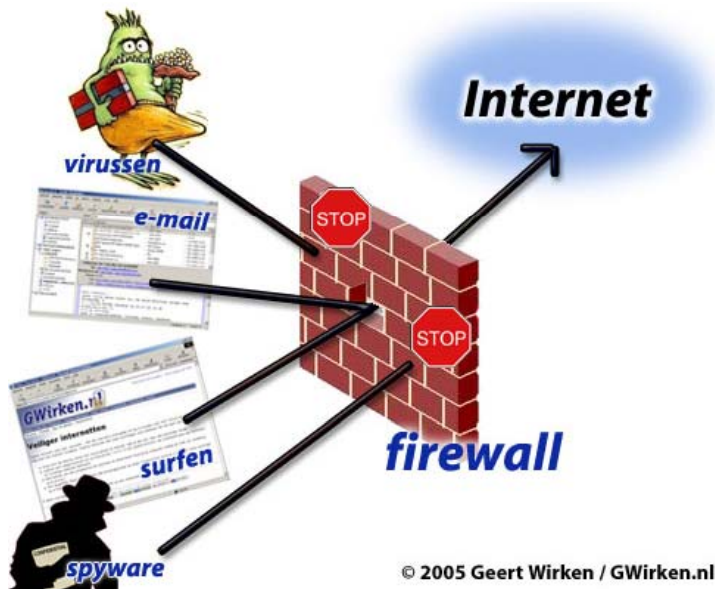


TCP WRAPPER

1



Muhammad Zen S. Hadi, ST. MSc.

