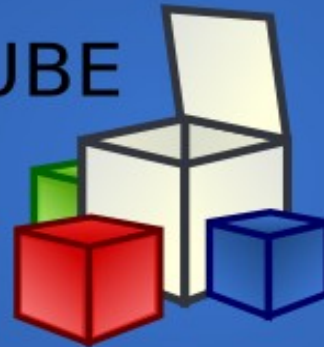


FOSS to the rescue

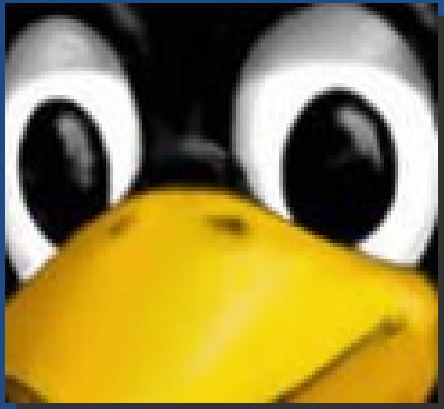
Securing your Windows Network

By
Buddhika Siddhisena
Co-Founder & CTO

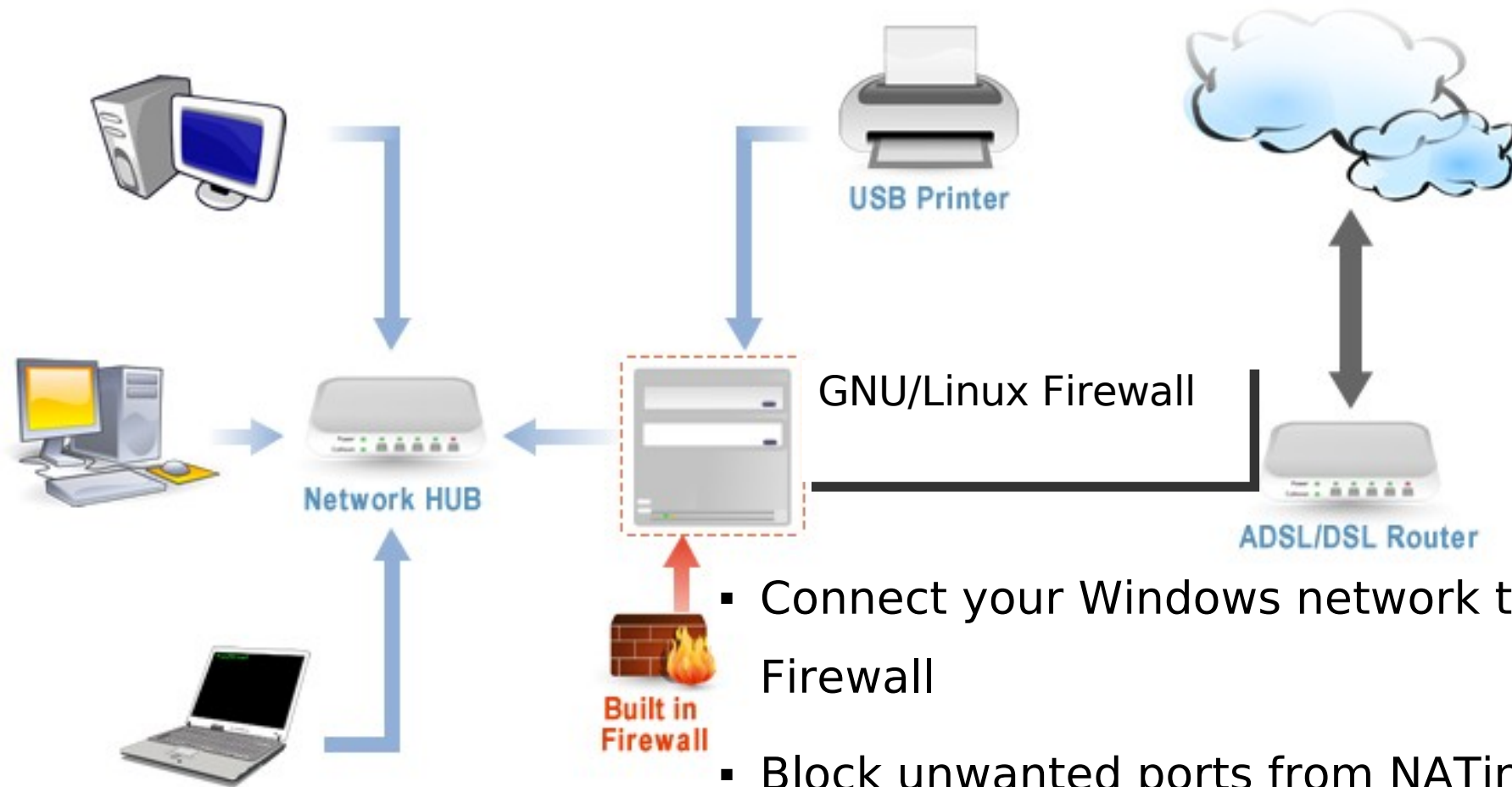
THINKCUBE



Senior Member of the Lanka Linux User Group

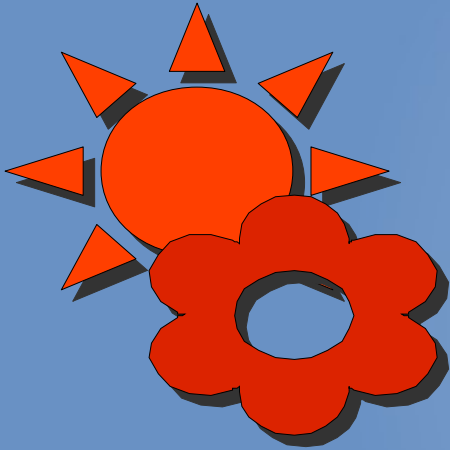


FOSS to the rescue



- Connect your Windows network through a Firewall
- Block unwanted ports from NATing out to the network, especially port 25

CLAMAV – The Free Virus Guard



Consumer Alert: Massive Virus Outbreak

A quick test by PC World shows that many antivirus programs fail to catch today's nasty Storm Worm variant.

