Campus-wide Firewall Project

Anne Oribello, Brown University

What We Were Seeing

- Defacement of web servers
- Compromises to research machines
- Denial of Service attacks against central service and departmental machines
- Constant reports of student machine compromises

The Impact of these Attacks

- Misuse of systems
- Extensive unavailability of machines during clean-up
- Potential data corruption
- Exposure of private information
- Man months of effort to restore compromised machines
- Potential litigation

These Problems Were the Result of

- Many machines being taken from box to desk with no reconfiguring
- Turnkey systems delivered without hardened OSs
- Applications that were downloaded which automatically reconfigured machines

These were problems that a firewall could help mitigate

What a Firewall Will Accomplish

- Provide additional security tool to areas that need protection
  - Administrative computing
  - Centralized services (post office, Kerberos, etc.)
  - Network systems
  - General campus – protect the ignorant, require active act to open services

What a Firewall Won’t Fix

- Viruses, worms and other infestations
- Determined hacker
- Users intentional stupidity!

Firewall Options

- Multiple Firewall-1 machines (too expensive)
- A CISCO PIX firewall
- And then along came NetScreen -

Capabilities of NetScreen 1000

- Gigabite throughput with multiple gigabite ports
- Stateful inspection of packets
- Configurable for 5-100 vertual systems (vsys)
- Significant redundancy
- Compatible with smaller NetScreen firewalls (5,25,50,100, etc.)
- Delivered code protects against DOS attacks

Virtual System Usage

(note that some departments have their own firewall)

- core campus services (e.g. post office, Kerberos)
- administrative systems (e.g. mainframe, admin servers)
- network systems (e.g. routers, switches)
- dorm subnets
- “rest of the campus”

Early Successes

- core campus services (e.g. post office, Kerberos)
- administrative systems (e.g. mainframe, admin servers)
- network systems (e.g. routers, switches)

All in place with rule sets by early December

Determining the Campus-wide Policy

- Committee formed with the following representation:
  - Central computing services (CIS)
  - Universities Libraries
  - Internal Audit
  - General Counsel
  - Faculty representative
  - UG representative
  - Grad representative

Firewall Policy

- separate VSYS for dorms from rest of campus
- both VSYSs will appear as a single firewall, initially
- all outgoing traffic allowed unless violates policy
- all incoming traffic in response to an outgoing request allowed
- Incoming traffic from a trusted VSYS
- no other incoming traffic allowed unless specifically opened by end users (no review of end user requests)

Automatic Ruleset Definition

- Web form to open specific services
  - For students, allowed to register their own machine (renewed each semester)
  - For departmental servers, only sysadmin can register (reviewed annually)
  - For departmental workstations, depending on policy of department, may allow individual user or be managed by departmental computing coordinator
  - For cluster machines, cluster administrators would configure rules (reviewed annually)

Initial Implementation Tasks

- install upgrade from vendor to allow OSPF
- produce Web interface software for automatic rule creation
- obtain policy approval
- PR with end users

Status of These Tasks

- OSPF delayed indefinitely
- consolidation router reseller delayed order so delivered in late January
- programmer for rule changing software moved to Minnesota
- CIS without permanent VP from 7/1/01-2/1/02 so no policy decisions made

Things were not moving along well!

Current Status of Tasks

- New consolidation router installed in January
- Plan to put firewall inline by mid March but with no apparent rules in place (mostly logging)
- Plan to activate rules during the summer

Future Plans

- increase user awareness
- add VSYSs to offer to departments
- Periodic re-evaluation of policy, making changes where appropriate
- separate dorms from the “rest of the campus”