SkyScan Anti-Porn (AP)

SkyScan AP, a porn filtering service, is powered by unique and patented Image Composition Analysis Software (ICA).

Image Composition Analysis (ICA)
ICA identifies pornographic images from leaving or entering your company's network boundaries. The filtering software carries out numerous detailed calculations at high speed to assess the nature of the attached image. In fact, ICA uses 22,000 different algorithms to define the content of any one image, without hindering the speed at which the software operates.

The software is driven by a number of different attributes relating to the image. For example, ICA can determine whether or not a photograph has been taken indoors or outdoors. It can also identify where and how many faces are contained in the image. When an image attachment is analysed, the patented artificial intelligence within ICA combines the results, based on the various image attribute settings from its growing knowledge base, to reach an intelligent decision as to whether an image is pornographic. Furthermore, SkyScan AP customers can alter the sensitivity of the porn filtering service depending on their business policies, via InSight – the MessageLabs customer extranet.

Similar to the Skeptic software, ICA is continuously processing and storing data to increase its knowledge base, therefore continually improving overall performance levels.

SkyScan Anti-Spam (AS)

SkyScan AS protects a mail domain from unsolicited e-mail, known as 'spam'. Through the use of public lists, SkyScan AS can identify known spam senders/offenders and block the spam e-mail immediately, then tag and re-route it to a designated server.

SkyScan AS additionally supports customer configurable white and blacklists. This option allows customers to build their own white and blacklists, preventing (or allowing) mail from known sources of unsolicited e-mail. Comprehensive logging of spam sources and regular reporting are available through InSight. Customers can also configure InSight to manage deleting, tagging or re-routing of spam to a specified customer destination.

Extranet Configuration and Reporting

The back-office architecture supports extranet administration management and reporting to end-users. A centralised server farm incorporates load balancing and redundancy to provide high performance, scalability and fault tolerance for management of customer configuration and statistical data – accessed and supplied through the InSight web-based reporting tool. This enables all e-mail and scanning data to be completely transparent to the customer.

Control Tower

System Reporting and Management

- All statistics logged
- Individual company reports and statistics can be remotely accessed through MessageLabs' web-based reporting tool, InSight
- InSight enables customers to track e-mail and virus trends 24x7x365
- The Control Towers and network are monitored 24x7x365 by support technicians and network operators

System Architecture and Configuration

- Multi-Server structure, globally distributed and mirrored for extra resilience
- Located in secure data centres at major exchange points
- Scalable and resilient
- Fault-tolerant network, server, messaging and database technology
- Vendor & carrier independent
- Dual 100Mb bandwidth per Tower
- Centralised management and control
- Automated intelligence gathering and systematic updates
- Extranet based configuration management and reporting

SkyScan Technical Overview

MessageLabs is a Managed Service Provider (MSP) specialising in e-mail security. Our revolutionary SkyScan portfolio of services enables customers to be protected from threats such as viruses, pornographic material and unsolicited mail, long before they reach the network boundaries.

SkyScan Infrastructure and Global Network

MessageLabs' SkyScan service portfolio is powered by a global network comprising of fault tolerant clusters of e-mail processing engines or 'Control Towers', strategically positioned at key Internet exchange points across the globe.

The MessageLabs network comprises a globally distributed architecture; through protected Control Towers hosted in secure data centres, with redundant connectivity into multiple Internet backbones. Each Control Tower provides a secure, high performance, resilient and scalable infrastructure on which e-mail security applications run. The overall global infrastructure is managed and monitored from the MessageLabs Global Operations Centre (GOC) and is capable of processing millions of e-mails every day.

The SkyScan infrastructure has Control Towers located in the UK, Europe, US (East and West Coasts) and Asia Pacific.

Control Tower Components
Each Control Tower comprises messaging, filtering, monitoring and replication of network components to ensure maximum availability. Processes systematically gather information from various intelligence sources to a central database; updates are then propagated to the localised Tower databases to support message filtering.

The network is connected with a minimum 100Mb bandwidth; with the load optimised through state-of-the-art switching technology and multi-processor servers. The Control Towers are globally distributed with the back-up Towers located in separate data centres. As a result, should a whole Tower become unreachable, it has a twin ready to take over with immediate effect.

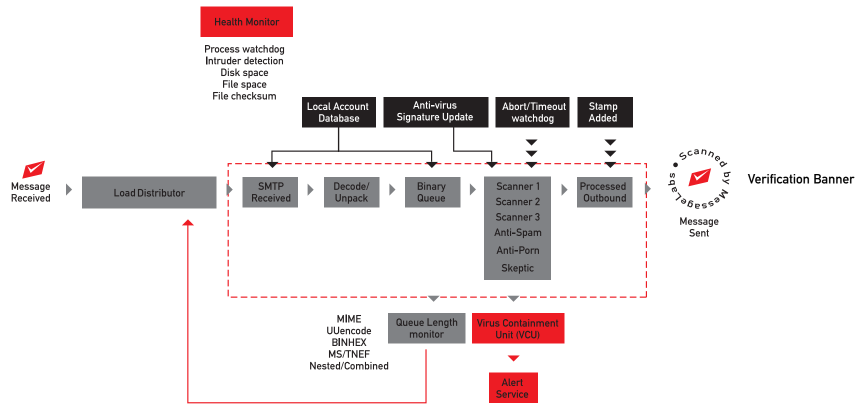
This multi-site redundancy is achieved using the inherent structure of the e-mail systems.

