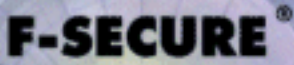
The logo features the text "F-SECURE" in a bold, black, sans-serif font, positioned above a stylized shield emblem. The shield is composed of several geometric shapes in shades of blue and black, forming a triangular-like structure with a central void.The background of the top half of the page is a faded, light-colored world map showing the continents of North and South America. The map is overlaid with a grid of latitude and longitude lines.

# F-Secure Anti-Virus for Firewalls 6.20

Windows version

Administrator's Guide

**PALO ALTO NETWORKS Exhibit 1019 Page 1**

The F-Secure logo features the text "F-SECURE" in a bold, black, sans-serif font, positioned above a stylized shield emblem. The shield is composed of several overlapping geometric shapes in shades of purple and black, creating a sense of depth and protection.

# 1. Introduction

## 1.1 About this Guide

**Chapter 1. *Introduction*** – gives general information about F-Secure Content Scanner Server and F-Secure Anti-Virus Mail Server and Gateway products.

**Chapter 2. *Deployment*** – describes how to set up your network environment before you can install F-Secure Anti-Virus for Firewalls.

**Chapter 3. *Installing F-Secure Anti-Virus for Firewalls on Windows*** – describes how to install and set up F-Secure Anti-Virus for Firewalls.

### NOTE:

F-Secure Anti-Virus for Firewalls is part of F-Secure Anti-Virus Mail Server and Gateway product line that has a common backend – F-Secure Content Scanner Server. Therefore some chapters mention F-Secure Content Scanner Server, although this manual is Administrator's Guide for F-Secure Anti-Virus for Firewalls.

**Chapter 4. *Administering F-Secure Anti-Virus for Firewalls in Centralized Administration Mode*** – describes how to administer F-Secure Content Scanner Server and F-Secure Anti-Virus for Firewalls. The chapter explains all the settings and statistics of the program.

**Chapter 5. *Administering F-Secure Anti-Virus for Firewalls in Stand-alone Mode*** – describes how to administer F-Secure Content Scanner Server and F-Secure Anti-Virus for Firewalls using the local user interface.

**Chapter 6. *Configuring Firewalls*** – describes how to set Firewalls to work with F-Secure Anti-Virus for Firewalls. This chapter includes sample settings for several firewalls.

**Chapter 7. *Updating Virus Databases*** – gives instructions how to update the virus definition database.

**Chapter 8. *Troubleshooting*** – solves some common problems.

**Appendix A. *Warning Messages*** – lists variables that can be included in virus warning messages.

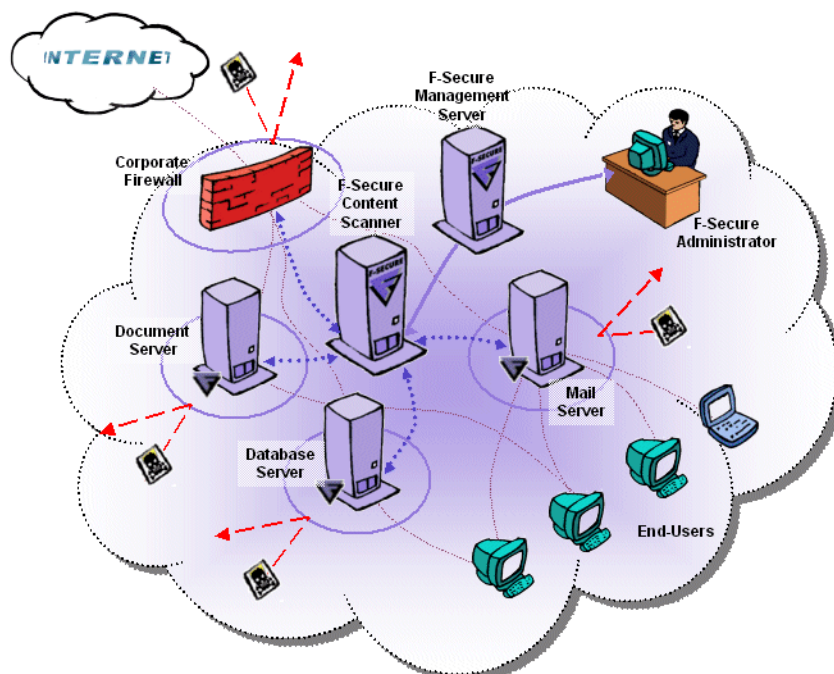
**Appendix B. *Alerts*** – lists all error messages and appropriate actions to be taken.

