F-Secure Messaging Security Gateway—Virtual Appliance

F-Secure® Messaging Security Gateway™ Virtual Appliance brings the benefits of server virtualization to the enterprise messaging security market. It offers the same perimeter security, antispam, antivirus, secure messaging and outbound content security capabilities found in F-Secure's award-winning hardware appliances as an easy-to-deploy virtual appliance for VMware's virtualization products.

Features

F-Secure Messaging Security Gateway Virtual Appliance delivers the same best-in-class protection as F-Secure's hardware appliances, combined with the many benefits of virtualization—including cost savings, rapid deployment and provisioning, simplified change management, easy backup and disaster recovery:

> Secures your network against spam, known viruses, emerging virus outbreaks, connection-level attacks, and hackers—right at the gateway.
> Proofpoint MLX™ machine learning technology provides unrivalled antispam effectiveness and content filtering accuracy.
> Protects your enterprise from liability created by incompliant or offensive emails.
> Protects the privacy and security of customer and employee data.
> Protects valuable intellectual property and trade secrets.
> Deploys in just minutes by simply loading into your VMware environment, including VMware Server or VMware ESX (available in Q1/2007)
> High-performance MTA proven in the most demanding enterprise e-mail infrastructures.
> Hardened and vulnerability-tested virtual appliance exceeds enterprise and government security requirements.
> Integrates with enterprise identity management systems such as Active Directory, Domino Directory, and other LDAP sources.
> Intelligent perimeter security features such as MLX Dynamic Reputation™ and SMTP rate control protect against malicious connections including Denial-of-Service and Directory Harvest Attacks.
> A true "zero administration" solution with unified policy management and robust reporting features.

Secure. Effective. Easy to deploy.

Those are just a few of the ways to describe the F-Secure Messaging Security Gateway Virtual Appliance. It's the industry's most powerful messaging security solution—packaged as an enterprise-ready virtual appliance that offers:

> Unbeatable spam detection
> World-class virus and outbreak protection
> Comprehensive content security
> Policy-based message encryption
> Impenetrable e-mail firewall
> Enterprise-grade performance
> Rapid deployment & provisioning
> Easy backup & disaster recovery
> Optimal scalability architecture
> Futureproof technology

MLX Technology

Advanced message security

The power behind F-Secure's enterprise messaging security solutions—Proofpoint MLX—is an advanced, patent-pending machine learning system. Based on advanced statistical techniques including logistic regression and information gain analysis, MLX enables the accurate classification and identification of unstructured content, such as the contents of e-mail messages and valuable company documents.

Unparalleled accuracy

MLX is the basis for the unrivalled antispam accuracy delivered by F-Secure Messaging Security Gateway Virtual Appliance. Using MLX, F-Secure analyzes more than 200,000 structural and content attributes to accurately differentiate between spam and valid messages. Traditional antispam solutions evaluate only a limited number of attributes and are unable to decisively classify spam, leading to low effectiveness and a high rate of false positives.

Futureproof intelligence

F-Secure's intelligent antispam technology is continually being trained by scientists to defend against new forms of spam. This training allows MLX to predict and adapt to new forms of spam as they appear. Unlike other antispam solutions, F-Secure's ability to defend against spam attacks does not degrade over time—and updates to the MLX antispam engine are automatically delivered to your F-Secure gateway on a regular basis. MLX is constantly evolving to counter emerging threats, ensuring that your messaging infrastructure is secure against tomorrow's spammers as well as today's.

MLX technology also powers the intelligent perimeter security features of the E-mail Firewall and MLX Dynamic Reputation service.

All-in-one messaging security

Why purchase yet another point solution? F-Secure's messaging security platform provides comprehensive defense against both inbound threats and outbound content security risks—and F-Secure's modular architecture lets you easily deploy new defenses as your needs change.

Spam Detection

Powered by MLX machine learning technology, the F-Secure Spam Detection module examines more than 200,000 structural and content attributes in every e-mail to block the most spam and phishing attacks, automatically adapting to new attacks as they appear. And the F-Secure Dynamic Update Service automatically keeps your spam protection up to date, ensuring maximum effectiveness at all times. Individually controllable spam and adult content scores allow you to enforce zero-tolerance policies against pornographic spam. Antiphishing features stop the spread of phish and other identity theft attacks from stealing personal information from employees. F-Secure Spam Detection is multi-lingual and offers outstanding accuracy against spam in any language—including hard-to-analyze, multi-byte character languages such as Japanese and Chinese. And F-Secure Spam Detection can be uniquely customized to the environment and lexicon of each organization.

Virus Protection & Zero-Hour Anti-Virus Defenses

Deeply integrated virus engines provide convenient, centralized administration of antivirus policies from the same interface used to manage spam and content policies. Messages are efficiently scanned for viruses in parallel with spam and message content, protecting end users from viruses, worms, and other malicious code. Additionally, the optional F-Secure Zero-Hour Anti-Virus™ module protects against emerging viruses in the earliest stages of their proliferation on the internet—hours before competing solutions even begin to react.

