FRISK Software International

F-Prot AVES

Managed E-mail Security Service

WHITE PAPER

Table of Contents

Introduction

Many companies are currently wrestling with the growing need for managed e-mail security. The greatest threat to e-mail security are viruses, trojans and the ever increasing flow of unsolicited e-mails, better known as spam. FRISK Software International has developed the F-Prot Aves Service to meet this need for managed e-mail security.

F-Prot AVES is an on-line managed service that protects users from e-mail based security threats by intercepting all incoming mail and passing it through an advanced filter system. The filter system scans for threats using the most up-to-date version of FRISK Software International's F-Prot Antivirus scanning engine and virus definitions. The service also passes the messages through a number of generic security filters and specialised e-mail heuristics to block whole classes of security risks and protect users from new threats. All messages are also scanned with the F-Prot SpRS spam filter, which labels potential spam or blocks it completely.

Why develop F-Prot AVES?

An increasing number of viruses spread through e-mail

E-mail currently poses a number of security risks, including:

- Untargeted attacks, such as viruses and worms
- Targeted attacks, e.g. Trojan horses designed for industrial espionage

Either of these risks commonly lead to data loss, wasted time and increased maintenance costs for the recipient.

Unsolicited e-mail (spam) has become a problem

Most e-mail users recognise unsolicited e-mail, or spam. The volume of spam is ever increasing and senders of such e-mail are continuously getting better at masking spam as legitimate e-mail. A special concern regarding the increase of such e-mail is that the cost is greater for the recipient than the sender. Unsolicited e-mail is costing companies work-hours because the recipients have to spend time sorting through their e-mail and deleting irrelevant material. Unsolicited e-mail can also open a doorway into a companies' network for all sorts of dubious material.

F-Prot AVES is better than other current solutions

Current solutions to e-mail security often require complex software installations on end-users' PCs or corporate e-mail servers, which require time and maintenance oversight by companies. Nevertheless, this approach does not solve the core security issue of keeping the virus signatures and the antivirus software itself up-to-date. Updating the virus signature files is crucial to e-mail security. When left in the hands of end-users, however, they forget to update or do so infrequently, thereby rendering their protection useless.

The F-Prot AVES service offers proactive gateway protection far away from the networks and their PCs. FRISK Software deploys and maintains the service with our security experts. This means that your company and end users do not have to install anything and do not have to maintain anything.

F-Prot AVES as a backup system

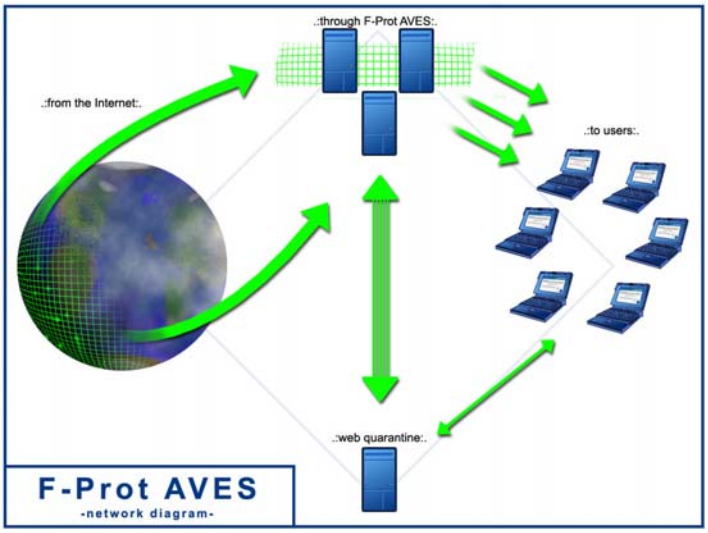
Due to hardware, software or user errors, the recipient can occasionally lose valuable information contained in e-mail. A comprehensive real-time backup system therefore both increases security and saves time and money.

Product description and analysis

All inbound e-mail is routed through one of the F-Prot AVES™ Scanning Clusters and scanned by four scanners: F-Prot Antivirus™, F-Prot SafetyNet, F-Prot SpRS and the Anomy Sanitizer.

- **F-Prot Antivirus** is the long time flagship product of FRISK Software, known for its high scanning speed and exceptional and consistent virus detection rates.
- **F-Prot SafetyNet** is FRISK Software's proprietary e-mail security scanner, providing protection against various e-mail client/server exploits and HTML/JavaScript misuse.
- **F-Prot SpRS** is the spam filter. FRISK Software uses the most current technology available in addition to in-house systems to produce a secure and practical way of getting rid of spam.
- **The Anomy Sanitizer** is a rule based e-mail content filtering scanner. Started as an open source project, its development is now fully supported and sponsored by FRISK Software.

How F-Prot AVES™ works



If an e-mail violates the recipient's security policy then a clean version that complies with it is delivered and the original copy is stored in the F-Prot AVES Message Quarantine (for 30–90 days). Otherwise, if the e-mail did not violate any rules then it is immediately delivered to the recipient. Potential spam is either marked as such to simplify client-side filtering, or simply detained in the recipients' Message Quarantine. Users have access to the Message Quarantine through a secure Web site.

The whole process has no noticeable effect on e-mail delivery. On average it only takes 1.5 seconds to scan each e-mail.

