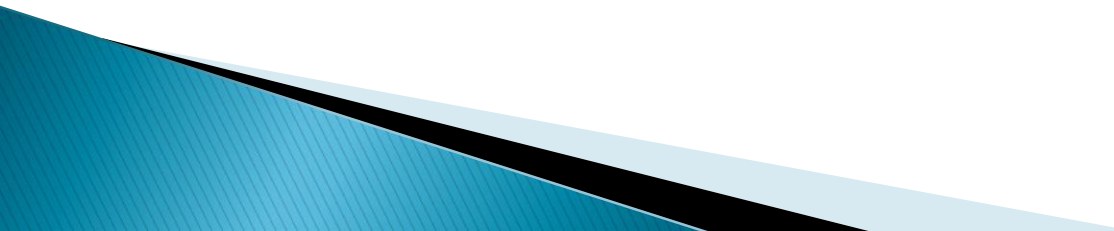
# Dasar Firewall

Firewall didefinisikan sebagai gateway atau server akses (berbasis perangkat keras atau perangkat lunak) atau beberapa gateway atau server akses yang ditetapkan sebagai buffer antara jaringan publik dan jaringan pribadi.

Firewall adalah alat yang memisahkan jaringan yang terpercaya dari sebuah jaringan yang tidak dipercaya. Firewall dapat berupa sebuah router, sebuah PC yang menjalankan perangkat lunak khusus, atau kombinasi dari perangkat-perangkat tertentu.



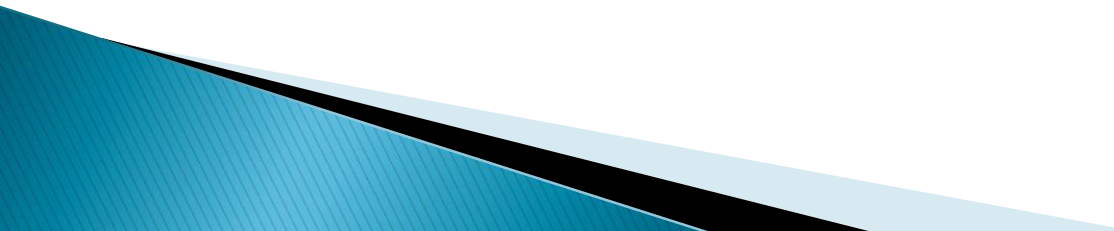
# Access Control List

- ▶ ACL terdiri atas aturan–aturan dan kondisi yang menentukan trafik jaringan dan menentukan proses di firewall/router apakah nantinya paket akan dilewatkan atau tidak
  - ▶ Daftar ini memberitahu firewall/router paket–paket mana yang akan diterima atau ditolak
- 

# Contoh ACL

```
access-list 1 permit 10.1.4.3  
access-list 1 deny 10.1.0.0 0.0.255.255  
access-list 1 permit 10.0.0.0 0.255.255.255
```

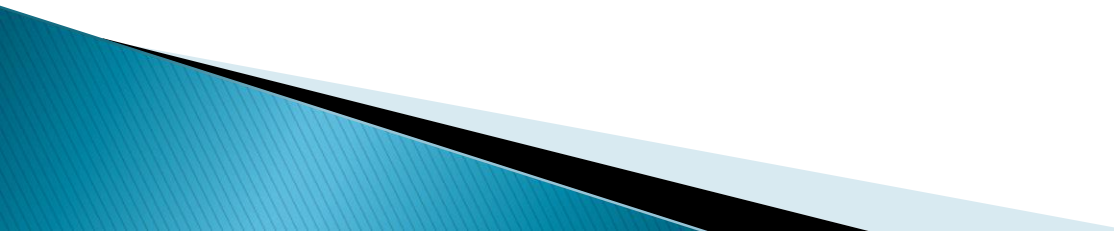
# Metode Inspeksi pada Firewall

- ▶ Packet filtering or stateless filtering
  - ▶ Stateful filtering
  - ▶ Deep packet layer inspection
- 

