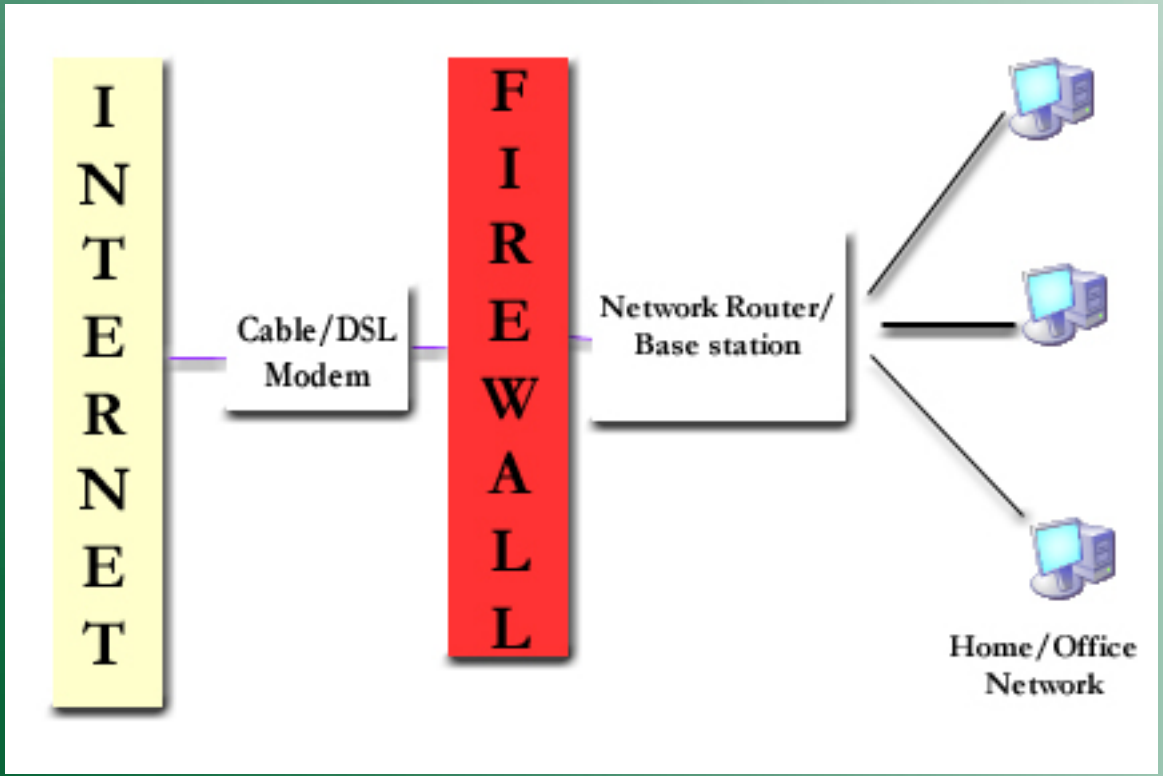
Do We Need to Worry?

- IP, port, protocol, service, application, password, operating system, network vulnerabilities
- Linux system architecture and file system is more secure with less application vulnerability
- Security configuration was enabled by default
- Your security is my security, social engineering
- We live in the attacker world, notorious criminals and undergorund organized crime

The Firewall

- A typical firewall configuration



How Firewall Works?

- Separating external/internal networks with DMZ, isolating internal network with IP translations
- Prevent unwanted incoming connection
- Stealth mode: discarding pings (hiding)
- Port forwarding and blocking unused port
- Packet filtering: allow, disallow, drop, reject or forward the traffic
- Limitating services, application and run level

Limiting Service, Apps, Run Level

- Shutdown unused services, do not install unused apps, use appropiate run level configuration
- 0 The halt runlevel - system shuts down
- 1 Single runlevel - single user mode, only the root user, does not start any networking or X. Ideal for system maintenance or repair activities
- 2 Boots - multi-user mode, text based console, but not, however, start the network

Run Level (Cont')

- 3 Similar to runlevel 2 except that networking services are started, without X
- 4 Undefined runlevel. This runlevel can be configured to provide a custom boot state
- 5 Boots the system into a networked, multi-user state with X Window System capability suitable for desktop or workstation use
- 6 Reboots the system