Firewalls & VPNs

Topics

- Terminology
- Anatomy of IP packets
- What is a Firewall?
- Proxy Services
- Firewall Configuration
- VPNs

Terminology

- Zones – LAN, WAN, fw, VPN, DMZ
- NAT
- Proxy
- IP Addressing

Anatomy of IP packets

- Header
  - Protocol
  - Source Address
  - Destination Address
  - Protocol Dependant
    - Source & Destination Ports
- Payload
  - Application Data

What is a Firewall?

- Protection
- Router
- Address Translation
- Specialised Distributions
  - Smoothwall GPL
  - Mandrake MNF
  - SuSE Firewall on CD
  - freesco

Smoothwall GPL

- www.smoothwall.org
- 2.2 kernel – Ipchains packet filtering
- ~20MB on CD
- Small footprint
- Web admin
- 3 networks
- Restricted VPN
- Proxy Services

Mandrake MNF

- www.mandrakelinux.net
- 2.4 kernel – Iptables packet filtering
- ~250MB on CD
- Medium footprint
- Web admin
- 6 networks
- unrestricted VPN
- Proxy Services

Proxy Services

- DNS
  - Caching DNS server
  - Caches all requests
- Web
  - Caches frequently accessed pages

Firewall Configuration

- Not all requirements are the same
- Default policies
- Specific rules
  - NAT/Masq.
  - Port forwarding
- Blacklists

Firewall Monitoring

- Can monitor ALL traffic
- IDS
- Web Filtering
  - URL
  - Content
- Usage Graphs
- Legal Implications

VPNs

- Secure link over internet
- Network – Network
- PC – Network
- Protocols
  - IPSEC – Strong Encryption (3DES)
  - PPTP – Weak Encryption (40 bit)

VPN Config

- LAN addresses
- Public addresses
- Next hop
- Authentication