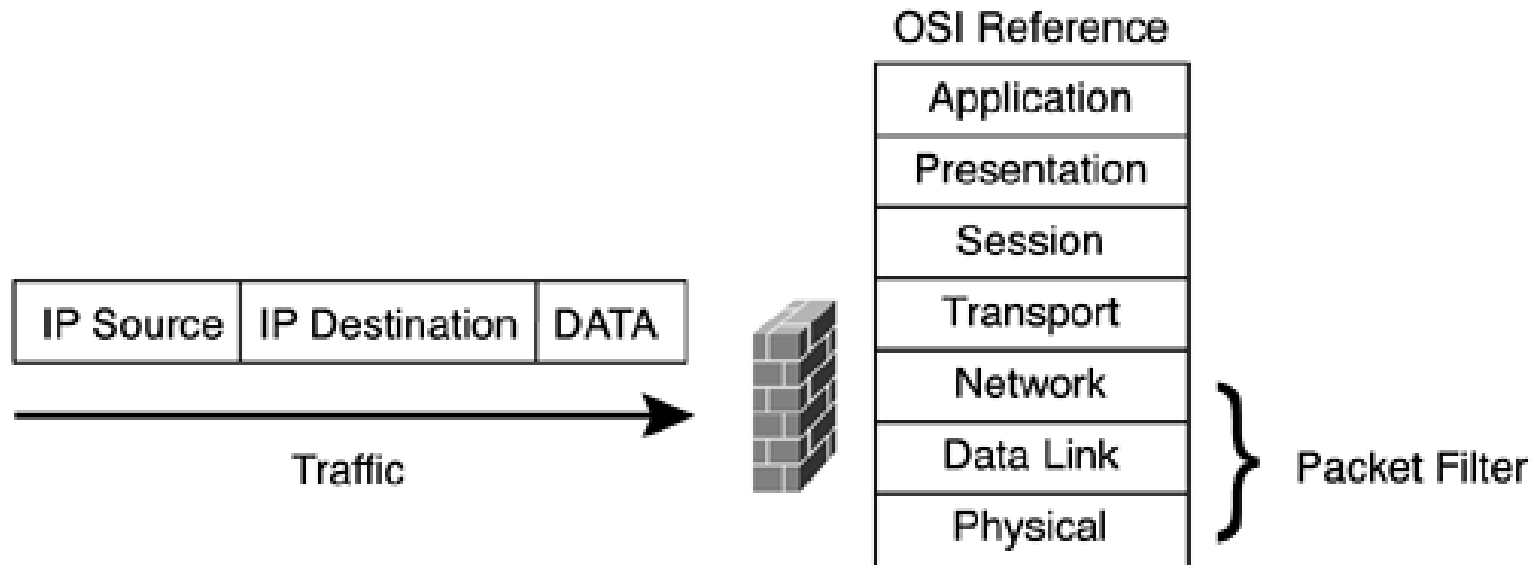
# Packet Filtering/Stateless Firewall

Firewall adalah sebuah router yang mampu melakukan penapisan atau penyaringan terhadap paket-paket yang masuk. Perangkat jenis ini umumnya disebut dengan *packet-filtering router*.

Bekerja dengan cara membandingkan alamat sumber dari paket-paket tersebut dengan kebijakan pengontrolan akses yang terdaftar dalam access control list firewall.