Server Overview
Each Tower comprises a number of switchable, dual-processor, high-performance servers with server monitoring, and adjoining temperature and fan monitors. The Tower servers are dedicated to specific functions, and can (within seconds) be recycled to perform the functions of any other server in the Tower.

Deployed in each Tower are a number of resilient monitor servers ensuring that all mail servers are running correctly, that virus signatures, filtering options and configuration files are all up-to-date, and that the operating parameters are within acceptable tolerances.

The Mail Server
All virus scanning, porn and spam filtering takes place on clustered servers which power the MessageLabs' proprietary messaging engine. Externally, the pool of mail servers appears as a single entity; incoming mail is distributed evenly across the individual mail servers by the load balancers. This number can be increased in order to scale the Tower's capacity, as well as upgraded without service downtime, simply by replacing them individually.

The mail servers have hard drives, each with redundancy and enough disk space to retain its queue for at least 7 days. So, if a customer's mail server should fail, the Tower can queue the mail for delivery when the mail server returns to normal service. Moreover, in the unlikely event of a mail server failure, the load balancers ensure no mail is distributed until it returns to service.



SkyScan E-mail Process Model

The Database Servers

All e-mail filter activity-logging is completed by the Tower's local database servers, which also provide its configuration. Information exchange is achieved through replication technology between the local Towers and the central database at the Global Operations Centre.

Information Update

Regular sharing and distribution of information is fundamental to the performance of all the SkyScan services. Each Tower automatically shares information to ensure the overall infrastructure is operating with the latest information; e-mail volumes and traffic, virus signature updates, porn and spam detection levels. Each managed service is continually building a knowledge base of information, which is then uploaded to the operating infrastructure, enabling all services to achieve optimum performance levels.

Global Operations Centre (GOC)

The MessageLabs Global Operations Centre is the nerve centre of MessageLabs' network and technical operations. All Control Towers are continuously monitored and managed by a team of specialist technicians from the GOC, based in the UK, providing a complete managed service.

These specialist technicians are highly skilled in Internet, messaging and security technologies and are responsible for the on-going monitoring, maintenance and development of the network and SkyScan services.

Continual analysis of the Internet and e-mail activity allows the MessageLabs technicians to identify trends and signs of a new threat to ensure immediate protection. The Global Operations Centre is staffed 24 hours a day, 7 days a week throughout the year, housing intelligence systems designed to specifically monitor Internet level e-mail activity. E-mail is now a business critical communication tool that is "always on" and therefore demands the highest levels of service and support.

Global Operations Centre (GOC)

To find out more about MessageLabs and to access VirusEye, our live virus information service, visit our web site at www.messagelabs.com or e-mail info@messagelabs.com

SkyScan Services

SkyScan Anti-Virus (AV)

Virus Scanning Process

When an e-mail enters a Tower, the SMTP session is distributed to one of the scanning e-mail servers, and is authenticated against the customer database to ensure the e-mail is coming from (or going to) a known customer. The e-mail and its associated file attachments are first decoded and then passed to the binary queue for scanning.

Each file is then passed through three commercial AV scanners and Skeptic™, MessageLabs' own proprietary heuristics and rules-based scanner used to detect new viruses for which no signature is available. If a virus is detected, the e-mail is moved to the quarantine area. If the e-mail is clean, it is passed to the Processed Queue where a 'Scanned by' verification banner is added – the MessageLabs symbol of clean e-mail.

Signature Updates

The three commercial AV scanners operating within each Tower are reliant on regular signature updates. These take place automatically, with signature servers used to check the vendors' websites and/or information sites for new updates every 10 minutes. If a new signature is found, it is automatically downloaded, quality assured and then distributed to all the Towers. A similar mechanism allows for an 'instant update' to be performed in a new outbreak situation.

Skeptic™

Skeptic, MessageLabs' revolutionary and patented virus scanner, is the most advanced anti-virus technology in the world for identifying new viruses. Skeptic is a heuristics and rules-based scanner that uses a constantly growing knowledge-base of virus techniques and behaviour to identify new viruses or new strains. Unlike traditional AV software, Skeptic is not dependent on having the latest signature updates.

Skeptic's knowledge-base is compiled from years of experience scanning large volumes of e-mail at the Internet level and through close analysis of every virus intercepted by the SkyScan AV service. This ground-breaking technology means there is no longer the 'window in time' between a virus outbreak and downloading a new signature – a flaw that e-mail viruses have exploited so successfully in the past.

Since the introduction of Skeptic, MessageLabs has protected all its customers from every new virus outbreak, including the notorious Lovebug, Melissa, Sircam and Nimda. In fact, Skeptic was the first scanner in the world to stop the Lovebug virus, having detected a similar technique in a virus intercepted some months earlier.

Recent developments in Skeptic allow it to not only apply its knowledge-base to individual e-mails, but to patterns of movement. From MessageLabs' unique position at the Internet level, anti-virus technicians are able to identify distinct patterns in the movement of infected e-mail during a new outbreak situation. And act upon it.

Secure Data Centre