

Loughborough University



Managing Firewall Devices

Matthew Cook
Network & Security Manager
Loughborough University

Loughborough University

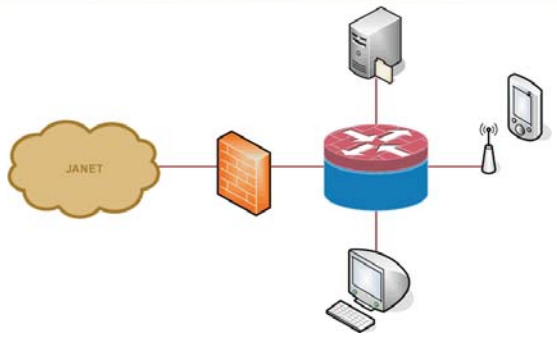
Managing Firewall Devices



2

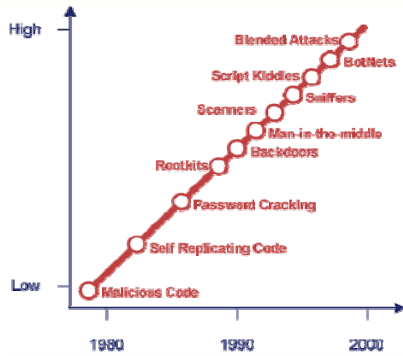
Loughborough University

Who do you trust?



3

How much do you need to worry?



4

Firewall Policy

- Two types of firewall policy
 - Default Allow
 - Default Deny
- Historically a Default Allow
- Initially blocking a few malicious attacks
- Resource Intensive

- Most sites now have a Default Deny policy.

5

How Secure are Virtual Machines?

- Can secure Virtual Machines exist on the same host?
 - Do you want to run your Web and SQL server on the same physical computer, even if virtualised?
 - Breaking out of the VM is possible
- Is automatic provisioning a good idea?
- Where is the traditional DMZ?
- Shared VM Services
 - Anti Virus
 - HIDS/HIPS



6

Level of Inspection

- Deep Packet Inspection (DPI) or Layer 7
- Examines Payload (IDS/IPS like functions)
- Packet: dropped, tagged, rate limit or logged
- Overhead, performance and ASICs
- Mitigation early in packet life cycle
- Wirespeed issues



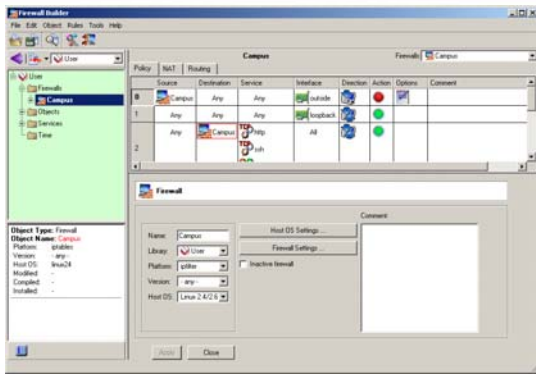
Implementation Requirements

- Interface
- DMZ
- Failover and Load Balancing
- Operational
- Speed
- Authentication
- Content Filtering
- Virtualisation
- Platform
- Reporting and Management
- Documentation and Support
- Added Value

Smoothwall / IPCop

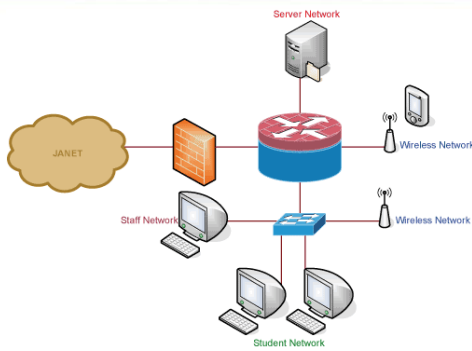
- Dedicated appliances based upon Linux
- Smoothwall created summer 2000
- Simple firewall appliance
- Split to IPCop
- Features include:
 - Secure configuration
 - Multiple Interfaces
 - DHCP Server
 - VPN Support
 - Caching DNS Server
 - Web Cache
 - Intrusion Detection System
 - Traffic Shaping and QoS facilities

