How to Create Firewall Service on the Cheap

Daniel Adinolfi, CISSP
Senior Security Engineer
Cornell University
March 12, 2004

Information Technology Security Office

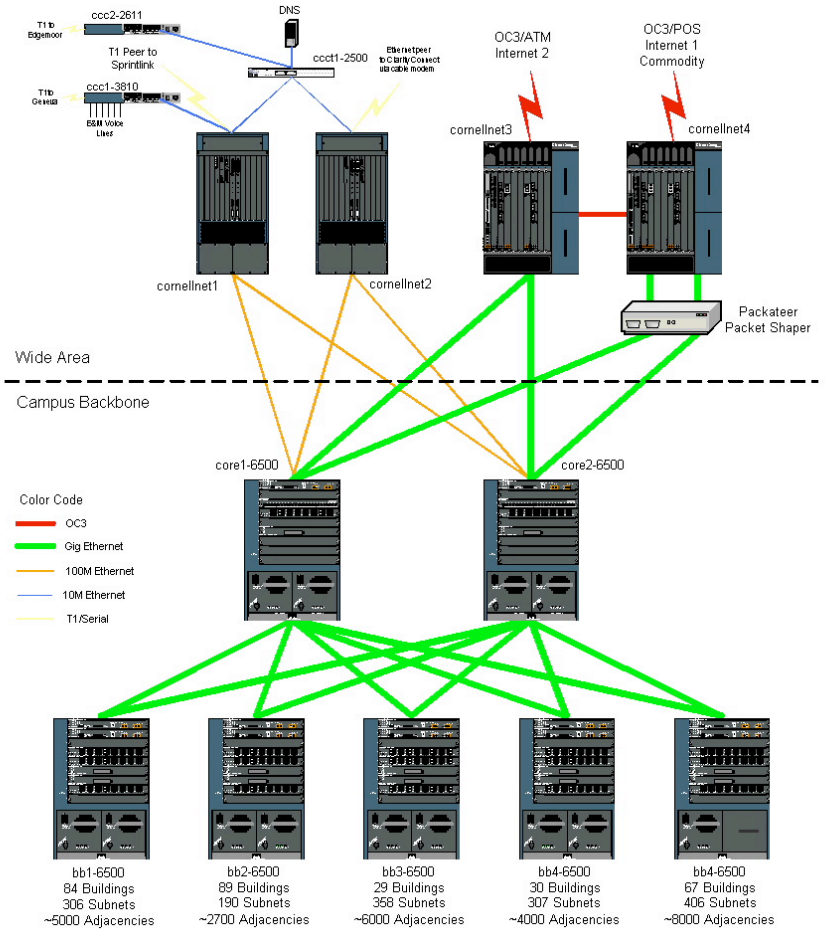
Objectives

- Outline the Cornell IT environment
- Describe the ACL deployment architecture, processes, and details
- Discuss the costs of program design, roll-out, and up-keep

Cornell Environment

- 40,000 nodes
- Three Class B networks with about 750 subnets
- 110 residential networks with about 6500 nodes
- Each subnet is a unique VLAN and insolated to a single router interface
- Diverse user base: students, faculty, staff, researchers, public library users, visitors, etc.

Cornell Network



Network Administration

- Local (departmental and program-wide) support providers administer the majority of campus subnets
  - Varying degrees of technical skills
  - Some small departments (a few systems), some large departments (hundreds of systems)
- Few departments run own network infrastructure
- Handful of firewalls deployed by departments

Security Challenges

- Around 40,000 components on the network
  - Infrastructure components
  - Faculty, staff, student, and public systems
  - Any and every type of OS imaginable
  - Some systems supported *better* than others
- Most common vulnerabilities
  - Weak or no account passwords
  - Un-patched and exploitable systems
  - Open file sharing
  - Virus infection

Security Challenges, cont.

- Daily observances
  - Several virus infections
  - Several compromised systems (mostly used for file sharing, spamming, or scanning)
  - Abuse cases (spam, harassment, etc.)
  - Hundreds of (observed) scans from off-campus
  - On-campus scans? Dunno.

ACL Deployment Architecture

- Use of existing packet filtering capabilities in routers
- Homegrown scripts to automate implementation
- Complement to other hardware or software firewall implementations
- Does not interfere with existing anti-spoofing, routing, and multicast ACL rules
- No special budget allocated for this project.

Program Traits

- Not for ad hoc blocks
  - Intended for static environments
  - Not intended for incident response
  - One to two business day turn around
- Limited filtering
  - IP, TCP/UDP port, ICMP message type
  - More complex rules discouraged and rare

Scripts

- One script to generate “database”
- Additional script to upload configuration to router
  - ACLs created by hand in a text file in standard IOS format
  - Separate configuration file that tells the script which router, VLAN, and ACL files (configlets) to use

How an ACL is made

1. Initial query by registered net admin
2. Consultation with technical staff, in person, preferably (very important!)
3. ACL design
4. Implement, test, and document
5. Follow-up with customer

Issues

- No logging available to customers
- Does not scale when changes needs to be instantaneous or often
- “Outbound” filters only
- UDP protocols can be tricky

Census

- Approx. 275 subnets with Edge ACLs
- 45 campus departments plus ResNet
- Majority are blocking Windows Networking from off-campus
- Less than 10% involve complex requirements

Futures

- Higher percentage of networks with Edge ACLs (GLBA audits, other regulations, wider acceptance of best practices)
- Web-based interface for net admins
  - Access limited to net admins and only for their own subnets
  - Template-based configurations
  - Queries for existing ACLs
- Access to router logs (?)
  - syslog and ACL “hits”

Costs

- Development Time
  - One week for script development and database population
  - One day for testing and staff training
  - One day for documentation and marketing
- On-going Costs
  - Consumed staff time
  - Existing router maintenance costs
  - No significant financial impact on infrastructure
- We offer this for free! No cost recovery.

For more information

- http://www.cit.cornell.edu/computer/security/edgeacls/
- Email: security@cornell.edu

Thank You