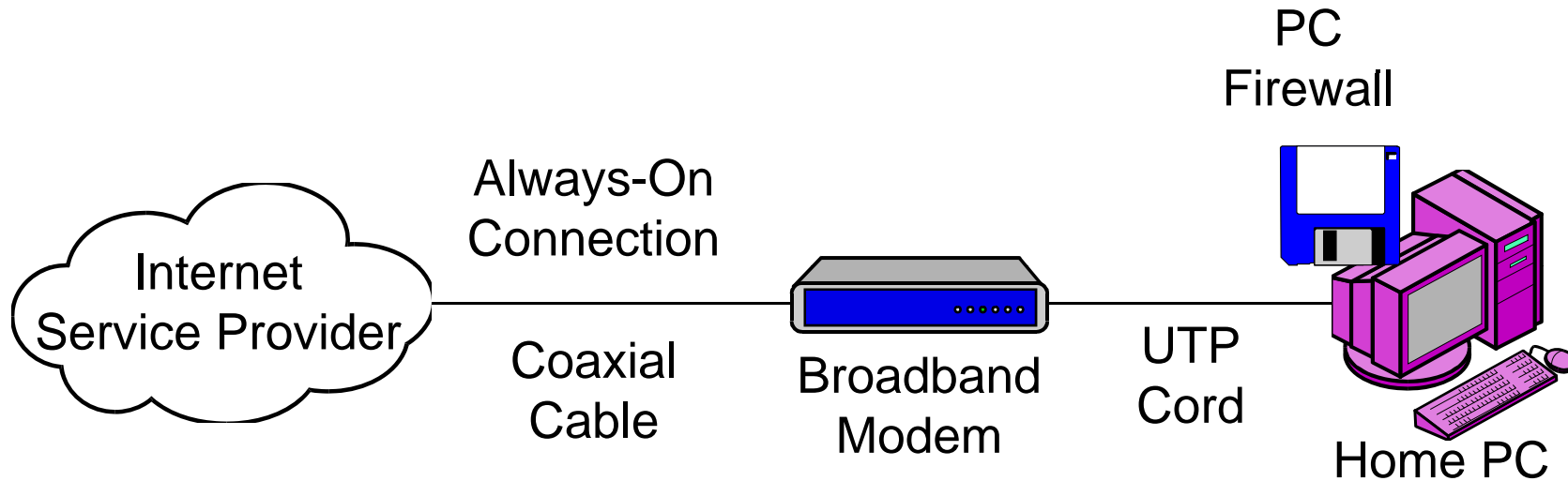
© 2005 Geert Wirken / GWirken.nl

Architecture Firewall

2

Home Firewall Architecture

3



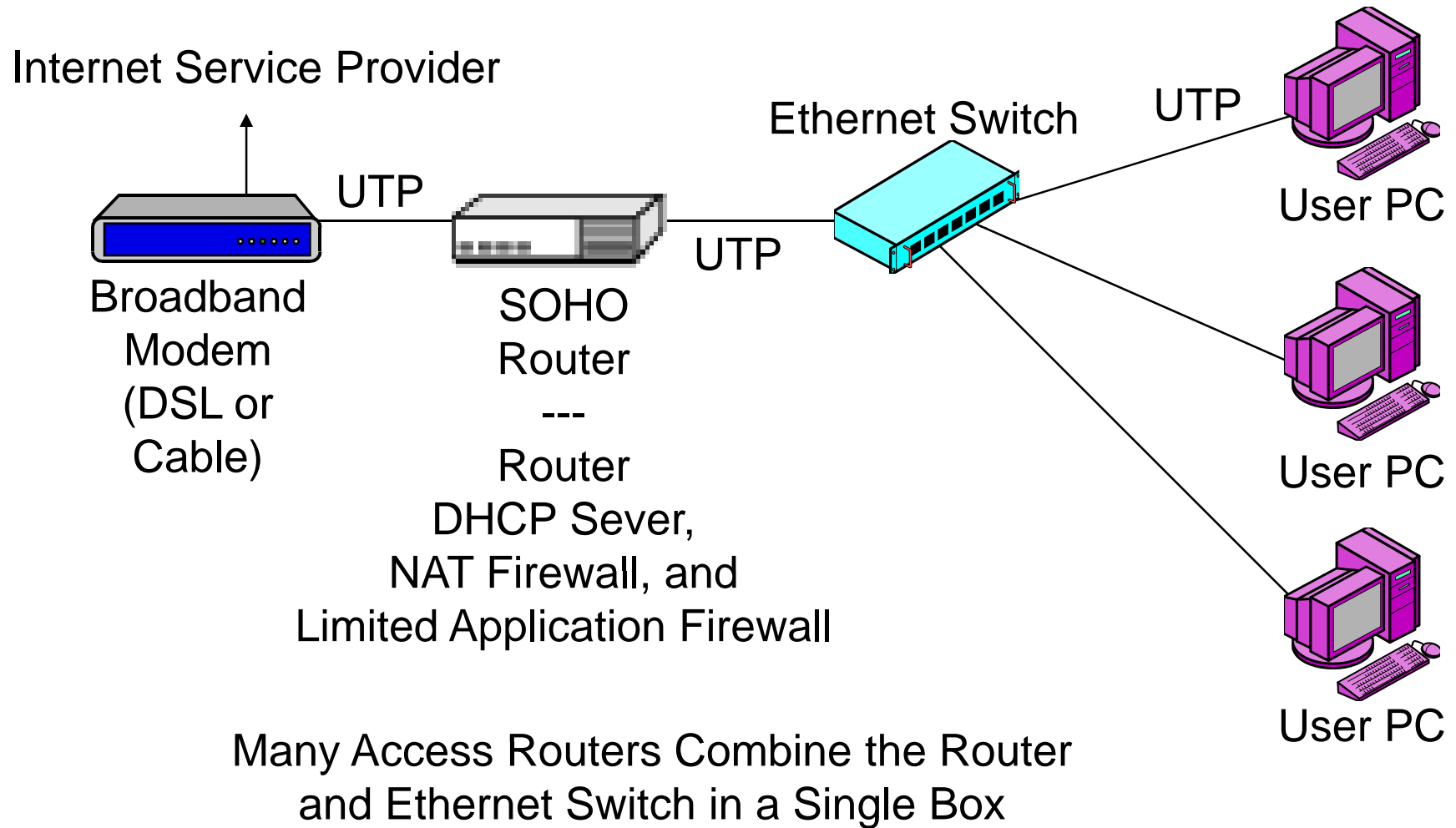
Windows XP has an internal firewall

Originally called the Internet Connection Firewall
Disabled by default

After Service Pack 2 called the Windows Firewall
Enabled by default

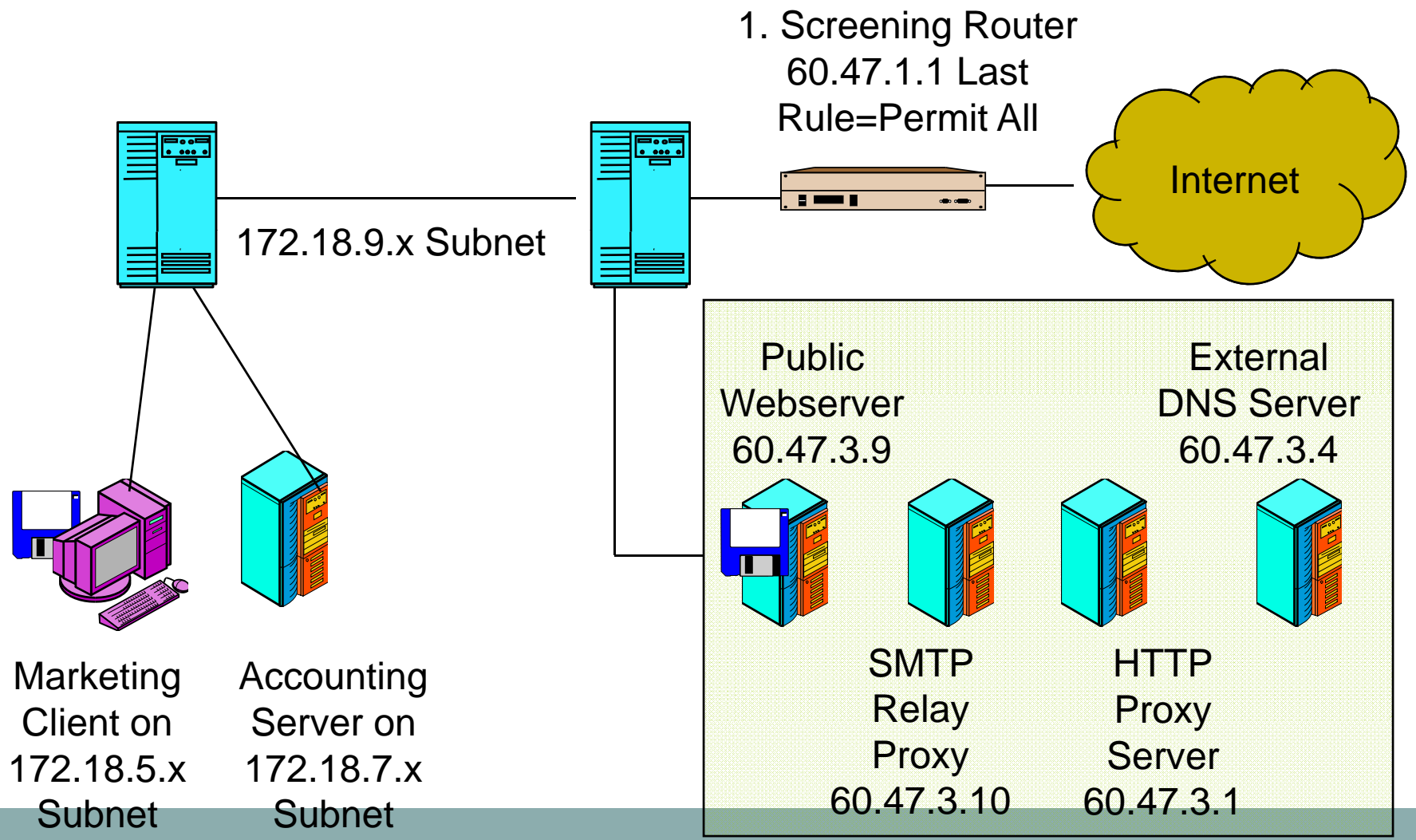
SOHO Firewall Router Architecture

4



Firewall Architecture for a Larger Firm with a Single Site

5



Setting Firewall

6

- Penggunaan “DMZ” (DeMilitarized zone)
- Firewalls sebagai perangkat Intrusion Detection