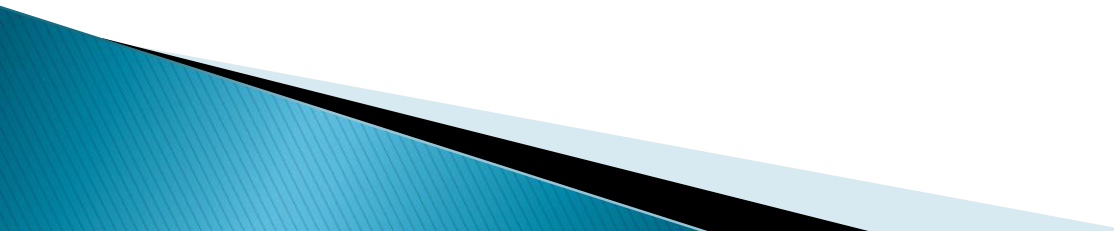


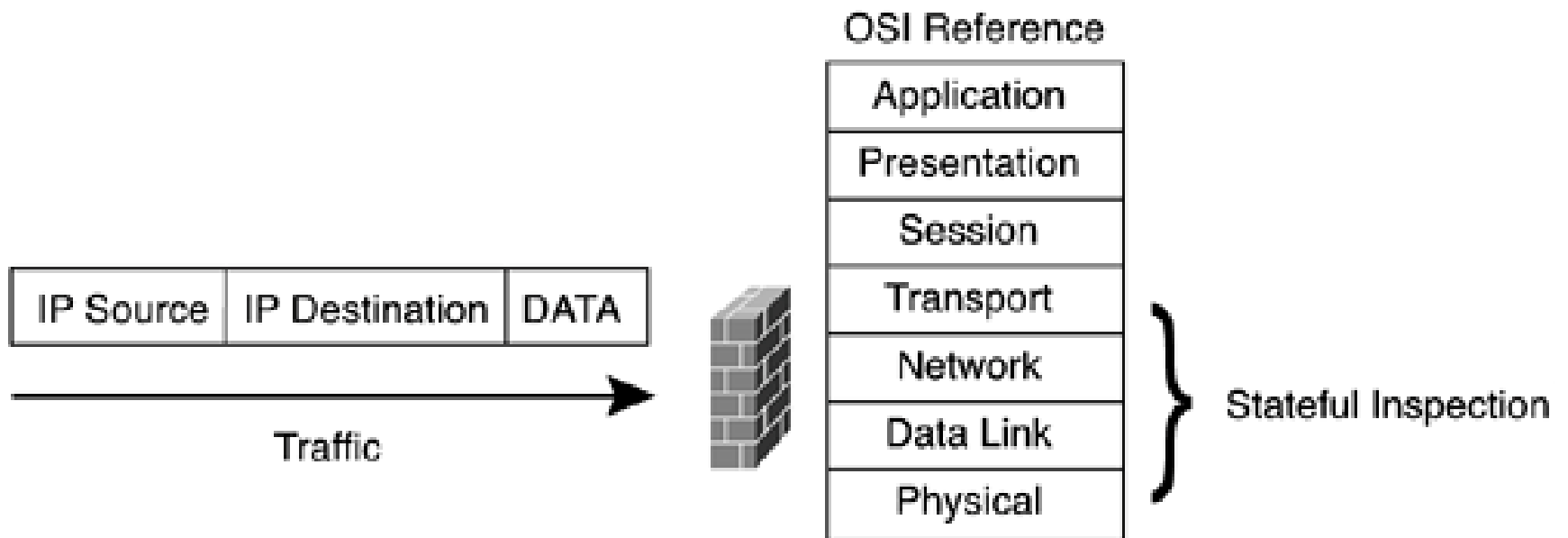
- ▶ Stateless firewall melakukan inspeksi sampai pada layer 3 (layer Network).
- ▶ Stateless melakukan inspeksi berdasarkan pada alamat sumber dan tujuan beserta port yang digunakan.



