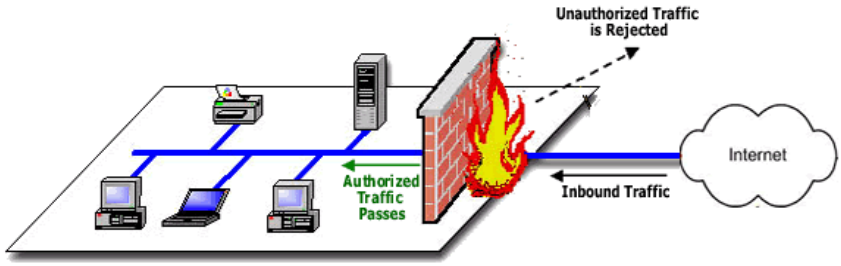
13. Firewall & Proxy

Pendahuluan

Firewall adalah perangkat keras ataupun perangkat lunak yang dirancang untuk melakukan pencegahan akses yang tidak berwenang ke atau dari jaringan privat. Firewall biasanya berupa kumpulan program yang terkait dan terpasang pada komputer gateway (router) yang melindungi sumber daya jaringan privat dari pengguna pada jaringan lainnya. Firewall, ditempatkan pada tingkat jaringan dan bekerja sama dengan router,menyeleksi semua paket jaringan untuk menentukan apakah dapat atau tidak untuk meneruskannya ke arah tujuan masing masing paket.

Dalam definisi lain, firewall adalah mekanisme atau metode untuk malakukan investigasi, seleksi, translasi, dan modifikasi paket jaringan yang masuk atau keluar dari suatu jaringan menunju jaringan lainnya.

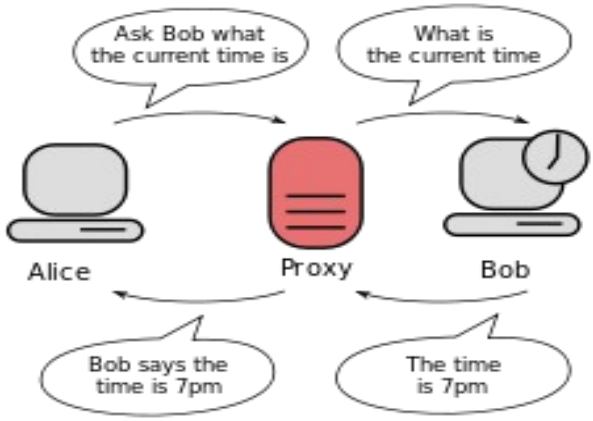


Gambar 1: Ilustrasi Firewall

Proxy Services

Layanan proxy adalah aplikasi atau program server khusus yang biasanya berjalan pada host firewall atau router (dual-homed host) dengan dua antarmuka, yang satu pada jaringan internal dan satu lagi di jaringan eksternal, atau pada host lain yang memiliki akses ke Internet dan dapat diakses dari jaringan internal. Program proxy ini mengambil permintaan pengguna untuk layanan Internet (seperti FTP dan HTTP) dan meneruskannya, sesuai sesuai dengan kebijakan keamanan, dengan layanan yang sebenarnya.

Proxy menyediakan koneksi pengganti dan bertindak sebagai gateway untuk layanan. Untuk alasan ini, proxy kadang-kadang dikenal sebagai gateway level aplikasi.



Gambar 2: Ilustrasi proxy

Lab 13.1. Pengaturan Firewall

- Gunakan tool iptables untuk mengatur rule firewall pada komputer Anda dengan skenario sebagai berikut:
  - Pada komputer Anda telah berjalan sejumlah service seperti service ssh (port 22), service web (port 80) dan service email smtp (port 25), dan pop3 (port 110) .
  - Hapus dahulu seluruh rule firewall yang mungkin telah ada sebelumnya
  - Komputer Anda berada dalam segmen jaringan 192.168.6.0/24 .
  - Anda akan mengatur kebijakan atau aturan firewall dimana komputer yang bernomor IP 192.168.6.200, 192.168.6.201 tidak diperbolehkan mengakses service email smtp dan pop3, namun service yang lainnya diperbolehkan. Komputer komputer yang lainnya dalam jaringan 192.168.6.0/24 diperbolehkan.
  - Anda juga akan mengatur bahwa komputer 192.168.6.100 tidak diperbolehkan mengakses service ssh. Sedangkan komputer lainnya dalam jaringan 192.168.6.0/24 diijinkan.
  - Anda juga akan mengatur bahwa komputer dengan range alamat IP mulai 192.168.6.60 s/d 192.168.6.70 tidak diijinkan mengakses layanan web.
  - Komputer 192.168.6.251 tidak dijinkan mengirim paket icmp (ping) ke komputer Anda.