- Konfigurasi VPN untuk management

DMZ Configuration

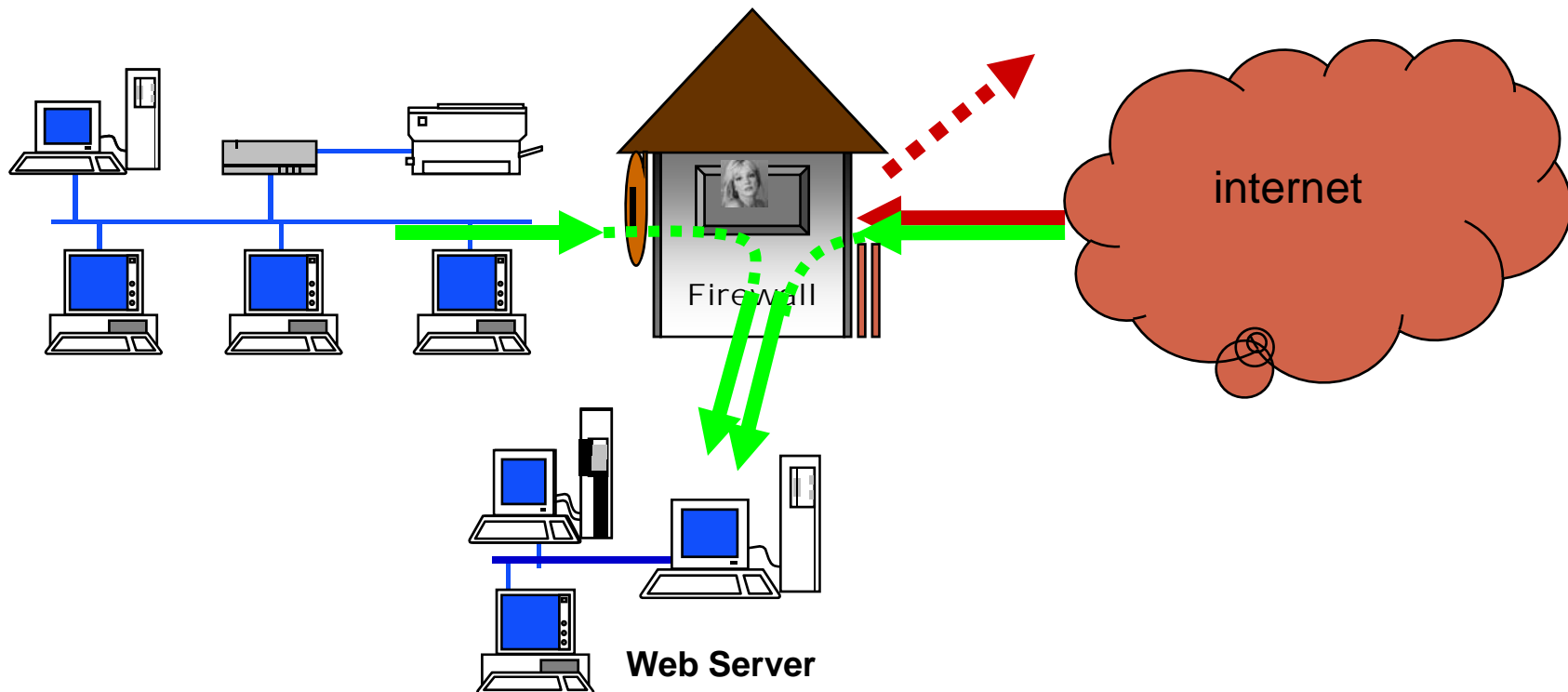
7

- Memisahkan area dengan firewall
- Membedakan segmen network yang mempunyai kebijakan yang berbeda pula
 - Departments
 - Service areas
 - Public Services
 - Internal Services
- Biasanya berbeda subnet
- Umumnya digunakan untuk melindungi mesin yang berhubungan lgs dengan internet (misal Web Servers)
- Mempunyai kebijakan firewall sendiri

DMZ Configuration

8

- Menempatkan web server dalam jaringan “DMZ”
- Hanya mengizinkan web ports (TCP port 80 dan 443)

