



# **F-Secure Distributed Firewall 5.35**

Windows 95, 98, NT4, 2000 and ME

*The Front Line of Enterprise Defense*

Administrator's Guide

All product names referenced herein are trademarks or registered trademarks of their respective companies. F-Secure Corporation disclaims proprietary interest in the marks and names of others. Although F-Secure Corporation makes every effort to ensure that this information is accurate, F-Secure Corporation will not be liable for any errors or omission of facts contained herein. F-Secure Corporation reserves the right to modify specifications cited in this document without prior notice.

Companies, names, and data used in examples herein are fictitious unless otherwise noted. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of F-Secure Corporation.

Copyright © 2000-2001 F-Secure Corporation. All rights reserved.

#12000027-1J05

# Contents

<b>1. Welcome!</b>	<b>1</b>
1.1 Security for the LAN	2
1.2 Security for the Mobile Workstation	2
1.3 Security for the Home Office	3
1.4 Features	3
1.5 How it Works	4
<b>2. Introduction to Firewalls</b>	<b>1</b>
2.1 What is a firewall?	1
2.2 Why do you need one?	1
2.3 Alerting and Preventing Incidents	2
2.4 Rule set Design Principles	2
2.5 Alerting	2
<b>3. Installing F-Secure Distributed Firewall</b>	<b>3</b>
3.1 Network Installation	3
3.2 Local Installation on Windows Workstations	5
Pre-Installation Procedures	5
Workstation Setup	5
<b>4. Using F-Secure Distributed Firewall</b>	<b>14</b>
4.1 F-Secure Distributed Firewall User Interface	14
Security Settings Dialog	15
Predefined Rulesets	16
Status Tab	18
Firewall Rules Tab	19

Alerts Tab .....	24
<b>5. Administering F-Secure Distributed Firewall</b>	
<b>Remotely .....</b>	<b>26</b>
5.1 Setting Up a Network .....	26
5.2 Creating Rules and Rule Templates .....	28
How Do Templates Work? .....	28
How Do Actual Rules Work? .....	28
Creating Rules and Templates .....	29
5.3 Example Policies .....	34
General Workstation Policy .....	34
Optional Security Measures .....	34
5.4 Server Policy .....	35
<b>Appendix A. Flag Options .....</b>	<b>36</b>
<b>Appendix B. Adding New Services .....</b>	<b>39</b>
<b>Appendix C. NSC Tables .....</b>	<b>45</b>
<b>Appendix D. Troubleshooting .....</b>	<b>46</b>
<b>Technical Support .....</b>	<b>49</b>
Web Club .....	49
Electronic Mail Support .....	49
<b>About F-Secure Corporation .....</b>	<b>51</b>
The F-Secure Product Family .....	52

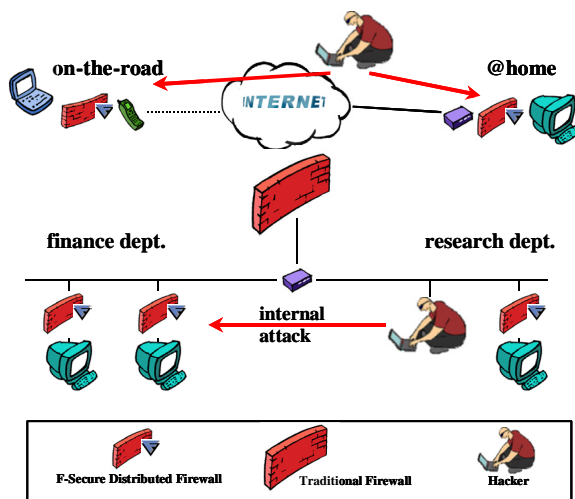


# 1. Welcome!

## NOTE:

This manual is written for F-Secure Distributed Firewall versions 5.30 and 5.35, which differ from the earlier versions in many respects.

F-Secure Distributed Firewall protects your computer while you connect to the Internet, to the corporate LAN in the office, work via the Internet while traveling, or telecommute from home with your always-on, broadband connection. With F-Secure Distributed Firewall, security follows you wherever you go, extending corporate security and eliminating new vulnerabilities. Best of all, an entire fleet of mobile workstations can be individually protected while centrally managed.



*F-Secure Distributed Firewall protects the Mobile Worker and the Home Office against network attacks from the Internet. In the company network it prevents the various departments in an organization from unauthorized access to information in other departments.*

## 1.1 Security for the LAN

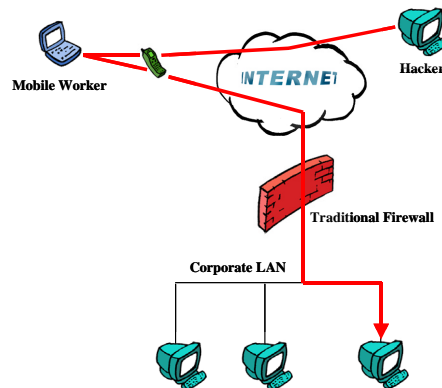
Traditional gateway firewalls protect corporate networks from outside attacks, but gateway firewalls are unable to protect against the internal hacker.

F-Secure Distributed Firewall enhances the traditional concept of a Firewall by enabling centrally managed, policy based traffic filtering at workstations and servers. In the enterprise network it provides an efficient method for building internal security zones.

## 1.2 Security for the Mobile Workstation

Mobile network users need Internet connectivity while on the road. Direct Internet connections are a security risk for the confidential information stored in the laptop, as hackers utilize security holes and software bugs for accessing the data. Also a compromised laptop can serve as the springboard for the hacker to get into the company network.

F-Secure Distributed Firewall enables the mobile employees to safely use local Internet access (e.g. hotel networks, local ISPs) for business communications and Internet services.



*The distributed, mobile nature of corporate resources is increasing the ability of external hackers to tap into companies' intranets through the Internet. The traditional firewall helps protect the LAN, but it cannot protect against an attack coming through the mobile device.*

## 1.3 Security for the Home Office

Home computers are often connected to the Internet with high-speed ADSL or cable modems. These computers are an easy target for hackers trying to take control of the home PC. The “always-on” connection and the fixed IP address of the home PC enable the hacker to try out different hacking tools and run through all possible attacks easily.

F-Secure Distributed Firewall protects confidential data from the curious eavesdropper living next door. Also, it guarantees proper operation of the home PC by blocking Denial of Service attacks coming from the Internet.

## 1.4 Features

F-Secure Distributed Firewall provides you with:

1. IP packet filtering for workstations and servers
  - intended for protecting data on mobile workstations, desktops and servers
  - designed for protecting the company network against attacks that use the mobile workstation or the home PC as a stepping stone to hack into the company network
  - meant for protecting the company workstations and servers against the inside hacker.
2. Filtering rules for inbound and outbound traffic
  - to create simple and effective rules, e.g. you can define a policy that denies all incoming connections to workstations.
3. Predefined network services like SMTP email, Windows file sharing, HTTP, and passive FTP
  - for easy configuration of the filtering rules.
4. Integrated with F-Secure Policy Manager to easily and remotely control the firewall settings in each workstation and server
  - designed for ease of deployment: the administrator does not need to walk to each PC for installation or configuration.
5. Local user interface for user defined firewall rules
  - for stand-alone installations
  - for troubleshooting
  - for small office or home use.

6. Alerting for rule hits.
  - for alerting about events such as network attacks or scans
  - for troubleshooting network problems
  - for verifying the correct behavior of local applications

## 1.5 How it Works

F-Secure Distributed Firewall intercepts IP packets at the NDIS (Network Device Interface Specification) layer. Each packet is checked against the filtering rules that define what kind of traffic is allowed to pass. Allowed incoming packets are forwarded to the TCP/IP stack and the networking applications. Similarly, allowed outgoing packets are sent out on the network interface.

With F-Secure Distributed Firewall the network administrator can define what kind of traffic (if any) is allowed from one network segment to another or between corporate departments. Also, it is possible to define filtering rules for host-to-host or host-to-network connections.

The network administrator configures the filtering rules with F-Secure Policy Manager. The filtering rules are distributed as security policies to all the workstations and servers in the network.



## 2. Introduction to Firewalls

### 2.1 What is a firewall?

A Firewall is a device or application that limits network traffic to specifically accepted services and communication partners. A traditional firewall is a dedicated machine that functions as a gateway between a local area network (LAN) with the local clients and remote communication partners or even the Internet.

F-Secure Distributed Firewall is a software-only firewall that is installed on all computers you want to protect. This makes it possible to have firewall protection even when you are not connected to the LAN, for example when you are at home connecting to the Internet via an ISP.

### 2.2 Why do you need one?

The reason such products are needed is that many computer systems are inherently insecure because of faults due to shortcomings, oversights, wrong assumptions and faulty design. These faults make it possible for someone to compromise the security of your system in many ways:

- The system can be made unavailable or even crashed using a Denial-of-Service (DoS) attack.
- It can be broken into and your stored data might be stolen, corrupted or otherwise abused.
- The system can be used as a stepping-stone to break into and compromise other systems, or for launching other attacks. This can make the system owner liable for litigations.
- Services inadvertently left open can easily be found and abused by outsiders.

## 2.3 Alerting and Preventing Incidents

Typical firewall functionality is to accept or deny traffic based on local and remote address, protocol and service used. It is also possible to issue an alert every time this rule is hit, which makes it easy to see what kind of traffic is going on in your system. These mechanisms make it easy to prevent many of the attacks mentioned above, and also to enforce security policies.

## 2.4 Rule set Design Principles

The main principle for making firewall rules is:

Allow only the needed services, deny all the rest. In this way the security risk is minimized and well-known. The drawback is that when new services are needed the firewall must be reconfigured, but this is a small price for the security.

The opposite concept, to deny dangerous services and allow the rest is not acceptable, because no one can tell with certainty which services are dangerous or might become dangerous in the future when a new security problem is discovered.

A good rule set would look something like this:

1. Deny rules for the most dangerous services or hosts, optionally with alerting
2. Allow rules for much-used common services and hosts
3. Deny rules for specific services you want alerts about, e.g. trojan probes, with alerting
4. More general allow rules
5. Deny everything else

For ruleset examples, see section "[Example Policies](#)" on page 34.

## 2.5 Alerting

Proper alerting can only be done by having proper granularity in the rule set: one rule for each type of alert you want. Designing alerting on "broad" rules will generate a lot of alerts, and any important information might be lost in large volumes of useless noise.

If you really want alerts on the last rule, deny everything else, then it might be a good idea to have deny rules without alerting before it that drop high-volume traffic with little interest. An example of this is NetBIOS name resolving broadcasts in a corporate LAN.

## 3. Installing F-Secure Distributed Firewall

### 3.1 Network Installation

The installation of F-Secure Distributed Firewall on a network is accomplished in five steps. Implement these steps in the order given below:

- Plan the implementation of F-Secure Distributed Firewall on your network.
- Install F-Secure Policy Manager Server and F-Secure Policy Manager.
- Configure the policy domains.
- Configure F-Secure Distributed Firewall for the hosts.
- Push the installations to the workstations. (Remote installation method.)

#### *A. Plan the Implementation of F-Secure Distributed Firewall On Your Network*

- Decide on which workstations and servers to install F-Secure Policy Manager console, F-Secure Policy Manager Server, and which hosts will be protected with F-Secure Distributed Firewall.

#### *B. Install F-Secure Policy Manager Server and F-Secure Policy Manager*

- Install F-Secure Policy Manager Server.
- Install F-Secure Policy Manager on the administrator's workstation. See the F-Secure Policy Manager Administrator's Guide for details.

### *C. Configure the Policy Domains*

- Run F-Secure Administrator and follow the instructions of the Setup Wizard.

### *D. Configure F-Secure Distributed Firewall for the Hosts*

- Run the Remote Installation Wizard in F-Secure Administrator to configure the installation of F-Secure Distributed Firewall. (See the F-Secure Policy Manager Administrator's Guide for details.)

