

email virus filtering at the gateway

Steve Rochford
College of North West London



Who?

- ◉ CNWL is a large GPFE College
- ◉ 14,000 students
- ◉ 1,000 staff
- ◉ 3,000 PCs
- ◉ 15k-20k emails per day in to staff
- ◉ Almost none in to students
- ◉ 1k-1.5k out per day from staff

What?

- ◉ Windows Active Directory (Server 2003)
- ◉ Separate domain for staff and students
- ◉ Exchange server 2003 (primary MX)
- ◉ FreeBSD/postfix (secondary MX)

Grey listing

- ◉ Grynx – free for Exchange 2003
- ◉ Checks IP of sender, address of sender, address of recipient
- ◉ Gives a “try later” if not recently seen
- ◉ Loses lots of spam
- ◉ Can lose genuine automatic mail

Split DNS - external

```
nslookup -q=mx cnw1.ac.uk
```

```
Server: tconw113.cnw1.ac.uk
```

```
Address: 195.194.12.10
```

```
cnw1.ac.uk      MX preference = 10, mail exchanger =  
tconw11.cnw1.ac.uk
```

```
cnw1.ac.uk      MX preference = 20, mail exchanger =  
tconw113.cnw1.ac.uk
```

```
tconw11.cnw1.ac.uk  internet address = 195.194.12.4
```

```
tconw113.cnw1.ac.uk internet address = 195.194.12.10
```

Split DNS - internal

```
nslookup -q=mx cnw1.ac.uk
```

```
Server: tconw123.cnw1.ac.uk
```

```
Address: 10.0.0.23
```

```
cnw1.ac.uk      MX preference = 10, mail exchanger =  
tconw115.cnw1.ac.uk
```

```
cnw1.ac.uk      MX preference = 20, mail exchanger =  
tconw11.cnw1.ac.uk
```

```
tconw11.cnw1.ac.uk      internet address = 10.0.0.1
```

```
tconw115.cnw1.ac.uk     internet address = 10.0.0.15
```

System layout



Tconwl1 – primary MX
Exchange 2003
Sophos Pure Message



Tconwl13 – secondary MX
FreeBSD
MailScanner
ClamAV



Tconwl15
Mail store
Exchange 2003
Sophos Pure Message

Basics

- ◉ Try to only accept “real” email
- ◉ Reject all invalid email addresses
- ◉ Simple GUI in Exchange
- ◉ Script runs for Postfix

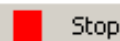
Activity monitor

Activity for server TCONWL1

SMTP

Exchange store

Server: TCONWL1



Clear

Connection filtering

Blocked hosts	0
Blocked senders	0
Rejected recipients	0

Messages processed: 40876

	Inbound	
Message category		
Spam		31196
Unscannable		1
Infected		0
Encrypted messages		0
Encrypted attachments		0
Suspicious attachments		0
Restricted attachments		0
Blocked phrase		0
Offensive language		0
Action		
Deleted		29669
Replaced attachments		0
Quarantined		1527
Delivered		4100

04/02/2008 15:55:19 Detected spam message '<000901c86746\$047b247a\$8df14b96@aejhrwu>' (spam score 100)
04/02/2008 15:55:19 Deleted message '<000901c86746\$047b247a\$8df14b96@aejhrwu>' for recipients 'Craigie-Lee.Paterson@cnwl.ac.uk'
04/02/2008 15:55:20 Detected spam message '<002d01c8680f\$e10294a0\$aa83d442@kyb>' (spam score 100)
04/02/2008 15:55:20 Deleted message '<002d01c8680f\$e10294a0\$aa83d442@kyb>' for recipients 'Steve.Rochford@cnwl.ac.uk'
04/02/2008 15:55:23 Detected spam message '<06338370.20080204155812@cnwl.ac.uk>' (spam score 100)
04/02/2008 15:55:23 Deleted message '<06338370.20080204155812@cnwl.ac.uk>' for recipients 'Debbie.Pole@cnwl.ac.uk'
04/02/2008 15:55:25 Detected spam message '<001201c8674f\$1fef1a60\$026cc4f0@bruno9b5xjgahv>' (spam score 99)
04/02/2008 15:55:25 Deleted message '<001201c8674f\$1fef1a60\$026cc4f0@bruno9b5xjgahv>' for recipients 'Alemishet.Demissie@cnwl.ac.uk'
04/02/2008 15:55:29 Detected spam message '<38802.constantine@hamid>' (spam score 100)
04/02/2008 15:55:29 Deleted message '<38802.constantine@hamid>' for recipients 'carlton.bryan@cnwl.ac.uk'

