TREND MICRO

ServerProtect 5®

The key to efficient network antivirus management

for Network Appliance™ filers

Getting Started Guide

TREND MICRO™

www.antivirus.com

your Internet VirusWall®

Document Part No.: SPEQ50758/10426
Release Date: September 2008

At Trend Micro, we are always seeking to improve our documentation. If you have questions, comments, or suggestions about this or any Trend Micro document, please contact us at support@trendmicro.com. Your feedback is always welcome.

Contents

ServerProtect® for Network Appliance™ filers

Trend Micro ServerProtect for Network Appliance filers (SPNAF) is an enhanced version of ServerProtect developed exclusively to provide antivirus solutions for Network Appliance filers. Scalable and reliable, SPNAF protects Network Appliance's line of filers against viruses, Trojans, and other malicious codes.

This addendum manual includes the following sections:

- System Requirements
- Overview
- Installing ServerProtect for Network Appliance filers
- Specific Functions for Network Appliance filers

System Requirements

ServerProtect for Network Appliance filers requires the following:

Scan Server

- Microsoft Windows 2000/2003 Server/Advance Server (Service Pack 3 or above).
- Computer with an Intel Pentium® III 500MHz processor (or equivalent).
- 256MB RAM or above.
- 70MB free disk space.
- Monitor with 800 x 600 or higher resolution.

Note: In the original ServerProtect documentation, the scan server is called "Normal Server". However, this document uses the term "scan server" to describe the machines in Information Server domains that protect the Network Appliance filer.

Information Server

- Microsoft Windows 2000/2003 Server/Advance Server (Service Pack 3 or above).
- Computer with an Intel Pentium® III 500 MHz processor (or equivalent).

- 256MB RAM or above.
- 70MB free disk space (90MB if installing Control Manager agent).
- Monitor with 800 x 600 or higher resolution.

Management Console

- Microsoft Windows 2000/2003 Server/Advance Server (Service Pack 3 or above).
- Computer with an Intel Pentium® III 500MHz processor (or equivalent).
- 256MB or above.
- 70MB free disk space.
- Monitor with 800 x 600 or higher resolution.

Network Appliance filer

- The filer must be AV-enabled with an RPC agent running to communicate with ServerProtect—the filer must have the proprietary OS Data ONTAP 6.1 or above installed.

Note: For optimal scanning performance, we recommend the connection between the filer and a scan server to have at least 1 Gbps bandwidth.

Overview

Protecting the filer is the main focus of SPNAF. In SPNAF, virus scanning is made in "on-access" mode, and takes place on a separate machine (a "scan server") that is running Windows Server or Advance Server. The Normal Servers of the ServerProtect three-tier architecture act as scan servers and protect the filer. This differs from the original version of ServerProtect whose focus is to protect the Normal Server.

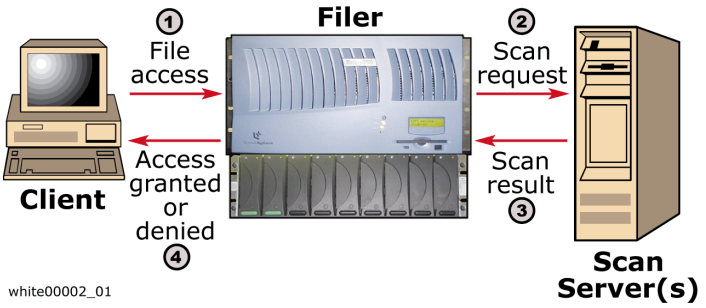


FIGURE 1-1. ServerProtect for Network Appliance filer product architecture.

In SPNAF when a user tries to access a file in the filer or store a new file to the filer, the filer performs a virus check. If the filename extension matches the file scanning criteria (e.g., an ".EXE" or a ".VBS" file), the filer sends a scan request to a scan server. The scan result is passed back to the filer from the scan server and according to the scan result, the user is either allowed to open/save the file or is denied access to the file (to set filer file scanning criteria, refer to your Network Appliance filer documentation).