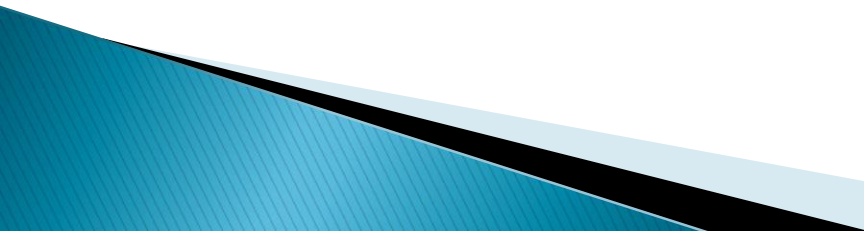


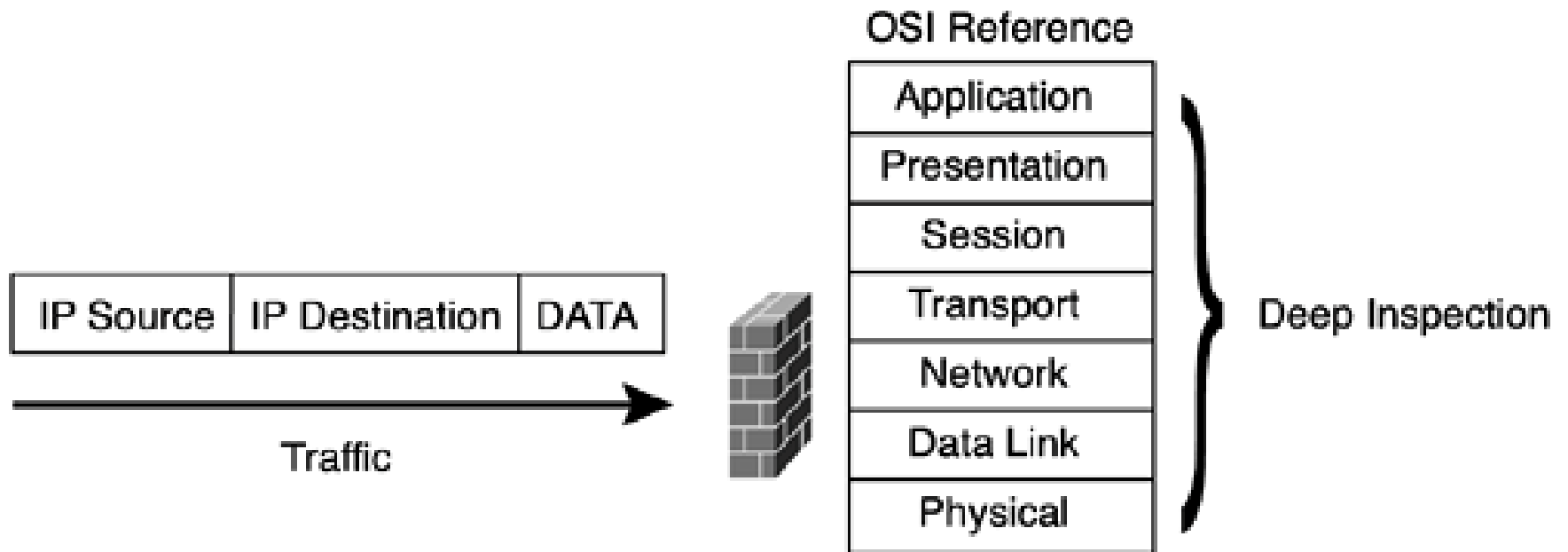
# Statefull Firewall

- ▶ Statefull Firewall membatasi informasi jaringan dari sumber ke tujuan hanya berdasarkan pada alamat ip sumber dan tujuan, dan alamat port sumber dan tujuan.
  - ▶ Statefull firewall dapat melakukan inspeksi isi dari data dan mengenali anomali dalam sebuah protokol transport.
  - ▶ Statefull firewall melakukan inspeksi sampai pada layer 4 (layer Transport)
- 