Firewall Builder Tool



10

Isolating different classes of user



11

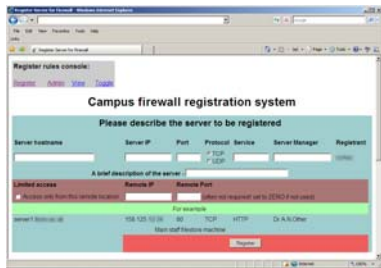
Consultation

- Opinions about change differ
- Manage change expectations:
 - Firewall policy change
 - Hardware/software change
- Communication is important
 - Driver for change clear?
- There is never a right time

12

Registration

- Open policy
- Paper form
- Web based



Creation of Policy

- Policy should contain at least:
 - Who is managing the policy?
 - Which senior member of staff is supporting the policy?
 - How often is the policy reviewed, and by whom?
 - How are changes requested?
 - How are disputes resolved?
 - What is the Service Level Agreement (SLA)?
 - How is logging data managed and what is the data retention period?
- Technical policy

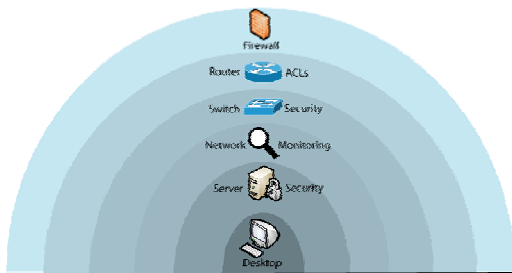
Monitoring the firewall

- Web interface
 - SSL enabled?
 - Functions (dashboard overview)
- Syslog
 - Flag rules with a higher priority
- SDEE
 - Security Device Event Exchange
- SNMP
 - Abuse
- TIDP
 - Threat Information Distribution Protocol
 - Integration with other products i.e. Lancope Stealth Watch.

Auditing, Pentesting Review

- Protection morphs with every rule change
- Impractical to audit after each change
- Periodically perform testing
- Penetration Tests
 - In-house
 - Commercial company
 - Permission
- Procedures

Layered Security

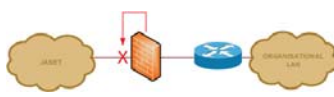


Integration with IDS and IPS

External IDS/IPS



Inline Mode



Promiscuous Mode



Hardware

- Started with TCP Offloading Network Cards
- Takes away processing from the CPU
- TCP/IP designed for slower connection
- Processing Overhead
- Degradation in performance
- More obvious on some machines
- Not everything can be offloaded
- Gaming developments
- Firewall on a card, for example: Yoggie

JANET Training Courses

Introduction

- Introduction to JANET – Bristol 11th June 2008
- Introduction to DNS – Abergavenny 22nd October 2008

Technical

- Basic Networking – Birmingham 4th July 2008
- Basic Router Configuration – Bristol 12th June 2008

Security

- Using Logfiles for Security – Abergavenny 21st October 2008
- Managing IT Security – Manchester 6th August 2008
- Firewalls: Planning and Implementation – Birmingham 22nd July 2008

Wireless

- Wireless LAN Fundamentals – Birmingham 30th October 2008

Videoconferencing

- Introduction to Videoconferencing - TBA
- Technical Support for Videoconferencing - TBA

JANET Services

- Implementing Shibboleth at your Organisation – Manchester 27th November 2008

JANET Training Website <http://www.ja.net/services/training/>

JANET CSIRT Conference October 2008

- JANET CSIRT Conference booked for October 2008
- Sir Denis Rooke Building, Holywell Park, Loughborough University
- Thursday 23rd October 2008
- Full day programme
- Further Details:
<http://www.ja.net/services/csirt/>





Questions?
Matthew Cook
<http://escarpment.net/>