When a user or application attempts to open, create or change the file in the filer, the filer sends a scan request and the scan server performs a Manual Scan (Scan Now) on the file. If the file contains a virus, SPNAF performs a designated action (refer to *Actions Taken on Infected Files* in the ServerProtect Administrator's Guide). For example, if the file is cleanable and SPNAF is configured to perform a Clean action the following occurs:

1. The scan server cleans the file and informs the filer of non-infection.
2. The filer allows its client to access the cleaned file and replaces the original file with the cleaned one.

Note: The filer "trusts" registered scan servers, so if a scan server also acts as a Normal Server and sends a file to the filer, the file is not scanned. Therefore, if you want to use a scan server as a Normal Server (as a file or data server), you must set the ServerProtect Real-time Scan to "Incoming & outgoing". See *To set Real-time Scan to Incoming & outgoing:* on page 16.

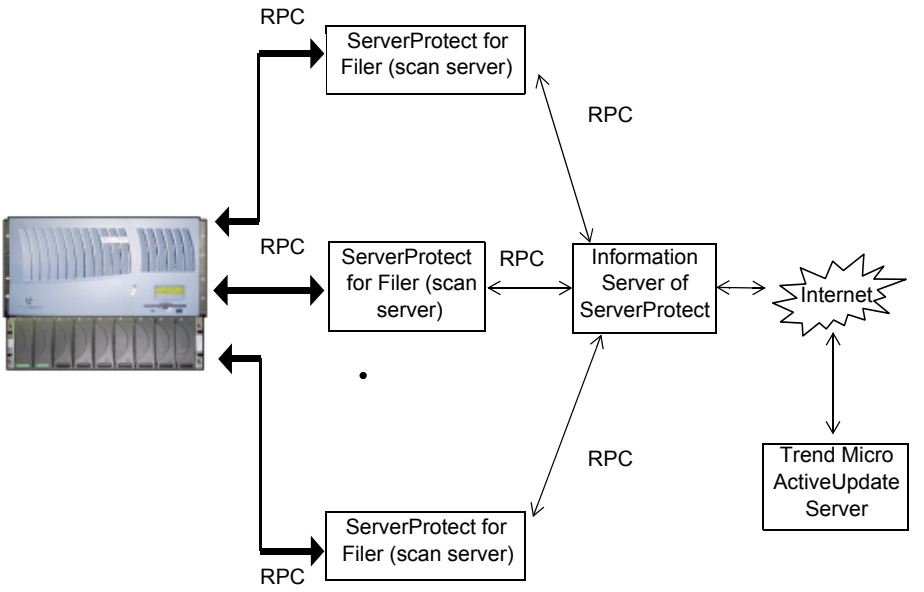


FIGURE 1-2. ServerProtect for Network Appliance filer organizational flow

ServerProtect for Network Appliance filers consists of an agent that communicates with the filer via remote procedure calls (RPCs). This agent provides the following functions:

- Registers the Normal Server with the filer as a "scan server." This informs the filer of the availability and location of a scan server
- Watches for filer file-scanning requests
- Returns scan results to the filer
- Answers any queries from the filer
- Informs the filer of any pattern file or scan engine updates
- Communicates with the filer to check the connection between the scan server and the filer

Original ServerProtect Architecture Review

As previously mentioned, ServerProtect for Network Appliance filers is an enhanced version of the original ServerProtect. To understand the ServerProtect

for Network Appliance filers enhancements, it is useful to review the architecture of the original ServerProtect.

The original ServerProtect protects networks through a three-tier architecture: the Management Console, the Information Server, and the Normal Server. You can use the Management Console to configure the Information Server (IS), which lets you control the Normal Servers in the IS's domain.

The three layers are independent from each other, and can be installed all on the same machine, on separate machines, or in a combination (for example, you can install the Management Console on one machine, and you can install the Information Server and the Normal Server on a different machine).

Management Console- this portable console gives you centralized control of multiple network servers and domains. The Console lets you simultaneously configure servers in the same IS domain and generate integrated virus incident reports for all servers. The ServerProtect domain browser tree shows all the ServerProtect servers installed on Windows Servers and Novell NetWare servers along with the status of each server. Status information includes: the version of the virus pattern, scan engine, and program file, type and version of operating system, direction of real-time scanning, etc. The Console can be installed on any Win32 machine.