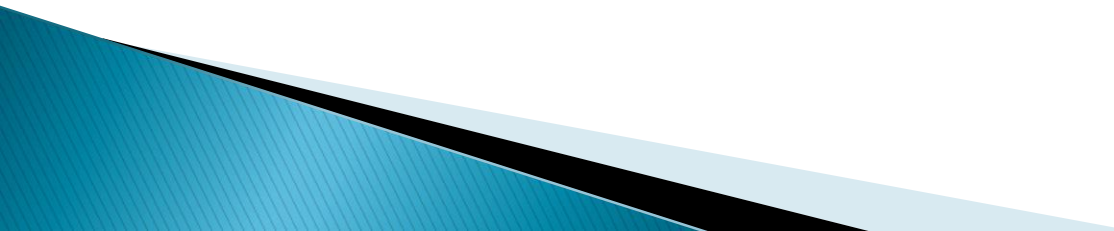


# Deep packet layer firewall

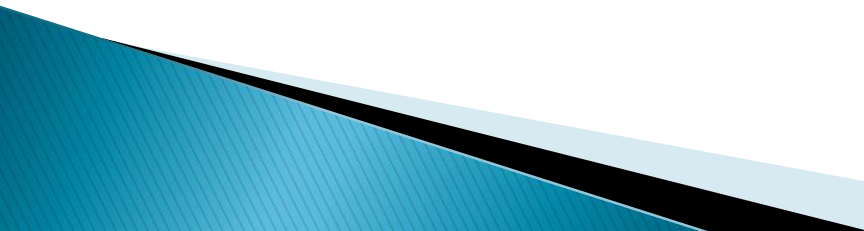
- ▶ Dengan Deep packet layer firewall melakukan inspeksi informasi jaringan berdasarkan alamat ip sumber dan tujuan serta alamat port sumber dan tujuan
  - ▶ Deep packet layer firewall juga menginspeksi protokol dan melakukan monitor terhadap sebuah penyerangan pada tahap aplikasi
  - ▶ Deep packet layer firewall juga menjaga integritas dari data yang berjalan diantara perangkat jaringan
- 



# Feature dari Firewall

- ❑ NAT
  - ❑ Proxy services
  - ❑ Content filtering
  - ❑ Antivirus software
- 

# NAT (Network Address Translation)

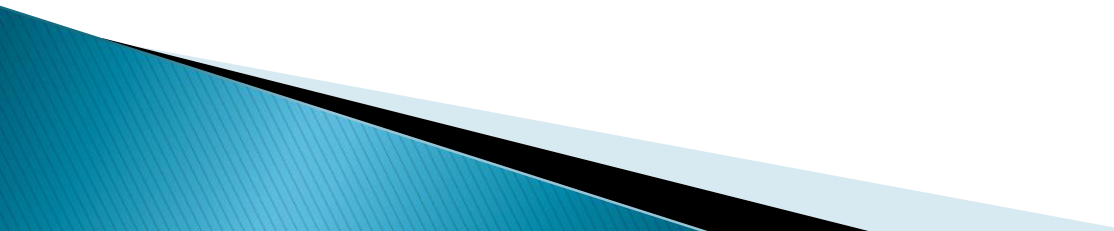
- ▶ Sebuah router atau firewall memiliki fungsi yang tujuan utamanya adalah untuk menerjemahkan alamat host di balik firewall atau router
  - ▶ Mengatasi kekurangan alamat IP pengguna saat ini
  - ▶ Nat mentranslasikan alamat ip privat yang tidak terdaftar kesebuah alamat ip global(unik) sehingga jaringan lokal pun dapat berkomunikasi dengan internet(web).
  - ▶ Command untuk menampilkan tabel translasi NAT pada CLI interface → **show ip nat translations**
- 

```
IAR#show ip nat translation
```

Pro	Inside global	Inside local	outside local	Outside global
tcp	171.71.1.1:3598	10.10.10.2:3598	198.133.219.25:80	198.133.219.25:80
tcp	171.71.1.1:3612	10.10.10.3:3612	198.133.219.25:80	198.133.219.25:80
tcp	171.71.1.1:3616	10.10.10.4:3616	198.133.219.25:80	198.133.219.25:80
tcp	171.71.1.1:3620	10.10.10.5:3620	198.133.219.25:80	198.133.219.25:80

