UNISYS
imagine it. done.

Lazy Management of a Secure Gateway

System Administration Miniconf
Tuesday, 25th January 2010
LCA2011, Brisbane, Australia

Mark Suter
Senior Gateway Engineer
Unisys Australia Pty Limted

Overview

Prefer going to great effort to reduce overall energy expenditure? That's my kind of Laziness. Add some Perl-ish Impatience and Hubris and you have a good description of my current workplace.

This talk is a "How we do things" walk-through of my workplace with most of the focus on what works for us, minus some detail to keep the security people onside ;)

My workplace is a secure gateway for a large government client. It has many different types of devices all forming part of a managed response to the risks we face in connecting to the world.

Of course, I'll mention the Wiki that I presented on last year but this time with more about how it fits into our workplace and almost nothing on the wiki itself.

Click to add an *awesome* title

- Click to add an *awesome* outline

Lazy Management?

Laziness is the quality that makes you go to great effort to reduce overall energy expenditure. It makes you write labor-saving programs that other people will find useful, and document what you wrote so you don't have to answer so many questions about it.

http://c2.com/cgi/wiki?LazinessImpatienceHubris

Secure Gateway?

- Government Client
- Large internal network
- Many B2B links
- Let people work with protection and audit.
- PSM / ISM / IRAP

INFOSEC REGISTERED ASSESSOR PROGRAM

IRAP

STATEMENT OF COMPLIANCE

This is to state that

Unisys

has successfully demonstrated Australian Government IT Security policy best practice standards for the maintenance of

PROTECTED SGS Gateway

as assessed by *Barry Grek* who is an I-RAP Registered Assessor recognised by the Defence Signals Directorate as endorsed to carry out assessment work for Australian Government agencies (and others) to Australian Government best practice standards under the following categories:

a) Gateway assessments of IT systems at X-IN-CONFIDENCE, PROTECTED and RESTRICTED levels,

b) Information System reviews for compliance with Part C of the Protective Security Manual (PSM), and consistency with the Australian Communications-Electronic Security (ACSI 33) and AS/NZS standards, for X-IN-CONFIDENCE, PROTECTED and RESTRICTED level systems, and

c) FedLink audits for agencies that have conducted FedLink self-review connection at X-IN-CONFIDENCE level and FedLink Connection Assessments.

In accordance with the requirements of the Policy and Procedures for the Infosec-Registered Assessor Program, (I-RAP).

This Statement of Compliance is valid for a period of twelve months from the date of issue unless otherwise stated in the attached I-RAP report.

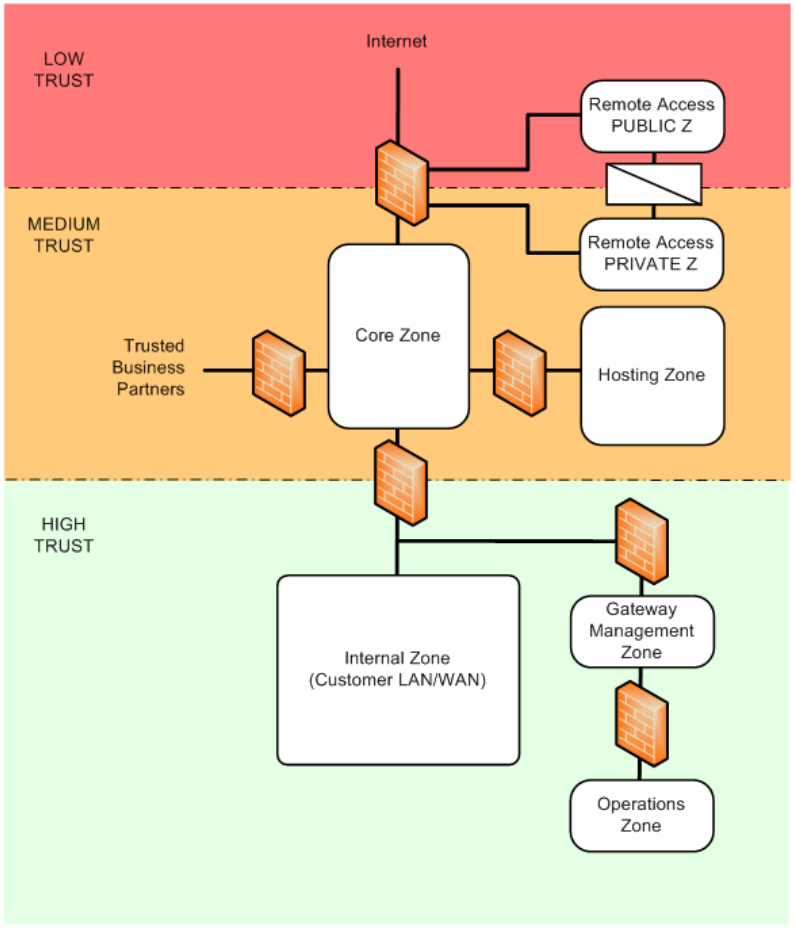
This Statement is issued on *31 October 2010*