For more Management Console information, refer to *Introducing the Management Console* in the ServerProtect Administrator's Guide.

Note: SPNAF includes a function to update filer information and can only be installed on Windows Server or Advance Server.

Information Server- a communications hub for coordinating antivirus defense activities within its domains. An Information Server (IS) provides you with a single point of contact for assigned Normal Servers. This saves time and hassle because the Information Server makes it unnecessary to directly communicate with each individual Normal Server.

What are Domains?

In ServerProtect, domains are virtual groupings of Normal Servers that simplify the identification and management of Normal Servers. You can create, rename, or delete domains according to your network needs (refer to *Managing Domains* in the ServerProtect Administrator's Guide.)

If there are a large number of Normal Servers in a domain, you can add more Information Servers and divide the number of Normal Servers among them. For example, if a domain has 100 Normal Servers assigned to one IS, you can share the

workload among the two IS by adding another IS and assigning each IS to 50 Normal Servers. The IS also collects log files.

For more Information Server information, refer to *Managing Information Servers* in the ServerProtect Administrator's Guide.

Note: In addition to managing only scan servers, the SPNAF Information Server can also manage original version ServerProtect Normal Servers.

Normal Server- the first line of defense in the ServerProtect architecture and where all the scanning takes place. The Normal Servers are the machines in the organization which typically act as file servers, data servers, etc. Normal Servers can scan both manually and in real time.

For more Normal Server information, refer to *Managing Normal Servers* in the ServerProtect Administrator's Guide.

Note: In SPNAF, Normal Servers are known as "scan servers" and scan files in the filer on access.

Key differences between the ServerProtect versions are listed in the following table:

	ServerProtect for Network Appliance filers	ServerProtect
Protection Focus:	Network Appliance filer.	Normal Servers (the machines in the organization which act as file servers, data servers, etc.).
Normal Server Role:	Acts as a filer "scan server" and scans files in the filer on access.	First line of defense in the ServerProtect architecture. These servers perform the actual antivirus functions of the system.

Table 1-1. ServerProtect Version Comparison

Enabling Trend Micro ActiveUpdate

A virus scanner must have the latest updates to be effective. You can configure ServerProtect for Network Appliance filers to automatically download the newest virus patterns and scan engine updates. To minimize download times and preserve network bandwidth, distribution to the designated servers is done via an incremental update mechanism. This ensures SPNAF downloads only the latest virus signatures that have been added since the last version.

For detailed information about Trend Micro ActiveUpdate, refer to *Configuring Updates* in the ServerProtect Administrator's Guide.

Installing ServerProtect for Network Appliance filers

You need to perform the following before installing SPNAF.

- Make sure vscan is enabled
- Confirm the default CIFS default share (C$) still exists
- Delete connections between scan servers and a filer

To ensure ServerProtect for Network Appliance filers functions correctly, it is important you perform the necessary pre-installation checks and actions.

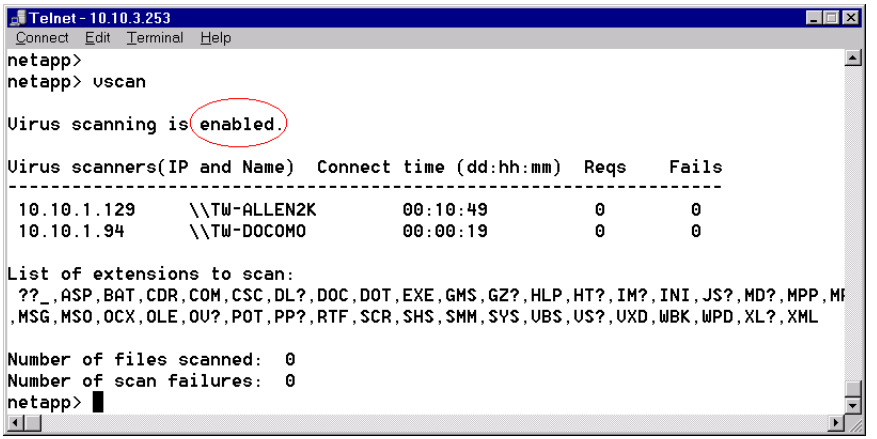
Making Sure vscan is Enabled

Before installing ServerProtect you need to make sure vscan is enabled.