F-Secure E-mail Firewall for complete perimeter security

The integrated E-mail Firewall provides the SMTP-level perimeter security features demanded by today's enterprise, creating an impenetrable shield around your messaging systems. Proofpoint's MLX Dynamic Reputation™ technology and SMTP rate control features work together to protect your network from all types of malicious connections.

MLX Dynamic Reputation and SMTP rate control

Proofpoint MLX Dynamic Reputation technology constantly monitors SMTP connections at the IP address level, looking for suspect or malicious activity. F-Secure Messaging Security Gateway monitors the number of connections, type of activity, and content of messages coming from each IP address. MLX machine learning techniques are used to analyze network activity in real-time and assess the risk associated with each connection. Based on this analysis, F-Secure Messaging Security Gateway Virtual Appliance takes automatic, corrective action using SMTP rate control. Malicious connections are automatically blocked or throttled based on fully customizable mail traffic policies. The E-mail Firewall provides an impenetrable defense against a wide variety of network-level attacks, including Denial-of-Service, Dictionary, and Directory Harvest Attacks, keeping your network and email users safe while preserving network bandwidth.

Centralized Administration

Web-based administration with complete end-user control

F-Secure Messaging Security Console™ provides a centralized, 100% web-based administration interface to Proofpoint's unified policy management framework, ensuring consistent application of corporate messaging policies. The Console makes it easy to monitor and control your messaging infrastructure and define messaging policies. You can even define and enforce different policies for different groups of end users.

Robust reporting

The Console also provides access to more than 45 real-time, graphical reports and alerts that give complete visibility into the state of your enterprise messaging system. Reports can be easily e-mailed or posted as HTML/XML.

F-Secure's "active" reports deliver key information but also allow administrators to take immediate action (for example, simply click a link to block an abusive sender). Easy-to-understand end-user reports and controls, such as end-user digest and personalized safe- and block-lists, give users complete control over their own spam preferences.

Zero Administration

Always up-to-date protection with zero administration

With automatic installation and notification of updated components, F-Secure provides a true "zero administration" solution. F-Secure Dynamic Update Service ensures that your network always has the highest level of protection from message-borne threats. It provides continuous updates for every component of F-Secure Messaging Security Gateway Virtual Appliance, including the hardened operating system and MTA, spam and virus engines.

Benefits both lab and production deployments

F-Secure Messaging Security Gateway Virtual Appliance is ideal for enterprises that have adopted or are moving to the VMware environment. All of the benefits of virtualization can be realized with the virtual appliance including:

> Cost savings related to infrastructure simplification: Reduced hardware, power, cooling and space requirements.
> Reliability, backup and disaster recovery: Snapshots of an entire environment can be easily taken and restored at any time leveraging VMware's infrastructure management tools.
> Deployment and scalability: New virtual servers can be rapidly deployed on existing hardware. F-Secure's optimal horizontal scalability architecture allows new virtual appliances to be provisioned in minutes to address changing e-mail requirements. Any number of virtual agent appliances can be deployed at zero incremental cost on top of existing F-Secure Messaging Security Gateway P-series hardware or Virtual Appliances.
> Change management: New versions and configuration changes can be tested in a zero-risk environment using a snapshot of the production environment.

F-Secure Messaging Security Gateway hardware appliance customers can deploy the Virtual Appliance in lab or test environments free of charge. New virtual test environments can be quickly brought up or taken down on an as needed basis.

Fast and easy evaluation for any organization

In addition to enabling the rapid deployment of F-Secure's messaging security features in VMware production and testing environments, the F-Secure Messaging Security Gateway Virtual Appliance also provides a fast, easy and risk-free way for organizations to evaluate the F-Secure appliance. A downloadable trial version of the F-Secure Messaging Security Gateway Virtual Appliance can be installed and run on any x86 desktop or server hardware using the free VMware Server.

Any number of virtual appliances can be deployed without penalty and F-Secure's optimal scalability architecture lets you manage all agent gateways from a single master console. Automatic configuration propagation, centralized message quarantine, and centralized reporting simplify maintenance and reduce total cost of ownership.

Free trial version—try it today!

Visit www.f-secure.com/sg and register to download the fully-functional, trial version of F-Secure Messaging Security Gateway Virtual Appliance. The virtual appliance can be deployed in a matter of minutes, immediately protecting your e-mail users from all message-borne threats. It features 100% browser-based configuration and is interoperable with any e-mail server solution.

System Requirements

F-Secure Messaging Security Gateway Virtual Appliance is a fully pre-installed and pre-configured small business and enterprise messaging security application designed for VMware virtualization products. For product deployments, VMware Server or VMware ESX (available in Q1/2007) is required. For evaluation and lab deployments, VMware Server can be used. For details in system requirements, please check the F-Secure Messaging Security Gateway Installation Guide.

Browsers

All configuration and administration is handled through F-Secure's 100% browser-based interface. Supported browsers include:
Microsoft® Internet Explorer 6.0 or higher Mozilla Firefox 1.2 or higher
Netscape® 7.0 or higher

fsmsgva0601204

F-Secure Corporation | Tammasaarenkatu 7 | PL 24 | 00181 Helsinki | Finland | Tel. +358 9 2520 0700 | www.f-secure.com