### *E. Installing F-Secure Distributed Firewall to Workstations*

---

**NOTE:**

If you install F-Secure Distributed Firewall as a part of a package from your ISP it will be configured and installed via the BackWeb service. Please consult the documentation provided by your service provider for more information.

- If your clients are already running the FSMA (F-Secure Management Agent), you can install or upgrade the firewall software by creating a policy that upgrades the software and distribute this to the clients.
- If your clients are running Windows NT or 2000, you can do a remote install even on "blank" machines by using the "Auto discover" wizard to install the software on all or selected machines in an NT Domain.
- If your clients do not have F-Secure Management Agent and do not run Windows NT or 2000, you will have to install the software by other means. For more information on this, refer to the F-Secure Policy Manager manual.

---

**NOTE:**

F-Secure Policy Manager was formerly known as F-Secure Management Tools.

## 3.2 Local Installation on Windows Workstations

This section describes how to install F-Secure Distributed Firewall locally on Windows workstations.

### Pre-Installation Procedures

F-Secure Distributed Firewall includes a packet filtering driver for secure IP-based protocols.

Pre-installation checklist:

1. The machine to which you are installing F-Secure Distributed Firewall needs to have a network interface or a dial-up adapter installed.
2. Make sure the TCP/IP protocol is installed and that IP networking is functioning properly.
3. Windows NT or 2000 local administrator privileges are required to install the driver and service components.

---

**NOTE:**

Protocols other than TCP/IP on your F-Secure Distributed Firewall node will not be filtered unless they are transported on top of IP. See the Release Notes for more information on other protocols.

### Workstation Setup

When you have installed F-Secure Policy Manager Server and F-Secure Policy Manager, run the F-Secure Distributed Firewall installation and use either centralized management or a configuration disk prepared for each client. Centralized management is the recommended installation method.

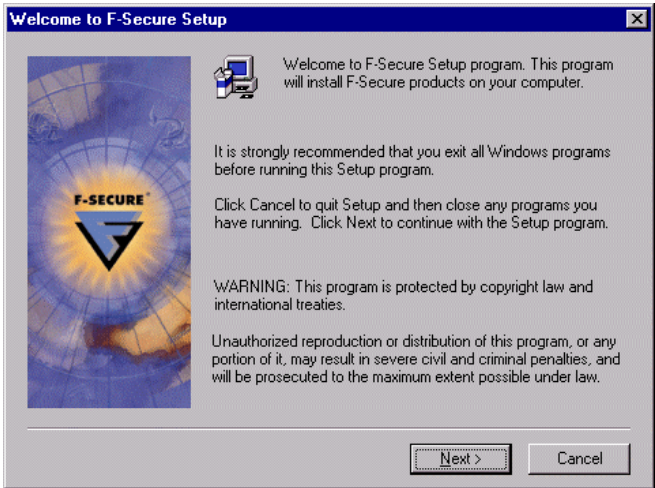
#### *Installing with Centralized Management*

The workstation setup process allows the user to install the required software components from the CD-ROM. The administrator must have the administrator public key file (*Admin.pub*) available, either on a prepared configuration floppy disk or on a shared NT or 2000 drive. You can get the *admin.pub* file from the \Program Files\F-Secure\Administrator directory on the drive where you installed F-Secure Policy Manager Server.

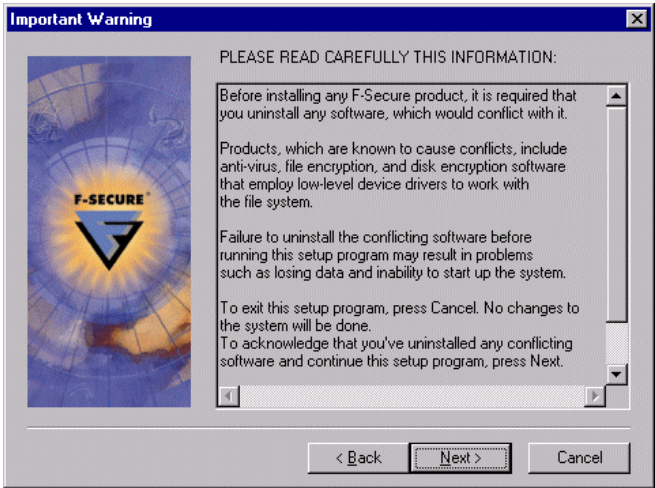
This key, which is used for signing policy files, is generated when F-Secure Administrator is run for the first time.

**Running the Installation**

The InstallShield Wizard will guide you through the setup. Click **Next** to continue.

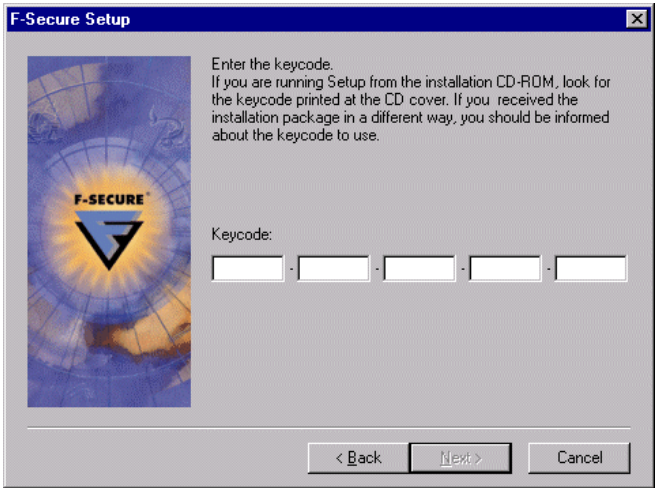


Read the Important Warning dialog box and click **Next**.

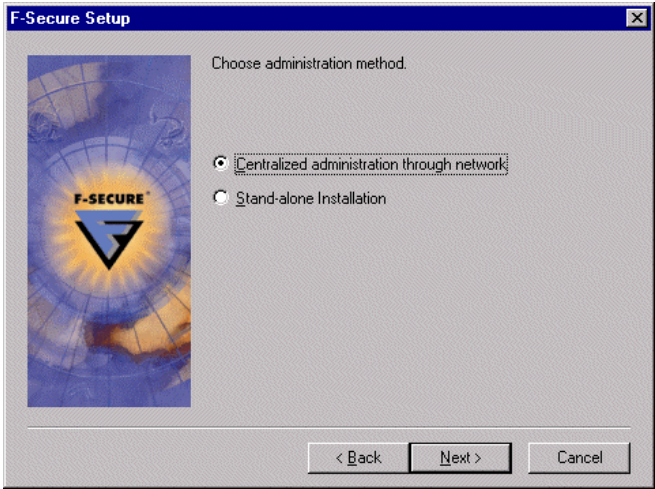




Enter your CD-ROM key that you get with your F-Secure Distributed Firewall license, and click **Next**.



In the next dialog box, you must choose the administration method.

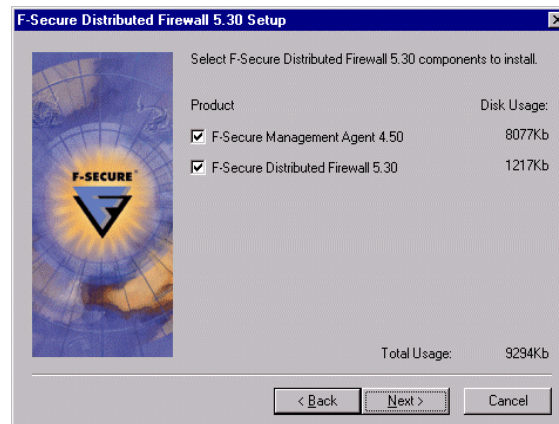


Choose Centralized Administration Through Network to allow the computer to access the Policy Manager Server for centralized management. Stand-alone Installation will not allow the workstation to access the Management Server. It is useful for standalone workstations and servers that do not need to access the Management Server, for home users and for installations managed by BackWeb. In stand-alone installations, if centrally managed configuration is desired, the configuration files must be copied manually to the host.

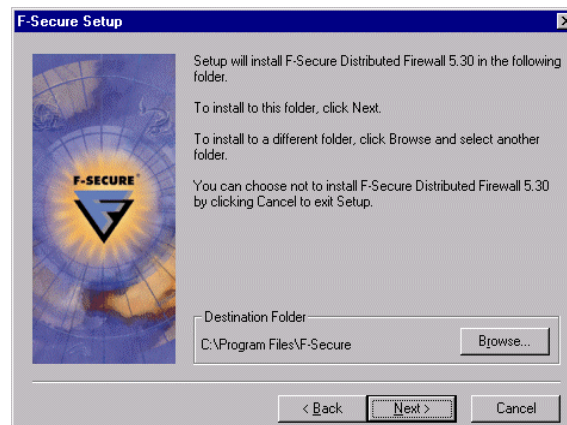
Click **Next** to continue.

In the next dialog box, you must choose the products to install. F-Secure Management Agent is the component used by all F-Secure products for transferring data to F-Secure Administrator via the Management Server and for fetching policies.

After choosing the products to install, click **Next**.



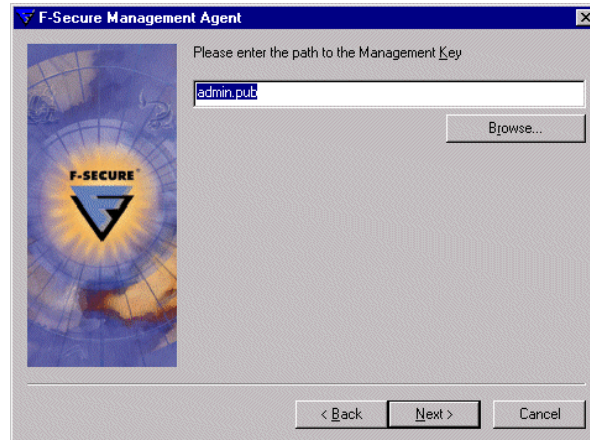
In the next dialog box, you can choose the folder where the software will be installed. We recommend installing the software to the default destination folder *C:\Program Files\F-Secure*. Several subdirectories will be created, including a directory for program files and a directory for configuration files. Click **Next** to continue.



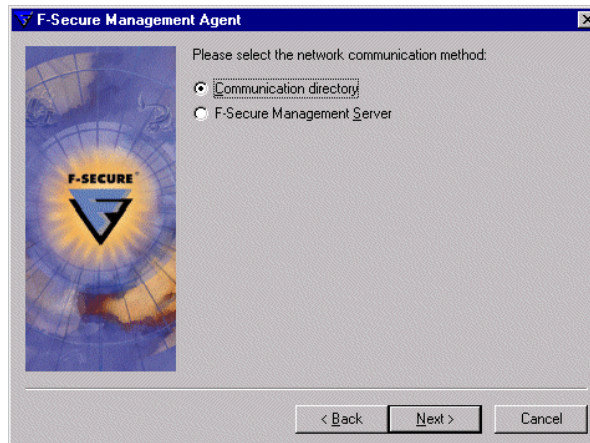


The following dialog boxes will only appear if you selected "Centralized administration through network".

In the next dialog box, you will need to enter the path to the management key (*admin.pub*). Click the **Browse** button to browse for the management key that was created during the F-Secure Policy Manager setup. Click **Next** to continue



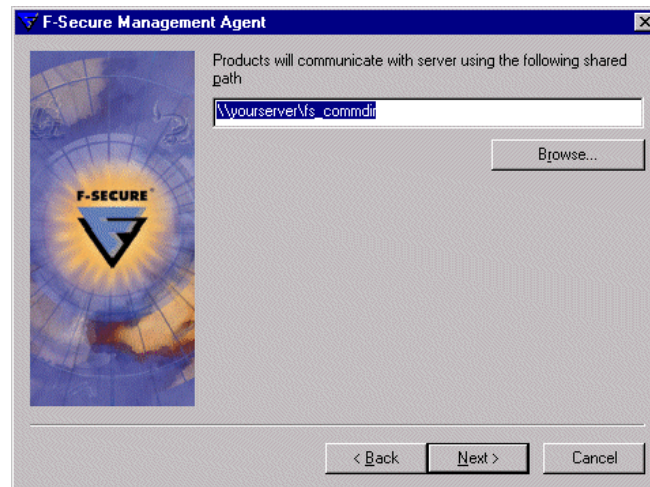
Choose the communication method. This option depends on the installation you chose during the Policy Manager installation. For small installations, the Communication directory can be used. For larger installations we strongly recommend using the F-Secure Management Server communication method.