Avoiding back-scatter

Anti-virus

Inbound messages		ON
On infection	Delete message	Alert
On encrypted message	No action	
On encrypted attachment	No action	
Outbound messages		ON
On infection	Delete message	Alert
On encrypted message	No action	
On encrypted attachment	No action	
Internal messages		ON
On infection	Delete message	Alert
On encrypted message	No action	
On encrypted attachment	No action	

Alert configuration

Send email alerts to

- Administrators
- Message recipients
- Message sender

OK Cancel Help

Vaguer filters

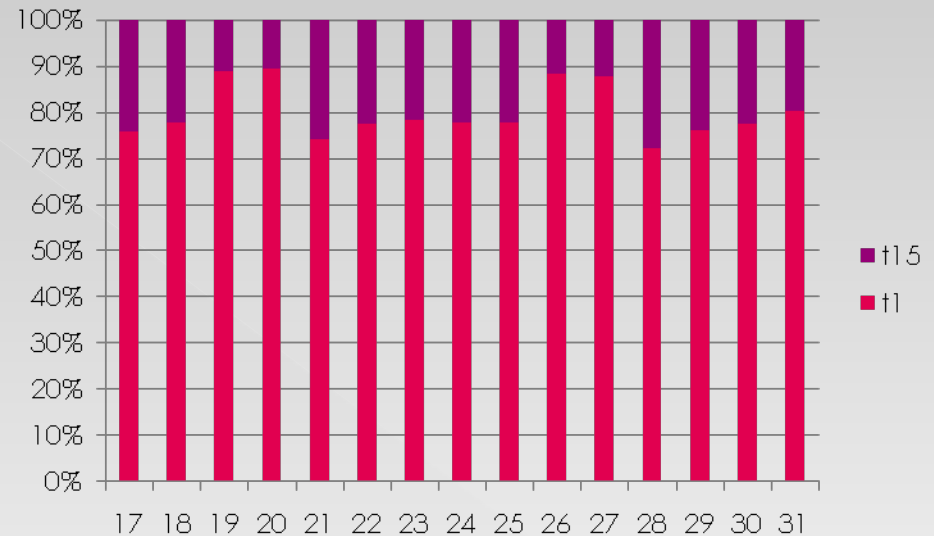
Content filtering				
Inbound messages				ON
<input type="checkbox"/> On suspicious attachment	Define	Quarantine message	Alert	
<input type="checkbox"/> On restricted attachment	Define	No action Deliver message Replace with text Delete message Quarantine message	Alert	
<input checked="" type="checkbox"/> On blocked phrase	Define	Quarantine message and deliver Quarantine message	Alert	
<input type="checkbox"/> On offensive language	Define	Quarantine message	Alert	
Outbound messages				ON
<input type="checkbox"/> On suspicious attachment	Define	Quarantine message	Alert	
<input type="checkbox"/> On restricted attachment	Define	Quarantine message	Alert	
<input checked="" type="checkbox"/> On blocked phrase	Define	Quarantine message	Alert	
<input type="checkbox"/> On offensive language	Define	Quarantine message	Alert	
Internal messages				ON
<input type="checkbox"/> On suspicious attachment	Define	Quarantine message	Alert	
<input type="checkbox"/> On restricted attachment	Define	Quarantine message	Alert	
<input checked="" type="checkbox"/> On blocked phrase	Define	Quarantine message	Alert	
<input type="checkbox"/> On offensive language	Define	Quarantine message	Alert	

Pure message summary

Summary statistics for today	
Transport (SMTP) Scanning	
Message volume	10964
Virus volume	1
Spam volume	6986
Average daily message volume	11919
Top viruses	Mal/HckPk-A
Exchange store scanning	
Attachments processed	0
Viruses detected	0
Quarantine	
Quarantine database size (MB)	29
Quarantine folder size (MB)	65

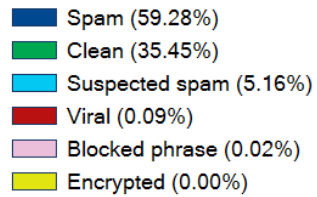
“junk” mail

Day	t1	t15	% junk
17	17835	5744	67.8%
18	17633	5048	71.4%
19	14125	1756	87.6%
20	13998	1674	88.0%
21	16971	5922	65.1%
22	19018	5561	70.8%
23	19503	5411	72.3%
24	18455	5269	71.4%
25	17132	4945	71.1%
26	13370	1765	86.8%
27	11348	1570	86.2%
28	16011	6210	61.2%
29	16726	5295	68.3%
30	18396	5327	71.0%
31	19328	4790	75.2%



