

Replacing ISA

How we can help you

- Consulting: we specialise in deploying Open Source alternatives to ISA. Deployment
 - Training: we can train your staff to it themselves. Training
 - Support: we're happy to offer support and advice for businesses keen to replace ISA themselves.
- SupportThe Sirius Way - 8 Steps for Success
- Ensure the deployment strategy matches business strategy.
 - Never deploy technology for technology's sake.
 - Get the business on board.
 - Achieve full buy-in and commitment, by targeting clear business benefits.
 - Plan the 'when'.
 - The when is crucial.
 - Know business cycles, windows, and people availability.
 - Ensure contingency is built-in, right from the start.
 - Be ready for the unexpected.
 - Have a clear, agreed, documented backout plan.
 - Never rely on enthusiastic amateurs.
 - Have access to proven, high quality, on demand, professional support.
 - Document the deployment.
 - Continually learn and improve.
 - Six months down the line, you'll know what you did!
 - Measure the results.
 - And publish them so they are open, visible, and seen by the business.
 - Celebrate success.
 - With your IT team and with the business. Technologies

Squid

Squid is a caching proxy server. Most companies require some or all of their users to have web access, but do not wish to attach modems to every single users machine. Users web browsers are pointed at the proxy server, which downloads web pages on their behalf and serves them to their browser. A caching proxy server will save a copy of all web sites it has downloaded so that next time a user looks it up, only files that have changed need to be downloaded again. Caching will, over time, save a company a huge amount of bandwidth as most users view the same sites, and certain sites are viewed again and again. Squid is:

- a full-featured Web proxy cache
- designed to run on Unix systems
- free, open-source software
- the result of many contributions by unpaid (and paid) volunteers

Squid supports...

- proxying and caching of HTTP, FTP, and other URL's
- proxying for SSL
- cache hierarchies
- ICP, HTCP, CARP, Cache Digests
- transparent caching
- WCCP (Squid v2.3 and above)
- extensive access controls
- HTTP server acceleration
- SNMP
- caching of DNS lookups

Iptables

Iptables does stateful packet filtering. Packet filtering is the process of inspecting incoming and outgoing network traffic to see whether it is allowed according to some security ruleset. Statefull packet filtering is an enhancement whereby packets can be accepted or denied depending on recent history (this helps protect against certain kinds of attack). The intention of this is to define which services (e.g. email, web access) are allowed to pass the packet filtering machine, and which services (e.g. network logins, access to files on the network, etc.) are denied. Packet filtering is perhaps the most important function of any product purporting to be a Firewall. Iptables runs under the Linux operating system.

The netfilter/iptables project is the Linux 2.4.x / 2.5.x firewalling subsystem. It delivers you the functionality of packet filtering (stateless or stateful), all different kinds of NAT (Network

Address Translation) and packet mangling.

SpamAssassin

SpamAssassin SpamAssassin(tm) is a mail filter to identify spam. Using its rule base, it uses a wide range of heuristic tests on mail headers and body text to identify "spam", also known as unsolicited commercial email.

The spam-identification tactics used include:

- header analysis: spammers use a number of tricks to mask their identities, fool you into thinking they've sent a valid mail, or fool you into thinking you must have subscribed at some stage. SpamAssassin tries to spot these.
- text analysis: again, spam mails often have a characteristic style (to put it politely), and some characteristic disclaimers and CYA text.

SpamAssassin can spot these, too.

- blacklists: SpamAssassin supports many useful existing blacklists, such as mail-abuse.org, ordb.org or others.
- Razor: Vipul's Razor is a collaborative spam-tracking database, which works by taking a signature of spam messages. Since spam typically operates by sending an identical message to hundreds of people, Razor short-circuits this by allowing the first person to receive a spam to add it to the database -- at which point everyone else will automatically block it. Once identified, the mail can then be optionally tagged as spam for later filtering using the user's own mail user-agent application.

SpamAssassin requires very little configuration; you do not need to continually update it with details of your mail accounts, mailing list memberships, etc. It accomplishes filtering without this knowledge, as much as possible. The distribution provides a command line tool to perform filtering, along with Mail::SpamAssassin, a set of perl modules which allow SpamAssassin to be used in a wide range of products.

SpamAssassin lives at spamassassin.org or in CPAN, and is distributed under Perl's Artistic license. ('SpamAssassin' is a trademark of Network Associates, Inc.)

Features

- Wide-spectrum: SpamAssassin uses a wide variety of local and network tests to identify spam signatures. This makes it harder for spammers to identify one aspect which they can craft their messages to work around.
- Free software: it is distributed under the same terms and conditions as Perl itself.
- Easy to extend: Rules, weights and user-visible text are stored in text configuration files as much as possible, which the user (or sysadmin) can edit to modify or add new rules.
- Flexible: SpamAssassin encapsulates its logic in a well-designed, abstract API. As a result, it's not limited to the traditional local-delivery-to-spool case; using the Mail::SpamAssassin classes, it can be used in a wide variety of setups. This means that SpamAssassin support is available for a variety of mail systems -- traditional procmail, a Mail::Audit plugin, qmail, MIMEDefang, Postfix, and many others.

Snort

Snort is an open source network intrusion detection system, capable of performing real-time traffic analysis and packet logging on IP networks. It can perform protocol analysis, content searching/matching and can be used to detect a variety of attacks and probes, such as buffer overflows, stealth port scans, CGI attacks, SMB probes, OS fingerprinting attempts, and much more.

Snort uses a flexible rules language to describe traffic that it should collect or pass, as well as a detection engine that utilizes a modular plugin architecture.

Snort has a real-time alerting capability as well, incorporating alerting mechanisms for syslog, a user specified file, a UNIX socket, or WinPopup messages to Windows clients using Samba's smbclient. Snort has three primary uses. It can be used as a straight packet sniffer like tcpdump(1), a packet logger (useful for network traffic debugging, etc), or as a full blown network intrusion detection system.

Webmin

Webmin is a web-based interface for system administration for Unix. Using any browser that supports tables and forms (and Java for the File Manager module), you can setup user accounts, Apache, DNS, file sharing and so on.

Links to Key Projects

All of the key Open Source technologies that enable you to replace ISA are linked to below:

[Squid](#)
[Squid Documentation](#)
[Netfilter](#)
[Netfilter Documentation](#)
[netfilter_log_analyzer](#)
[SpamAssassin](#)
[SpamAssassin Documentation](#)
[Webmin](#)
[Webmin Documentation](#)
[Snort](#)
[Snort documentation](#)