If you selected "Communication Directory", enter the path to the Communication directory.

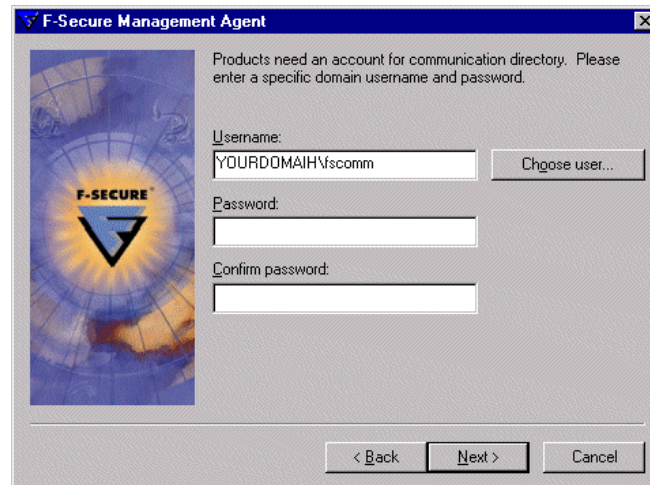
**NOTE:**

If you use communication directory, make sure that the path can be resolved correctly. This can be done either by specifying the IP address for the server in the path, or by adding rules to allow resolving of the server name: Windows Networking (1), WINS (1) and WINS (2), DNS and DNS (TCP).



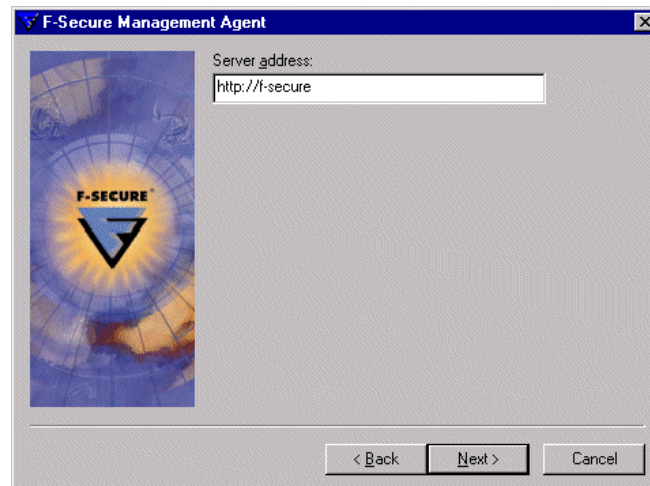
Click **Next** to continue.

If you selected "Communication directory", enter a domain username and password, and click **Next** to continue.



The dialog box is titled "F-Secure Management Agent". It features a vertical banner on the left with the F-Secure logo. The main text area contains the instruction: "Products need an account for communication directory. Please enter a specific domain username and password." Below this, there are three input fields: "Username:" with the text "YOURDOMAIN\fscomm", "Password:", and "Confirm password:". To the right of the Username field is a button labeled "Choose user...". At the bottom of the dialog are three buttons: "< Back", "Next >", and "Cancel".

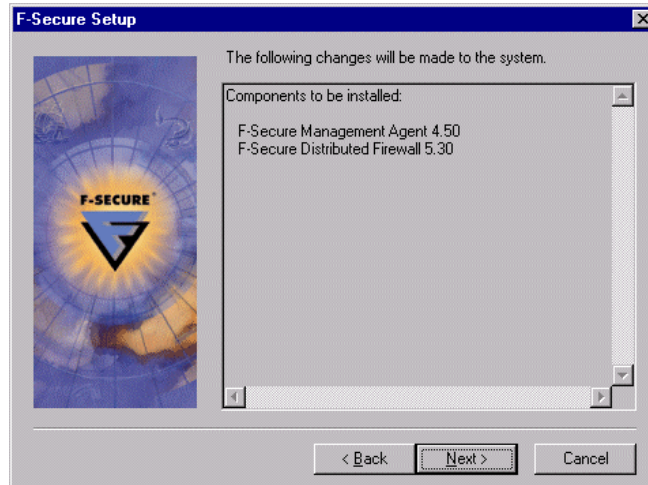
If you selected "F-Secure Management Server", enter the HTTP address of the F-Secure Management Server (for example, `http://f-secure`). You must use `http://` at the beginning of the address.



The dialog box is titled "F-Secure Management Agent". It features a vertical banner on the left with the F-Secure logo. The main text area contains the label "Server address:" followed by a text input field containing the value "http://f-secure". At the bottom of the dialog are three buttons: "< Back", "Next >", and "Cancel".

Click **Next** to continue.

A list of changes that will be made to your system is displayed.

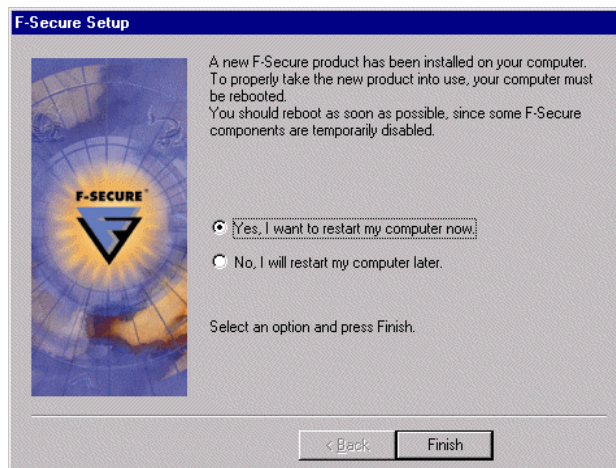


Click **Next** to complete the setup. The default installation folder is *C:\Program Files\F-Secure*.

The following subdirectories will be created:

- *\COMMON\* — Contains all of the F-Secure Management Agent executable files, *admin.pub* (the management public key), and *policy.bpf* (the Base Policy file). (The *policy.bpf* file will be copied later from the Policy Manager Server.)
- *\VPNPLUS\Program* — Contains all of the executable files.

A *readme.txt* file will be placed in the root. After all the files are copied to the hard drive, you will be prompted to read the latest release information.






Next, you will be asked if you want to restart your computer. When you restart your computer, F-Secure Distributed Firewall will be running.



## 4. Using F-Secure Distributed Firewall

### 4.1 F-Secure Distributed Firewall User Interface

To open the F-Secure Distributed Firewall user interface directly, double-click on the Distributed Firewall icon  on the System Tray, in the lower right hand corner of your screen. If the icon is blinking , it means there are alerts to be checked, and double-clicking the icon takes you directly to the *Alerts Tab* of the user interface. Otherwise, the window that opens is the Security Settings Dialog, where you can set the general level of security you want enforced on the firewall. You can also access the user interface by double-clicking the F-Secure Settings and Statistics icon , selecting F-Secure Distributed Firewall and clicking the **Properties** button. The user only needs this user interface when F-Secure Distributed Firewall is installed locally as a standalone product, not when it is centrally administered through F-Secure Administrator. However, the administrator can give the user the option to create their own rules supplementing the centrally enforced ones. In that case, the user creates the rules with the user interface. For more information on creating user definable rules in F-Secure Administrator, see the section "[Creating Rules and Templates](#)" on page 29.

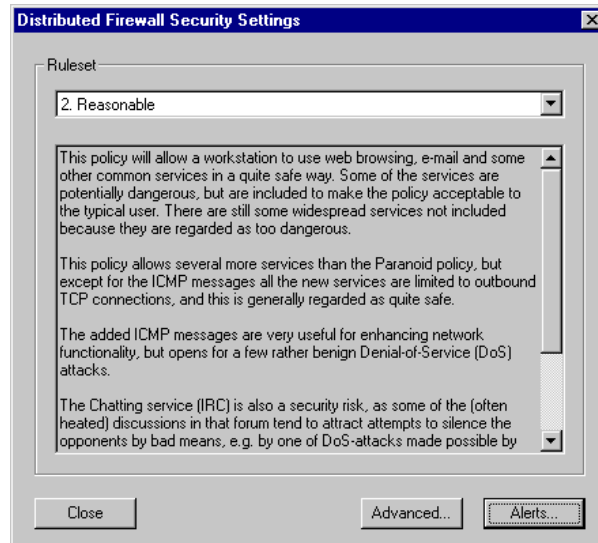
For information on how to create firewall rules in the local user interface, see the section "[Firewall Rules Tab](#)" on page 19.

For information on alerts, see the section on defining alerts, "[Rule Properties: Advanced Properties](#)" on page 22 and the section on alerts reporting, "[Alerts Tab](#)" on page 24.



## Security Settings Dialog

In the Security Settings Dialog, you can set one of four different predefined rulesets that are enforced on the firewall. To change the ruleset, select one from the drop-down menu. For a description of the rulesets, see the section "[Predefined Rulesets](#)" below.



Clicking the **Advanced** button opens the *Status* tab of the F-Secure Distributed Firewall Status Dialog. From there you can also access the *Rules* tab and the *Alerts* tab. For a description of the Advanced tabs see sections "

[Status Tab](#)" on page 18, "[Firewall Rules Tab](#)" on page 19 and "[Alerts Tab](#)" on page 24.

Clicking the **Alerts** button opens the *Alerts* tab of the F-Secure Distributed Firewall Status Dialog directly. Clicking the **Close** button closes the dialog.

## Predefined Rulesets

The four rulesets are (from the strictest to the most customizable):

1. Paranoid
2. Reasonable
3. Partly Customizable
4. Fully Customizable

### *Paranoid Ruleset*

This ruleset will allow a workstation to use e-mail and web browsing in a safe way. This means that the more dangerous protocols, such as Microsoft Exchange Mail, RealAudio, Napster and NetMeeting are not included, which might make the ruleset unacceptable to many users.

With this configuration it will be very difficult to attack the firewalled machine without using a Trojan to gain remote access or a logic bomb to destroy data on the machine. A Trojan has very few available outbound ports to use with this ruleset, so the chances of discovering the Trojan are good.

If the operating system platform (Windows) is not patched, it might be possible to hijack connections, but this is a problem mainly in the server end.

This ruleset does not set any alerting.

### *Reasonable Ruleset*

This ruleset will allow a workstation to use web browsing, e-mail and some other common services relatively safely. Some of the services are potentially dangerous, but are included to make the ruleset more acceptable to the typical user. There are still some widespread services not included because they are regarded as too dangerous.

This ruleset allows several more services than the Paranoid policy, but except for the ICMP messages all the new services are limited to outbound TCP connections, and this is generally regarded as quite safe.

The added ICMP messages are very useful for enhancing network functionality, but open up possibilities for a few rather benign Denial-of-Service (DoS) attacks.

The Chatting service (IRC) is also a security risk, as some of the (often heated) discussions in that forum tend to attract attempts to silence the opponents by bad means, for example with one of the DoS attacks made possible by the partial opening for ICMP.

All services are by default allowed outbound to anybody; it is beneficial to limit this.

No inbound connections are allowed at all, and the end user is not allowed to add rules.

This ruleset does not set any alerting.



### *Partly Customizable Ruleset*

This ruleset will allow a workstation the same functionality as the Reasonable ruleset. It will be even more acceptable to end users because it gives them the opportunity to add the services they need. This is only done after denying some of the most dangerous traffic, thereby reducing the risks.

The denied services are:

- Windows Networking (1), which is NetBIOS browsing and name resolution
- inbound TCP
- system services like network management protocols (ICMP and SNMP)

The rule "Alert on Trojan probes" will deny inbound Trojan probes and generate a security alert. The rule "Alert on inbound TCP" will generate a warning alert.