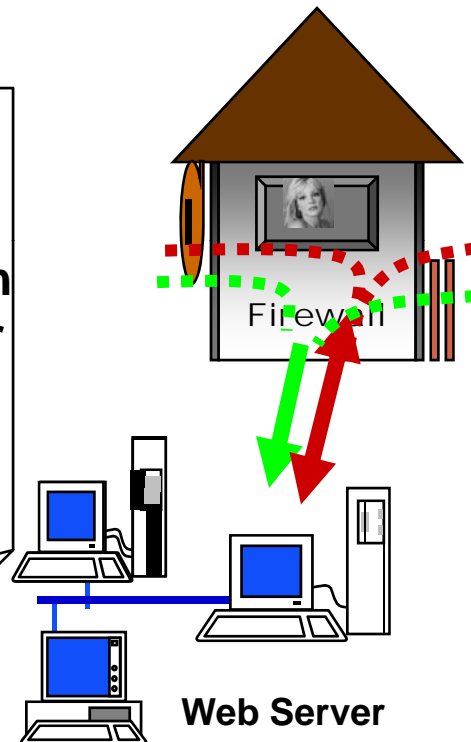


DMZ Configuration

9

Jaringan Lokal:

- Semua boleh menghubungi web-server (port 80/443)
- PC-PC tertentu boleh menghubungi server lewat SSH (port 22)
- Server tidak boleh menghubungi jaringan lokal



Internet:

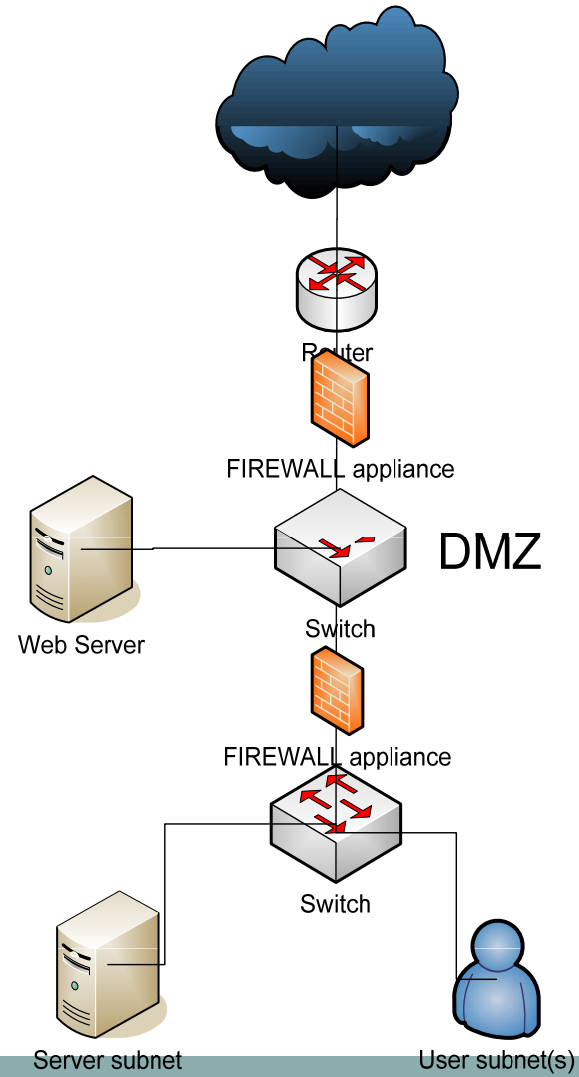
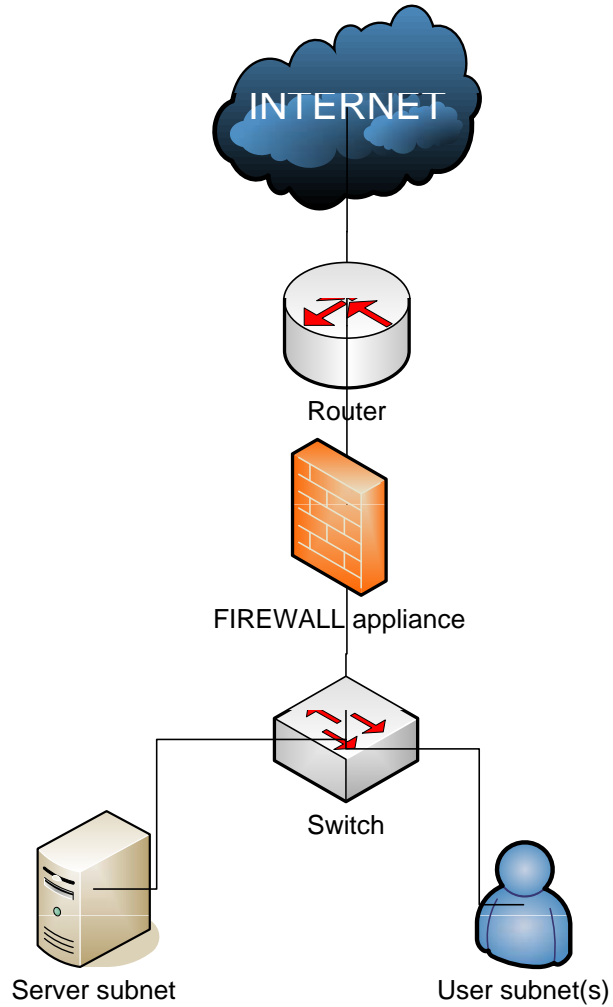
- Semua boleh menghubungi web-server (port 80/443)
- Selain layanan web tidak diperkenankan
- Server tidak boleh jalan-jalan di internet