To make sure vscan is enabled, on the filer console at the command prompt type the following:

```
vscan
```

You should be able to view it like the following:



If the vscan is disabled, you must enable it so SPNAF can function correctly.

To enable the vscan, at the command prompt, type:

```
vscan on
```

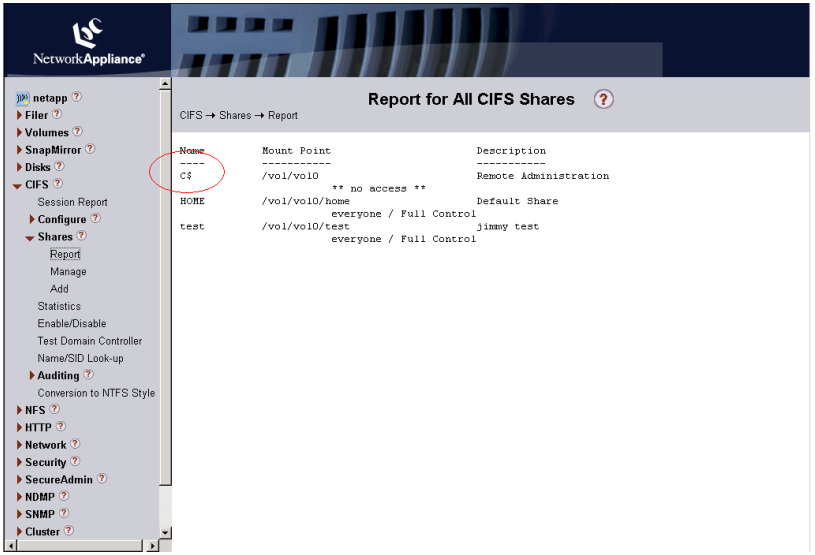
For more information, at the command prompt type `vscan help` or refer to your Network Appliance filer documentation.

Confirming the CIFS Default Share (C$) Still Exists

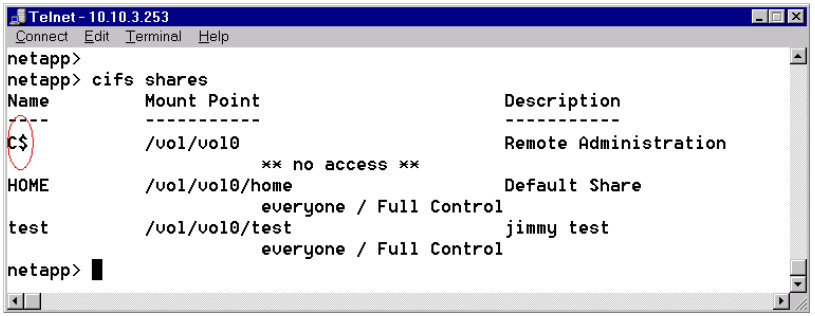
You must confirm that CIFS default share (C$) of the filer wasn't removed.

To confirm the default CIFS default share (C$) of the filer still exists, do one of the following:

- Use the FilerView™ administration tool.



- On the filer console, type the command `cifs shares`.



WARNING! *If you delete the default share, ServerProtect will not function correctly. To learn more about the filer administrative operations, refer to the Network Appliance filer System Administrator's Guide.*

Deleting Connections Between Scan Servers and a Filer

To prevent the scan server from failing to register to the filer, you need to delete all original connections between the scan servers and the filer. This ensures scan servers use the correct credentials to make successful connections with the filer.