### *Fully Customizable Ruleset*

This ruleset is similar to the default ruleset in the product. It allows the end user to add their own allow and deny rules before the default rules, thus making it possible to override or modify them.

This means that the Fully Customizable ruleset gives all power to the user, and at the same time gives acceptable functionality and some basic security if the user does not add any allow rules.

The ruleset even puts the BackWeb service at the users mercy, allowing them to block it if they want to.

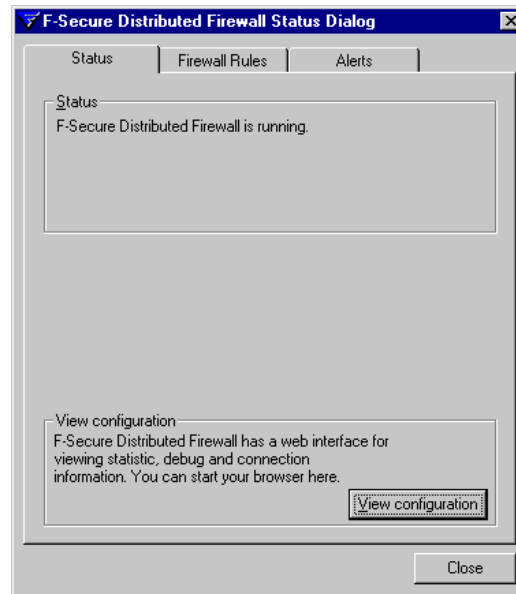
The user can add anything she wishes, so no assumptions about the inherent security of the policy can be made.

With this ruleset the user is basically on her own.

The ruleset offers some added security in that inbound TCP and some of the UDP traffic are denied. It is nevertheless very open, and when the users can add anything they wish the host might be easily compromised. So the user should be aware that this setting is inherently insecure.

The rule "Alert on Trojan probes" will deny inbound Trojan probes and generate a security alert. The rule "Alert on inbound TCP" will generate a warning alert.

## Status Tab

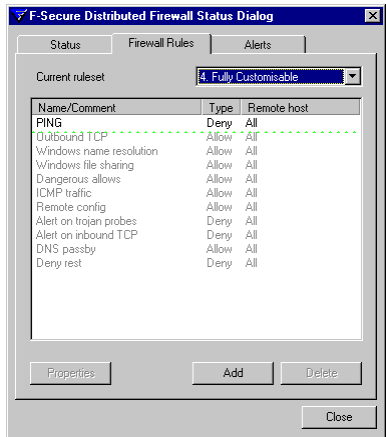


In the Status pane you can see the current status of F-Secure Distributed Firewall.

In the View Configuration pane, the user can view F-Secure Distributed Firewall statistics by clicking the **View configuration** button. The following statistics will be displayed in HTML format.

- Firewall rules
- Error log
- Full log
- Configured services
- Firewall alerts

Firewall Rules Tab



In the *Firewall Rules* Tab, you can manage your user-defined firewall rules and view your enforced rules. The rules in gray are enforced, and you can not edit or delete them, but only view their properties. If your ruleset is either Paranoid or Reasonable, you can not add any user-defined rules. You may also have grayed-out, i.e. enforced rules if your F-Secure Distributed Firewall is remotely managed.

If you add a rule allowing or denying all services to and from everywhere, all the rules beneath it on the list will turn blue. This indicates that those rules will never be checked because all traffic will match the "All services everywhere" rule you created. The blue color is a warning code for your convenience, because this behavior might not be what you wanted to create.

After highlighting a rule, you can delete it, edit it, move it up or down the list, or add new rules above or below it. These options are available by right-clicking on a highlighted rule. By adding rules, you can deny or allow specific traffic.

NOTE:

In the Fully Customizable ruleset you can add rules above all the default rules (above the dotted green line), which means you can override any default rules.

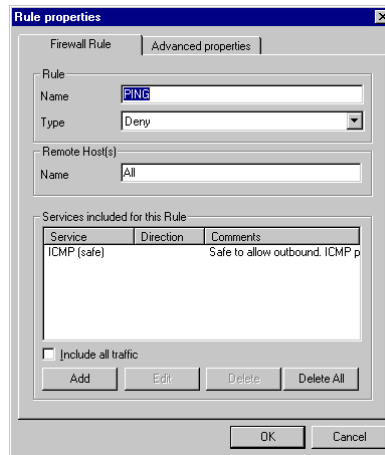
In the Partly Customizable ruleset you can add rules to a specific area between the default rules (between the dotted green lines). This means that you can override any of the rules below the user-defined area, but the rules above the user-defined area are always enforced no matter what rules the user creates.

The order of the rules is important. The rules are read from top to bottom, and the first rule that applies to a connection attempt is enforced. For example, if you have a rule that allows a telnet connection to a specific host defined above a rule that denies all telnet traffic, you are still allowed to make the connection to that one host. If the rule that denies all telnet traffic comes

first, any other telnet rules below that rule are ignored and no telnet connections can be made. Keeping this in mind, the **Add Above** and **Add Below** items in the right-click menu are used to specify where exactly you first want to create the new rule. By default a new rule is added below the highlighted rule. If no rule is highlighted, the rule is added to the bottom of the user-defined rules list. If you later want to change the order of the rules, you can do so by either dragging a rule to a new location with your mouse or by selecting the rule you want to move and clicking on the **Move Up** and **Move Down** items in the right-click menu. Note, however, that changing the order of the rules may affect all the other rules you have created.

The **Properties** button can be used to edit an existing rule. You can delete a rule by selecting it and clicking on the **Delete** button. To add a new rule, click **Add**. The *Rule Properties* dialog box will open.

### *Rule Properties: Firewall Rule*



In the *Firewall Rule* tab of the *Rule Properties* dialog, enter a descriptive name for your rule in the Name field. Giving a unique name to a rule will make it easier to manage your rules on the list. In the Type field, you can define what the rule does. You can deny all traffic matching the rule by choosing 'deny', or allow them through by choosing 'allow'.

In the 'Remote host(s)' field, you can define the hosts/networks the rule applies to. There are several ways in which you can specify the host, and you can enter several hosts or networks by separating them with a comma. The different entries allowed here are:

1. as an IP address to a single host, such as 10.30.11.1
2. as an IP address with NSC notation to a network of hosts, such as 10.20.0.0/16. The NSC notation for a single host is /32, which can be left out. NSC notation is explained on the next page.
3. as a DNS name, such as [www.f-secure.com](http://www.f-secure.com)

- 4. you can define a rule to apply everywhere by either giving the IP address 0.0.0.0/0 or by simply entering the word "All". If you define "All", all other remote host entries are removed from the rule as they are covered by "All".

It is not recommended to use the DNS format, because using DNS names makes your firewall vulnerable to DNS-based attacks. An attacker can trick you into using wrong addresses by spoofing DNS replies, using Denial of Service (DoS) attacks by similar mechanisms etc.

If you enter an IP address, you can enter the address using NSC notation. NSC notation is a standard shorthand notation that combines a network address with its associated netmask. NSC notation defines the number of contiguous one-bits in the netmask with a slash and a number following the network address. Here is a simple example:

Network Address	Netmask	NSC Notation
192.168.0.0	255.255.0.0	192.168.0.0/16
192.168.1.0	255.255.255.0	192.168.1.0/24
192.168.1.255	255.255.255.255	192.168.1.255/32

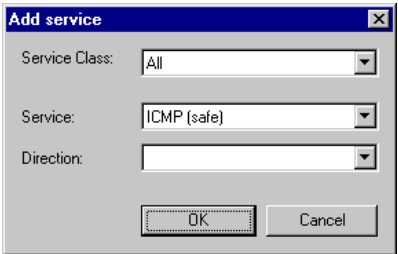
NSC notation is not compatible with networks that use "comb" style netmasks, where all one-bits are not contiguous. For a complete list of Netmask to NSC bit conversions, see [Appendix C. NSC Tables](#) on page 45.

In the *Services Included for this Rule* pane you can add, edit and delete services to allow or deny for the rule you are creating/editing. Services are used to specify which connection types the rule affects. For example, if you want to deny all inbound telnet traffic, press the **Add** button and select 'telnet' and 'inbound' (remember to select deny from Connection page). You can also change the rule to affect only outbound telnet traffic by pressing the **Edit** button and switching the 'inbound' field to 'outbound'.

The default value for including the services is to include all traffic to both directions. This is achieved simply by selecting the *Include all traffic* check box in the *Services Included for this Rule* pane. The *Include all traffic* check box is cleared if you add a new service to the rule.

To delete a service from the rule, select the service and click the **Delete** button. To delete all services from the rule, just click the **Delete All** button. Also, if you select the *Include all traffic* check box, the services defined for this rule will be replaced by *All* to *Both* directions.

To add to the rule, click the **Add** button. To edit a service already in the rule, select the service and click the **Edit** button. This opens the *Add service* dialog shown below.

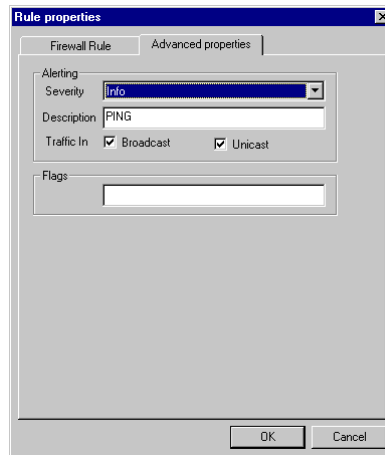


You can select the service class from the *Service Class* drop-down list. Selecting something other than *All* from the list just narrows the list of services down to make it easier for you to find the service you want to allow or deny from the *Service* drop-down list.

Next, select the service you want to allow or deny from the *Service* drop-down list. Then select the direction in which the service is denied or allowed. The choices are *Inbound*, *Outbound* and *Bi-directional*. If you leave the selection empty, it defaults to *Bi-directional*.

### *Rule Properties: Advanced Properties*

In the *Advanced Properties* tab you can specify whether you want to receive alerts when someone either uses a service that is allowed or tries to use a service that is denied in the rule you are editing.




Select the severity class of the alert for the rule you are defining from the Severity drop-down list. The severity class is shown as a color code in the *Alerts Tab* of the F-Secure Distributed Firewall Status Dialog. The options to choose from are:


- None

When someone tries to use a service denied in this rule, you will not receive alerts.


- Info

Info alerts are preceded by a blue bullet in front of the alert in the alert log. They are to be used for alerting you about a normal connection attempt (whether successful or not). They are typically used to indicate an outbound connection or a denied common inbound connection attempt. When someone tries to use a service denied or allowed in this rule, the F-Secure Distributed Firewall icon  in the taskbar will start to blink and you will get an alert in the *Alerts* dialog. You can access the *Alerts* dialog quickly by double-clicking the blinking icon.

- Warning

Warning alerts are preceded by a yellow bullet in front of the alert. They are typically used to indicate a suspicious connection that carries a moderate security risk. When someone tries to use a service denied or allowed in this rule, the F-Secure Distributed Firewall icon  in the taskbar will start to blink and you will get an alert in the *Alerts* dialog. You can access the *Alerts* dialog quickly by double-clicking the blinking icon.

- Security Alert

Security Alerts are preceded by a red bullet in front of the alert. They are typically used to alert you about a connection that is probably used to attempt to compromise the security of your system. Connections like these are for example port scans or connection attempts to Trojan viruses and similar software. When someone tries to use a service denied or allowed in this rule, the F-Secure Distributed Firewall icon  in the taskbar will start to blink and you will get an alert in the *Alerts* dialog. You can access the *Alerts* dialog quickly by double-clicking the blinking icon.


In the *Description* field, you can enter a description to show in the *Alerts* dialog. For example, if you create a rule that denies incoming ping packets, you can enter a description like "Someone tried to ping you" to find all ping attempts in the *Alerts* dialog more easily.

