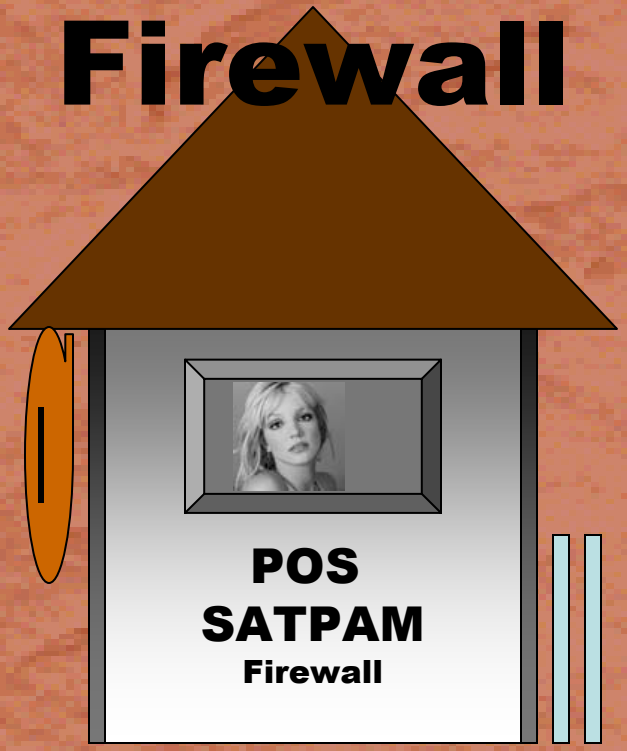
Firewall



Yudhie Kurnia Moeljanto

Apa itu firewall

- Firewall adalah suatu mekanisme, sehingga suatu client dari luar dilarang/dibolehkan mengakses ke dalam jaringan (atau client yang berada di dalam dilarang/dibolehkan mengakses keluar jaringan) berdasarkan aturan-aturan yang ditetapkan.
- Seperti pos satpam di suatu instansi/perumahan
- Bekerja di layer: antara 3 dan 4 (bahkan 5) di TCP/IP Model

Istilah-istilah

- **Masquerading**
  - Allows many machines to use the appear to come from the same IP address
  - Connections can only be initiated by internal host
- **NAT –** Network Address Translation
  - The term “NAT” can mean many different things, see RFC2663 for details
  - Generally some router-level mapping and conversion between a set of private IP addresses and a single public IP address (IP Masq) or set of public IP addresses.

