Network Firewalls
From Policy to Practice

EDUCAUSE Southeast Regional Conference
June 19, 2002

Richard Gadsden
Director, Computer and Network Security
Medical University of South Carolina
gadsden@musc.edu
Copyright Richard Gadsden 2002. Permission is granted for this material to be shared for non-commercial, educational purposes, provided that this copyright statement appears on the reproduced materials and notice is given that the copying is by permission of the author.
Abstract

Firewalls are an essential tool for managing risks in today's networks, but developing good firewall policies and practices for the diverse stakeholders in the academic enterprise is difficult. This case study of a successful perimeter defense implementation at MUSC will illustrate the need for tight coupling between policy and practice.
Topics

- Basic firewall concepts
- Common problems with firewalls in edu's
- Role of policy in risk management process
- Case study
- Lessons learned
What Is a Firewall?

- One type of security control, used to manage risks
  - Restricts traffic between networks
  - Provides a choke point for logging and analysis
- Enforces a network-wide security policy
- Several basic flavors
  - Packet filters
  - Stateful inspection filters
  - Application gateways
Customary Benefits of Firewalls

1) Protection of internal assets from external risks
2) Good citizenship
   - i.e. may also protect external people and things from risks originating on internal network
   - e.g. anti-spoofing filters
By definition, the owner of the inside network (the one *behind* the firewall) also owns the firewall and sets its policies.
Firewalls in Edu Networks
What Can Firewalls Do?

• Contribute to all of the Big Four security goals:
  
  – **Avoidance**
    • Lower risk of accidental or intentional damage
  
  – **Assurance**
    • Ensure effectiveness of all safeguards taken together
  
  – **Detection**
    • Enable early detection leading to effective response
  
  – **Recovery**
    • Investigate source of breach and restore operational environment
What Can't Firewalls Do?

- Affect any traffic which isn't visible to them
  - Traffic which takes some other route
  - Traffic which is tunneled
- Always be reliable
  - Designed, built and administered by humans
- Always be transparent to users
- Be anything more than a *first* line of defense
- Be simultaneously good, fast *and* cheap
Firewalls and Higher Ed

• No organization *needs* a firewall
  – An organization should secure each of its internal systems
  – Even in the best of worlds, this is unrealistic
  – Defense in depth is generally a Good Thing

• Edu's *need* firewalls
  – Who else runs such large networks hosting so few computers that they actually control?
Reality Check

• If firewalls and edu are such a perfect match...
  – Why don't all edu's have firewalls?
  – Why do so many of the firewalls that we do have work so poorly?
  – Why are both firewall administrators and users so frustrated?
Security 101: Risk Management

- Assess Risks
- Central Focal Point
- Policies and Controls
- Monitor and Evaluate
- Promote Awareness
High Road to Firewall Nirvana

- Carefully scoped risk analysis
- Thoughtful policy development
- Implementation of the policy
- Communication and awareness building
- Monitoring and evaluation
Usual Road to Firewall Hell

- Carefully scoped risk analysis
- Thoughtful policy development
- Implementation
- Communication and awareness building
- Monitoring and evaluation

- Crisis occurs... mgmt needs to demonstrate due diligence!
- Procure 'good' firewall hardware and software
- Assign most available (least talented) staff
- Mgmt tunes out until next crisis
- Repeat until done
Moral

You can't do good practice without good policy.
What Is A Security Policy?

• A statement of what needs protection and why
  – Sets priorities about what must be protected first and at what cost
  – Seeks explicit agreement across the organization about the value of security
• Defines responsibilities
  – Provides security staff with authority to say no when needed
  – Prevents security staff from acting arbitrarily
• Describes consequences of violations
Barriers to Setting Policy

- Competing priorities
  - Creating policy takes time and resources
- Internal politics
  - May encounter active resistance
- It is *hard*
  - Tendency for scope creep
  - Impossible to anticipate and cover everything
  - Interaction effects with other policies
Policy Tips

• A good policy now is better than a great policy never.

• A simplistic policy that is well distributed and understood is better than a complete policy that no one has ever seen or accepted.