Statistics – front end server

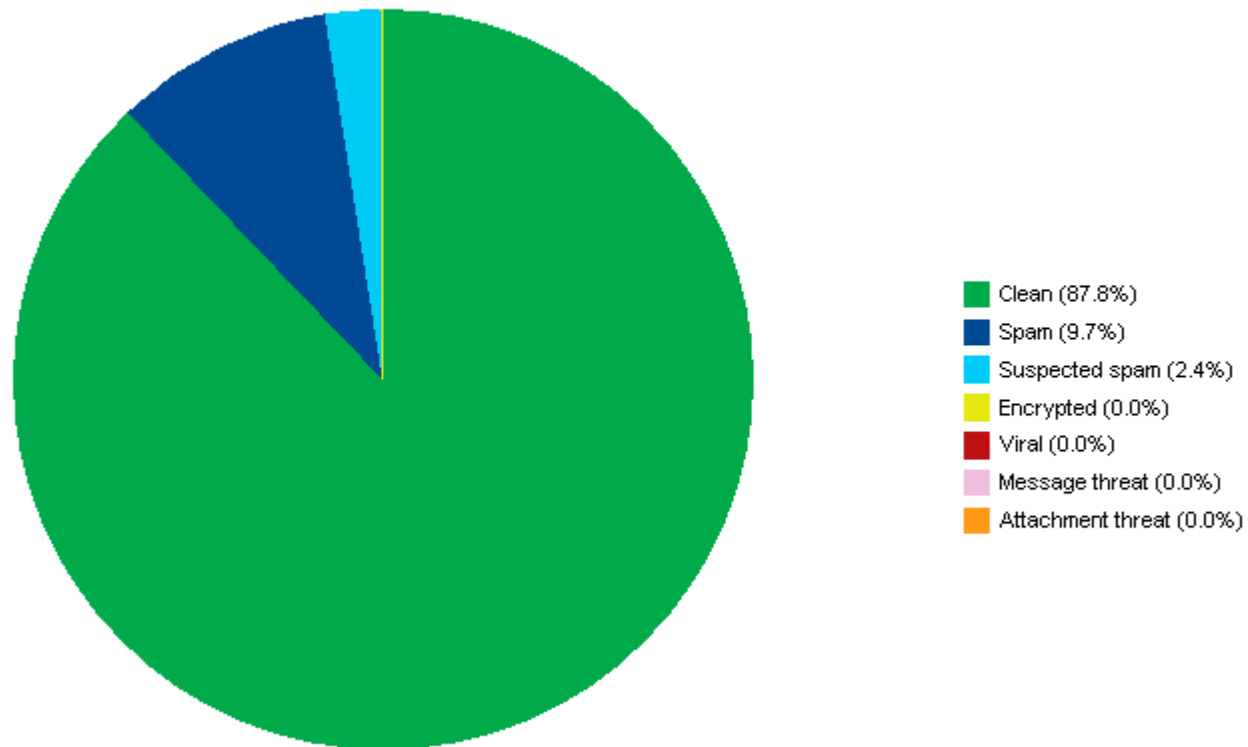
Message categorization for TCONWL1 from 01/10/2007 to 31/01/2008



Month	Virus%
Nov-07	0.13%
Dec-07	0.02%
Jan-08	0.01%

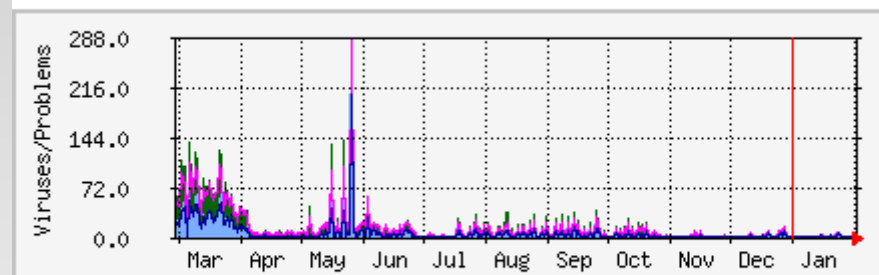
Statistics – backend server

Message categorisation for TCONWL15 from 01/10/2007 to 03/02/2008



Virus stats – secondary MX

'Yearly' Graph (1 Day Average)



	Max	Average	Current
Infected Mail	286.0	10.0	0.0
Viruses Detected	283.0	8.0	0.0

Protecting you from us

- ◉ No user workstation has public IP
- ◉ Users access internet through proxy server
- ◉ Router configured to only allow port 25 from designated SMTP (not proxies!)

Web mail

- ◉ Many users access Hotmail etc
- ◉ Client side virus scanner
- ◉ Picks up more viruses
- ◉ Also configured to just delete silently