To delete connections between scan servers and a filer, at the command prompt type:

```
net use \\Filer-Machine\C$ /delete
```

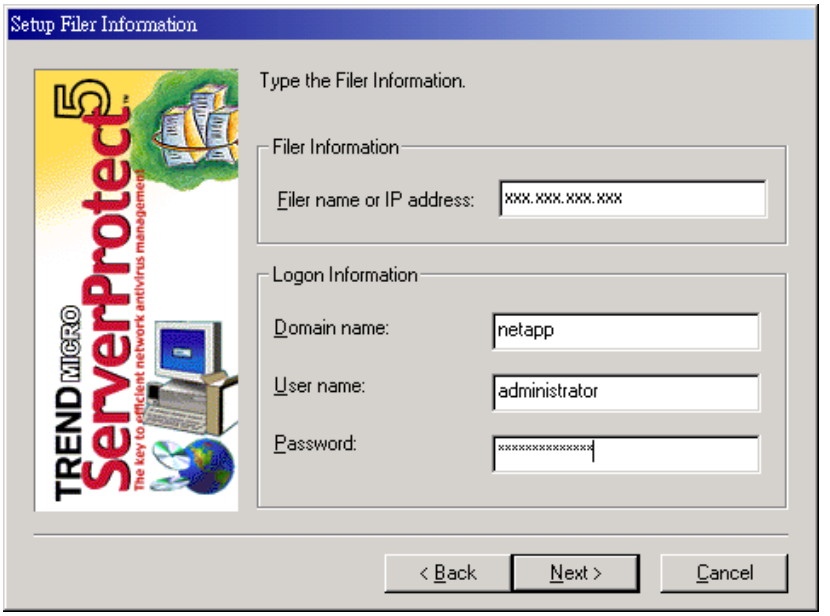
With the exception of one step, the installation procedure for SPNAF is the same as the original ServerProtect (refer to *Installation Planning* in the ServerProtect Administrator's Guide).

Note: While performing a remote installation, the filer information will be copied from a source scan server to the target scan server. For more information refer to *Installation Planning* in the ServerProtect Administrator's Guide.

Before you install an SPNAF scan server you also need to know the following:

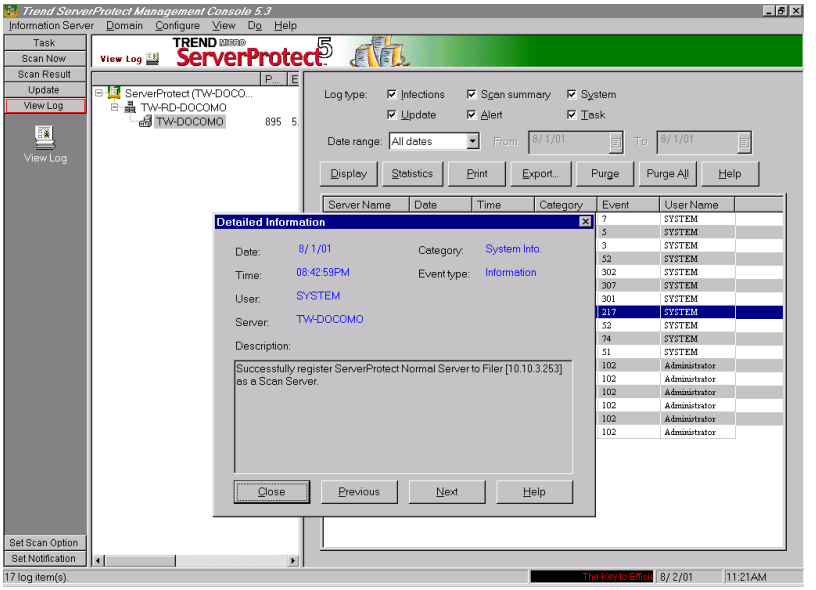
- The filer name or IP address.
- Name of the domain where the filer is located.
- User name and password needed to access the filer (you need filer backup operator or above privileges).

During installation, after you select the **Install Server as a ServerProtect Normal Server** check box on the Select Components screen, the next screen that appears is the Setup Filer Information screen.



1. Do the following:
   - In the *Filer name or IP address* text box, type the filer name or the filer IP address.
   - In the *Domain name* text box, type the name of the domain where the filer is located.
   - In the *User name and Password* text box, type your filer logon credentials (you need filer backup operator or above privileges).
2. Click **Next** and continue following the directions in the *Installing ServerProtect* section of the ServerProtect Administrator's Guide.