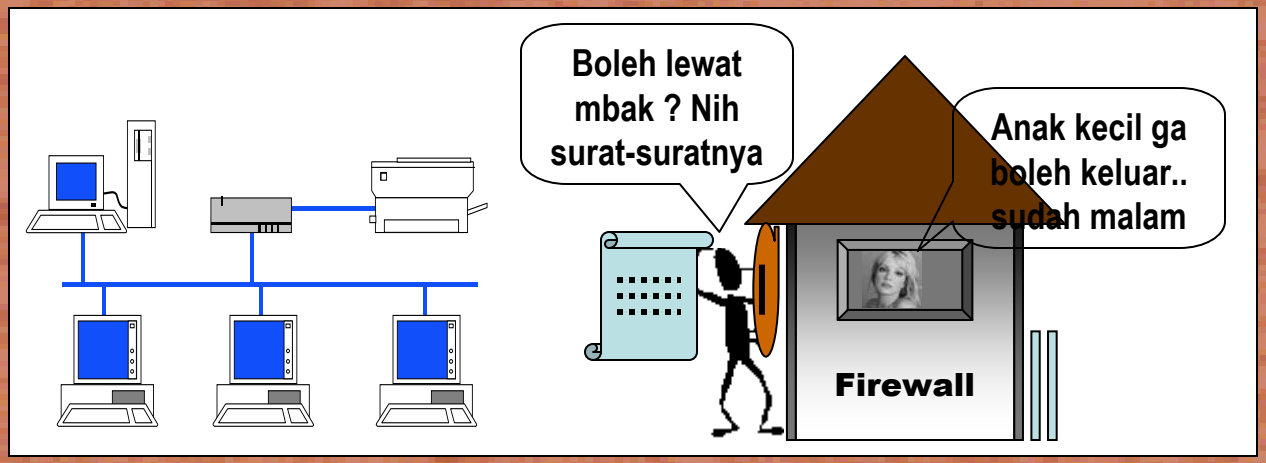
Mengapa butuh

- To implement your policy!
- To manage the risks of providing your services.
- To segregate networks with different policies.
- To provide accountability of network resources.

- Firewalls mitigate risk
- Blocking MOST threats
- They have vulnerabilities as well
- Improper configuration is the largest threat

Cara kerja

- Dengan meneliti paket-paket yang lewat firewall itu dan mencocokkannya dengan melihat daftar/aturan yang diberikan kepadanya.
- Firewalls block certain traffic, while allowing other traffic to pass.
- Different types of firewalls pass traffic using different methods
  - Packet Filtering
  - Proxy
  - Connection State Analysis



Ada dua tipe utama

- Firewalls rules are created to match policy
- Rules are based on:
  - Routing based filters (Who – siapa)
    - Sender and Destination
    - berasal dari mana ?
    - Mau ke mana ?
    - **Tidak peduli mau ngapain di sana**
  - Content based filters (What – mau apa)
    - TCP/IP Port numbers and Services
    - Apa yang akan kamu lakukan di sana ?
    - Tidak semudah yang nomer 1, sebab kadang-kadang bisa ditipu seorang client

Dua pendekatan aturan

- Default allow
  - Mengijinkan semua lewat kecuali yang terdaftar
  - Place roadblocks/watch gates along a wide open road.
- Default deny
  - Semua dilarang lewat kecuali yang terdaftar
  - Build a wall and carve paths for everyone you like.

Packet Filtering

- Simplest form of firewalling
- Can often be implemented on network equipment (routers, switches)
- Blocks certain TCP/IP Ports, protocols, and/or addresses.
- Rules are applied to the headers of the packets
- Contoh: iptables,ipchains (Linux)

Packet Filtering

- Advantages of Packet Filtering
  - High Performance
  - Can usually be applied to current routers/switches (No additional equipment!)
  - Effective
- Disadvantages of Packet Filtering
  - Can quickly become a very complex configuration
  - Easy to misconfigure
  - Difficult to configure for dynamic protocols (like FTP)
  - Can’t do any content-based filtering (remove e-mail attachments, javascript, ActiveX)

Contoh Packet Filtering

An abbreviated packet…

```
Source          SrcPort  Destination   DestPort
204.210.251.1   8104     128.146.2.205    31337
```

A Cisco packet filter

```
access-list 2640 deny any 128.146.2.0 0.0.0.255 gt
   1023
```

Proxy

- Firewall accepts requests, and executes them in behalf of the user
  - I want to see http://www.osu.edu
  - Firewall gets http://www.osu.edu content
  - Firewall sends content to requester
- Contoh: Squid

Proxy

- Advantages of Proxy Firewall
  - They don't allow direct connections between internal and external hosts
  - Can support authentication, 'classes' of users
  - Can allow/deny access based on content
  - Can keep very detailed logs of activity (including the data portions of packets)
  - Caching

Proxy

- Disdvantages of Proxy Firewall
  - Slower than packet filter firewalls
  - Require additional hardware
    - more hardware for more users
    - slow hardware = slow service
  - Some firewalls require special client configurations on the workstations.
  - Some protocols may not be supported (AIM, RealAudio, Napster, H.323) Varies by vendor.
  - Configuration can be complex
    - Must configure proxy for each protocol

Connection State Analysis

- Similar to packet filtering, but analyzes packets to make sure connection requests occur in the proper sequence.
- Example:
  - ICMP Echo Replies are not accepted through the firewall unless there is an outstanding ICMP Echo Request.

