Must have duct tape...lots of duct tape.

- MacGyver

or

Building a walled garden on a shoestring

Scott A. McIntyre
XS4ALL Internet, KPN-CERT, FIRST

Summary

- History of how we did abuse handling
- Problems with initial approach
- Enhanced abuse handling
  - And some problems
- The Walled Garden
- Next steps
  - Constantly evaluating and improving

XS4ALL

- Security & Abuse incident management
  - Router tricks & bulk handling of huge number of events. Automated warning, walled garden, free home AV, Abuse Centre, free email scanning for spam/malware
  - 6 customer facing ACers, 4 in SOC/System Admin dept
- We *do* more than most, we *cost* more than most.
  - These costs you save on helpdesk calls
  - €5/call on average
- It's all about the time & money we *save*
  - Inaction is a threat to our business, and our customers.
  - We choose how we want to spend our time (and money), we prefer not to let the surprises choose for us!

That was then...

The early days

- Most customers were on dialup
  - Kicking offline was a matter of setting login shell to xsh and clearing their session on the terminal server
- Attitude of sysadmins
  - “We only care about abuse from customers, not to.”
- Only 100Mbit to all of DSL
  - Easy to do IPS and control traffic
- Setting IOS ACLs controlled problems
  - But I hate IOS ACLs

DSL increases...

- 100M > 200M -> 400M > 1G -> 2G -> ..
- Created firewall statements in JunOS
  - Referenced Prefix Lists.
  - Login to router, add someone to list, kick 'em off.

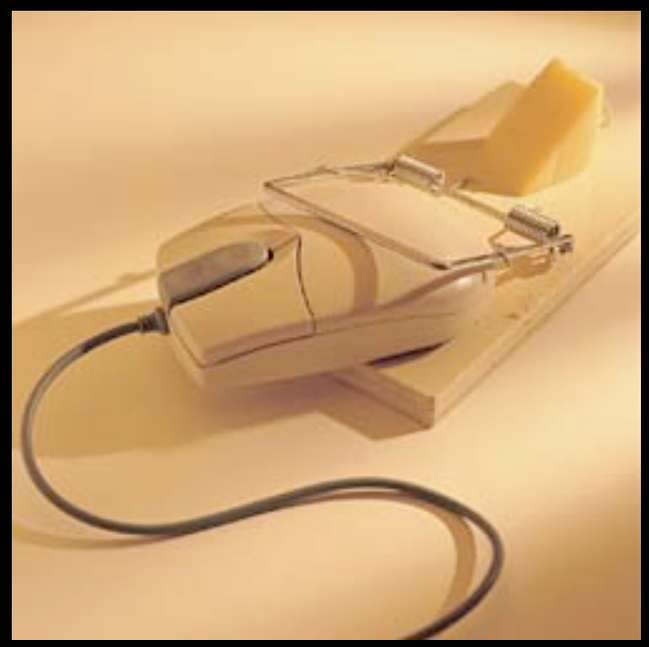
A very binary solution...

```
term evil-discard {
    from {
        source-prefix-list {
            EVIL;
        }
    }
    then {
        count evil;
        discard;
    }
}
```

Problems

- Full shut off of customer no panacea
- Less modems out there, no dialup way in
- Customers were annoyed
- Helpdesk was annoyed
- Regulatory headaches
  - VoIP, 112, etc.

So we built a better mousetrap.



XS4ALL

FIRST
Improving Security Together

kpn

Overall procedure

Find → Notify → Filter → Resolve

Sometimes we shorten this a bit...

Find

A daily nfdump is healthy.

```
/usr/local/bin/nfdump -R /nfdump/$DATE1 -o "fmt:%ts %sa %sp
%da %dp %pr %flg" '(dst port 42 or dst port 1433)  and flags
S and not flags A and not flags F and not flags R a
nd not flags P and not flags U and (src AS xxxx or src AS
yyyy) and src port > 1024'
```

nfdump for evil ports which are likely to indicate a problem.