3. After installation is complete, you should see the correct system log from the View Log pane of the ServerProtect Management Console.



Specific Functions for Network Appliance filers

A scan server receives a scan request from the filer when a user tries to open a file that matches the file scanning criteria (to set file scanning criteria, refer to your Network Appliance filer documentation). The scan server then scans the file using the ServerProtect Manual Scan function. For more information about Manual Scans, refer to *Manual Scanning (Scan Now)* in the Administrator's Guide.

If the file is infected, the scan server performs any of the following actions, depending on what you have previously configured:

- **Bypass/Ignore**- Skips over the file without taking any corrective action in a Manual Scan.
- **Delete**: Deletes the infected file.
- **Rename**: Changes the name of the infected file by modifying the file extension to ".VIR".
- **Move**: Moves the infected file to a designated folder.

- **Clean**: Attempts to clean the virus code from the file.

For more information about these actions and configuring actions, refer to the *Actions Taken on Infected Files* and *Defining Actions Against Viruses* sections respectively, in the ServerProtect Administrator's Guide.

Note: By default filers do not include "zip" in the set of file extensions that will be scanned. To scan for ZIP files, use the filer command "vscan extensions add zip". This applies to other types of compressed files as well. For more information about filer commands, refer to your Network Appliance filer documentation.

Updating Filer Information

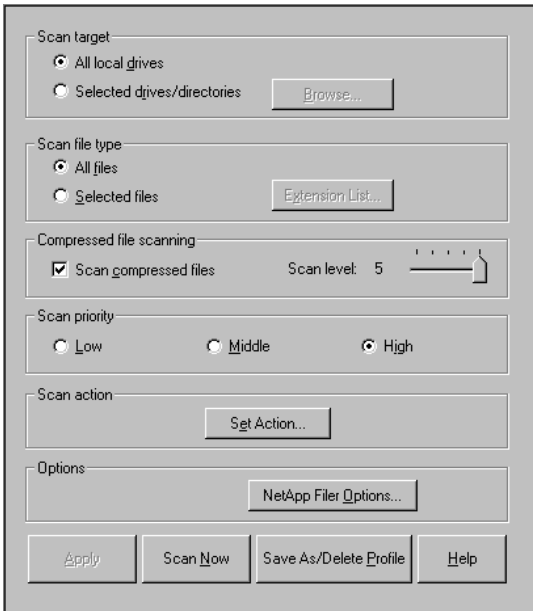
Despite the many changes "under-the-hood" and the differences in focus, the changes to the SPNAF user interface are minimal.

If you change filers or the information of a filer, you need to update the information in SPNAF. You need the following to update a filer in SPNAF:

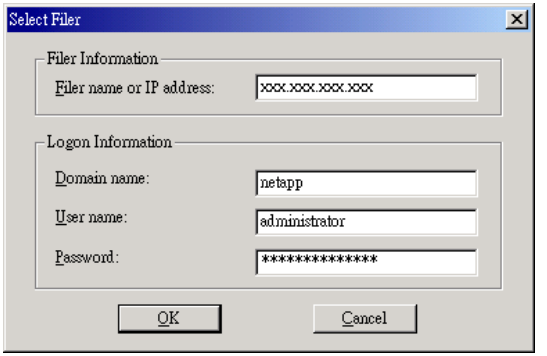
- an account on the filer with backup operator privileges or above
- filer name or IP address
- filer logon credentials (user name, password)

To update filer information:

1. In the ServerProtect bar, click **Scan Now**.
2. Click the Scan Now icon  . The Scan Now property sheet appears.



3. Click **NetApp Filer Options**. The Select Filer dialog box appears.



4. Do the following:
   - In the Filer name or IP address text box, type the name or IP address of the filer.
   - In the Domain name text box, type the name of the domain where the filer is located.

- In the User name and Password text box, type your filer logon credentials (you need backup operator or above privileges).

