

CipherTrust IronMail 305



Despite the proliferation of managed services many enterprises prefer, from a security perspective, to manage and maintain all network services internally. This includes anti-spam measures - and the IronMail appliances from CipherTrust look ideal candidates for just such a job, as they provide a complete range of tools for separating the guff from the good stuff. Along with an arsenal of spam detection techniques, the IronMail family offers optional content filtering capabilities and virus scanning and ties them all together under a smart web browser management interface.

Spam control at the enterprise level demands good performance and the IronMail 305 on review doesn't attempt to hide its pedigree, as the hardware comes courtesy of a good quality IBM eServer xSeries 305 1U rack server. IronMail is designed to sit between your mail servers and firewall where it can be placed on the LAN or in a DMZ. Installation is simple enough as you point a browser at the appliance's default IP address and follow a quick-start wizard, which takes you through the network and mail server setup.

A wide range of network scenarios are supported but you'll need to configure your mail server to only accept connections from the IronMail's IP address. It

acts as a proxy through which all incoming and outgoing mail is routed, so you must set up your mail server to send all outbound mail to the appliance. However, IronMail does much more than a simple proxy as it examines all the data in every email that passes through and subjects it to a barrage of tests.

Tools such as reverse DNS lookup are used to verify the sending mail server and RBLs (real-time blackhole lists) confirm whether the sender is a known spammer. All data in each message is then checked for payloads that may contain an attack or virus and it can also protect Web Mail services as its intrusion detection engine uses signatures to identify and block over 700 attack patterns. With the ability to check and verify message content IronMail allows you to deploy and enforce strict policies for controlling email usage.

The browser interface is a tidy affair with a row of tabbed folders providing easy access to each licensed feature. Rather than use a single spam control solution, a range of detection tools are employed allowing administrators to easily customise these to suit. Alternatively, the confidence-based detection uses all available tools to calculate a spam probability score. Along with attack detection and prevention, the IronMail monitors all user's mail server passwords and maintains lists showing who is using strong

and weak passwords. The Policy Manager is where all the action takes place and once you've determined basic mail firewall characteristics, rules can be used to strictly control what mail is allowed to enter or leave your company.

With usage policies in place reporting needs to be good - and IronMail doesn't disappoint. Event logging and alerting are extensive, while a wide range of HTML and CSV reports can be generated on each IronMail service and the data can be scheduled for regular archiving over FTP or SCP (Secure Copy). You also get plenty of performance monitors with a smart dashboard that provides a single-screen readout on all IronMail services, the status of each mail queue, spam policy activity and virus detection.

IronMail 305 is an impressive messaging security gateway that looks capable of scaling across a wide range of business use. It provides excellent protection against spam and all manner of Internet nuisances and backs this up with extensive rules, allowing you enforce strict policies controlling the use of company mail systems. **NC**

For more information on CipherTrust or IronMail, please contact:

Tel: +44 (0)870 990 5516

Fax: +44 (0)870 990 5517

Email: emea.sales@ciphertrust.com

www.ciphertrust.com