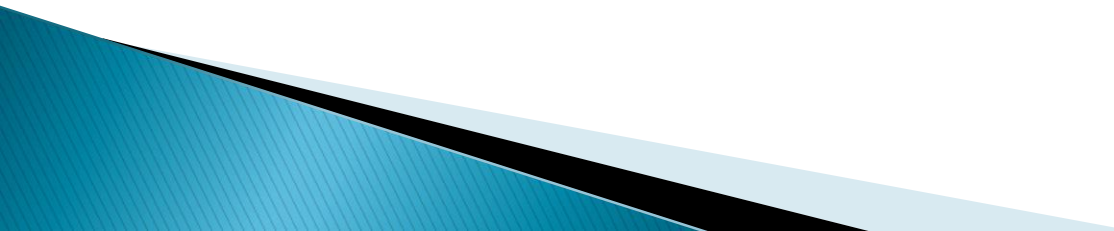
```
IAR#
```

- ▶ Inside local → Alamat IP yang ditetapkan untuk sebuah host pada jaringan internal, yang merupakan alamat logis yang tidak diiklankan ke Internet. Ini adalah alamat yang umumnya diberikan oleh administrator lokal. Alamat ini bukan alamat Internet yang sah.
- ▶ Inside global → Sebuah alamat IP terdaftar yang sah sebagaimana ditugaskan oleh interNIC
- ▶ Outside local → Alamat IP dari host di luar jaringan yang sedang diterjemahkan pada saat itu muncul di dalam jaringan.
- ▶ Outside global → Alamat IP dari sebuah host di jaringan luar yang sedang di translasikan oleh pemiliknya sendiri.

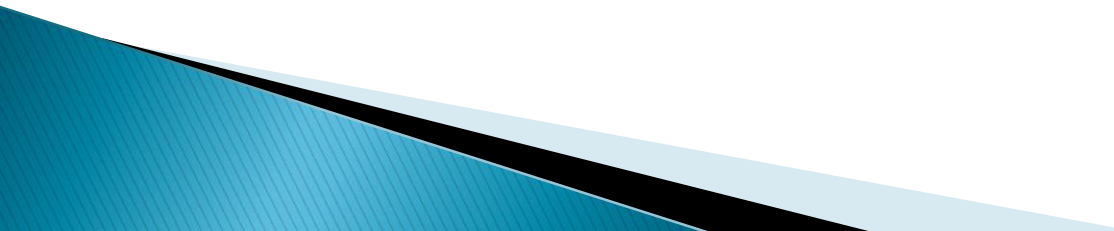
- ▶ PREROUTING → Mengubah paket yang masuk
  - ▶ POSTROUTING → Mengubah paket sebelum dikirim keluar interface
  - ▶ OUTPUT → Ubah paket lokal sebelum dikirim keluar interface
  - ▶ CHAIN = Sekumpulan Rule
- 



