

Fire fight

InterChange is a medium-sized charity, based in north London, which provides both services and a home for a number of projects including those in education, music and the performing arts. Capital funding from the National Lottery had made expansion possible, with a move to the refurbished Hampstead Town Hall Centre in 2000. IT requirements increased accordingly, with full internet access now an expectation of charity workers and centre users alike. The security implications of these demands became clear, but not until some expensive lessons had been learned.

Gradual IT deployment since the 1970s had eventually built a heterogenous network serving around 50 desktops and laptops, with both Windows and Apple clients served from NT4 and Apple machines. Single office peer-to-peer networks had been replaced by site-wide Ethernet, and Internet access had broadened from individual modems to ISDN, which was in turn replaced by a Cisco 1601 router and leased line. This enabled the installation of an in-house DNS and web server running Red Hat Linux.

Permanent Internet access to the network exposed the vulnerabilities of the servers and workstations in the various departments. The DNS and web server was compromised by an external attacker, and it was only when legitimate users were disallowed from making FTP connections that InterChange IT staff realised something was wrong. The NT-based file and mail server was cracked a month later. Basic services were taken off-line while the machines were rebuilt with security patches.

Adding up downtime, extra work for IT staff and consultancy fees, the cracking incidents had cost thousands. The unexpected nature of the attacks put strain on the charity's limited IT budget. Something had to be done to tighten up network security, but research indicated a proprietary firewall solution would cost a further £2000-£2500 for the hardware alone. Training and support for the fire-



With a Linux firewall, even a charity can afford to keep the crackers out, reports Daniel James

wall would create an additional cost burden, as the in-house personnel had little Unix experience.

Fleeta Siegel is responsible for IT at InterChange's Weekend Arts College, which provides arts education for excluded and disenfranchised young people. Realising that doing nothing was not an option, but recruiting a Unix guru to the staff was not financially feasible either, he started to look into the free software alternatives.

Amongst retired Intel hardware, Siegel had a Fujitsu desktop machine with a Pentium 200Mhz MMX processor, 64MB RAM and 2GB hard disk. He fitted the PC with three network cards, and enlisted the help of *LinuxUser*, who contacted the UK-based SmoothWall development team. SmoothWall is a free Linux-based firewall designed for modest hardware and ease of use, which has already gained hundreds of thousands of users around the globe.

Paul Tansom of the SmoothWall project volunteered to help. SmoothWall version 0.9.9 was installed on the Fujitsu box, and the task of configuring it for the InterChange network began. "They had a range of 128 real IP addresses that were being allocated by an NT DHCP server," he says, "and the Cisco box that they had routing traffic out was not doing any NAT, so basically they were

De-worming Nimda with Squid

It's not just Windows email clients that are vulnerable to internet viruses any more. Thanks to the ability of Internet Explorer to run many kinds of executable file without prompting the user, the Nimda worm was able to be picked up unnoticed through the browser while viewing sites hosted on infected IIS servers. The file in this case was named 'readme.eml'.

Since users can't be relied upon to protect their workstations from this kind of attack, a site-wide remedy can be applied quickly and easily using the free Squid http proxy server, included in SuSE's CD-based firewall and many other Linux distributions.

All that's required is to add three lines to the /etc/squid.conf configuration file:

```
acl nimda urlpath_regex -i \.eml$
acl nimda urlpath_regex -i \.nws$
http_access deny nimda
```

and restart Squid to read the new configuration. www.squid-cache.org

wide open. Their only server that needed supporting was a Microsoft Exchange server that was handling their email, so the solution fell into place with minimal impact."

A spare IP address was allocated to the Internet-facing network card of the SmoothWall, colour coded as the 'Red' interface. The 'Green' card was configured for the internal network, and the 'Orange' card for the 'demilitarised zone', where internet-facing servers would reside in future. SmoothWall was set to use the Cisco router as its gateway and the DNS servers provided by InterChange's ISP.

The SmoothWall box was installed between the internal network and the Cisco router, with a crossover cable on the Red interface and the Green network card connected into the main hub where the router had been. This was quickly followed by reconfiguring the client machines to use the SmoothWall as both internet gateway and DNS proxy server.