Connection State Analysis

- Advantages
  - Caching
  - Content Monitoring
- Disadvantages
  - Performance
  - Overhead requires more expensive system

Topologi

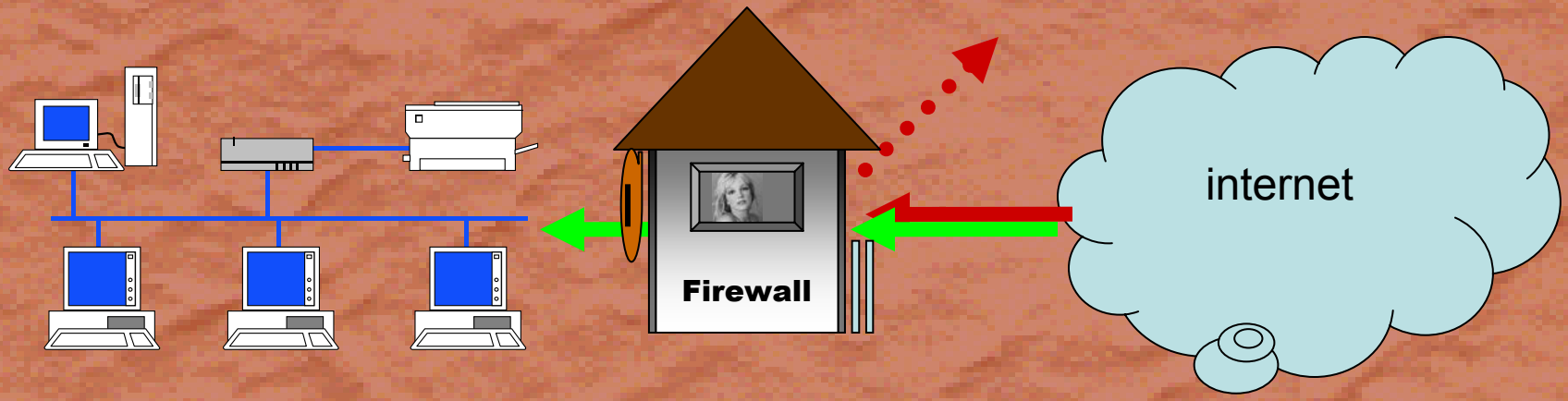
- Bridge-type firewall
  - Invisible to users
  - Easy to install for already existing networks
- Router-type firewalls
  - Has IP Address, visible to users

Topologi

- Advantages of Bridge-type firewall
  - Invisible to users
  - Easy to install for already existing networks
- Disadvantages of Bridge-type firewall
  - Requires more equipment than packet filtering
  - Rules may be more confusing to configure
- Advantages of Router-type firewall
  - Rule configuration slightly better than bridge
- Disadvantages of Router-type firewall
  - System is ‘visible’ to users and outsiders