- Dengan skenario seperti yang telah ditentukan diatas, lakukan konfigurasi atau pengaturan firewall dengan perintah berikut ini:
  - Menghapus rule firewall yang telah ada sebelumnya:

```
# sudo iptables -t filter -F
# sudo iptables -t nat -F
# sudo iptables -t mangle -F
# sudo iptables -t filter -P ACCEPT
```

- Lakukan pengaturan firewall untuk skenario diatas, dengan menjalankan perintah berikut.

```
# sudo iptables -I INPUT -m multiport -p tcp --dports 25,110 -s
192.168.6.200 -j REJECT
# sudo iptables -I INPUT -m multiport -p tcp --dports 25,110 -s
192.168.6.201 -j REJECT
# sudo iptables -I INPUT -p tcp --dport 22 -s 192.168.6.100 -j
DROP
# sudo iptables -I INPUT -m iprange -p tcp --dport 80 –src-range
192.168.6.60-192.168.6.70 -j DROP
# sudo iptables -I INPUT -p icmp --icmp-type 8 -s 192.168.6.251
-j DROP
```

- Lihat daftar rule firewall saat ini dengan perintah :

```
# sudo iptables -nL –line-numbers
atau
# sudo iptables -nvL –line-numbers
```

- Lakukan pembuktian !! apakah rule rule tersebut berjalan sebagaimana yang diharapkan
- Simpan rule firewall tersebut.

```
# sudo iptables-save > /etc/myrules-iptables.txt
```

- Agar tiap kali proses booting komputer seluruh rule yang telah Anda buat selalu diterapkan, maka tambahkan perintah berikut ini kedalam isi file /etc/rc.local, diatas perintah 'exit 0' :

```
/sbin/iptables-restore < /etc/myrules-iptables.txt
```

Lab 13.2. Instalasi squid proxy server

- Periksa apakah pada sistem komputer Anda telah terinstal aplikasi squid proxy server

```
# sudo dpkg-query -l squid3
# sudo which squid3
```

- Jika belum terinstall squid maka lakukan instalasi squid dengan perintah berikut ini:

```
# sudo apt-get install squid3
```

- Pastikan service squid berjalan dengan merestart service squid:

```
# sudo /etc/init.d/squid3 restart
atau
# sudo initctl stop squid3
# sudo initctl start squid3
```

- Uji coba squid dengan cara mengatur web browser pada komputer Anda agar menggunakan proxy dengan mengatur koneksi jaringan pada konfigurasi web browser menggunakan proxy secara manual. Tentukan host proxy dengan alamat IP komputer proxy Anda, dan isilah nomor port dengan nomor 3128 .
- Coba kemudian Anda mengakses internet apa yang terjadi ?

Lab 13.3. Mengatur ACL pada Proxy

- Aturlah kontrol akses (ACL) pada proxy server Anda dengan skenario berikut ini:
  - Diasumsikan jaringan komputer Anda memiliki alamat jaringan 192.168.6.0/24
  - Atur agar proxy server hanya mengijinkan akses internet untuk seluruh komputer dalam jaringan 192.168.6.0/24 pada hari senin sampai dengan jumat , mulai jam 09.00 sampai 13:00
  - File pdf dan mp3 tidak diperbolehkan diakses
  - Beberapa situs berikut tidak diperbolehkan diakses, yaitu situs www.detik.com dan www.kompas.com
  - Komputer dengan alamat IP 192.168.6.10 sampai 192.168.6.20 diperbolehkan akses apapun dan kapanpun
- Dengan skenario seperti yang telah ditentukan diatas, lakukan konfigurasi atau pengaturan proxy dengan mengedit file /etc/squid3/squid.conf ,dan tambahkan baris-baris berikut ini di bawah baris dengan keterangan " *INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS FROM YOUR CLIENTS*" :

```
# Definisi ACL
acl mynet src 192.168.6.0/24
acl waktu_boleh time MTWHF 09:00-13:00
acl vip src 192.168.6.10-192.168.6.20/32
acl file_diblok url_regex -i \.pdf \.mp3
acl web_diblok dstdomain .detik.com .kompas.com

# Definisi Rule HTTP akses
http_access allow vip
http_access deny !waktu_boleh
http_access deny file_diblok
http_access deny web_diblok
http_access allow mynet
```

- Setelah itu coba restart service proxy
- Dan lakukan pengujian sesuai skenario
- Perhatikan log squid, dengan perintah berikut ini:
  `# sudo tail -f /var/log/squid3/access.log`
- Berdiskusilah dengan rekan Anda !