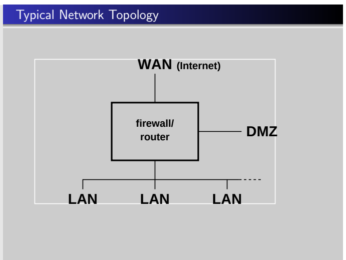
2006-11-25

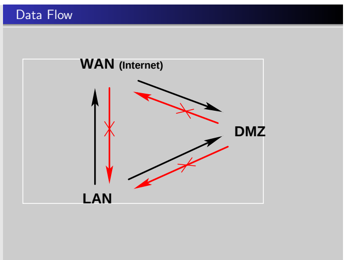
SOHO Firewalls
└What is it: Networks and Firewalls / Routers
└Typical Network Topology


Typical Network Topology

- WAN—Wide Area Network. The internet at large, the “outside”.
- LAN—Local Area Network. The internal network connecting all local computers.
- DMZ—De-Militarised Zone. Physically seperate network segment used for servers which are accesssible from the “outside”. Not used for servers which are only internal.

2006-11-25

SOHO Firewalls
└What is it: Networks and Firewalls / Routers
└Data Flow

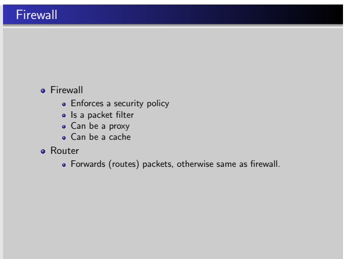

Data Flow

- LAN: can access “outside” (=internet), perhaps with exceptions. Can access DMZ.
- WAN: can only access DMZ server!!
- DMZ: can access nothing (perhaps with well-reasoned exceptions), but especially not the “inside” LAN.
- Many other policies are possible!
- Arrows show the direction of the originating request. Obviously, the answer has to go the other way.

  It’s important to keep connection state—to recognize answer packets.

2006-11-25

SOHO Firewalls
└─What is it: Networks and Firewalls / Routers
└─Firewall



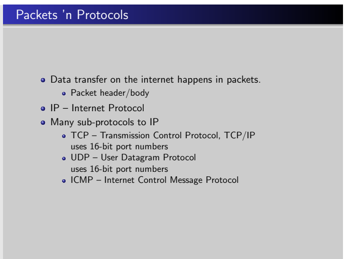
Firewall

- Firewall
  - Enforces a security policy
  - Is a packet filter
  - Can be a proxy
  - Can be a cache
- Router
  - Forwards (routes) packets, otherwise same as firewall.

- Proxies are better placed on separate hosts, though this depends also on resources, threat levels and value of what has to be protected "inside".
- Cache is also better placed on another host.

2006-11-25

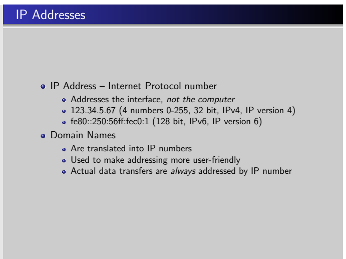
SOHO Firewalls
└─Nitty Gritty: Packets, Protocols and Services
└─Packets 'n Protocols



Packets 'n Protocols

- Data transfer on the internet happens in packets.
  - Packet header/body
- IP – Internet Protocol
- Many sub-protocols to IP
  - TCP – Transmission Control Protocol, TCP/IP
    uses 16-bit port numbers
  - UDP – User Datagram Protocol
    uses 16-bit port numbers
  - ICMP – Internet Control Message Protocol

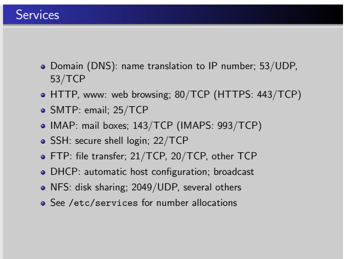
- TCP: Used by almost all commonly known services.
- UDP: Used when no "connection state" is desirable.
- ICMP: Used e.g. for "ping": "echo request", "'echo response"; or "network unreachable" messages.



IP Addresses

- IP Address – Internet Protocol number
  - Addresses the interface, *not the computer*
  - 123.34.5.67 (4 numbers 0-255, 32 bit, IPv4, IP version 4)
  - fe80::250:56ff:fec0:1 (128 bit, IPv6, IP version 6)
- Domain Names
  - Are translated into IP numbers
  - Used to make addressing more user-friendly
  - Actual data transfers are *always* addressed by IP number

- Mensch/Maschine: human: name, computer: number



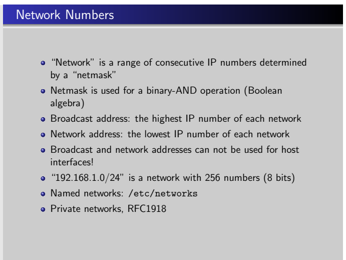
Services

- Domain (DNS): name translation to IP number; 53/UDP, 53/TCP
- HTTP, www: web browsing; 80/TCP (HTTPS: 443/TCP)
- SMTP: email; 25/TCP
- IMAP: mail boxes; 143/TCP (IMAPS: 993/TCP)
- SSH: secure shell login; 22/TCP
- FTP: file transfer; 21/TCP, 20/TCP, other TCP
- DHCP: automatic host configuration; broadcast
- NFS: disk sharing; 2049/UDP, several others
- See `/etc/services` for number allocations

- Name-to-address translation (name resolution) can also be achieved with the `/etc/hosts` file.
- FTP uses dynamically allocated ports and needs special tracking code in packet filters.
- DHCP: Returns IP number, gateway IP number, etc. on request.
- NFS uses a number of ports and port ranges for its sub-parts. It even has a port-mapper service to keep track of it. Very difficult to filter. It is typically only used on LANs but not over WANs.
- Services are provided by daemons.
- Both TCP and UDP ports are allocated to a service, although mostly only one is used.