Beneath the *Description* field, you have two check boxes for two kinds of traffic. You can select either or both of them. If you select *Broadcast*, you will receive alerts for all broadcast traffic that is denied by the rule. If you select *Unicast*, you will receive alerts for all traffic that is directed at your computer specifically and denied by the rule.

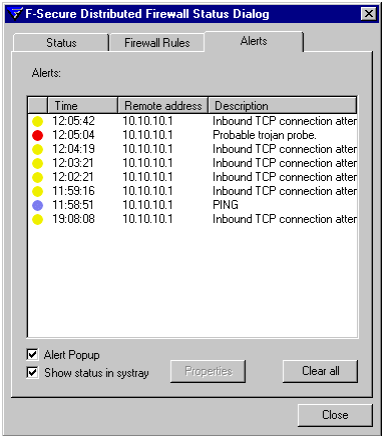
You can enter special flags in the *Flags* field. Flags are extra information about when to apply the rule. With flags, rules can be configured to apply only when you are using a dialup connection or only when you are running certain software.

For example, if you want to enable HTTP connections only when your web browser is running, define a rule that denies all traffic (select deny and 'include all traffic' from the Services page). Then add a new allow rule above the deny rule, allowing the HTTP service to both directions, and enter "-application:netscape.exe" (or whatever is the executable name) in the Flags field. Again, the order of the rules is important, as the first rule that applies to a connection attempt is applied. For more information on flags, see [Appendix A. Flag Options](#) on page 36.



## Alerts Tab

You can open the *Alerts* tab either from the F-Secure Distributed Firewall Security Settings dialog by clicking the **Alerts** button, or directly by double-clicking the F-Secure Distributed Firewall icon  in the system tray when it is blinking. In the *Alerts* tab you see all the alerts you have received since you last cleared the alerts. The alerts are color-coded according to how they have been defined in the *Advanced Properties* dialog when the rule was created. To look at how the alerts are defined, see section "[Rule Properties: Advanced Properties](#)" on page 22. The color codes are:

- (blue) for Info alerts
- (yellow) for Warnings
- (red) for Security alerts




The color-coded bullet is followed by a timestamp for the alert, the IP address of the remote host that triggered the alert and the description according to how it was defined in the *Advanced Properties* dialog when the rule was created.

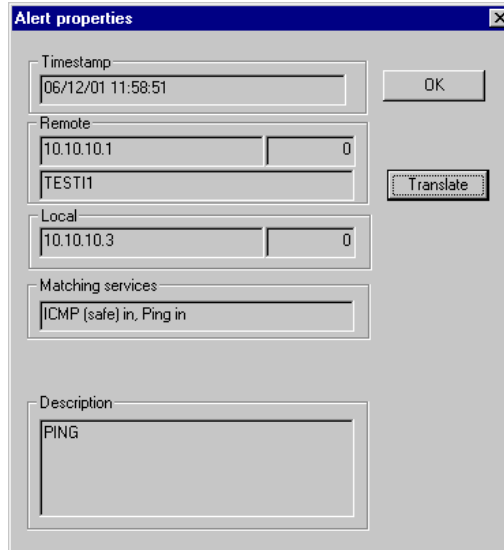
If you select the *Alert Popup* check box, the *Alerts* tab will be shown to you as soon as an alert is received. If you select the *Show status in systray* check box, you will see the F-Secure Distributed Firewall icon  in the system tray. If you unselect this check box, you can still access the user interface by double-clicking the F-Secure Settings and Statistics icon , selecting F-Secure Distributed Firewall from the dialog box that opens and clicking the **Properties** button.

To clear an alert from the log, right-click on it and select *Clear*. To clear several alerts, you can select the alerts you want to delete using the standard Windows way of selecting items, i.e. using the CTRL and SHIFT keys while left-clicking on the alerts. You then right-click on one of the selected alerts and select *Clear*, which will clear all the selected alerts. To clear all the alerts from the *Alerts* window, click the **Clear all** button or right-click on one of the alerts and



select *Clear all*. The F-Secure Distributed Firewall icon  will blink in the system tray until all alerts are cleared, provided the *Show status in systray* check box is selected.

To get more information on a specific alert, either select the alert and click the **Properties** button or simply double-click the alert. You will see the following dialog:



The *Timestamp* is the exact date and time when the alert occurred.

*Remote* is the IP address of the remote host from or to which the access was denied. If you click the **Translate** button, the program will attempt to find the DNS name associated with the IP address.

*Local* is the IP address of the local machine from or to which the access was denied.

*Matching Services* shows the specific services within the rule that caused this alert.

*Description* is the description given to the alert in the *Advanced Properties* dialog when the rule was created.



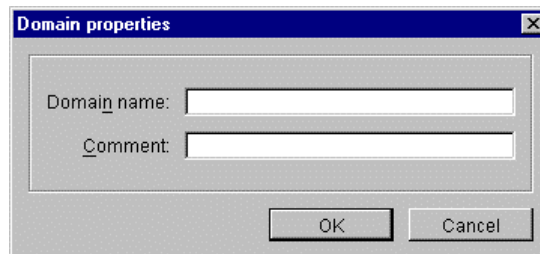
## 5. Administering F-Secure Distributed Firewall Remotely

### 5.1 Setting Up a Network

After F-Secure Administrator is first installed, there is only one domain, Root, in the Policy Domains pane. You can add hosts directly to the top domain, or you can create subdomains. You may start configuring your network by creating separate subdomains for hosts and servers. To do this, select the top domain and click the **New Policy Domain** button, or select *New Domain* from the Edit menu.

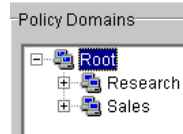
#### NOTE:

Policy Domains are neither Windows NT domains nor IP domains. They are groups of objects (hosts and subdomains) that share a security policy.

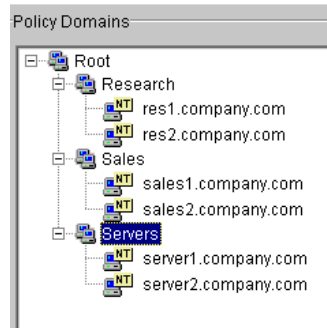


You will be prompted to enter a name for the domain. An icon for the domain will be created in the Properties pane.

Now you can add hosts directly to the top domain, or you can create subdomains. You may start configuring your network by creating separate subdomains for hosts and servers. To do this, select the top domain and click the **New Policy Domain** button, or select *New Domain* from the Edit menu.



To add hosts and servers to domains, select the domain or subdomain, and either choose *Add Host* from the Edit menu, or click the **New Host** button. Alternatively, you may choose Import Autoregistered Hosts but only if you selected Centralized Administration Through Network during the Distributed Firewall installation. Another alternative is to use Autodiscover Windows Hosts, which will define hosts from an Windows NT or 2000 domain and install the client software on them. For more information on using Autodiscover Windows Hosts, see the F-Secure Policy Manager manual.



If you want to allow each server and workstation in your network to access each other, you can create an 'allow all' template from the Root domain to the Root domain. If you only want to allow the servers to access all workstations and each other, and all workstations to access all servers, you can create an 'allow all' template between the Servers subdomain and the Root domain. Instructions for creating templates are given in the next section.

F-Secure Administrator will dynamically create the connections for each host and server. To check the connections, select the Connections table for any computer, and click the **Actual Connections** button in the Editor pane.

## 5.2 Creating Rules and Rule Templates

You can easily define and distribute F-Secure Distributed Firewall rules for your entire network with F-Secure Administrator. These rules let you configure all the computers centrally.

### How Do Templates Work?

Using F-Secure Administrator, you can create templates that automatically create rules for the individual workstations. To do this, you should first create policy domains in the Policy Domains tree. You should create a policy domain for each group of servers or workstations that share a common set of connection rules. The policy domains can have any number of subdomains to any level of depth.

By default, any rules defined for a higher hierarchy domain are created in the rules table below the rules of the lower hierarchy subdomains. This is feasible as the subdomains include rules that are basically exceptions to the rules defined for the higher domains, and the higher domain rules apply to all of their subdomains, unless they have their own special rules.

The templates are dynamic, i.e. whenever the domain hierarchy is changed, the template is automatically updated on all hosts. For example, let us assume that you have a rule template between two domains that enables any host in either domain to contact any other host. When you add a new host to either domain, the template automatically generates a rule between the new host and the other hosts in both domains. To enforce the rules on the hosts, you need to distribute the policies.

### How Do Actual Rules Work?

An actual rule is only created on the host you create it for. If you create an actual rule from one host to another host, the same rule is not created on the other host. The difference to templates is that if you create a rule template from one domain to another, for example denying telnet traffic from A to B, all hosts on A receive a rule forbidding them to send telnet requests to all hosts on B, and all hosts on B get rules refusing all incoming telnet requests from any host on A. On the other hand, if you create an actual rule denying telnet traffic from host FOO to host BAR, no rules are created on host BAR.

Endpoint1 of an actual rule cannot be a policy domain; it has to be one of the defined hosts. Endpoint2 can be a policy domain, a host or an external IP address.

# Creating Rules and Templates

**NOTE:**

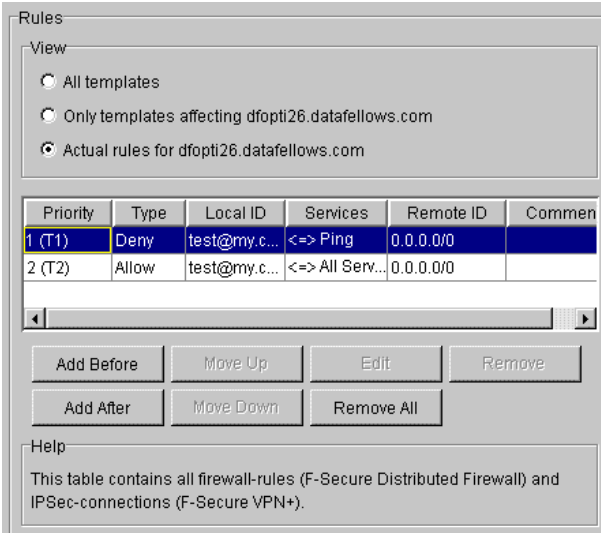
If you are creating large domain-to-domain rules, updating the rule tables will take a lot of time. No progress indicator will be displayed during the updating.

Start F-Secure Administrator. To create a template, select the host or domain/subdomain in the Policy Domain pane.

Expand the F-Secure Distributed Firewall/Settings tree in the Properties pane and select the Rules table.



Next, select the domain or host you want to create the template or actual rule for from the Policy Domains pane. From the Rules pane, select View all templates if you are creating a template and View actual rules for... if you are creating an actual rule. If the Rules table is empty, click **Add**. If you have already created rules, select the rule next to which you want to create the new rule. To select the location for the policy, click the **Add Before** button or the **Add After** button.

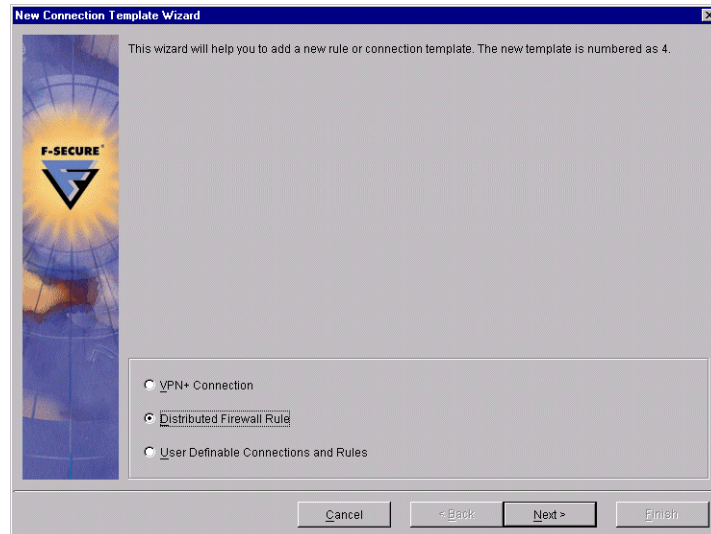


The rules are read from top to bottom, i.e. the first rule that applies to a connection attempt takes priority over any rules listed below it. Take this into account when placing rules in the Rules table. For example, if you have a policy allowing incoming telnet traffic from a certain host at the top of the table, and a policy denying all telnet traffic to and from the whole network listed below it, the incoming telnet connection will be allowed from that host. If the denial policy is listed above the allowance policy, telnet connections can not be used.

