

The Good, the Bad and the Ugly - Institutional Firewalls

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



Introduction

Matthew Cook
Senior IT Security Specialist


Loughborough University
<http://www.lboro.ac.uk/computing/>

Project Team: Alan Buxey, Martin Hamilton,
Gary Parker and Paul Whitton.

2

Migration to Default Deny

- Current firewall rules/policy not adequate
 - Change in business
 - Who really needs no protection?
- 972 Firewall rules with a default allow policy
- Two redundant Linux based firewalls
 - One for development and testing



3

Consultation

- Obtain Requirements from user base
 - Some form of autonomy
 - A lot more protection
 - To be able to think less about firewalls
- Consultation over a eight month period
 - Discussed at April consultation session
 - Formal project raised
 - Agreed by University management
 - Distributed project and reminded stakeholders
- Timescales
 - There is never a good time
- Externally what were others doing

4

Proposal

- Use the same current software/hardware
- Default deny firewall policy
 - What do we mean by default deny?
 - How do we manage existing rules?
- Web based management of rules
- Policy of vulnerability scanning for hosts
 - Before connection
 - At regular intervals
- Method of creating a server audit

5

Getting the Job Done

- Apply a dynamic iptables ruleset at the end of the existing rules
 - Provides ease of transition
 - Strict rules (Default deny in/out all protocols)
- Web interface manages rules using a MySQL database
- Rules are compiled and migrated to the firewalls at 15 minute intervals.
- Longer term clean up of the static rule set

6

Web Interface

Campus firewall registration system

Please describe the server to be registered

Server hostname	Server IP	Port	Protocol	Service	Server Manager	Registrant
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

A brief description of the server -

For example

server1.lboro.ac.uk	158.125.12.34	80	TCP	HTTP	Dr A.N.Other	
---------------------	---------------	----	-----	------	--------------	--

Main staff store machine

Time of registration: 2006-04-05 11:28:40

Servers that you have already registered:

Name	Address	Port	Protocol	Service	Registration Time	Status
<input type="button" value="Delete"/> server1	158.125.12.34	80	TCP	HTTP	2005-12-09 21:54:19	ALLOW
<input type="button" value="Delete"/> server2	131.231.80.52	22	TCP	SSH	2005-12-09 21:54:09	ALLOW

Admin Interface

Administration console: cmisc

Key:

Sort by: Sort by:

Name	Address	Port	Protocol	Service	Registration Time	Action	Reason
158.125.12.34	158.125.12.34	80	TCP	http	2006-01-05 12:01:53	<input type="button" value="Scanned - Okay"/>	<input type="button" value="Go"/>
158.125.12.34	158.125.12.34	6701	TCP	irc	2006-01-24 16:12:39	<input type="button" value="Scanned - Okay"/>	<input type="button" value="Go"/>
158.125.12.34	158.125.12.34	80	TCP	http	2006-02-27 13:45:20	<input type="button" value="Scanned - Okay"/>	<input type="button" value="Go"/>
158.125.12.34	158.125.12.34	5900	TCP	RealVNC	2006-03-01 09:53:19	<input type="button" value="Scanned - Okay"/>	<input type="button" value="Go"/>
131.231.80.52	131.231.80.52	22	TCP	ssh	2005-12-13 10:54:10	<input type="button" value="Scanned - Okay"/>	<input type="button" value="Go"/>
131.231.80.52	131.231.80.52	25	TCP	smtp	2005-12-13 10:57:04	<input type="button" value="Scanned - Okay"/>	<input type="button" value="Go"/>
131.231.80.52	131.231.80.52	80	TCP	http	2005-12-13 10:54:45	<input type="button" value="Scanned - Okay"/>	<input type="button" value="Go"/>
131.231.80.52	131.231.80.52	443	TCP	https	2005-12-13 10:55:10	<input type="button" value="Scanned - Okay"/>	<input type="button" value="Go"/>
131.231.80.52	131.231.80.52	465	TCP	SSLed SMTP	2006-01-08 16:57:55	<input type="button" value="Scanned - Okay"/>	<input type="button" value="Go"/>
131.231.80.52	131.231.80.52	993	TCP	msn	2005-12-13 10:56:29	<input type="button" value="Scanned - Okay"/>	<input type="button" value="Go"/>
131.231.80.52	131.231.80.52	4443	TCP	https	2005-12-13 10:57:37	<input type="button" value="Scanned - Okay"/>	<input type="button" value="Go"/>

Initial Problems

- People did not remember to register
- Off Campus Access to services
- Problems with Video Conferencing
- Problems with Building Management
- Important machines that were insecure

○ Produced 20 point FAQ
<http://www.lboro.ac.uk/computing/security/firewall-faq.html>

Four Months Onwards

- System has worked really well
- Managing 409 rules through web interface
- Started tidying up the older static rules
- Reduced ingress traffic
- Periodic security scanning works well
 - Sendmail vulnerability
- Requirements for rule toggle functionality
- No compromised machines on campus since the default deny rules implemented!

10

Lessons to be Learnt

- Consultation often falls on deaf ears
 - Meet people face to face
 - A little information and frequently
- Not everyone has the same priority
 - Insecure machine vs important research
- Provide comprehensive advice and guidance
 - Our FAQ increased in size dramatically
- Certainly a worthwhile exercise
 - ...but not the answer to everything

11

Is this the Right Answer?

- Is there a right answer?
- Are we addressing the right problem?
 - Move to a better firewall policy
 - Still have the problems with mobile users
 - Insecure services still a problem
 - Bridging campus network with wireless Aps
- Separate netblocks or VLANs
- Institutional firewalls play an important part
 - However they should not be the only line of defense

12

The Future

- Layered approach to firewalls
 - Multi vendor
 - Dedicated firewalls for sensitive machines
- Providing segregation of departments
 - Router/Switch ACLs VS Firewalls?
 - Users working in two departments?
- Managing higher wire speed connections
- Providing the firewalls with a clean feed
- Looking at expanding 'default deny'?

13

Personal Firewall Future

- Personal firewalls cause problems
 - Poorly configured
 - Users do not understand the technology
- If centrally implemented have limited use
 - Essential for machine leaving campus
 - Open ports for required service
 - Software firewalls fail open
- The future
 - Hardware ASIC firewall on network cards
 - Central management of rules
 - Location aware firewalls

14

Questions?

Slides at:
<http://escarpment.net/>
or
Networkshop 34 web site

15