2006-11-25

SOHO Firewalls
└Nitty Gritty: Packets, Protocols and Services
└Network Numbers



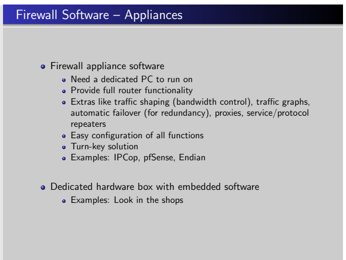
Network Numbers

- “Network” is a range of consecutive IP numbers determined by a “netmask”
- Netmask is used for a binary-AND operation (Boolean algebra)
- Broadcast address: the highest IP number of each network
- Network address: the lowest IP number of each network
- Broadcast and network addresses can not be used for host interfaces!
- “192.168.1.0/24” is a network with 256 numbers (8 bits)
- Named networks: `/etc/networks`
- Private networks, RFC1918

- Number of IPs in each network usable for host interfaces: two less than the number of IP numbers in the network.
- RFC1918: `http://www.ietf.org/rfc/rfc1918.txt`
  192.168.0.0/16, 172.16.0.0/12, 10.0.0.0/8
- Private networks are not to be routed over the internet! Their numbers can be re-used on each LAN.

2006-11-25

SOHO Firewalls
└Putting it into practice: Software
└Firewall Software – Appliances



Firewall Software – Appliances

- Firewall appliance software
  - Need a dedicated PC to run on
  - Provide full router functionality
  - Extras like traffic shaping (bandwidth control), traffic graphs, automatic failover (for redundancy), proxies, service/protocol repeaters
  - Easy configuration of all functions
  - Turn-key solution
  - Examples: IPCop, pfSense, Endian
- Dedicated hardware box with embedded software
  - Examples: Look in the shops

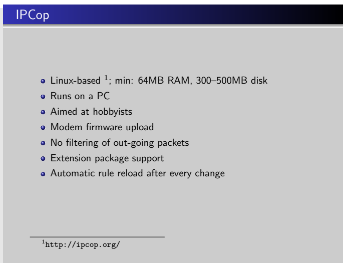
- Very small hardware can be bought to install firewall appliance software on, but a retired PC is about as powerful and *much* cheaper.

  Of course it doesn’t have the geek factor,
  but the cost of the power for running it is much lower.

- Demonstration/evaluation with VMware-server
  - Host-only networking
  - 3 network interfaces (vmnet1-3)
  - host: 3 class-C nets, e.g. 10.10.xyz.1; browse to 10.10.x.9
  - guest: LAN: fixed IP, e.g. 10.10.x.9, peer is .x.1
    WAN: DHCP

2006-11-25

SOHO Firewalls
└Putting it into practice: Software
└IPCop



IPCop

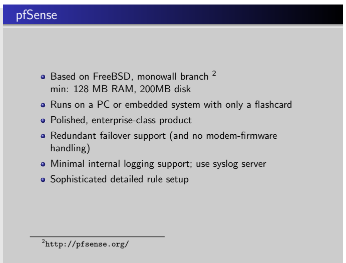
- Linux-based [1]; min: 64MB RAM, 300–500MB disk
- Runs on a PC
- Aimed at hobbyists
- Modem firmware upload
- No filtering of out-going packets
- Extension package support
- Automatic rule reload after every change

[1] `http://ipcop.org/`

- Extension packages of variable quality; segfaults and blank screens possible.
- Extension packages increase minimal system requirements.
- Interfaces

2006-11-25

SOHO Firewalls
└Putting it into practice: Software
└pfSense

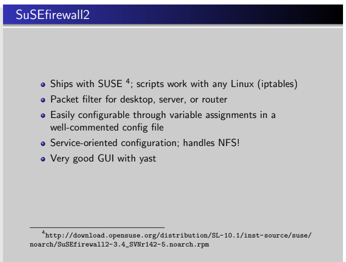


pfSense

- Based on FreeBSD, monowall branch [2]
  min: 128 MB RAM, 200MB disk
- Runs on a PC or embedded system with only a flashcard
- Polished, enterprise-class product
- Redundant failover support (and no modem-firmware handling)
- Minimal internal logging support; use syslog server
- Sophisticated detailed rule setup

[2] `http://pfsense.org/`

- Small ringbuffer RAM logging only: suitable for flashcard systems.
- Extension packages increase minimal system requirements.
- The BSD pf packet filter works differently to Linux iptables. Specifically, with NAT the destination port is not available for filter rules.



SuSEfirewall2

- Ships with SUSE [4]; scripts work with any Linux (iptables)
- Packet filter for desktop, server, or router
- Easily configurable through variable assignments in a well-commented config file
- Service-oriented configuration; handles NFS!
- Very good GUI with yast

[4] `http://download.opensuse.org/distribution/SL-10.1/inst-source/suse/noarch/SuSEfirewall2-3.4_SVNr142-5.noarch.rpm`

- Supports multiple interfaces on LAN, DMZ, and (sort of) WAN.
- Configuration is above the a-port-a-rule level.
- Because it's a shell script, modifications in a few places are much easier than starting over.