Barry Grek
I-RAP Registered Assessor

I-RAP is a program administered by Securelink Pty Ltd

High Level Architecture

- Primary and Secondary Sites
- Over 200 pieces of kit
- Multiple redundant traffic paths
- Single point of entry/exit
- Extensive Monitoring



Customer Common Services

- Web Browse, including content filtering
- Internet Email (SMTP), including anti-spam
- DNS: Public, Gateway, Business Partners, etc
- Business Partner Connections
  - 20 + links to Business Partners
  - Specific data requirements
  - Failure closes borders (Airports and Cruise Ships)
- Secure File Transfer (drop box w/ automation)
- Remote Access VPN Solutions (collect them all!)

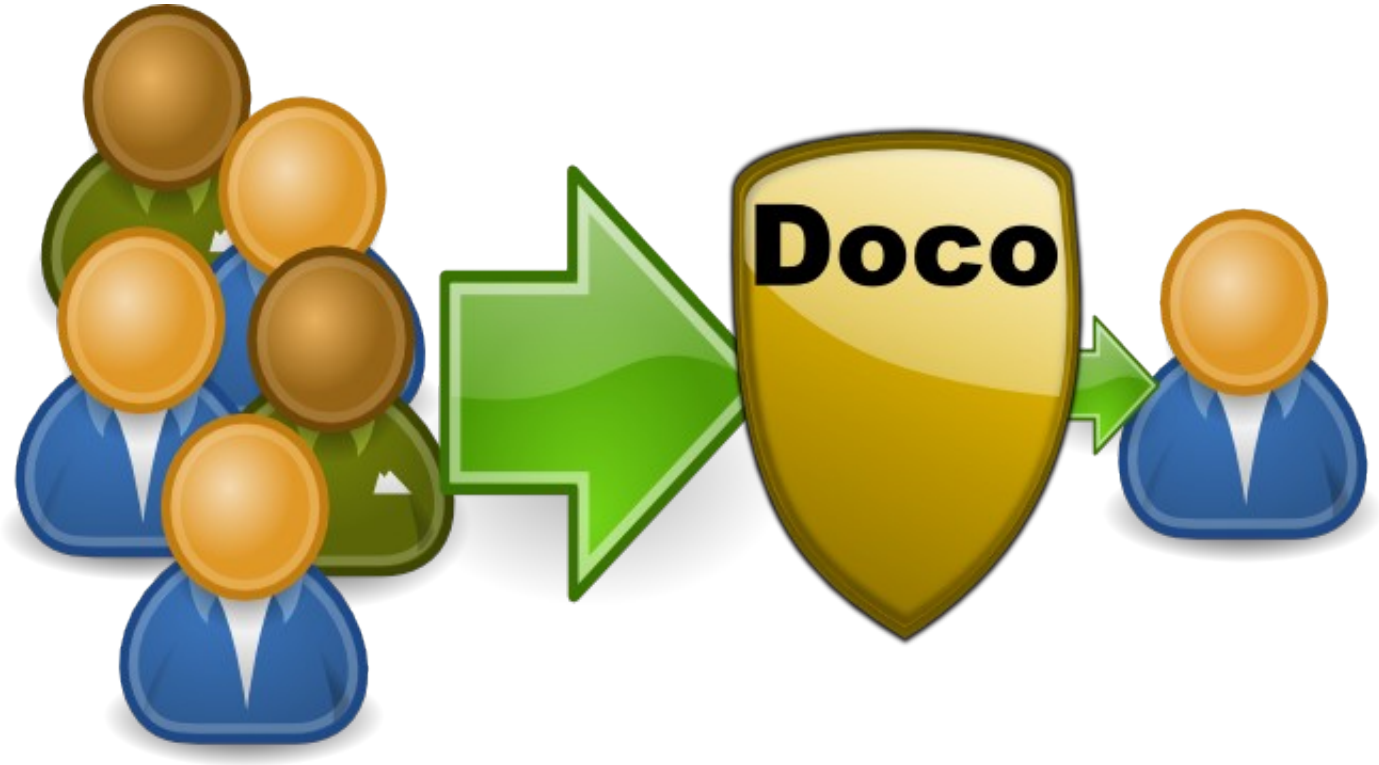
What we do (1/2)

- Firewall Administration
  - Multiple Vendors
- IDS/IPS Administration
- Router/Switch Administration
- Linux Administration (DNS, NTP, Logging, etc)
- Log Analysis
  - Including Anomaly Detection
- System Monitoring and Reporting

What we do (2/2)