See the **F-Secure Policy Manager Administrator's Guide** for detailed information about installing and using the F-Secure Policy Manager components:

- **F-Secure Policy Manager Console**, the tool for administering F-Secure Anti-Virus for Firewalls.
- **F-Secure Policy Manager Server**, which enables communication between F-Secure Policy Manager Console and the managed systems.

## 1.2 Overview

Malicious code, such as computer viruses, is one of the main threats for companies today. In the past, these spread mainly via disks and the most common viruses were those that infected disk boot sectors. When users began to use office applications – such as Microsoft Office – with macro capabilities to write documents and distribute them via mail and groupware servers, macro viruses started spreading rapidly. Nowadays the virus problem has another new dimension: e-mail. Modern viruses can even use e-mail to spread themselves without any user intervention and that is why e-mail worm outbreaks, like Klez and BadTrans, have caused a lot of damage around the world.



F-Secure Anti-Virus Mail Server and Gateway products are designed to protect your company's mail, groupware, database or document servers. The protection can be implemented on the firewall level to screen all incoming and outgoing e-mail (SMTP), web surfing (HTTP) or file transfer (FTP) traffic. It can also be implemented on the mail server level so that it does not only protect inbound and outbound traffic but also internal mail traffic and public sources, such as public folders on Microsoft Exchange server.

Providing the protection already on the gateway level has plenty of advantages. The protection is easy and fast to set up and install compared to rolling out anti-virus protection on hundreds or thousands of workstations. The protection is also totally invisible to the end users, thus ensuring that the system cannot be by-passed and it is easy to maintain. Of course, protecting the gateway level alone is not enough to provide a complete anti-virus solution; file server and workstation level protection is needed, also.

## 1.3 How F-Secure Anti-Virus for Firewalls Works

F-Secure Anti-Virus for Firewalls is designed to detect and disinfect viruses and other malicious code from data transmissions through all CVP compliant firewalls. The scanning is done in real time as the data is transmitted through the firewall.

F-Secure Anti-Virus for Firewalls is based on agent and server technology. However, F-Secure Anti-Virus for Firewalls does not employ a separate F-Secure Anti-Virus Agent. The firewall itself acts as the CVP agent and sends data streams passing through it to inspection and F-Secure Anti-Virus for Firewalls acts as a CVP server. The data traffic that needs to be scanned can be redirected to the product from the rule base of the firewall itself.

If the data transmitted by the CVP agent contains malicious code, F-Secure Anti-Virus for Firewalls can be configured to disinfect or drop the content. If the data is disinfected, it is sent back to the firewall that sends it to the original recipient. Any malicious code found during the scan process can be placed in the quarantine, where it can be further examined. For example, an infected attachment in an e-mail message can be removed and replaced with a disinfected attachment.

F-Secure Anti-Virus for Firewalls has extensive alerting functions: information, warning, and security alerts can be sent to the local log file, Windows NT application event log, F-Secure Policy Manager Console or to the administrator's e-mail address via SMTP. The administrator can also specify the recipient inside the company network to be notified about an infection found in the data content.

F-Secure Anti-Virus for Firewalls can be installed on a dedicated Windows NT, Windows 2000 or Linux server. Any additional software does not have to be installed on the firewall itself, so the firewall can be on any platform.

# Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

## Real-Time Litigation Alerts



Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

## Advanced Docket Research



With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

## Analytics At Your Fingertips



Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

## API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

## LAW FIRMS

Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

## FINANCIAL INSTITUTIONS

Litigation and bankruptcy checks for companies and debtors.

## E-DISCOVERY AND LEGAL VENDORS

Sync your system to PACER to automate legal marketing.