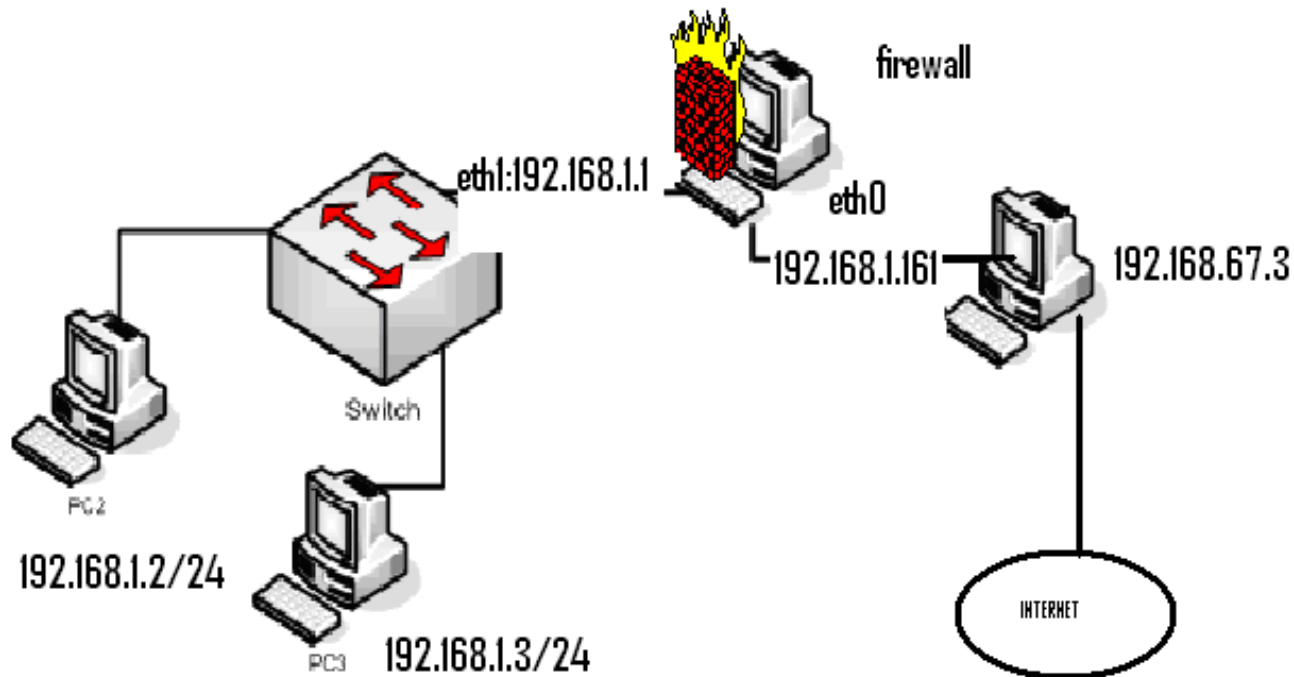
# Proxy Service

- ▶ Proxy dapat digunakan untuk menyembunyikan alamat ip real user.
  - ▶ Jika menggunakan sebuah proxy, maka semua route akan diarahkan melewati proxy tersebut.
  - ▶ Proxy juga dapat menyimpan informasi yang sering digunakan oleh seorang user
- 

# Content Filter

- ▶ Memungkinkan adanya sebuah desain kebijakan mengenai akses yang diperbolehkan ataupun tidak.
  - ▶ Memonitor, mengatur dan membatasi akses terhadap penggunaan internet
  - ▶ Cisco menyediakan beberapa mesin untuk content filtering yang akan menolak akses ke sebuah URL yang ada dalam sebuah list, mengizinkan akses hanya ke URL tertentu, menggunakan server autentikasi dengan skema penyaringan URL tertentu.
- 

# Contoh penerapan Iptables



# IPTABLES

Saat ini iptables merupakan firewall yang cukup dominan digunakan karena memiliki berbagai macam kemampuan untuk melakukan pengaturan terhadap keluar masuknya paket data. Pada dasarnya terdapat 2 aturan utama atau biasa disebut dengan *CHAINS*.

- ▶ INPUT

Aturan yang digunakan oleh firewall untuk mengatur paket – paket data yang menuju Firewall.

- ▶ FORWARD

Aturan yang digunakan oleh firewall untuk mengatur paket – paket yang meninggalkan Firewall menuju ke jaringan yang lain.

- ▶ Paket – paket data yang ada akan diperiksa untuk kemudian diberikan keputusan, ada beberapa keputusan yang diterapkan antara lain :

- ▶ ACCEPT

Apabila ditemukan paket yang sesuai dengan aturan untuk di-ACCEPT, maka firewall akan langsung menerima untuk kemudian meneruskan paket tersebut.

- ▶ DROP

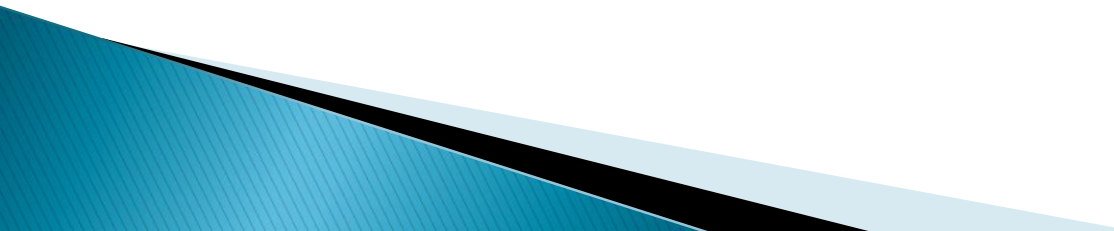
Apabila ditemukan paket yang sesuai dengan aturan untuk di-DROP, maka firewall akan langsung membuang paket tersebut tanpa mengirimkan pesan ERROR apapun ke pengirim.