Firewall rules



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

DMZ Configuration



Firewall sebagai IDS

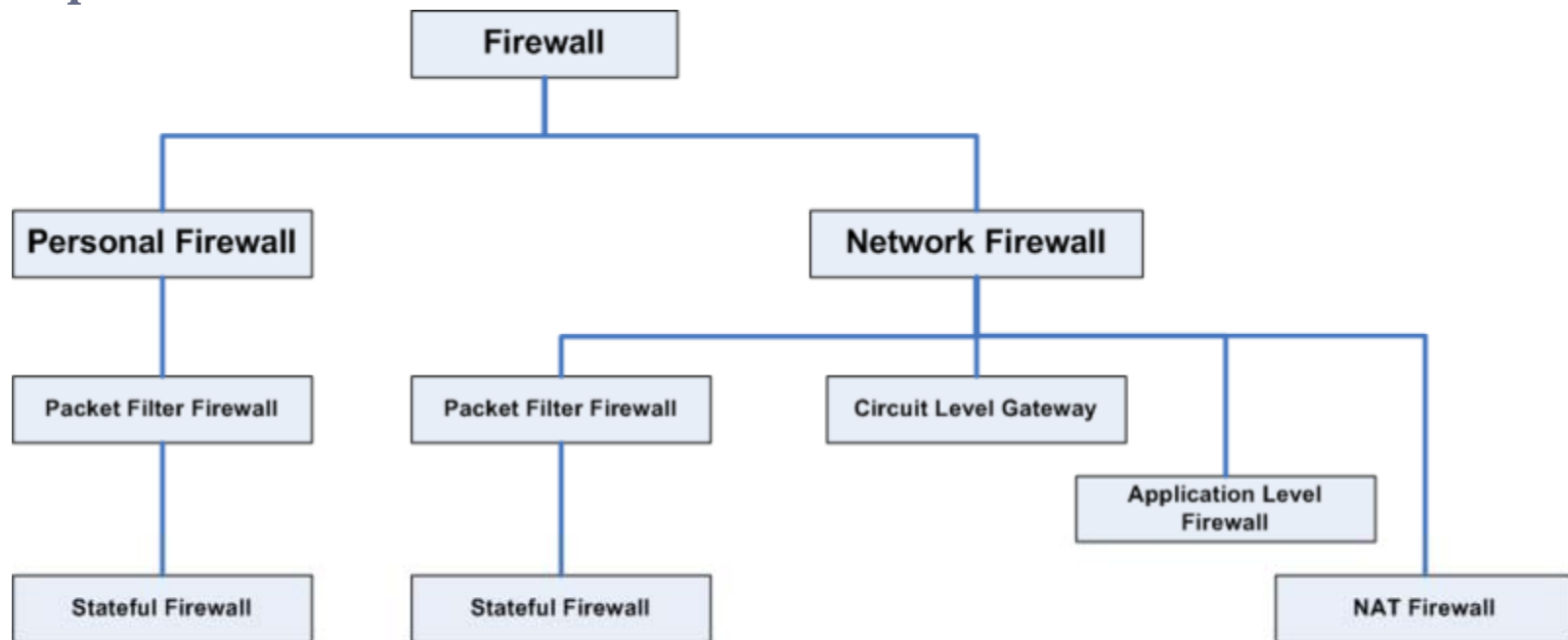
12

- **IDS = Intrusion Detection System**
- **Mengumpulkan informasi log dari aturan yang ditolak**
- **Mencari Portscanning, hacking, dll...**
- **Bisa digunakan untuk memblokir portscan**
- **Perhatikan trafik yang meninggalkan DMZ**

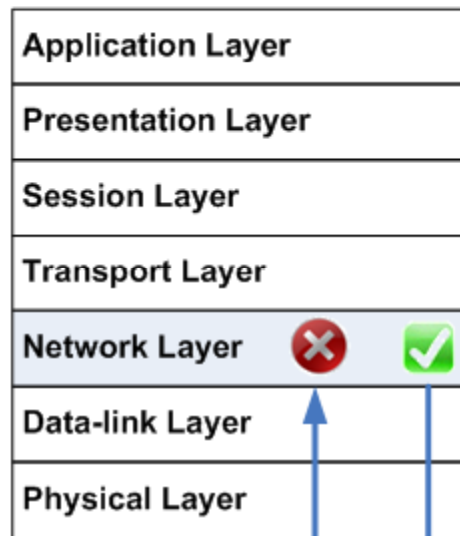
Firewall



- Packet filter
- Stateful
- Application proxy firewalls
- Implementation:
 - iptables



Packet Filtering Firewall



Lalu lintas akan disaring berdasarkan banyak karakteristik, seperti alamat IP atau nomor port.

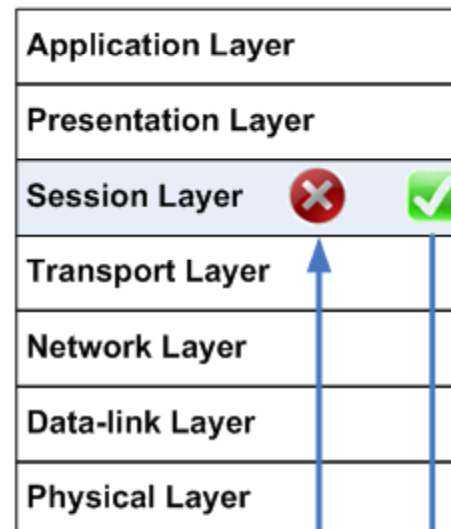
Lalu lintas yang tidak lolos penyaringan akan diblok pada level network layer