"The mail server was moved onto a static internal IP address from a small range that had been reserved for this purpose," Tansom continues. "Once this was done it was simply a case of setting up port forwarding on the SmoothWall box to send all traffic on port 25 (SMTP) to the Exchange mail server." Rather than let just any machine connect with the mail server via port forwarding, access was tied down so that only connections on port 25 originating from the fallback mail servers at InterChange's ISP would be allowed. This effectively left the port closed to all other machines, allowing the Exchange server to collect mail from the ISP with less worry about being compromised. "For ease of configuration I decided to place the firewall on the same IP address that the mail server had used, as this removed the need to change any of the MX records, and minimised down time. A quick visit to Setup through an SSH shell sorted this out without any problems, or the need for a reboot."

The previously easy-going culture of the InterChange network has had to be

reconciled with security needs, so that external users (such as staff working from home) can no longer pick up their email or transfer files in the way they used to. Siegel says: "For the most part, the solution is invisible for the people on our side of the firewall – they should not notice any difference in access. It's only the people on the external side trying to upload files or get in to the network that will notice there is now a barrier, and they will have to configure their machines differently."

This issue was highlighted when the first support call came in. A user phoned up to say that they could no longer get their email from outside the local network. A crude solution would have been to open up the POP3 port to forwarding, but since the majority of dial up users are assigned dynamic IP addresses and could be using any ISP's range, this would have meant leaving the port wide open.

Tansom discussed a number of options with Siegel for resolving the issue securely. These included getting static IP based dial-ups for those users who really needed external access, and port forwarding only those addresses to port 110. One alternative would be to use a browser-based IMAP email solution over SSL, while a more exotic option would be to equip each external user with their own SmoothWall box and use the VPN features to enable secure network access. Siegel was relieved to find that browser-based Linux firewall configuration could be quickly grasped by an IT administrator without significant Unix command-line experience: "Paul was able to show us, in less than an hour, the entire SmoothWall interface." The deployment has been trouble-free since installation, and has solved a problem that Siegel described, in his New York accent, as a considerable "pain in the butt".

Tansom concludes by saying that free software firewalls are "an ideal solution for small and medium-sized organisations to secure themselves without the high price tag of some other solutions, but still with confidence that they are extremely well protected."

Hello crackers!

The legacy of the NetBIOS network architecture has meant that average PC users leave their computer wide open every time they go on to the Internet. Introduced in the early 1980s, with NetBEUI (NetBIOS Extended User Interface) appearing in 1985, it remains the default file sharing protocol in many Windows machines, despite the emergence of the TCP/IP standard. Rather than ditch the obsolete non-routable technology when global networks became widely accessible in the 1990's, Microsoft used 'binding' to piggyback Windows machines onto TCP/IP networks. The result is that a simple program executed from the Internet can peer deep into the ubiquitous Windows desktop machine. Steve Gibson's web-based utility 'Shields UP!', available at grc.com, is able to reveal enough to panic the average privacy-conscious Windows user. Since NetBIOS authorisation is almost non-existent, passwords being optional, the utility can retrieve user, machine and workgroup names from the LAN on demand.

Third-party 'software firewalls' installed on individual machines have become a popular bolt for the stable door. But with these products built on such shaky foundations, clued-up users in the era of always-on connections are turning to Linux on dedicated hardware.

Key link

SmoothWall
www.smoothwall.org

Saving users from themselves

Installing a Linux firewall on a Windows network might prevent attackers from going through the front door, but it can't protect nasty things from being dropped into the mailbox. Since email became widely used in the workplace, a rash of email attachment viruses has caused significant cost and network congestion to enterprises all over the world. Windows users can be educated not to send or open executable attachments, but some programs will insist on running viruses on a users behalf, notably the widely used Microsoft Outlook.

For those organisations not ready to replace Windows on the desktop with something more robust, a Linux solution at the network infrastructure level can be used to filter email and strip viruses from attachments. Qmail-Scanner (aka scan4virus) is an addition to the free Qmail server which can be used in conjunction with proprietary virus scanners. It can also deal with email that contains specific strings identifying it as the carrier of a virus, or problematic attachment types such as Visual Basic, and is capable of scanning both local and relayed email.
qmail-scanner.sourceforge.net