XS4ALL

FIRST
Improving Security Together

kpn

Daily EvilFlow

Find

Date flow start	Src IP Addr	Src Pt	Dst IP Addr	Dst Pt	Proto	Flags
2008-01-20 23:59:18.405	194.109.163.13	38332	194.19.5.18	139	TCP	....S.
2008-01-20 23:59:41.451	194.109.163.13	36275	192.168.127.33	445	TCP	....S.
2008-01-20 23:59:50.425	194.109.163.13	38441	194.19.5.163	445	TCP	....S.
2008-01-21 00:00:03.697	194.109.163.13	38474	192.168.40.181	139	TCP	....S.
2008-01-20 23:59:52.635	82.92.28.58	25484	194.109.152.38	139	TCP	....S.
2008-01-20 23:59:22.414	194.109.152.134	1670	194.109.154.48	1433	TCP	....S.
2008-01-21 00:00:08.320	212.83.240.227	1537	194.109.35.13	1433	TCP	....S.
2008-01-21 00:00:39.242	82.92.215.82	19282	161.89.56.69	139	TCP	....S.
2008-01-21 00:01:01.186	194.109.163.13	38161	194.19.6.155	1433	TCP	....S.
2008-01-21 00:01:03.610	194.109.163.13	40113	194.19.6.209	135	TCP	....S.
2008-01-21 00:00:20.237	80.127.172.42	4593	43.124.63.170	139	TCP	....S.
2008-01-21 00:00:42.178	83.68.73.47	51037	83.68.27.225	445	TCP	....S.
2008-01-21 00:00:40.814	80.88.172.114	1126	80.127.231.96	135	TCP	....S.
2008-01-21 00:01:04.814	80.88.172.114	1154	80.127.240.98	135	TCP	....S.
2008-01-21 00:00:48.814	80.88.172.114	1122	80.127.234.99	135	TCP	....S.
2008-01-21 00:00:35.814	80.88.172.114	2179	80.127.229.105	135	TCP	....S.
2008-01-21 00:00:32.814	80.88.172.114	4404	80.127.227.244	135	TCP	....S.
2008-01-21 00:00:52.193	82.67.136.175	1364	82.94.228.155	445	TCP	....S.
2008-01-21 00:00:44.949	212.238.206.170	7280	213.222.13.134	139	TCP	....S.
2008-01-21 00:00:51.883	82.93.182.198	64617	82.0.0.78	139	TCP	....S.
2008-01-21 00:01:04.305	82.229.159.227	2010	82.94.197.10	445	TCP	....S.
2008-01-21 00:01:31.216	194.109.163.13	40466	192.168.88.112	445	TCP	....S.
2008-01-21 00:02:16.113	194.109.163.13	38910	194.19.7.189	139	TCP	....S.
2008-01-21 00:02:07.942	194.109.163.13	36555	192.168.79.249	445	TCP	....S.
2008-01-21 00:01:28.630	80.126.6.24	35232	192.168.16.2	135	TCP	....S.
2008-01-21 00:01:41.509	82.92.37.47	55790	192.168.200.6	445	TCP	....S.
2008-01-21 00:01:31.269	83.68.73.55	4801	83.68.30.72	139	TCP	....S.
2008-01-21 00:01:22.209	194.109.34.76	1309	194.109.34.4	1433	TCP	....S.
2008-01-21 00:02:15.449	82.93.182.198	64764	82.0.0.234	139	TCP	....S.
2008-01-21 00:01:31.173	212.83.240.227	3080	194.109.35.13	1433	TCP	....S.
2008-01-21 00:02:05.755	213.84.26.228	34953	172.29.1.43	135	TCP	....S.
2008-01-21 00:03:03.073	194.109.163.13	38891	192.168.54.150	1433	TCP	....S.
2008-01-21 00:02:14.416	80.127.90.79	38106	81.4.95.90	1433	TCP	....S.

XS4ALL

FIRST
Improving Security Together

kpn

Filter

Walking on xshs

- From unix shell
  - Used to block slip/ppp auth by changing valid shell
- NSA development
  - Our provisioning system inherited the use of xshs
- Hierarchy led to xsh as attachment
  - Any component can have the xsh
  - Regular exports of data affect service delivery with xshs
- Functional impact important
  - So is political!
  - Customers must fix problems before starting new ones

SUIsite is painless

- Sales/User Interface
- Graphical overview of customer
  - All packages and mutations
  - Billing information, links to payment information
- Respects our authorisation matrix
  - Can’t see or access what your role doesn’t permit
- Displays minimal information for XSHd
  - Enough to direct customer to the right department

Still not ideal...

- Difficult to maintain “whitelist” of IPs
  - Known good IP addresses for customers to talk to
  - Confusing with stuff like Akamai
  - Router can’t handle DNS (good thing, really)
- Still tough to get fixes
  - Dialup gone, CD’s slow, ...
- We needed a technical solution which also made customers happier
  - And the helpdesk.
  - Advising on setting proxy settings became quite time consuming