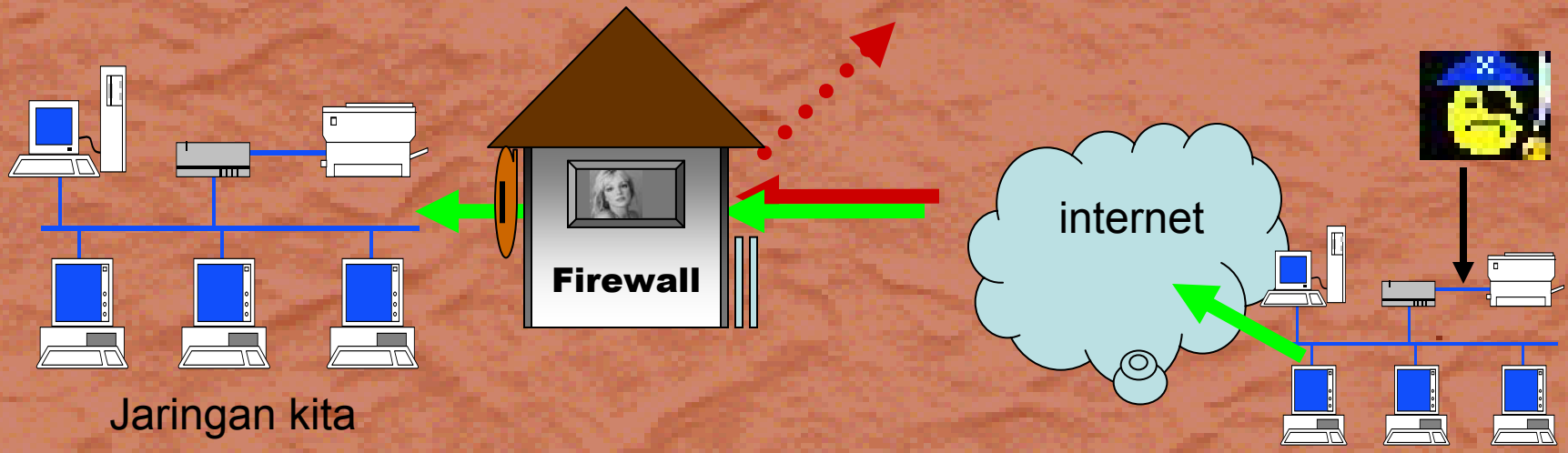
Problems

- Firewalls as filters can be considered for most part to be infallible... but as a security measure? They can only enforce rules (generally static)



Problems

- “Crunchy on the outside, but soft and chewy on the inside.”



Setting Firewall

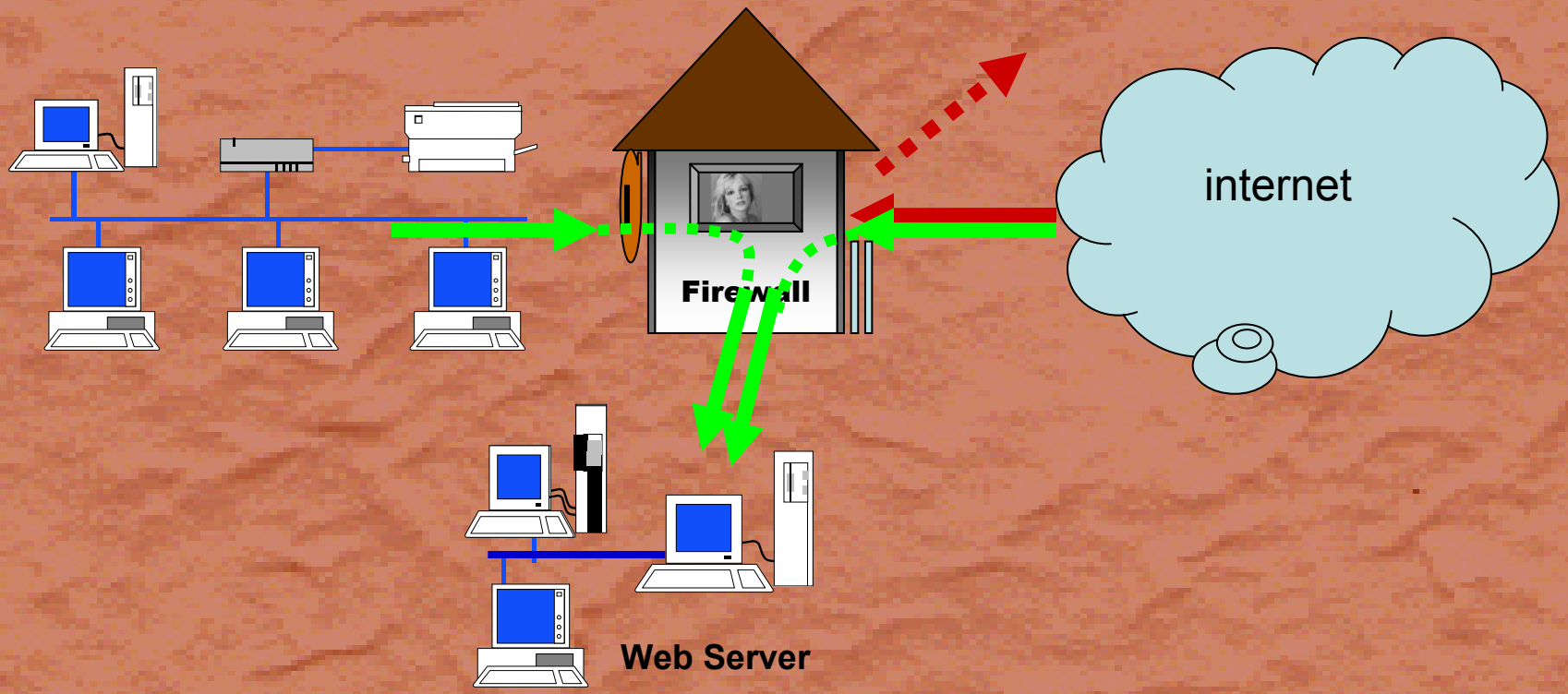
- Using the “DMZ” (DeMilitarized zone) to your advantage
- Firewalls as Intrusion Detection devices
- Configure VPN’s for management