- ▶ REJECT

Apabila ditemukan paket yang sesuai dengan aturan untuk di-REJECT, maka firewall akan langsung membuang paket tersebut namun disertai dengan mengirimkan pesan ERROR ICMP “port unreachable”

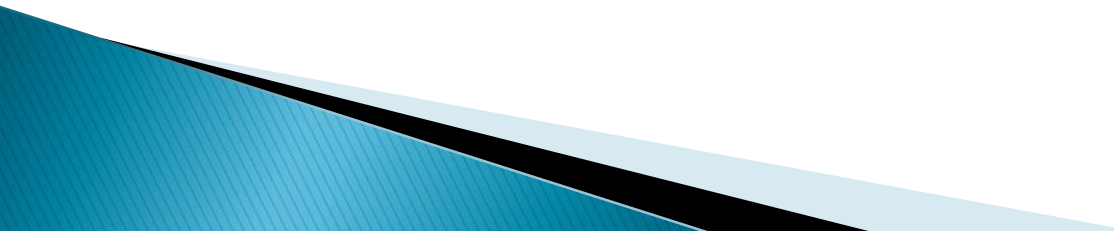
- ▶ **-L [list]**
- ▶ Perintah ini digunakan untuk menampilkan semua aturan yang telah dibuat sebelumnya
- ▶ **-A [append]**
- ▶ Perintah ini digunakan untuk menerapkan satu aturan baru yang akan ditempatkan di baris yang paling bawah dari aturan – aturan yang telah dibuat sebelumnya.
- ▶ **-R [replace]**
- ▶ Perintah ini digunakan untuk memasukkan aturan baru yang diletakkan pada baris yang kita tentukan sendiri dan aturan yang ada pada baris tersebut akan dihapus.
- ▶ **-D [delete]**
- ▶ Perintah ini digunakan untuk menghapus baris aturan yang telah dibuat sebelumnya. Gunakan perintah iptables -L terlebih dahulu untuk mengetahui urutan baris aturan yang ada.
- ▶ **-F[flush]**
- ▶ Perintah ini digunakan untuk menghapus semua aturan yang telah ditetapkan.
- ▶ **-p [jenis protocol]**
- ▶ Parameter ini berfungsi untuk membuat aturan berdasarkan jenis protocol yang digunakan, misalnya TCP,UDP,ICMP.

## Target

- ▶ Iptables memiliki sejumlah keputusan untuk diterapkan terhadap suatu paket yang diawali dengan -j [jump]. Adapun beberapa keputusan yang sering dipakai adalah sebagai berikut :
  - ▶ DROP
  - ▶ REJECT
  - ▶ ACCEPT
- 

- ▶ `Iptables -t NAT POSTROUTING -o eth0 -s 192.168.10.0/29 -j SNAT --to 202.100.10.1`  
(mentranslasikan alamat lokal 192.168.10.0/29 sehingga bisa berkomunikasi ke internet:202.100.10.1)
- ▶ `Iptables -A INPUT -i eth1 -j DROP`  
(efeknya: workstation hanya bisa berkomunikasi sampai pada eth1)
- ▶ `Iptables -A INPUT -i eth1 -s 192.168.10.2 -j DROP`  
(hanya workstation 192.168.10.2 saja yang tdk bisa ke firewall)

# KASUS

1. koneksikanlah agar ip 192.168.1.0/24 bisa melakukan transmisi dengan internet
  2. Port yang diijinkan adalah hanya port 80 selain itu ditutup
  3. Semua koneksi ke internet hanya bisa melalui web cache port 8080
  4. Firewall bisa diremote dengan ssh selain itu tutup namun dari firewall bisa melakukan ftp dan ssh ke gateway selain itu tutup
- 



1. `iptables -t nat -A POSTROUTING -o eth0 -s 192.168.1.0/24 -j SNAT --to 202.101.10.1`

2. `iptables -A FORWARD -p tcp -d  
202.101.10.1 --dport 80 -j ACCEPT`

`iptables -A FORWARD -p tcp -d  
202.101.10.1 -j DROP`