Email Filtering with Open Source Software

OLUG – June 7, 2005

Presenter Bio

- Undergraduate Education
  - Nebraska Wesleyan University
    - B.A. Business Administration
    - Minor Computer Science
- Professional Experience
  - 3 years experience as Software Engineer
    - Vertical Market Software Application Development
  - 5 years as Network Engineer
    - VAR / Consulting Industry

This Presentation

- Will be ‘High Level’ – the proposed solution is simple to install and configure by anyone with Basic to Intermediate Linux skills
- Presenter not an experienced speaker
- Please ask questions or elaborations at any time!
- Handout with resources available

Spam/Virus in Email – Well Known Problem

- Spam, virus, worms, spyware, phishing attacks on the rise.
- Problem increasing for companies, both large and small.

Commercial Solutions

- Expensive
- Many do not work very well
- Customization tricky in some areas
- Stability

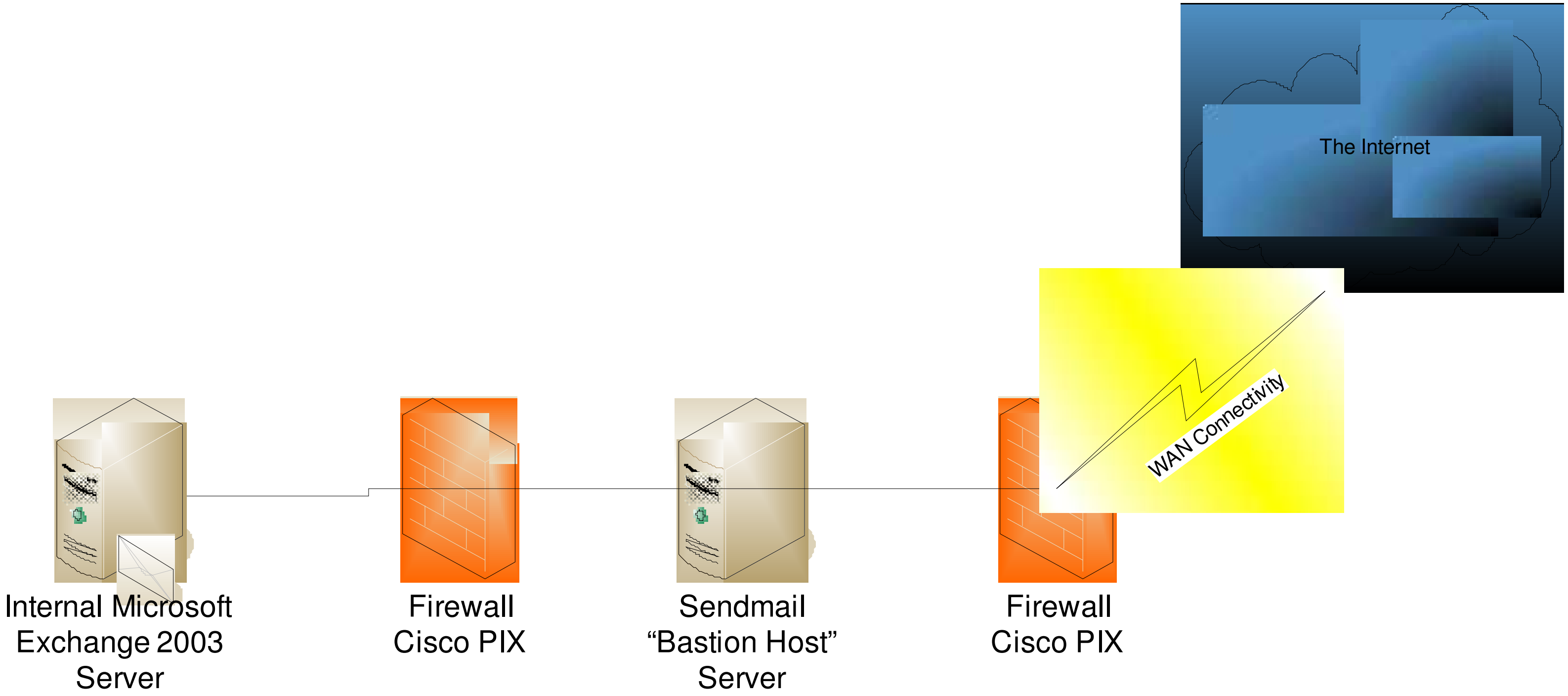
Open Source – A better solution using Best of Breed Tools

- Sendmail – Ubiquitous open source mailer
- MimeDefang – Open source framework for filtering e-mail
- ClamAV – Open source virus scanner
- SpamAssassin – Open source spam filter.