Lalu lintas yang datang → ← Lalu lintas yang diizinkan

Contoh : router

Contoh : proxy server

Circuit Level Firewall

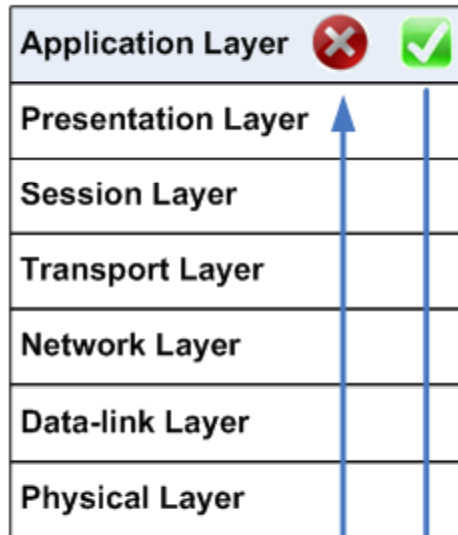


Lalu lintas akan disaring berdasarkan peraturan sesi yang spesifik.

Lalu lintas yang tidak lolos penyaringan akan diblok pada level Session layer.

Lalu lintas yang datang → ← Lalu lintas yang diizinkan

Application Layer Firewall



Lalu lintas akan disaring berdasarkan peraturan aplikasi yang spesifik.

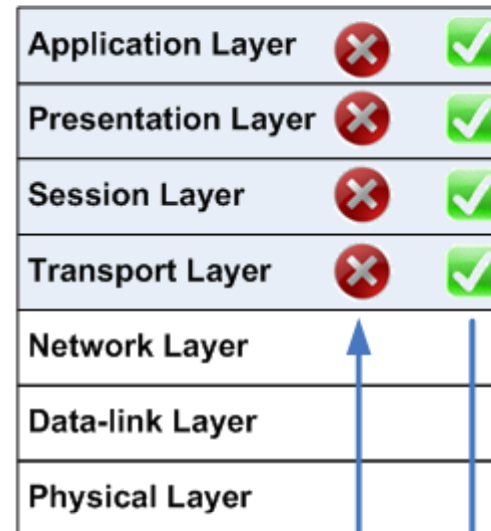
Lalu lintas yang tidak lolos penyaringan akan diblok pada level application layer.

Lalu lintas yang datang

Lalu lintas yang diizinkan

Contoh : proxy FTP / SMTP,
TCP Wrapper

Contoh : Gabungan
Cisco PIX – Private Internet Exchange
Cisco ASA – Adaptive Security Appliance
Stateful Firewall



Lalu lintas akan disaring pada banyak level berdasarkan peraturan packet filtering, session, atau aplikasi.

Lalu lintas yang tidak lolos penyaringan akan diblok pada level Network Layer

Lalu lintas yang datang

Lalu lintas yang diizinkan

TCP Wrapper

16

Pengertian TCP Wrapper



- TCP wrapper merupakan salah satu metode filter (*access control list*) di sistem operasi Unix Like untuk membatasi suatu host yang ingin menggunakan service yang ada di server.
- Program ini bekerja dengan cara membungkus `inetd` ([internet](#) daemon : aplikasi yang menjalankan servis-servis internat) agar lebih aman.
- **TCP Wrapper** – lapisan network yang digunakan untuk memonitor dan mengontrol trafik TCP di server pada level aplikasi.