- Incidents, Problems and Changes
- External Hosting Infrastructure
  - Reverse Proxies
  - SSL Decryption
  - Anti-virus Checking
- Web (XML) Messasging Gateways
- Documentation
- Certification

Documentation



Openness

- Very good relationship with customer
- Saves a huge amount of time
  - e.g., B2B “Link Documents”
- Un-needed secrecy **hurts** Security

Firewall Rulesets

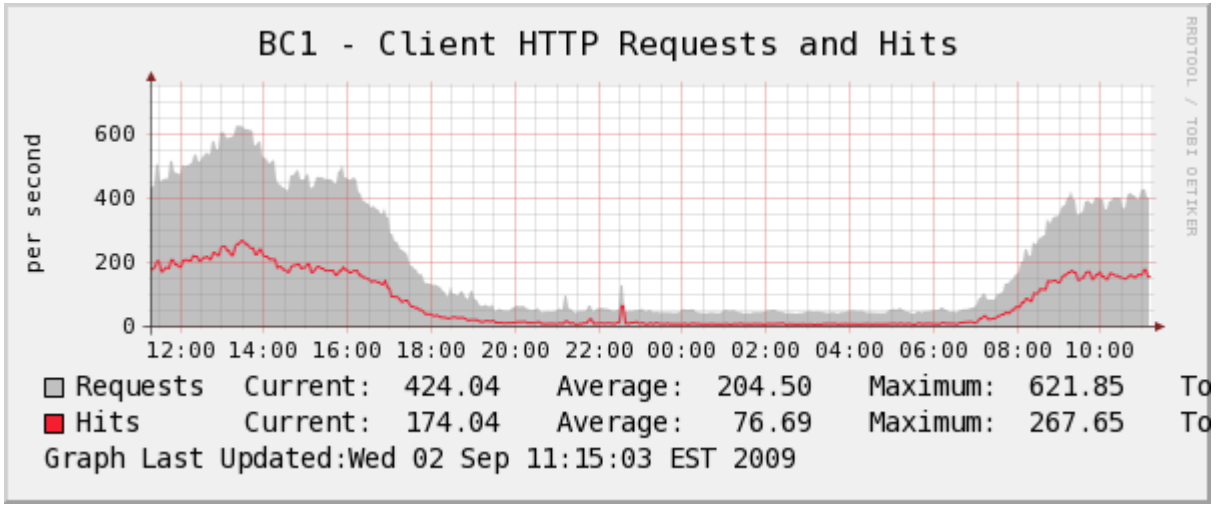
- Live Rules
- Exports into Subversion (web viewable)
- Wiki versions of B2B “Link Documents”

Naming and Addressing

- IP Plan
- Multi-split DNS
- Public space but with many “private” ranges and a lot of NAT :(

Web Browse: what we use

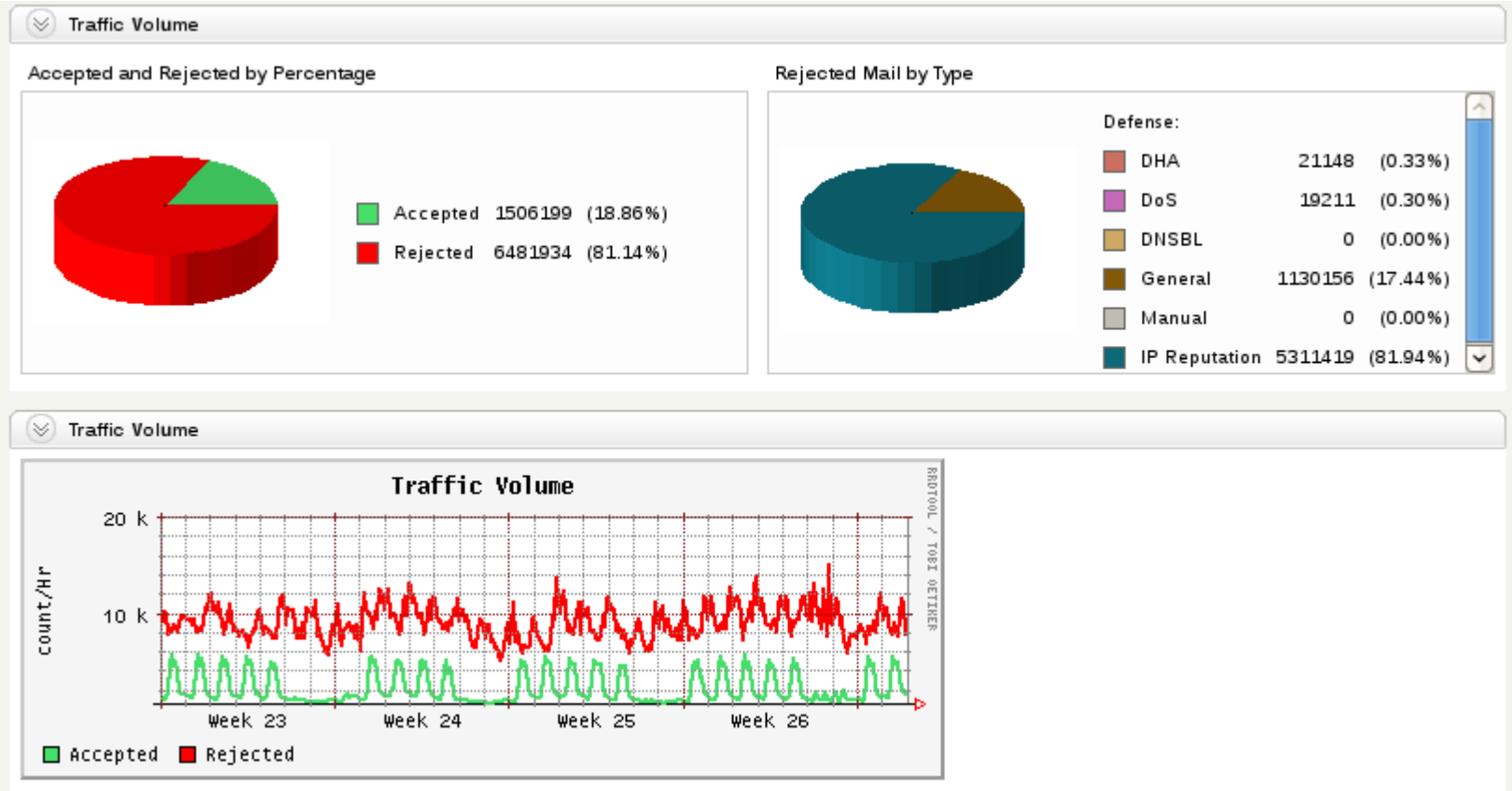
- Blue Coat ProxySG Appliances
- SSL Intercept aka “Man in the Middle”
- Blue Coat Web Content Filtering
- Blue Coat Anti-virus appliances