**NOTE:**

By default, F-Secure Distributed Firewall allows all outbound TCP traffic, outbound WINS, DNS and Windows network browsing and denies everything else.

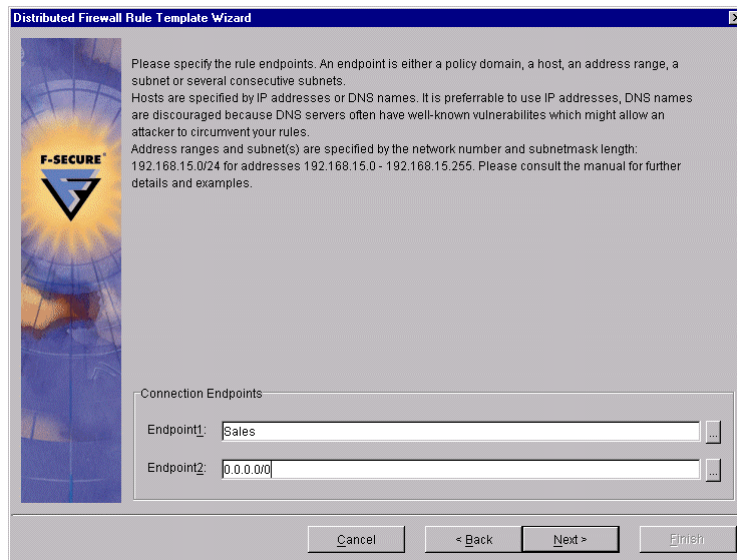
The Template Wizard will guide you through the creation of a template. Once you click **Add** or **Add Before/After**, the following dialog box will appear:



If you want to allow users to create their own policies, you can create a User Definable Rule. If you select this option, you will only be asked for a comment, which will be shown next to the rule. Put all other rules that you absolutely want to enforce above the user definable rule, as they will take priority to any rule created by the user. To create a normal rule, select Distributed Firewall Rule. Click **Next**.



Choose the rule type, i.e. whether you want to create a deny rule or an allow rule. Click **Next**.



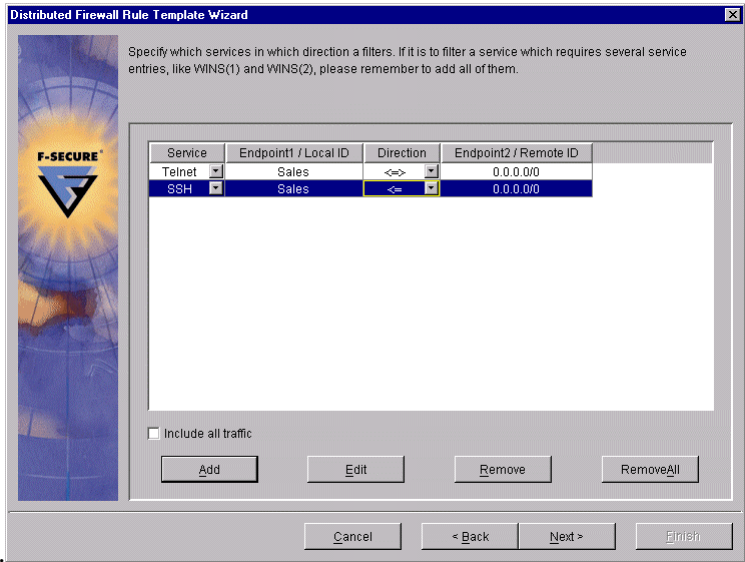
Select the two Endpoints. Endpoint1 is by default the currently selected policy domain or host. You can select another endpoint by clicking on the square button next to the Endpoint1 field. You can only select Endpoint1 from among the domains or hosts of your defined policy domains. Endpoint2 may either be an IP address (with or without the netmask), or you may browse for the Endpoint2 from among the domains or hosts of your defined policy domains by clicking the square button to the right of the Endpoint2 field.

If you use an IP address, subnet, or range, you can enter the address using NSC notation. NSC notation is a standard shorthand notation that combines a network address with its associated netmask. NSC notation defines the number of contiguous one-bits in the netmask with a slash and a number following the network address. Here is a simple example:

Network Address	Netmask	NSC Notation
192.168.0.0	255.255.0.0	192.168.0.0/16
192.168.1.0	255.255.255.0	192.168.1.0/24
192.168.1.255	255.255.255.255	192.168.1.255/32

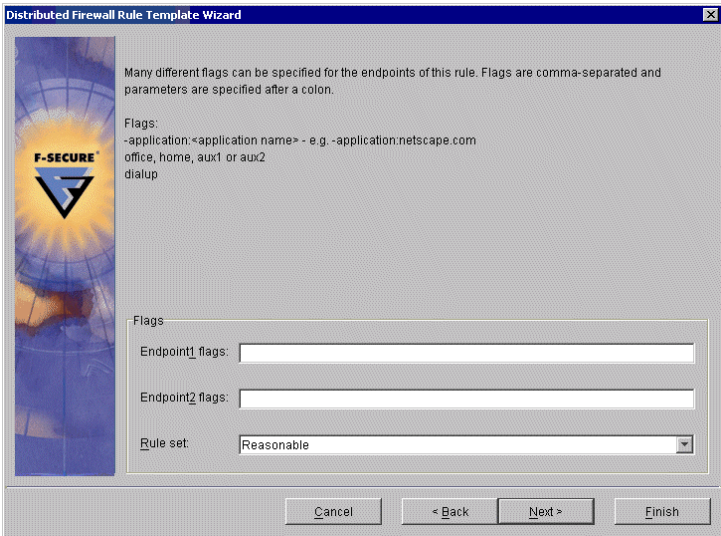
NSC notation is not compatible with networks that use "comb" style netmasks, where all one-bits are not contiguous. For a complete list of Netmask to NSC bit conversions, see Appendix D on page 45.

Click **Next** to continue.

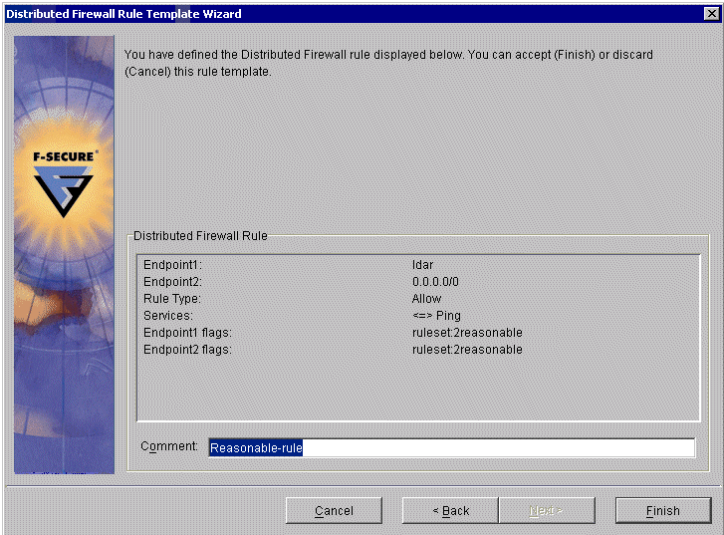


Choose the services to allow (or deny) for the selected policy domain. You can enter several services at once by clicking on **Add**. You can select the direction of the rule, i.e. you can deny or allow any service either to one direction only or to both directions. If you want to create a rule that allows or denies all traffic between the selected endpoints, select the Include all traffic check box. Click **Next**.



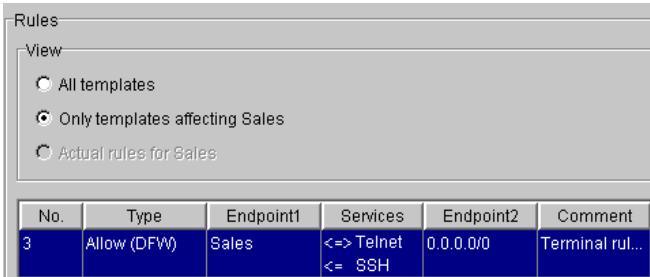


In the Flags box, enter optional parameters to be issued as flags. Separate each parameter by a space. See [Appendix A. Flag Options](#), on page 36 for a list of available parameters. After entering the flags, click **Next**. A dialog box will display your template.



You can enter a comment that describes the rule and check that the information you have given is correct. You can go back to edit the rule by clicking **Back**. If you are satisfied with the rule, click **Finish**.

You can now see the new policies in the Rules pane of F-Secure Administrator.



## 5.3 Example Policies

### General Workstation Policy

As workstations should not run server applications, such as mail or web servers, there is no need to accept inbound TCP connections. The only exceptions are some network management applications like SMS Remote Control. Allow inbound SMS Remote Control service only if needed. Here is an example of a simple workstation policy:

- i. Allow, to 0.0.0.0/0, services: TCP outbound, Windows Networking (1) both ways, Windows Networking (2) outbound, ICMP (safe) outbound
- ii. Allow, to <your DNS server IP address>, DNS outbound
- iii. Allow, to <your WINS server IP address>, WINS (1) both, WINS (2) outbound

The following services are allowed by default:

DHCP (Dynamic Host Configuration Protocol) traffic is always allowed if it is enabled in the operating system settings. DHCP traffic can be denied only by disabling it from the network settings in the control panel of the OS.

IPSec and IKE traffic is allowed by default if F-Secure VPN+ is installed.

### Optional Security Measures

You might want to disable network services that transfer confidential information like passwords unencrypted. It is especially recommended to deny FTP and Telnet services to and from any host.

## 5.4 Server Policy

Servers can be protected in the same way as workstations, except in this case the direction of the services is inbound. The servers might also need things like name resolution, access to other servers etc. to do their job properly.

---

**NOTE:**

The F-Secure Distributed Firewall Client is not intended for protecting network servers as this requires too much CPU resources, and it might not behave as expected on hosts with multiple IP addresses (multi-homed hosts) or multiple network cards.

Example of a web server policy:

- i. Allow, to 0.0.0.0/0, HTTP inbound
- ii. Allow, to <other web servers>, HTTP outbound
- iii. Allow, to <your DNS server IP address>, DNS outbound.



## Appendix A. Flag Options

Here is a list of optional parameters for flags, with tips and examples.

### **alertseverity:{info|warning|securityalert}**

*Function:* Set the alert severity level. For more information on the severity levels, see section "[Rule Properties: Advanced Properties](#)" on page 22.

*Example:* `alertseverity:warning`

### **alertcomment:"<comment>"**

*Function:* Enter a comment to be displayed in the alert log when the alert is triggered.

*Example:* `alertcomment:"A successful connection to your HTTP server was made."`

### **alertoninbound:[u][b]**

*Function:* Specify if you want to set the alert to be triggered for both or either of two kinds of traffic. If you select *b* (Broadcast), you will receive alerts for all broadcast traffic that is allowed or denied by the rule. If you select *u* (Unicast), you will receive alerts for all traffic that is directed at your computer specifically and allowed or denied by the rule.

*Example:* `alertoninbound:ub`

### **alerttrap:<trap-number>**

*Function:* Enter a trap number that can be used by management systems to trigger actions in response to alerts.