• A policy that is constantly updated is better than a policy that is obsolete and dead.
Nirvana vs. Hell

• Leadership must value the right things
• Leadership must be willing to assign and/or recruit resourceful, talented people to:
  – First develop policy
  – Then implement policy
• And especially for edu's:
  – Security staff must work hard to meet special needs
  – Must excel at communications
About MUSC

- Medical College of South Carolina founded 1824
- MUSC now 6 colleges, with 2300 students, 1200 faculty, 9000 staff (including Medical Center)
- Affiliated Medical Center (600 beds, tertiary care)
- Primary care physician network
- SC Area Health Education Consortium
- Annual revenues > $1B
- Research awards > $120M
MUSC Network Background

- 1980's: Campus-wide network, BITNET
- 1990: Internet
  - TAMU Drawbridge ca. 1991
    - An early open source packet filter
    - No policy, ad hoc procedures
    - Firewall admins and users increasingly unhappy...
  - Checkpoint Firewall-1 ca. 1995
    - Needed 'easier to manage' and 'less open to criticism'
    - Still no policy, still ad hoc procedures
    - Downhill slide continues...
Hurting for Policy

• Litany of horrors
  - No guiding principles for firewall administrators, users or system administrators
  - Undocumented protocol and port ranges open for incoming connections to all internal systems
  - Useless but dangerous protocols (e.g. NetBIOS)
  - No mechanism for expiring obsolete rules
  - Logging/auditing capabilities spotty (at best)
  - No assurance that exposed servers are not vulnerable
  - No internal protections against exposed systems
Road to Recovery

• June 2000
  – Infrastructure Committee established
    • subcommittee of MUSC's executive-level Information Management Committee (which reports to President)
    • comprised of IT people, each of whom represents one or more of the executives on the IMC
    • focused on setting enterprise-wide policies, priorities, and strategies for MUSC's network infrastructure
  – provided a shoulder to cry on
Road to Recovery cont'd

• Jul 2000 - Jan 2001
  - Firewall admins work with Infrastructure Committee
    • Reviewed litany of horrors with current firewall
    • Benchmarking (against policies/practices at other edu's)
    • Education (terminology and policy issues)
    • Risk assessment
Risk Analysis: Topology
Road to Recovery cont'd

• Mar - Sep 2001
  – Firewall Policy developed
  – Changes required to MUSC Computer Use Policy
    • vetted by Faculty Senate and SGA
    • approved by Board in Oct 2001
Changes to Computer Use Policy

The University reserves the right to monitor user activities on all University computer systems, and to monitor communications utilizing the University network, to ensure compliance with University policy, and with federal, state and local law. Monitoring shall be performed only by individuals who are specifically authorized, and only the minimum data necessary to meet institutional requirements shall be collected. Data collected through monitoring shall be made accessible only to authorized individuals, who are responsible for maintaining its confidentiality. [Section II, Privacy and Confidentiality]

Any computer system which is connected to the University network must be maintained in accordance with generally accepted security principles. [Section V.D, Security]

An audit trail of all remote access activity must be maintained by any facility which provides remote access, and audit trail records must be accessible by authorized University officials. [Section V.D, Security]
MUSC Firewall Policy: Outline

I. Purpose and scope
II. Principles
III. Default policies for inbound/outbound
IV. Exceptions to default policies
I. Purpose and scope

MUSC's Internet Firewall is an important element in the overall security of MUSC's campus network. The Internet Firewall restricts MUSC's Internet traffic in specific ways, and it allows MUSC to analyze its Internet traffic in specific ways. Combined with other, complementary security controls, the Internet Firewall can protect MUSC's information assets from some of the security threats associated with MUSC's connection to the Internet. In addition to preventing some Internet security problems, the Internet Firewall improves MUSC's ability to detect and respond to any Internet security problems which do occur.

This Policy explains the role of the Internet Firewall in contributing to the security of MUSC's data network. It highlights where complementary security controls are needed. It covers the responsibilities of both network administrators and end users, and the consequences if responsibilities are not met.