Email: what we use

- Axway Mailgate SMTP Appliances
- Very strong tagging/policy capability
- Anti-spam
  - IP Reputation Filtering
  - SMTP checks (good behaviour)
- Approx 100,000 legitimate emails per day
- About 7% spam count (user web-based digests)
- > 80% connections rejected

Email: Anti-spam



Passwords

- Many different types of devices
- Many of each type of device
- Separate credentials per trust zone
- One central KeePassX file

Monitoring (1/2)

- Cacti – Capacity Planning
- Nagios – Everything okay right now?
- NetFlow – historical “tcpdump”

Monitoring (2/2)

- SourceFire – IPS/IDS
- Logs – syslog-ng /archive/yyyy-mm-dd/
- ArcSight – SIEM

LIME

Search Notes

Knowledge Base
Help / Feedback
Logout

Account matching "xxxx02"

2011-01-23 15:20

IDs:	xxxx02 / 12345 / 6789 / 60000007
Name:	Joe Citizen or CITIZEN, Joe
Email:	joe.citizen@immi.gov.au
Section:	Unisys Contractors
Floor:	Level 1 - Thynne Street, 9 Thynne Street Dunlop Court Fernhill Park, Bruce
Phone:	0-02-6225-8067 or 0-0411-262-316 Directory
Desktop:	pc00042 (192.0.2.42) Remote- C drive- Home- Profile
GRAS:	Digipass Go3, serial 12-3456789-4 2011-01-23 15:19 (0.0 days ago) Logs
Created:	2008-07-04 12:24 (933.1 days ago)
Changed:	2011-01-16 12:45 (7.1 days ago)
Expiry:	2011-07-01 23:00 (159.4 days)

+1s

SD0000259	Jan 13	C	System 42 Outage - Status Update
SD0000278	Jan 13	C	Request to speak to Brad
SD0000240	Nov 26	C	[IM000711] - Status Update
SD0000210	Nov 22	C	LAN Account Locked
SD0000227	Nov 10	C	Protect Drive - unlock
IM000708	Sep 21	C	pc00042 - no longer lightly managed
IM000771	Sep 19	C	Laptop - reimage required
IM000789	Sep 17	C	PC - Requesting version 42
IM000780	Sep 16	C	Unable to log into pc00042
IM000707	Sep 04	C	Access to Deakin IDC

+1s

xxxx02 ->	pc00042 -> Dell OptiPlex 42 (xxxxxxS)
	pc00042 -> Dell 19.4 inch (DxxxxxxxxxxS)
	pc00042 -> Dell 19.4 inch (DxxxxxxxxxxS)

+1s

# ↑	Name	Notes
8532	GR-Important-Group	Tom citizen is the authorising officer.
8532	GR-Other-Group	Harry citizen is the authorising officer.

+3s

Questions?

This presentation is at
http://zwitterion.org/talks/