In my tests of 31 programs, only four reported a virus --**ClamAV**, eSafe, Kaspersky, and Symantec--reported a virus.

Source: <http://www.pcworld.com/article/id,130686-c,virusesworms/article.html>

Safer Web Browsing

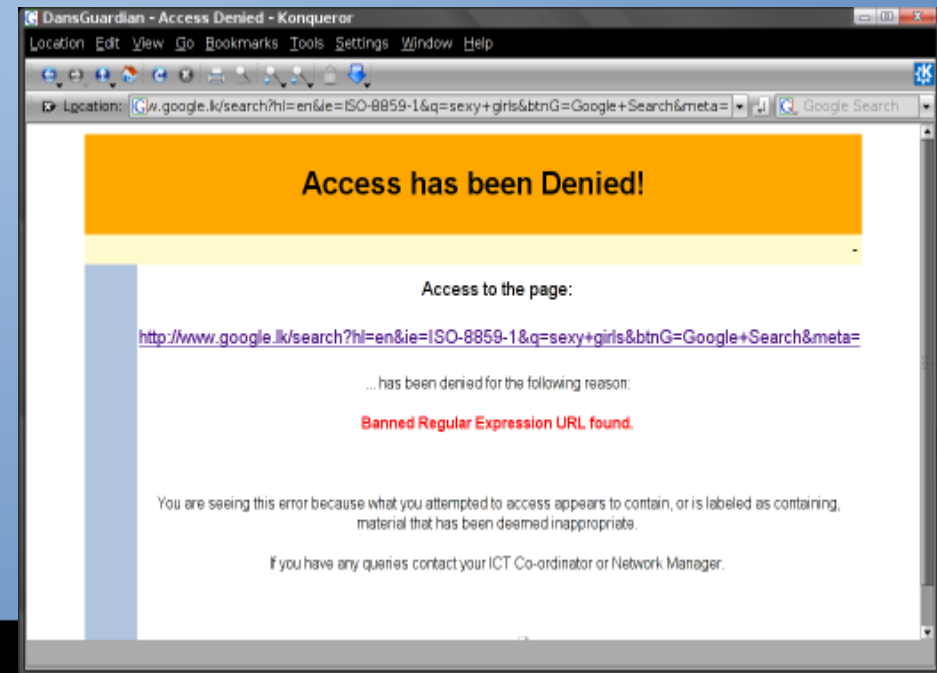


Virus Scanning Downloads

Downloading spyware & Virus infected files can be protected using SQUID Proxy Server and interfacing that with ClamAV using **SquidGuard**

Web Content Filter

DansGuardian is a content filter that can be used to block unwanted sites which is a main cause of Spyware

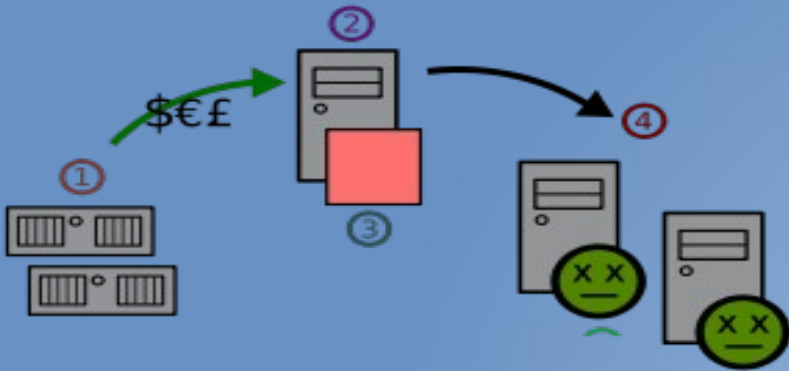


SPAM SPAM SPAM



- Over 60% of all emails sent are SPAM
- Email was designed when the net was innocent
- Zombie machines are the #1 cause of SPAM
-

HOW Mail works



- Client sends Mail to SMTP server
- SMTP Server accepts mail from client
- SMTP Server looks up the to address's domain using DNS MX record
- SMTP Server contacts the remote SMTP Server and delivers the mail
-

Preventing SPAM

- Don't run an Open Relay!
- Block port 25 on the network
- Configure Mail server not to accept unresolved Domains. Make them require a FQDN
- Configure RBL
- Greylisting which initially rejects mails and sends a try again request
- Try to implement SPF (Sender Policy Framework)
- Finally setup a Rule based / Statistical content filter such as **Spam Assassin** and **DSPAM**
- Configure Mail server to use ClamAV & SpamAssassin via **Amavis** or **MailScanner** for example

THANK YOU...

bud@thinkcube.com

THINKCUBE

