

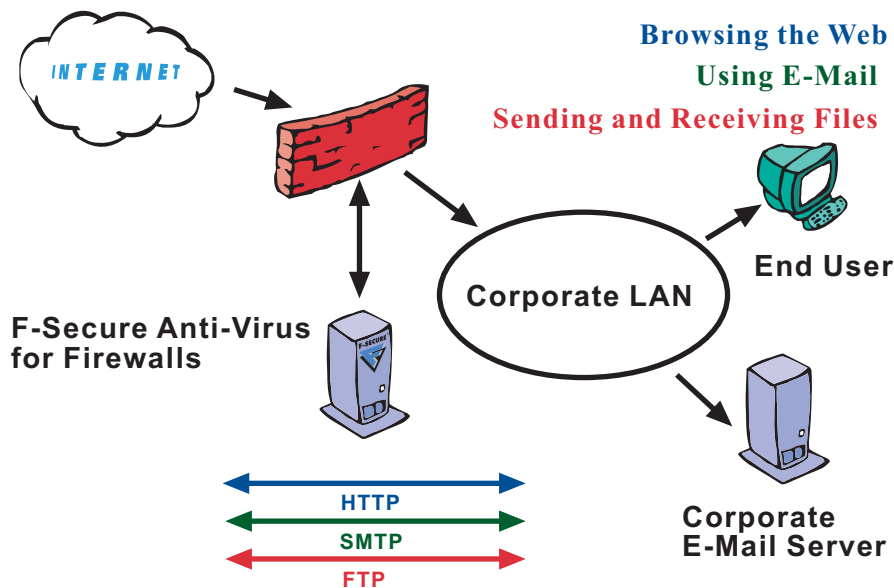


## F-Secure Anti-Virus for Firewalls

F-Secure® Anti-Virus™ for Firewalls provides unsurpassed detection and disinfection for Internet-borne viruses and malicious code passing through corporate firewalls. By automatically scanning HTTP, FTP and SMTP for malicious code as the data comes through the firewall from the Internet, F-Secure Anti-Virus for Firewalls stops viruses before they can compromise corporate security.

### Powerful Protection Against Malicious Code

To minimize the costs and damages caused by viruses and other malicious code, virus scanning should ideally be performed at the perimeter of the corporate network. F-Secure Anti-Virus for Firewalls is a gateway level solution ensuring that viruses and malicious code hidden in web and file transfers and e-mail attachments do not access or leave the corporate network. If a virus is found while employees transfer and receive files, use e-mail, or even browse the web, the file can be automatically disinfected before it is allowed to traverse through the firewall.



### Alerting

System administrators are automatically notified of security incidents and are always kept up-to-date on what is happening in the network proactively. The product can be configured to be totally transparent to the end user, or in the case of a detected virus, it can also alert the recipient. Infected attachments can be automatically disinfected and sent on to the intended recipient. Optionally, infected attachments can be dropped for further actions or deleted.

## KEY FEATURES

Maximizes protection through multiple scanning engines.

Protects against fast spreading worms by stripping attachments according to file extensions or file names.

Improves performance and throughput by caching recent transactions results. By scanning the first copy of the message and saving the scan result in the cache, scanning of frequently visited http pages and e-mail messages sent to mailing lists is fast.

Avoids timeouts with data trickling by specifying the amount of bytes sent to the firewall.

Guarantees interoperability at the policy level between FireWall-1 and best of class, leading edge security applications thanks to OPSEC (Open Platform for Security) certification. (F-Secure Anti-Virus for Firewalls 6.01, Windows version)

Supports all CVP compliant firewalls and is available for Windows and Linux servers.

Supports StoneBeat SecurityCluster from Stonesoft Corporation, a scalable load-balancing and high availability software solution.

Supports recursive scanning of archive files.

## Scalability with Load Balancing

By implementing load balancing with Check Point FireWall-1 and F-Secure Anti-Virus for Firewalls, the overall system performance is optimized. If you have two or more F-Secure Anti-Virus for Firewalls installations running for one Check Point FireWall-1, applying load balancing spreads data traffic evenly to these installations.

## Reliable and Flexible Scanning

With F-Secure Anti-Virus for Firewalls, antivirus protection is always on. Since the virus searches are done in real time as data is transferred through the corporate firewall, end users cannot bypass or disable it.

The scanning operations can be configured in several ways. For instance, different protocols can be configured separately. In case of FTP and HTTP traffic, the firewall can be configured to send only those transaction types that need to be scanned. If the firewall allows, the administrator can specify file extensions for scanning. Limiting the transaction types and files to be scanned minimizes traffic and improves performance. For example, if the firewall is configured so that .gif and .jpeg files are not sent for scanning, web browsing becomes faster.

## Centralized Management

F-Secure Anti-Virus for Firewalls can be centrally managed with F-Secure Policy Manager. F-Secure Policy Manager provides a scalable way to manage the security of multiple applications on multiple operating systems from one central location. With F-Secure Policy Manager, the administrator can centrally and easily manage configuration, administration, virus definition updates, and collection of statistics from one location.

## Automatic Virus Definition Updates

Automatic virus definition updates improve data security through added reliability and prompt delivery of critical signature files. Manual errors are eliminated, since there is no need for manual checking and downloading of databases. As updates are distributed automatically through F-Secure Policy Manager to F-Secure Anti-Virus for Firewalls, the security administrator can concentrate on security management and surveillance.

## Dedicated Virus Research

F-Secure Anti-Virus consistently ranks at the top when compared to competing products. Our team of dedicated virus researchers is on call 24-hours a day responding to new and emerging threats. In fact, F-Secure is one of the only companies to release tested daily virus definition updates to make sure our customers are receiving the highest quality service and protection.

## CERTIFICATIONS

Virus Bulletin 100% (November and December 2002, February 2003)

F-Secure Anti-Virus for Firewalls (version 6.01) is OPSEC certified.

F-Secure Anti-Virus is Checkmarked.



## PLATFORMS

*F-Secure Anti-Virus for Firewalls, Windows version*

Windows NT 4.0 (SP4 or later)  
Windows 2000

*F-Secure Anti-Virus for Firewalls, Linux version*

Red Hat Linux 6.1 (glibc 2.1.3-22 or later)  
Red Hat Linux 7.2  
SuSE Linux 7.3

*Firewall*

Any CVP-Compliant Firewall

*"F-Secure" and the triangle symbol are registered trademarks of F-Secure Corporation and F-Secure product names and symbols/logos are either trademarks or registered trademarks of F-Secure Corporation. Microsoft, Windows, and Windows NT are either trademarks or registered trademarks of Microsoft. Check Point, FireWall-1, and OPSEC are trademarks or registered trademarks of Check Point Software Technologies Ltd or its affiliates. StoneBeat is a registered trademark and SecurityCluster a trademark of Stonesoft Corporation*

F-SECURE®