This Policy applies to all components of the MUSC data network and to all of their authorized users, both local and remote.
II. Principles

MUSC's students, faculty and staff all benefit from their ability to access Internet resources with a minimum of restrictions. Teaching, learning, research and service would all suffer to some degree if Internet access were too much restricted. At the same time, MUSC has significant information assets entrusted to its care. MUSC has both legal and ethical responsibilities to protect these assets, whose confidentiality, integrity, and availability would be threatened if the assets were too little protected from Internet intrusions.

MUSC's Internet Firewall is a security control, whose goal is to reduce the risks, inherent in exposing MUSC's network to the Internet, to a level which MUSC can tolerate. The Internet Firewall must achieve this goal at the lowest possible cost, with the least possible intrusiveness and inconvenience to the network's authorized users, and with the least possible interference with the ability of MUSC and its individual units to efficiently meet their strategic objectives.
III. Default policies

• Definitions
  – Inbound, outbound connections
  – External, internal, perimeter networks

• Default connection policies

• Security requirements for perimeter hosts
  – Hardening, vulnerability scanning, central logging

• All packets subject to logging (headers), and to inspection (payload) if needed
IV. Exceptions

- Firewall rule requests
- Responsibilities of Network Security
- Responsibilities of system administrators
- Approvals and appeals process
- Renewals
Road to Recovery cont'd

- Mar - Sep 2001
  - Firewall Policy developed
  - Changes required to MUSC Computer Use Policy

- Jul - Sep 2001
  - Evaluation and testing of candidate hardware and software to implement new (draft) policy
An Incident Occurs

- Sep 2001: Nimda
  - Two exposed IIS servers infected
  - Chain reaction infecting *internal* IIS servers
- Existing firewall crashed
  - DoSed by traffic generated by internal infections
  - MUSC users cut off from Internet (probably would have pulled the plug anyway)
  - Headline: 'Worm virus cripples MUSC Internet link'
High Gear

- Ack! Test firewall becomes production firewall
- Golden opportunity to 'introduce' new firewall policy to broader user community
- Implemented core provisions of new firewall policy, literally overnight
  - Clean slate approach
Implementation Status

- Routing, filters, taps, IDS sensors implemented
- Workflow Manager (open-source app developed by MUSC's IT Lab) for managing exceptions to default firewall policies
  - [http://www.itlab.musc.edu/workflow](http://www.itlab.musc.edu/workflow)
- Vulnerability scanning, centralized logging, perimeter DNS services under development
- Migration of systems to Perimeter Network expected to begin in Fall
Workflow Manager

• Benefits
  – Firewall Administrators get all the info they need to handle requests from users, and to manage all firewall rule(s) over their complete life cycle
  – The user can track the status of his pending requests, and monitor the status of all his firewall rules

• The following slides show how a user (in this case, the sysadmin of a new DNS server) would request an exception to the firewall's default (deny all incoming connections) policy
User (gadsden) has just logged in...

Welcome Richard H Gadsden Jr (gadsden)

Your contact information has not been entered. Would you like to add the information?
First time user, so we verify his contact info...
The user can then register his target host...
He can now request one or more firewall rules for the host...

Request A New Rule for chimera.musc.edu

New rule requests must be approved, however you can view your Pending requests immediately after submitting them. Please provide the following information:

Protocol: (if both TCP and UDP ports must be open, please submit separate rules)

UDP  

Ports to open:

3

Open To: (IP address of host who can use this rule, or ALL)

ALL

Is this rule for a specific vendor to access this host?

Yes

If Yes, please select the vendor from the list below:

If the correct vendor is not listed, click here to add it.

N/A

Comments:

Submit Request  Clear Entries

Back to the host listing.
Worklow Manager cont'd

- The following slide shows the Firewall Administrator's view
- The top panel shows pending requests from users which need action (our Inbox is empty today)
- The bottom panel shows how the Firewall Administrator can search the database
  - Ex: Give me the userid's of everyone who administers an ssh server so I can e-mail them with some info on this latest vulnerability affecting OpenSSH...
Give me a list of everyone with port 22 (ssh) exposed ...
Lessons Learned

- Security policy *is* hard
  - But not as hard as practice without policy!
- If you are prepared, incidents are your friend
  - You can often *implement* policy rapidly in a crisis
  - But you can't *develop* policy rapidly
- So be prepared
  - Fill any 'missing policy' gaps
  - Keep existing policies current
References