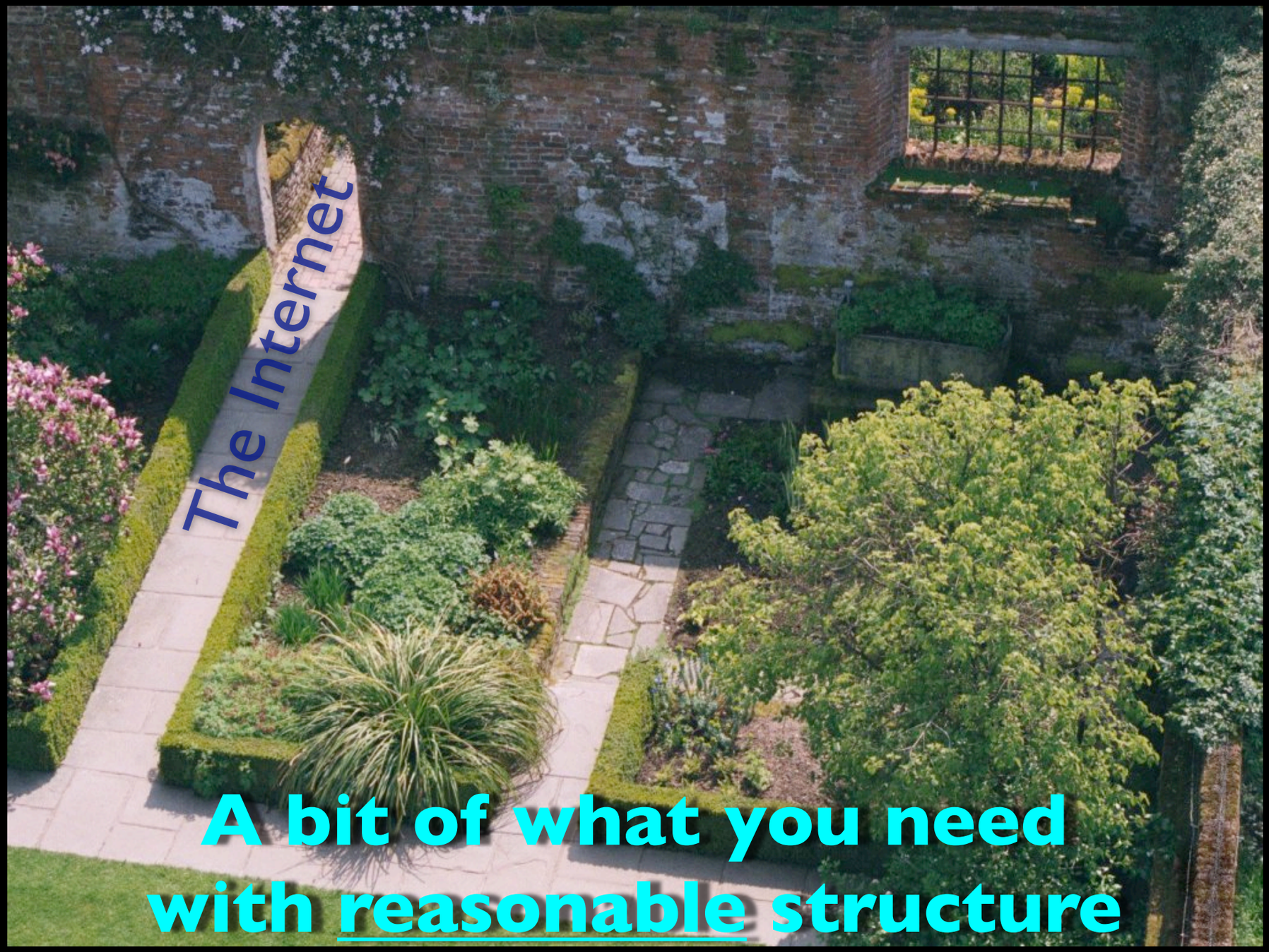
XS4ALL

FIRST
Improving Security Together

kpn

Resolve

Walled Garden



XS4ALL

FIRST
Improving Security Together

kpn

Resolve

Our walled garden

- JunOS prefix lists
  - Uploaded from the abuse tools hourly
- JunOS firewall statements
  - Refer to the lists; no need to change firewall often
- Policy based routing
  - Routing Instances in Juniperese
- Linux boxes with iptables & squid
- There are commercial options out there
  - This was cheaper, and probably better

JunOS config

```
term walled-garden {
    from {
        destination-address {
            194.109.6.92/32 except;
            0.0.0.0/0;
        }
        source-prefix-list {
            DSL-WORM;
        }
        protocol tcp;
        destination-port 80;
    }
    then {
        count garden;
        routing-instance garden;
    }
}
```

```
garden {
    instance-type forwarding;
    routing-options {
        static {
            route 0.0.0.0/0 next-hop 1.2.3.4;
        }
    }
}
```

Other firewall changes

- At the same time we added the WG, we made other changes:
- Permit SIP to/from us
- SSL
- Authenticated SMTP
- Various other communication enhancing things.
- But: Blocked *everything* else.