*Example:* `alerttrap:202`

The trap numbers are:

100	General FW alert
200	Service allowed
201	Service denied
202	Inbound service allowed
203	Inbound service denied

## Appendix A. Flag Options

204	Outbound service allowed
205	Outbound service denied
300	Potentially dangerous service allowed
301	Potentially dangerous service denied
302	Potentially dangerous inbound service allowed
303	Potentially dangerous inbound service denied
304	Potentially dangerous outbound service allowed
305	Potentially dangerous outbound service denied
400	Dangerous service allowed
401	Dangerous service denied
402	Dangerous inbound service allowed
403	Dangerous inbound service denied
404	Dangerous outbound service allowed
405	Dangerous outbound service denied
500	Potential Trojan probe
501	Potential inbound Trojan probe
502	Potential outbound Trojan probe

### **application:** application

*Function:* Defines an application that activates the rule when it is started.

*Example:* `-application:netscape.exe`

### **dialup**

*Function:* The Distributed Firewall Client will use this rule only when the dial-up interface is active.

*Tip:* There is no FSM plug-in switch. The switch is handled by Distributed Firewall itself. The rule will be used if at least one dial-up line is in use.

*Example:* `dialup`

### **ruleset:** [Paranoid|Reasonable|Partly Customizable|Fully Customizable]

*Function:* If the "Active Rule Set" variable is not set to Final the end user can choose which rule set is to be active on the DFW client. For a remotely managed machine these policies are not predefined, but are defined by the administrator. The way this is done is by defining all the desired rules and using the "ruleset" flag to specify which rule set each rule belongs to. That way the user gets only the rules belonging to the chosen policy.

The possibility of the end user choosing the rule set can be removed by setting the "Active Rule Set" to Final, and the drop-down box in the DFW client

## Appendix A. Flag Options

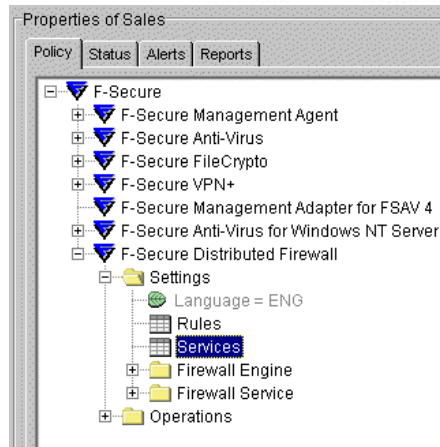
will disappear. The rules that are enforced then are the ones belonging to the rule set chosen in "Active Rule Set". If this variable is set to <undefined> it will be all the rules which don't have the "ruleset" flag.

*Example:* ruleset: Reasonable



## Appendix B. Adding New Services

To create a new service to be used in the rules and rule templates, select the Services table in the Properties pane of F-Secure Distributed Firewall.





## Appendix B. Adding New Services

UniqueName	Protocol	InitiatorPorts	ResponderPorts	Allow broadc...	Comment	Class
AH	51			No	Authentication Header protocol	1000
Backweb	17	371	370,>1023	No	Backweb Polite Protocol (UDP)	5000
Backweb v6	17	371, 9370-9400	370,>1023	No	Backweb v.6 Polite Protocol	5000
COMP	108			No	Compression Header protocol	0
DNS	17	>1023	53	No	Domain name service	7000
DNS (TCP)	6	>1023	53	No	Domain Name Service (TCP-based)	6000
EGP	8			No	Exterior Gateway Protocol	4000
ESP	50			No	Encapsulation Security Payload protocol	0
<b>Finger</b>	<b>6</b>	<b>&gt;1023</b>	<b>79</b>	<b>No</b>	<b>Finger</b>	<b>6000</b>
F-Secure Web o...	6	>1023	58590	No	Default web output port for F-Secure VPN+ and Distribut...	6000
FTP (Passive)	6	>1023	20-21,>1023	No	File Transfer Protocol, only in passive mode	6000
Game - Ashero...	17	9000,9001,9004...	>1023	Yes	Asheron's Call	9000
Game - Counter...	6	>1023	7002	No	Half-Life: Counter-Strike (1)	8000
Game - Counter...	17	>1023	27005-27020	Yes	Half-Life: Counter-Strike (2)	9000
Game - Half-Lif...	17	>1023	27015	Yes	Half-Life Counter Strike	9000
Game - Quake II	17	>1023	27911	Yes	Quake II	9000
Game - Quake I...	17	27960-27970	27960-27970	Yes	Quake III Arena	9000
GRE	47			No	Cisco Generic Routing Encapsulation (GRE) Tunnel	4000
HTTP	6	>1023	80	No	Web (in standard port)	6000
HTTPS (SSL)	6	>1023	443	No	Web, SSL encryption (in standard port)	1000
ICMP	1	0-255		No	Internet Control Message Protocol	3000
ICMP (safe)	1	8	0,3,11	No	Safe to allow outbound, ICMP ping (+ Time Exceeded an...	3000
IDP	22			No	Xerox NS Internet Datagram Protocol	0
IGMP	2			No	Internet Group Management Protocol	4000
IKE	17	500,>1023	500	No	Internet Key Exchange Protocol	1000
IMAP	6	>1023	143,220	No	Internet Mail Access Protocol	6000
IMAP (SSL)	6	>1023	993	No	Internet Mail Access Protocol, SSL encryption	1000
IPIP	4			No	IPIP Tunnels (IP in IP)	0
IPV6	41			Nn	IP Version 6 encapsulation in IP version 4	0

Add Edit Clear Row Clear All

Undo Restriction

You can add new services directly in the table by clicking **Add**. This will insert a new empty row in the table. You can add an entry in the row by either double-clicking in the cell you want to edit or by clicking on the cell and then clicking the **Edit** button.

You can edit an existing service by selecting a cell and clicking the **Edit** button or by double-clicking in a cell in the table and entering a new value.

In the *UniqueName* column, you need to define a unique name for the service; you can not have two services with the same name.

In the next *Protocol* column, select a protocol number for this service. You can select the most commonly used protocols (TCP, UDP, ICMP) from the drop down list. If your service uses any other protocol, refer to the table below and enter the respective number.

Here is a list of the most commonly used protocol numbers:

IP Protocol Name	Protocol Number	Full Name
ICMP	1	Internet Control Message Protocol
IGMP	2	Internet Group Management Protocol
IPIP	4	IPIP Tunnels (IP in IP)
TCP	6	Transmission Control Protocol

## Appendix B. Adding New Services

EGP	8	Exterior Gateway Protocol
PUP	12	Xerox PUP routing protocol
UDP	17	User Datagram Protocol
IDP	22	Xerox NS Internet Datagram Protocol
IPV6	41	IP Version 6 encapsulation in IP version 4
RSVP	46	Resource Reservation Protocol
GRE	47	Cisco Generic Routing Encapsulation (GRE) Tunnel
ESP	50	Encapsulation Security Payload protocol
AH	51	Authentication Header protocol
PIM	103	Protocol Independent Multicast
COMP	108	Compression Header protocol
RAW	255	Raw IP packets

### TCP/UDP Ports

If your service uses the TCP or UDP protocol, you need to define the initiator and responder ports the service covers in the *InitiatorPorts* and *ResponderPorts* columns respectively. The format for entering the ports and port ranges is as follows:

- “>port” all ports higher than *port*
- “>=port” all ports equal and higher than *port*
- “<port” all ports lower than *port*
- “<=port” all ports equal and lower than *port*
- “port”, only the *port*
- “minport-maxport”, *minport* and *maxport* plus all ports between *minport* and *maxport*. (notice, there’s no spaces in either side of the dash)

You can define comma-separated combinations of these items. For example ports 10, 11, 12, 100, 101, 200 and over 1023 can be defined as “10-12, 100-101, 200, >1023”.

## Appendix B. Adding New Services

### Example:

#### IRC – Internet Relay Chat

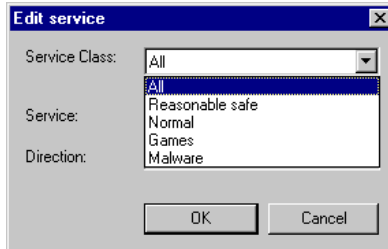
An IRC server usually listens to some of the following TCP/IP ports: 6666, 6667, 6668 and 6669. TCP uses ports higher than 1023 as source ports. To define this service, add a new service named for example “IRC-2”. In the *Protocol* column, define protocol “6” (TCP). In the *InitiatorPorts* column, enter “>1023”.

In the *ResponderPorts* column, enter “6666-6669”. Notice that this service is already defined among the default services of F-Secure Distributed Firewall.

For Services that use other than TCP, you may want to allow incoming broadcasts. To do that, select *Yes* from the drop-down list in the *Allow broadcast packets* column. This is very rarely necessary, and should usually be left as *No*.

In the *Comment* column, you can enter a comment that describes the service. This comment will be shown in the Alert log of the user interface when the alert is triggered.

In the *Class* column you can enter a service class for the service. You can group different but in some respect similar services together into a class by giving all the services you want to appear in the class the same class number. This class is useful in the F-Secure Distributed Firewall user interface where you can limit the number of services shown in the Service list in the Edit Service dialog box when you are creating a new rule.



Our predefined classes are listed at the end of this appendix. The new service has now been added to the Services table in F-Secure Administrator and can be enforced by distributing policies.

### ICMP Types and Codes

If your service uses the ICMP protocol, you need to define the ICMP message types the service covers, and you can also define ICMP message codes but they are not required. The MIB services table ICMP message type/code format [for ICMP services only] is a comma(and/or space)-separated list of the following items:

- >type
- >=type
- <type
- <=type

## Appendix B. Adding New Services

- type
- mintype-maxtype
- type:>code
- type:>=code
- type:<code
- type:<=code
- type:code
- type:mincode-maxcode

If we define the types and codes in the *InitiatorPorts* column and allow this service as “outbound”, we allow these defined ICMP types and codes outbound. If we were to define the same types and codes in the *ResponderPorts* column, and again allow this service outbound, these defined types and codes would be allowed inbound.

### Example:

Ping – ICMP echo request and reply

“ICMP echo request” uses ICMP message type “8” and “ICMP echo request reply” uses message type “0”. We need to cover type “8” to the defined direction, and type “0” to the reverse direction. To define this, select the Services table in the Properties pane of F-Secure Distributed Firewall and add a new service by clicking **Add** in the Services pane. In the first two columns, select a name, for example “Ping 2”, and IP protocol number “ICMP(1)” respectively. Then enter “8” in the *InitiatorPorts* column.

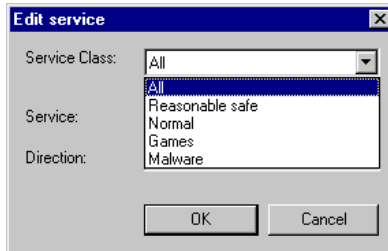
Enter “0” in the *ResponderPorts*. Now this service covers ICMP message type “8” to the defined direction and ICMP message type “0” to the reverse direction. Allowing this service outbound allows echo requests outbound and replies inbound.

You can also allow incoming broadcasts for this service. This is very rarely necessary, and the *Allow broadcast packets* column should usually be left as *No*. If you want to allow incoming broadcasts, select *Yes* from the *Allow broadcast packets* column drop-down list.

In the *Comment* column, you can enter a comment that describes the service. This comment will be shown in the Alert log of the user interface when the alert is triggered.

## Appendix B. Adding New Services

In the *Class* column you can enter a service class for the service. You can group different but in some respect similar services together into a class by giving all the services you want to appear in the class the same class number. This class is useful in the F-Secure Distributed Firewall user interface where you can limit the number of services shown in the Service list in the Edit Service dialog box when you are creating a new rule.



The new service has now been added to the Services table in F-Secure Administrator and can be enforced by distributing policies.

Our predefined classes are as follows:

0 (-999):	Reserved (bypasses for internal things, etc.)
1000 (-1999):	Well-known, encrypted (SSL & SSH) TCP based services
2000 (-2999):	Well-known reasonable TCP based services
3000 (-3999):	ICMP services
4000 (-4999):	Routing protocols
5000 (-5999):	Well-known reasonable UDP based services
6000 (-6999):	Other well-known TCP services
7000 (-7999):	Other well-known UDP services
8000 (-8999):	Other TCP services (games, etc.)
9000 (-9999):	Other UDP services (games, etc.)
10000 and beyond:	Trojans, backdoors, unauthorised RATs (RemoteAdministration Tools) and other malware.