5. Click **OK**. The filer information updates and a confirmation message appears.

6. Click **OK**.

Adding Scan Servers

ServerProtect for Network Appliance filers provides a fully scalable enterprise antivirus solution for organizations using Network Appliance filers.

If there is a large volume of incoming files to the filer, adding and registering multiple scan servers with the filer evenly distributes the workload among the registered scan servers. Files to be scanned are sent to scan servers in "round-robin" fashion. For example, if you have three scan servers and the filer has four incoming files, the first scan server scans the first file, the second scan server scans the second file, the third scan server scans the third file, and the first scan server scans the fourth file. An additional file, is scanned by the second scan server, the next file by the third scan server, and the next file again by the first scan server and so on. This even distribution of the workload reduces the loading of scan servers.

The procedure for adding additional scan servers is identical to the procedure for adding Normal Servers in the original version of ServerProtect (refer to *Adding a Normal Server* in the ServerProtect Administrator's Guide).

Note: You can only register a scan server to a single filer.

Using Scan Servers as Normal Servers

Although the ideal configuration is to have a machine act primarily as a scan server to protect the filer, there may be situations where a scan server must also serve as an organization's Normal Server (file server, data server, etc.).

If you choose to use a scan server as a Normal Server, its Real-time Scan function is constantly enabled.

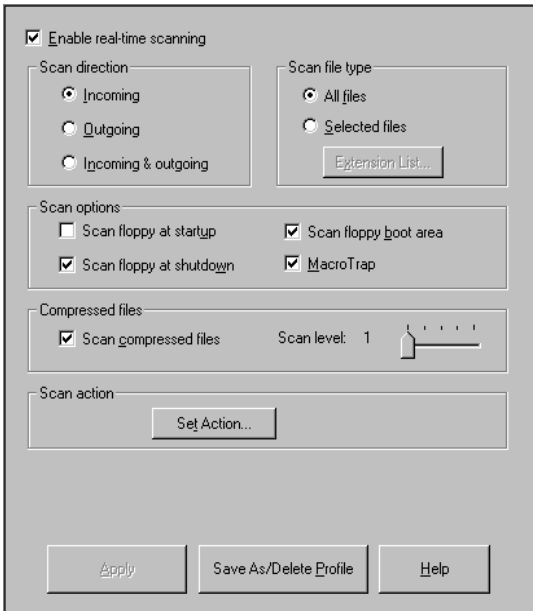
Real-time Scan has the following options:

- incoming (default)
- outgoing
- incoming & outgoing

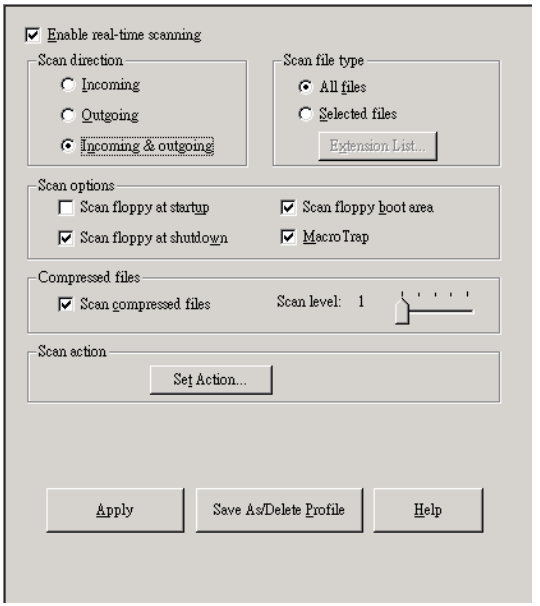
For the highest level of security you must set Real-time Scan to Incoming & outgoing. However, if the computer only performs as a scan server, you can use the default setting (Incoming).

To set Real-time Scan to Incoming & outgoing:

1. In the ServerProtect bar, click **Set Scan Option**.
2. Click the Real-time Scan icon  . The Real-time Scan property sheet appears.



3. Under Scan direction, click **Incoming & outgoing**.



4. Click **Apply.**

For more information about Real-time Scanning, refer to *Real-time Scanning* in the ServerProtect Administrator's guide.