SOHO Firewalls

Volker Kuhlmann

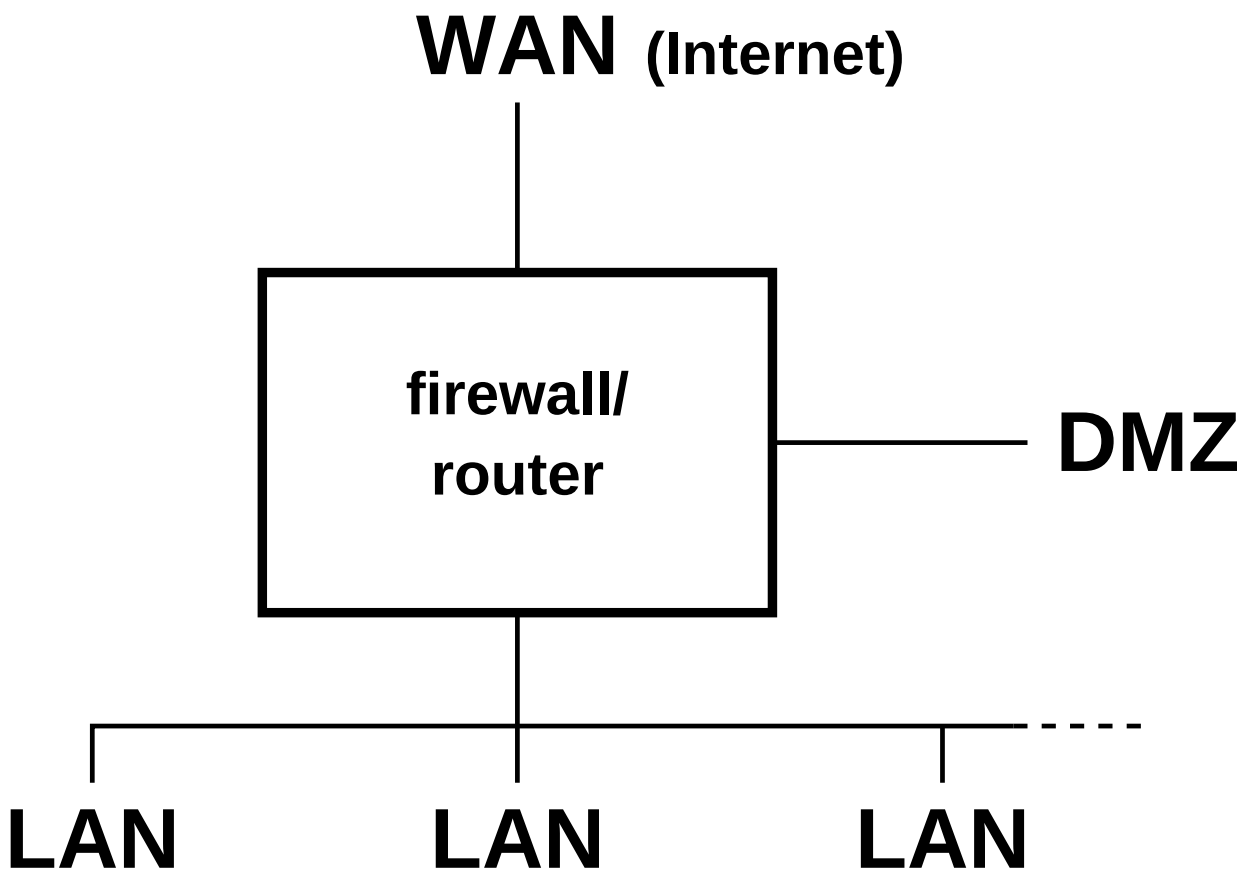
CLUG — Canterbury Linux Users' Group

14 November 2006

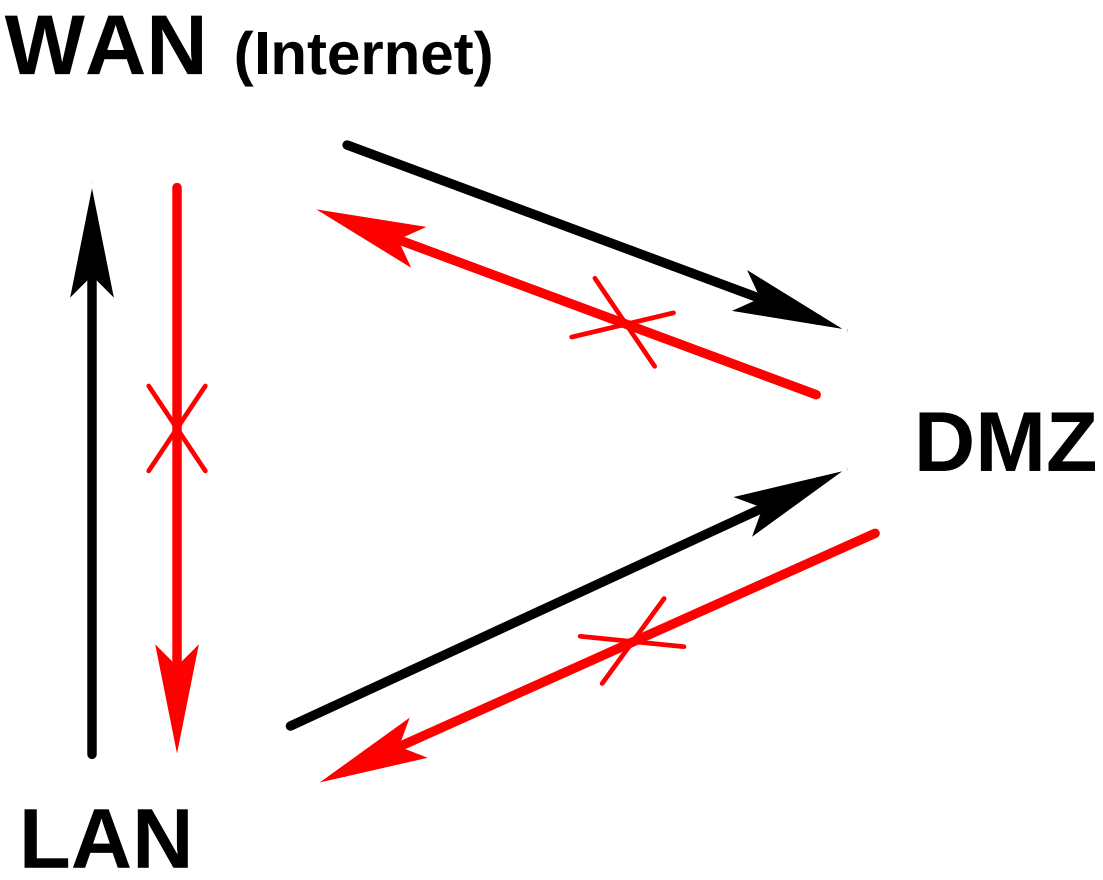
http://volker.top.geek.nz/linux/presentation/SOHO-Firewalls.pdf

Outline

Typical Network Topology



Data Flow



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.

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

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

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

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

Network Number Example

Use ipcalc:

```
ipcalc 192.168.1.0/24
```

gives

```
Address:   192.168.1.0          11000000.10101000.00000001 .00000000
Netmask:   255.255.255.0 = 24   11111111.11111111.11111111 .00000000
Wildcard:  0.0.0.255            00000000.00000000.00000000 .11111111
=>
Network:   192.168.1.0/24       11000000.10101000.00000001 .00000000
Broadcast: 192.168.1.255        11000000.10101000.00000001 .11111111
HostMin:   192.168.1.1          11000000.10101000.00000001 .00000001
HostMax:   192.168.1.254        11000000.10101000.00000001 .11111110
Hosts/Net: 254                  (Private Internet RFC 1918)
```

NAT

- NAT – Network Address Translation
- A LAN full of computers sharing one external IP address
- Router masquerades as each LAN PC simultaneously, and keeps track of (outgoing) connections to forward return traffic back to the correct PC.

- Provides a good level of basic security as LAN computers are not addressable from the outside Internet.

Firewall Software – Packet Filters

- Configurators for packet filters
  - Packet filter: iptables (Linux kernel)
  - Need a Linux system to run on (and the hardware!)
  - Provide only packet filtering/routing
  - Should be used on every desktop computer
  - Examples: SuSEfirewall2

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

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/

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/

Endian

- Based on IPCop [3]; is a bit heavier
- Smarter user-interface than IPCop
- Interface assignment through BUI
- Not as well-supported(?)

[3] http://www.endian.it/en/community/

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