Subscription Options

The F-Prot AVES service is not a "one size fits all" solution. It is designed to allow administrators to define default policies for entire domains or groups of users, while still allowing exceptions to address the needs of individual users. The service can easily be

customised, even down to an individual e-mail address. First a default policy is selected (or customised) for the company (a conservative policy is recommended). Then the settings for those e-mail recipients that require different policies can be customised on a departmental or individual level with the assistance of FRISK Software International's personnel.

The following features are available under F-Prot AVES:

- All attachments are virus scanned with F-Prot Antivirus using known threat lists, heuristics and the neural network.
- All e-mail is scanned with the F-Prot Safety-Net e-mail security scanner to guard against various e-mail client/server exploits.
- Any e-mail that violates the above policies will be rejected. The recipient will receive a notification that an e-mail has been blocked[1] including information on the date, subject and sender.
- Some executable attachment file types[2] are renamed/blocked, such as .BAT, .COM, .EXE, .MSI and .VBS.
- F-Prot SpRS utilises heuristics and content analysis to determine the likelihood of spam. The system labels e-mails that meet the outline of spam or blocks those e-mails entirely.
- Various, flexible virus scanning and disinfection policies.
- Permitted or banned attachment types with customisable lists.
- Preventative security measures, such as message header sanity checks, standard compliance checks and removal of JavaScript or "web bugs" from HTML e-mail.
- Access to the web interface can be controlled, giving some users permission to manipulate the contents of their own quarantine while others must seek assistance from a system administrator.
- The spam filters can be set to meet the customers' policy.

F-Prot Aves stores unmodified copies of infected messages and spam in a quarantine where the user can view a message log and see how and why the content was modified. The user can also bypass the security measures and resend the original to his/her mailbox. Infected originals and spam are kept in the Quarantine for 30-90 days.

The Message Quarantine

The Message Quarantine stores the original unmodified messages. A simple web-based interface enables subscribers to navigate within the Message Quarantine and trusted users can resend individual messages past the security filters when necessary.

Having a reliable, easy to use Quarantine allows users to select more conservative security or antispam policies than would otherwise be acceptable because the Quarantine makes dealing with exceptions or false-positives simply a matter of visiting a web site and pushing a button.

The Backup System

F-Prot AVES offers an e-mail backup system to ensure that no mail is lost due to hardware or software problems.

We usually take information that we keep on our computer for granted – until something happens to it. Information kept on computers is always in danger, especially in vulnerable applications such as e-mail. The F-Prot AVES Message Backup is a backup system for your incoming mail. It stores all your mail for 30-90 days so that if anything goes wrong you can access the e-mail intact through a simple web based interface to the Backup system.

[1] This does not apply to worms, such e-mails are simply dropped (blocked without any error or notification messages).
[2] The full list is in part derived from the list of attachment file types blocked by default by Microsoft Outlook XP but also contains entries added by our security experts.

Customers are usually very relieved to be able to resend messages in the event of a disk crash, or a mistakenly deleted message. The web-based interface to the Backup system is for most people much more accessible and easy to use than in-house backups.

Network Design

The F-Prot AVES Scanning Clusters are located throughout the Internet to make sure that there is no single point of failure. The system is centrally controlled from our headquarters but all components of the system are designed to be autonomous so that they can operate without any manual intervention and in the event of neural outages.

Network Configuration

The F-Prot AVES managed e-mail security service network is based on modifying the MX (mail exchange) entries in the DNS name server for the domain that will be filtered, to route all e-mail through the F-Prot AVES Scanning Clusters.

The Scanning Clusters are configured to route the clean and safe e-mail to the customer's pre-existing mail servers. This ensures that only a minimal setup effort is needed (selecting the desired security policy and re-configuring the DNS servers); regular users do not have to change any of their local configuration; they simply continue fetching their e-mail from the same mail server as before.

For added security, customers can configure their firewall to only accept incoming e-mail from the F-Prot AVES managed e-mail security service network. This prevents viruses/worms from bypassing the F-Prot AVES filter system and stop hackers from breaking into the mail server.

Each F-Prot AVES managed e-mail security service customer is configured to use a primary Scanning Cluster, then two of its mini-clusters and finally a fallback secondary Scanning Cluster. This setup utilises the built-in fallback in the DNS service and the SMTP mail delivery protocol, guaranteeing e-mail delivery in the event of a hardware or network failure.

Each MX entry in the DNS database has an associated priority and the clusters are contacted in that priority order when an e-mail delivery is attempted. The cluster has multiple machines and therefore multiple IP numbers. One of those numbers is selected at random by the sending mail server. If that particular machine within the cluster is not responding then the mini-clusters are contacted in order. If that fails then the secondary Scanning Cluster is contacted.

All the Scanning Clusters know how to process e-mail destined to any domain that uses the F-Prot AVES managed e-mail security service, both how it should be processed and where the clean and safe copies of the e-mail should be delivered.

About FRISK Software International

FRISK Software International, established in 1993, is a globally focused computer security company and one of the leading companies in antivirus product development and research today. FRISK Software offers comprehensive computer security solutions to its customers by providing managed e-mail security services, including virus and spam filtering, and antivirus products with advanced neural network and heuristic detection capabilities. With support for Linux, BSD and Windows, FRISK Software International is able to protect computer networks of any size, running on diverse platforms.

FRISK Software International
Thverholti 18
IS–105 Reykjavík
ICELAND

Telephone: +354–540–7400
Fax: +354–540–7401
Websites: www.f-prot.com
aves.f-prot.com
E-mail: sales@f-prot.com
support@f-prot.com
aves-sales@f-prot.com
aves-support@f-prot.com