TCP Wrapper

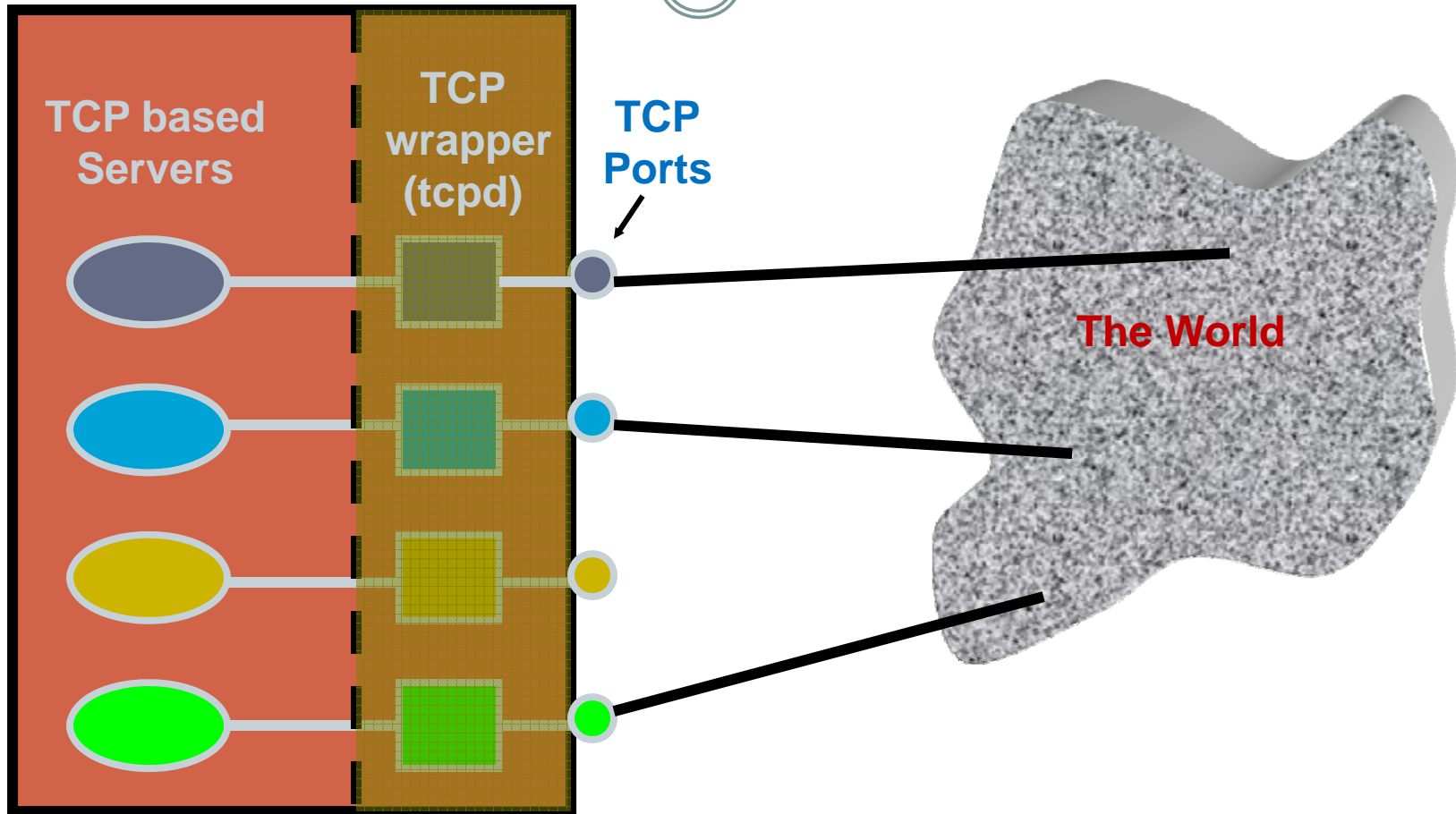
18

- TCP wrapper adalah sistem yang menyediakan fasilitas seperti firewall.
- Sebuah host (dengan beberapa service) diisolasi dari jaringan luar.
- Fungsi yang disediakan seperti log dari request dan access control.

TCP Wrapper

Single Host

19



tcpd

20

- **tcpd** daemon mengecek hubungan TCP yang datang sebelum real server mendapatkan koneksinya.
- **tcpd** dapat mencari alamat IP dan no port dari sumber (*authentication*).

tcpd (cont.)

21

- Log message yang dihasilkan menyatakan nama service, alamat client dan waktu koneksinya.
- `tcpd` dapat menggunakan alamat client untuk meng-otorisasi setiap permintaan layanan.

Typical `tcpd` setup

22



- `inetd` (the SuperServer) menginisialisasi `tcpd` sebagai pengganti real server.
- Super Daemon `inetd` sekarang memiliki tcp wrapper yang sudah built in sehingga semua service yang berbasis `inetd` dapat memanfaatkannya.
- `tcpd` mengenali client dengan memanggil fungsi `getpeername` pada descriptor 0.
- `tcpd` mengaktifkan real server dengan memanggil fungsi `exec`.

tcpd configuration

23

- Configuration file pada tcpd menentukan host mana yang diijinkan / ditolak (allow / deny) pada suatu service.
- Semua *domains* atau IP networks dapat diijinkan atau ditolak secara mudah.
- Service pada inetd

```
ftp      stream  tcp     nowait  root    /usr/sbin/tcpd  in.ftpd -l -a
telnet   stream  tcp     nowait  root    /usr/sbin/tcpd  in.telnetd
shell    stream  tcp     nowait  root    /usr/sbin/tcpd  in.rshd
login    stream  tcp     nowait  root    /usr/sbin/tcpd  in.rlogind
talk     dgram   udp     wait    nobody.tty /usr/sbin/tcpd  in.talkd
ntalk    dgram   udp     wait    nobody.tty /usr/sbin/tcpd  in.ntalkd
pop-3    stream  tcp     nowait  root    /usr/sbin/tcpd  ipop3d
imap     stream  tcp     nowait  root    /usr/sbin/tcpd  imapd
uucp     stream  tcp     nowait  uucp    /usr/sbin/tcpd  /usr/sbin/uucico -l
tftp     dgram   udp     wait    root    /usr/sbin/tcpd  in.tftpd
bootps   dgram   udp     wait    root    /usr/sbin/tcpd  bootpd
finger   stream  tcp     nowait  nobody  /usr/sbin/tcpd  in.fingerd
auth     stream  tcp     wait    root    /usr/sbin/in.identd  in.identd -e -o
```

TCP Wrappers



- Menggunakan 2 file untuk mendefinisikan akses ke service
 - `/etc/hosts.allow`
 - `/etc/hosts.deny`
- Dapat dibuat deny-by-default ke semua service yang menggunakan tcp wrappers
- Jangan berfikir bahwa hal ini akan mengamankan server 100%
 - Tidak semua service dapat menggunakan tcp wrappers
 - tcp wrapper adalah access control process

Konfigurasi TCP Wrappers

25

- File-file yang perlu diperhatikan dalam penyetingan TCP Wrappers antara lain :
 1. /etc/inetd.conf (konfigurasi internet daemon)
 2. /etc/hosts.allow (konfigurasi host-host yang diizinkan)
 3. /etc/hosts.deny (konfigurasi host-host yang ditolak)
- Pastikan dahulu bahwa TCP Wrappers sudah terinstal pada sistem kita. Untuk mengeceknya dapat dilihat pada file /etc/inetd.conf.
- TCP wrappers dapat memonitor dan memfilter incoming requests untuk telnet, ftp, rlogin, rsh, finger, talk, dan lainnya yang berjalan pada inetd.conf.
- Contoh :
telnet stream tcp nowait root /usr/sbin/tcpd in.telnetd