DMZ Configuration

- Separate area off the firewall
- Different network segments may have different policies
  - Departments
  - Service areas
  - Public Services
  - Internal Services
- Usually a different subnet
- Commonly used to house Internet facing machines (i.e. Web Servers)
- Has its own firewall policy

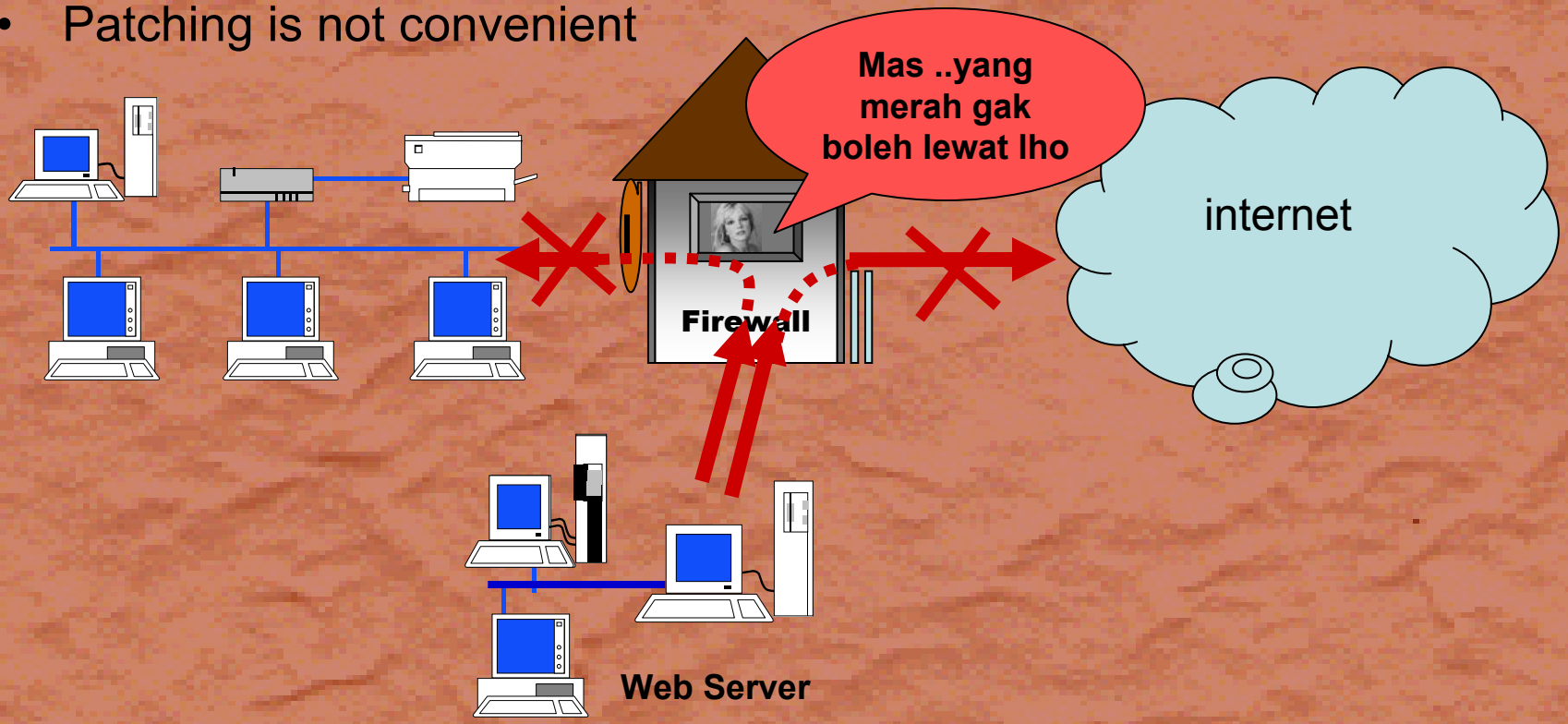
DMZ Configuration

- Place web servers in the “DMZ” network
- Only allow web ports (TCP ports 80 and 443)



DMZ Configuration

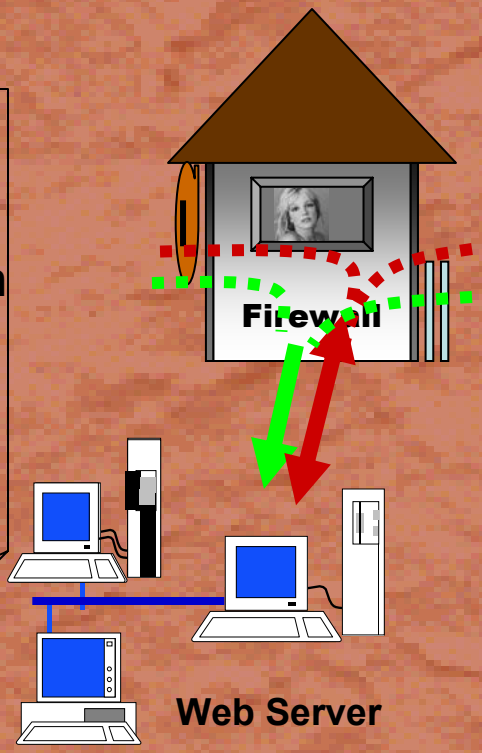
- Don’t allow web servers access to your network
- Allow local network to manage web servers (SSH)
- Don’t allow servers to connect to the Internet
- Patching is not convenient



DMZ Configuration

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 sebagai IDS

- IDS = Intrusion Detection System
- Collect log information from the deny rules
- Find Portscanning, hacking attempts, etc…
- Isolate traffic with deny rules helps cut down the information overload

Firewall sebagai IDS

- What to do with ALL that data…..Graph It!
- Shows trends, what people are looking for
  - Helps prioritize security tasks
- Occasionally you may want to block portscans

Firewall sebagai IDS

- Pay close attention to traffic leaving DMZ
- Often the first sign of a compromise
- Low traffic rules, so logs aren’t as enormous
- Email is nice, provided you’re the only one reading it

VPN

- VPN = Virtual Private Network
- VPN is far more secure than other management methods:
  - SSL and SSH are vulnerable to Man-In-The Middle Attacks
  - Telnet and SNMP are clear text
  - There are no known MIM attacks against IPSEC (Yet)

VPN

- VPN clients are supported on most platforms
- Most firewalls will work with most clients
- Netscreen now officially supports FreeSwan
- Mac OS X is now supporting VPN

Conclusions

- People don’t just put up a thick front door for their sensitive belongings, you shouldn’t for your network either.
- Firewalls are an effective *start* to securing a network. Not a finish.
- Care must be taken to construct an appropriate set of rules that will enforce your policy.