Linux iptables

```
Chain PREROUTING (policy ACCEPT)
target     prot opt source               destination
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:22
REDIRECT   tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:80 redir ports 3128
```

And of course all the normal filtering you'd do on a Linux box. This is just the NAT table.

Squid conf

```
emulate_httpd_log off
acl all src 0.0.0.0/0.0.0.0
acl localhost src 127.0.0.1/255.255.255.255
acl to_localhost dst 127.0.0.0/8
acl CONNECT method CONNECT
acl allowed-URLs dstdomain "/etc/allowed-URLs.conf"
http_access allow manager localhost
http_access deny manager
http_access deny !Safe_ports
http_access deny CONNECT !SSL_ports
http_access allow allowed-URLs
http_access deny all
http_reply_access allow all
httpd_accel_host virtual
httpd_accel_with_proxy on
httpd_accel_uses_host_header on
deny_info error.html    all
```

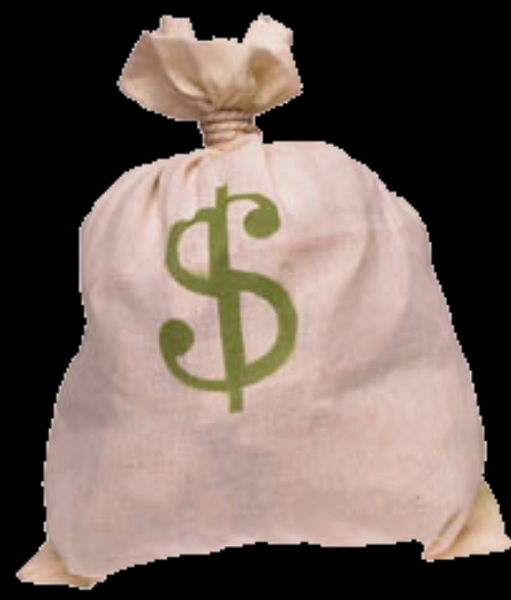
Allowed URLs

```
#general OSes
.ms.akadns.net
.microsoft.com
.microsoft.nsatc.net
.windowsupdate.com
.apple.nl
.apple.com
.verisign.com

#info URLs for lusers
www.waarschuwingsdienst.nl
www.govcert.nl
www.virusalert.nl
www.sans.org
www.sysinternals.com

#anti-virus and anti-spyware vendors
.mcafee.com
.symantec.com
.clamav.net
.avast.com
.trendmicro.com
.sophos.com
.viruslist.com
.zonelabs.com
.nod32.com
.swatit.org

# useful
.mozilla.org
ftp-mozilla.netscape.com
```

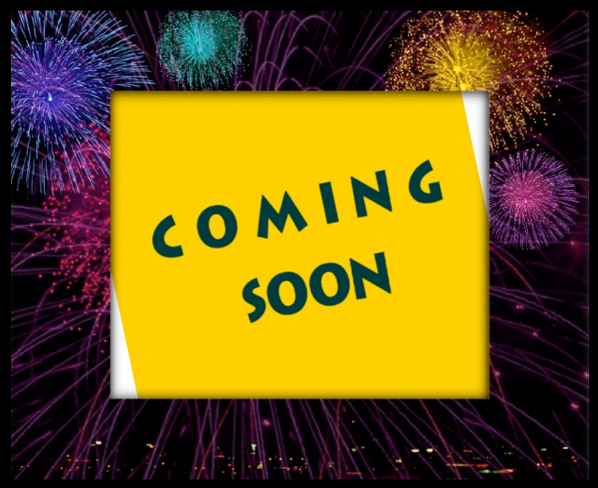
Just a snippet, many more listed and we review regularly

Walled Garden costs.

- Hardware: €3000
- Software development: €0
- Operating system license: €0
- Network technology: €0
- Value to business: ∞



An oz of prevention is worth a £ of cure.



Custom filters

- As a preventative measure for you and us
  - All customers put into “normal” level, blocks a lot of evil
- Gives us room to breathe
  - If customer is compromised, they won’t bother others or cause us direct damage in many cases
  - We’ll still notify, as the malware is not 100% stopped
- NOT being used for abuse handling
  - Perhaps eventually, but this is a provider-side firewall and being positioned as something to create a “cleaner” pipe
- Not DPI, purely port based

Custom filters

Level	Filter
Min	135, 445, 1434
Low	+ 135-139
Normal	+ 25, 1080
Secure	+ 2967, 2968, 1433, DNS
Strong	+ nosyn, 1026/1027, IRC

Flexible and somewhat dymanic based on current top threats, our darknets, etc.

Questions?