What TCP Wrappers does

26

1. Membuka file */etc/hosts.allow*. File ini berisi aturan akses kontrol dan aksi untuk setiap protokol.
2. Men-scan file, baris demi baris, sampai menemukan rule yang sesuai dengan protokol dan host sumber tertentu, yang terhubung ke server.
3. Menjalankan aksi yang ditentukan dalam rule diatas. Jika sesuai, kontrol akan dijalankan pada jaringan server.
4. Jika tidak ada yang match, file */etc/hosts.deny* dibuka dan akan dibaca secara berurutan baris demi baris. Jika ada baris yang sesuai, akses ditolak dan aksi yang berhubungan dengannya akan dilakukan.
5. Jika tidak ada yang sesuai pada file */etc/hosts.allow* atau */etc/hosts.deny*, kemudian koneksi akan diijinkan secara default.
Misal: */etc/hosts.deny* dapat berisi hanya sebuah rule "ALL:ALL" untuk menolak akses secara default.

TCP Wrappers

/etc/hosts.allow and **/etc/hosts.deny** syntax

daemon : hosts : options

allow
deny
spawn shell command
twist shell command
many more ...

ALL
or hostname(s)
or net., e.g. 192.168. matches all 192.168.x.x addresses
or net/netmask , e.g. 172.0.0.0/255.0.0.0 matches all
172.x.x.x addresses
more ...

ALL
or name of daemon

TCP Wrappers

- ***Daemon_list : client_host_list : option***
- Daemon List merupakan daftar daemon seperti telnetd, fingerd, ftpd, ssh, dll.
- Client Host List merupakan daftar user/host/network dan mempunyai bentuk sbb :
 - ALL : semua host
 - KNOWN : host yang terdaftar pada DNS server
 - LOCAL : host yang tidak dipisahkan oleh . (dot)
 - PARANOID : mempunyai nama dan IP address yang tidak sesuai jika dilacak dan dibandingkan antara pelacakan dari nama dengan dari nomor IP
 - UNKNOWN : host yang hanya mempunyai nomor IP tanpa nama internet
 - .eepis-its.edu : host dengan domain eepis-its.edu
 - 167.205.206.1: host dengan IP adress tertentu

TCP Wrapper Examples

```
[root@arwen ~]# cat /etc/hosts.allow
```

```
#  
# hosts.allow This file describes the names of the hosts which are  
# allowed to use the local INET services, as decided  
# by the '/usr/sbin/tcpd' server.  
#  
sshd: frodo  
vsftpd: 172.30.  
in.telnetd: 192.168.2.10 127.0.0.1
```

daemons

hosts

```
[root@arwen ~]# cat /etc/hosts.deny
```

```
#  
# hosts.deny This file describes the names of the hosts which are  
# *not* allowed to use the local INET services, as decided  
# by the '/usr/sbin/tcpd' server.  
#  
# The portmap line is redundant, but it is left to remind you that  
# the new secure portmap uses hosts.deny and hosts.allow. In particular  
# you should know that NFS uses portmap!
```

```
#deny everything
```

```
ALL: ALL
```

All daemons and all hosts

Penggunaan twist

- twist bisa digunakan untuk memberi keterangan kepada client.

- Contoh :

sshd : client1.xyz.com : twist /bin/echo "You, ip no %a, are prohibited from accessing this service!!" : deny

- Option :

%a — The client's IP address.

%A — The server's IP address.

%d — The daemon process name.

%h — The client's hostname (or IP address, if the hostname is unavailable).

%H — The server's hostname (or IP address, if the hostname is unavailable).

%p — The daemon process ID.

Contoh penggunaan tcp wrapper

- Isi /etc/hosts.allow

sshd : 202.91.15.0/28 : ALLOW

sshd : 202.91.8.36/32 : ALLOW

sshd : .akprind.ac.id : ALLOW

sshd : 10.15.74.81 : ALLOW

sshd : all : twist /bin/echo "Please call emergency service your IP %a "

- Isi /etc/hosts.allow

ALL : .xyz.com

- Isi /etc/hosts.deny

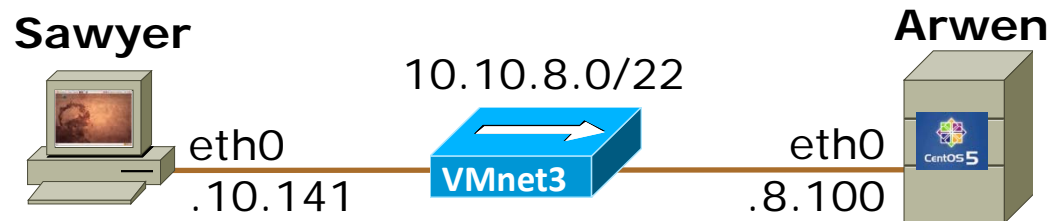
sshd : ALL EXCEPT 192.168.0.15

- Isi /etc/hosts.allow

in.telnetd : 192.168.5.5 : deny

in.telnetd : 192.168.5.6 : allow

Access controls using TCP Wrappers



- Terdapat service telnet , ssh, ftp pada Server Arwen.
- Konfigurasi di Arwen sebagai berikut :
 - a. telnet dan ssh bisa diakses oleh Sawyer
 - b. service lainnya akan ditolak oleh Arwen
 - c. Berikan keterangan pada Sawyer ketika ditolak oleh Arwen