# Appendix C. NSC Tables

The following table gives the number of bits for each permitted netmask. The 0.0.0.0/0 is a special network definition reserved for the default route.

<u>Netmask</u>	<u>Bits</u>	<u>Netmask</u>	<u>Bits</u>
128.0.0	1	255.128.0.0	9
192.0.0.0	2	255.192.0.0	10
224.0.0.0	3	255.224.0.0	11
240.0.0.0	4	255.240.0.0	12
248.0.0.0	5	255.248.0.0	13
252.0.0.0	6	255.252.0.0	14
254.0.0.0	7	255.254.0.0	15
255.0.0.0	8	255.255.0.0	16
255.255.128.0	17	255.255.255.128	25
255.255.192.0	18	255.255.255.192	26
255.255.224.0	19	255.255.255.224	27
255.255.240.0	20	255.255.255.240	28
255.255.248.0	21	255.255.255.248	29
255.255.252.0	22	255.255.255.252	30
255.255.254.0	23	255.255.255.254	31
255.255.255.0	24	255.255.255.255	32



## Appendix D. Troubleshooting

- Q: Application specific filters don't seem to work in my Windows NT, even though they are properly configured with the "-application:app.exe" flag.**
- A: Your Windows NT system might be missing PSAPI.DLL, which is required for application specific filters. It should be found in the "C:\WINNT\SYSTEM32" directory. Windows 95/98 versions do not require this DLL.
- Q: Why can't I create new rules in the F-Secure Distributed Firewall user interface?**
- A: In the user interface, all buttons are disabled and no rules are visible if your F-Secure Distributed Firewall is remotely managed and your network administrator has not added a 'User Definable Rule' in the rules table for your workstation. The administrator can also separately disable user definable rules from the Use Locally Defined Rules setting in F-Secure Administrator.
- Q: What services do I need to allow using F-Secure BackWeb to automatically fetch the virus database updates for my F-Secure Anti-Virus?**
- A: To get the automatic updates working, you need to allow the predefined BackWeb or BackWeb v6 service outbound to the server you use to get the updates from.
- Q: I installed F-Secure Distributed Firewall, and I noticed that FTP connections don't work. How do I get them work?**
- A: "Classic" FTP to outside servers is a big security risk, because it requires that the outside FTP server is able to make a TCP connection back to any port on your machine to transfer the requested data. This is obviously very dangerous and not recommended.
- There is a variety called Passive FTP that doesn't require inbound connections. This service is much safer and is included in the predefined services. You might consider using this.
- The default rule includes allow outbound TCP, which allows also using Passive FTP since it uses TCP-protocol. If you don't want to allow outbound TCP but you want to allow Passive FTP connections, you need to create an allow rule with FTP (passive) - service."

## Appendix D. Troubleshooting

Some FTP clients and servers software don't support this passive mode, but more and more do. The command-line default FTP utility in Windows unfortunately doesn't, but most browsers do. So to get files this way you can use a browser and write a URL like this:

ftp://ftp.server.address/

and you can get the files.

The recommended policy is therefore to encourage your users to switch to the passive FTP and not allow "Classic" FTP at all. You might have to open for the dangerous variety if some of the external servers lack this functionality. In that case it is crucial that the rule allows it only to specific, trusted servers. To open it just "Classic" FTP, add the service TCP allowed both ways between the client and server machines.

**Q: I am trying to push installations to workstations using Intelligent Installation. It is not working. Why?**

A: F-Secure Intelligent Installation requires inbound "Windows Networking (2)" (in the target workstations) from the F-Secure Administrator computer to be able to make push installations. Note, that you might need to use Intelligent installation for example to re-install products. Be sure to allow inbound "Windows Networking (2)" only from the F-Secure Administrator computer, otherwise this is a security hazard.

**Q: I use a DNS name in the URL to my management server. This worked for a while, but after I made a stricter policy the communication fails.**

A: The problem is probably that DNS name resolution does not work anymore, as the firewall always has an allow rule that allows management traffic. The reason DNS fails might be that your new policy denies outbound DNS traffic to the relevant DNS servers.

The problem can be avoided altogether by using the IP address of the server instead of the DNS name. This is better w.r.t. security too, as an attacker cannot attack the management mechanism by compromising the DNS services.

**Q: I used the NetBIOS servername to define the shared network directory communication mechanism, but after I distributed my new policy the communication failed.**

A: This is a similar problem to the one above, with a similar solution; use the IP address of the server. The problem is in fact even bigger here, because NetBIOS name resolution needs to use WINS or broadcast requests to find the server by name.

**Q: I am using Windows 2000 and want to use the Active Directory service. What do I need to allow?**

A: You need the following new services:

- Kerberos v5 outbound
- LDAP outbound
- LDAP (SSL) is even better if supported



## Appendix D. Troubleshooting

You might also need to allow the "classic" NT services:

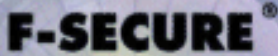
- Windows Networking (1) and (2) outbound
- possibly also WINS (1) and (2) outbound
- and perhaps DNS outbound

**Q: I tried to put alerting on a rule and defined it with the trap numbers 201, 301, 401 and 501. That way I should get different alerts depending on the severity of the traffic, right?**

A: No, the trap number is just a label that you define for your alert, for use in a network management system. Even if you define several labels for one rule only the last one will be communicated.

**Q: What is the default alerting that comes with the preset rule sets?**

A: 1. Paranoid doesn't have alerting, because the end user can't redefine it to turn alerting off. 2. Reasonable neither, for the same reason. 3. Partly customisable has alerting on the rule to deny trojan probes and the rule to deny inbound TCP connection attempts, and the same is true for 4. Fully customisable.

The F-Secure logo, featuring the text "F-SECURE" in a bold, black, sans-serif font, with a registered trademark symbol (®) to its upper right. Below the text is a stylized graphic consisting of a black triangle pointing downwards, with a white and grey geometric shape inside it that resembles a stylized 'F' or a shield.

## Technical Support

F-Secure Technical Support is available by e-mail or from our Web site.

### Web Club

The F-Secure VPN+ Web Club provides assistance to users. Right-click the F-Secure Settings and Statistics icon (located in the Windows taskbar), and choose the *Web Club* command to connect to the Web Club,

To connect to the Web Club directly from your Web browser, go to:

<http://www.f-secure.com/>

<http://www.europe.f-secure.com/>

The F-Secure Crypto Support Center can be found at:

<http://www.f-secure.com/support/>

### Electronic Mail Support

If you have questions about F-Secure not covered in the manual or on-line services at [www.F-Secure.com](http://www.F-Secure.com), you can contact your local F-Secure distributor or F-Secure Corporation directly.

For basic technical assistance, please contact your F-Secure distributor. If there is no authorized F-Secure Business Partner in your country, you can request technical assistance from:

[Crypto-Support@F-Secure.com](mailto:Crypto-Support@F-Secure.com)

## Technical Support


Please include the following information with your support request:

- Version number of F-Secure Distributed Firewall (including the build number).
- Name and version number of your operating system (including the build number).
- A detailed description of the problem, including any error messages displayed by the program, and any other details that could help us duplicate the problem.

When contacting F-Secure Corporation support by telephone, please do the following to save time:

- Be at your computer so you can follow instructions given by the support technician, or be prepared to write down instructions.
- Have your computer turned on, and (if possible) in the state it was in when the problem occurred; or you should be ready to replicate the problem on the computer with minimal effort.

After installing F-Secure software, you may find a README file in the F-Secure program group in the Windows Program Manager. The README file contains the latest information.



**F-SECURE**

## About F-Secure Corporation

F-Secure is a leading strategic provider of powerful data security solutions. The Company's products help enterprises protect corporate information and conduct electronic commerce securely. Customers in nearly every industry – Government, Manufacturing, Retail, Telecommunications, Finance, Energy, Transportation, High Tech and more – rely on F-Secure products to make information secure, reliable and accessible. F-Secure supports businesses with a broad range of centrally managed and widely distributed best-of-breed data security applications built on a highly scalable management infrastructure.

Both internal corporate IT departments and external service providers use the F-Secure approach to effectively deliver Security as a Service™ to millions of users. With F-Secure, security is centrally managed, widely distributed, seamlessly integrated, totally automated and transparent to the user.

Founded in 1988, F-Secure has been listed on the Helsinki Stock Exchange since November 1999. The company is headquartered in Espoo, Finland with North American headquarters in San Jose, California, as well as offices in Canada, Germany, Sweden, Japan and the United Kingdom as well as regional offices in the USA. F-Secure is supported by a network of VARs and Distributors in over 80 countries around the globe. Through strategic OEM agreements the company's security applications are integrated into the services and products of leading telecommunications equipment manufacturers, such as Cisco Systems, Ericsson, Nokia and Sonera.

F-Secure has tens of thousands of customers. These include many of the world's largest industrial corporations and best-known telecommunications companies; major international airlines; European governments, post offices and defense forces; and some of the world's largest banks. Well-known customers include NASA, the US Air Force, Yahoo, US Department of Defense Medical Branch, the US Naval Warfare Center, the San Diego Supercomputer Center, Lawrence-Livermore National Laboratory, IBM, Unisys, Siemens-Nixdorf, EDS, Cisco, Nokia, Sonera, UUNet Technologies, Boeing, Bell Atlantic and MCI.

F-Secure software products have received numerous international awards, prizes and citations. The company was named one of the Top 100 Technology companies in the world by Red Herring magazine in its September 1998 issue. The Company was named one of the 25 Hottest Startups in the world 1998 and its products have consistently won awards including the West Coast Labs Anti-Virus Checkmark 1999, the Virus Bulletin 100% award 1999, the Editor's Choice from the German PC Professional magazine (member of Ziff-Davis group) 1999, Hot Product of the Year 1997 from Data Communications Magazine for F-Secure VPN; and the 1996 European Information Technology Prize.

## About F-Secure Corporation

# The F-Secure Product Family

**F-Secure Anti-Virus** automatically and transparently delivers the most powerful and up-to-date protection against computer viruses and malicious code to your workstations, servers, firewalls, gateways, mobile devices, and e-mail/groupware servers under one common management framework.

**F-Secure Distributed Firewall** is a software-based personal firewall that protects the mobile workforce from one centrally managed location. It protects your computer while you connect to the corporate LAN in the office, work via the Internet while traveling on the road, or telecommute from home with your always-on, broadband connection.

**F-Secure VPN+** is a software-based virtual private network that provides end-to-end security by protecting every link in the corporate network including clients, servers, and gateways. It gives traveling employees secure access to corporate resources, IT staffs the ability to secure internal networks, and corporate partners secure access through an extranet.

**F-Secure FileCrypto** is the complete centrally managed solution for protecting files stored in desktops and laptops across the mobile, distributed enterprise. FileCrypto enables you to automatically, effortlessly, and transparently store local data securely and keep confidential files protected by offering transparent, on-the-fly encryption that is easy to manage and use.

**F-Secure Policy Manager** provides a flexible and scalable way to manage the security of multiple applications on multiple operating systems, from one central location. With a unique distributed architecture, the F-Secure Policy Manager keeps security software up-to-date, manages configurations, oversees enterprise compliance, and scales to handle large and mobile enterprises.

**F-Secure SSH** enables remote systems administrators to access corporate network resources securely by protecting the transmission of sensitive data. F-Secure SSH provides numerous features to make secure administration and remote access connections easy to use, in a user-friendly, terminal-based application running on a wide variety of platforms.

**F-Secure Workstation Suite** is a packaged solution integrating F-Secure Anti-Virus, FileCrypto, VPN+, and Distributed Firewall, providing all the essential functionality for desktop security. The suite includes F-Secure Policy Manager, which provides centralized management, empowering the corporate administrator to install, update, upgrade, and monitor the Workstation Suite from one location.