Overview of Solution

- Sendmail ‘Bastion’ host filters mail for a Microsoft Exchange Server
- Mail ‘tagged-and-forwarded’ for processing by the MUA (Outlook)
- Benefits
  - Exchange Server not on the Internet
  - Mail will store if Exchange server not available

Solution Diagram


The Internet
WAN Connectivity
Internal Microsoft Exchange 2003 Server
Firewall Cisco PIX
Sendmail "Bastion Host" Server
Firewall Cisco PIX

Overview of Solution - continued

- Mail scanned for
  - Virus
  - Phishing Attacks
  - Real-time blacklist listing (RBL)
  - Exploit blacklist listing (XBL)
  - Spam content
  - Un-allowed file extensions in Attachments
    - Inside Zip files
  - Malformed MIME
    - Takes advantage of flaws in the MUA (Outlook mainly)
  - Spam fingerprint/checksum check
    - Razor, DCC

Disadvantages of Solution

- Not tightly integrated with destination MTA (Microsoft Exchange in this case)
  - Users can’t self-manage whitelists, blacklists
  - Can’t auto-whitelist based on users address book
- May actually be seen as a benefit by reducing complexity

Sendmail Configuration

- 8.13.X – needed for milter support
- Configured with *Milter* support to allow MimeDefang to interface with Sendmail
- Configured with *mailertable* support which allows direction of scanned mail to internal Exchange Server
- Other then this, standard install – refer to MimeDefang howto

MimeDefang Overview

- Combination of Perl and C
- ‘Filter’ written entirely in Perl which allows for complete and easy control and customization over the entire process.
  - Uses common Perl Modules found on CPAN
    - Mime decoding
    - Zip decompressing
    - Syslog
    - Etc
  - Uses other well-written modules
    - Razor, DCC
- Well written and documented with an active mailing list
  - http://www.mimedefang.org

MimeDefang Configuration

- Compile, install, add to init scripts
- Stock Filter – very good start
- Enable different set of allowed extensions inside Zip archive
- Enable DCC and Razor spam fingerprint check
- Enable filter_recipient code to check for recipient in target organization
  - Entry in mimedefang-filter

ClamAV Overview

- Premier open source virus scanner
- Fast definition updates
- Support for blended threats such as recent Microsoft JPEG exploit and Icon overflow
- Support for blocking major Phishing attempts

ClamAV Configuration

- Compile and install
- Start clamd in init scripts
- Configure Freshclam – Runs via cron to keep virus database up to date
- New scanning engines require manual compilation and installation

SpamAssassin Overview

- Open source spam identification system
- Utilizes a scoring system
  - Tokens, scores, thresholds
- Can use Bayesian scoring to customize itself to the business
- Very easy to write your own ‘tests’
  - Ex: German spam from recent Sober Virus
  - Other 3rd party tests available

SpamAssassin Configuration

- Compile and install as outlined in the MimeDefang howto
- Not currently using Bayes features due to multi-business approach
- MimeDefang does not use spamd (SpamAssassin Daemon), but instead calls the Perl modules itself

Exchange Server Configuration

- Enable *Recipient Filtering* to allow Exchange to refuse non-existent users
  - Available in 2003, not on by default
- Could also use Sendmail's Access features or integrate LDAP lookups into the MimeDefang code

MUA Configuration - Outlook

- Create a server-side rule
  - Will run even when Outlook is closed
- Examine header – X-Spam-Status: Yes
- Send mail to ‘Junk Mail’ folder

- We do this to allow users to inspect their own junk mail. Another option would be a central quarantine

Testing

- Test MimeDefang
  - Send test banned attachments
- Test SpamAssassin
  - GTUBE – Generic test for unsolicited bulk email
- Test ClamAV
  - Harmless Eicar Virus – detected by most AV scanners
  - Worm.Sobig.F – Found at ClamAV Howto
  - TestVirus.org – Sends over 30 kinds of virus
- Put into production and watch logs!

Other Ideas

- Central Quarantine
- Bayes Scanning
- Scan outgoing email (ISP)
- Disclaimer Boilerplate
- Compliance Processing
- Rate Limiting/GreetPause
- Per user settings (whitelists, Bayes, blacklists, spam thresholds)
  - SQL Database
  - Web Front-end

Results

- 100% Uptime in 8 months service
- Easily deflected recent Sober.P outbreak
- Estimated 98% Spam catch
- Almost non-existent false positive rate
- Has deflected many JPEG, Icon, Phishing, and other non-virus threats

Resources

- The MimeDefang Howto
  - http://www.mickeyhill.com/mimedefang-howto/
- Using MimeDefang with ClamAV
  - http://sial.org/howto/mimedefang/clamav/
- SpamAssassin WIKI
  - http://wiki.apache.org/spamassassin
- Email Me:
  - drazak@materiamagica.com – Andrew Embury

Questions

- Open for questions