

EVALUATION GUIDE



Trend Micro ServerProtect® 5.3 for Network Appliance™ filers

Trend Micro, Inc.
10101 N. De Anza Blvd.
Cupertino, CA 95014
Phone: 1(800) 228-5651 / 1 (408) 257-1500
Fax: 1(408) 257-2003
Web: www.trendmicro.com or www.antivirus.com



Table of Contents

A NOTE TO REVIEWERS	3
VIRUSES AMONG NETWORK ATTACHED STORAGE DEVICES	4
SERVERPROTECT FOR NETWORK APPLIANCE FILERS	4
SYSTEM REQUIREMENTS	8
INSTALLATION	9
A NOTE ABOUT VIRUS DETECTION TESTING	12
TESTING.....	13
SUMMARY	18
APPENDIX A: VIRUS TEST FILES	19
APPENDIX B: ABOUT TREND MICRO	20

©2001 by Trend Micro, Inc.

All rights reserved. No part of this publication may be reproduced, photocopied, stored on a retrieval system, or transmitted without the prior written consent of the publisher. InterScan, eManager, Trend VCS, ScanMail, ServerProtect, OfficeScan, MacroTrap, Active Update, and SmartScan are trademarks of Trend Micro, Inc and registered in various jurisdictions worldwide. All other company and product names are trademarks or registered trademarks of their respective owners.

A Note to Reviewers

Last year computer viruses did an estimated \$1.5 trillion dollars of damage globally¹-- victimizing businesses, governments, and private users equally. As the threat of virus infection through email traffic continues to grow, most of the data storage industry has recognized the growing need for an antivirus solution for storage devices. Networked storage devices provide convenient data access, centralized file storage and powerful data management solutions for the enterprise.

Because a company's most precious assets are contained in its information, it is essential that data integrity is ensured and that data itself is kept virus-free. Storage systems, such as Network Appliance filers, are not immune to virus attacks. A single virus-infected file in a storage system such as Network Appliance filers, can be responsible for infecting large amounts of data, which can result in a disastrous breakdown of storage services and data management. The infected file can be retrieved by any number of storage users and can eventually result in the virus spreading to client systems.

This is especially a concern for those who use storage systems for their mail server, information store, or Web server database extension and those who feel threatened by network viruses such as Explore.zip and PE_MAGISTR.

Ensuring data integrity of Network Appliance filers is the main focus of Trend Micro ServerProtect® 5.3 for Network Appliance™ filers. This document provides a general introduction to the architecture, main features, system requirements, installation and testing guides.

¹ According to PricewaterhouseCoopers 2001 survey results

Viruses Among Network Attached Storage Devices

Like biological viruses, computer viruses can spread quickly and are often difficult to eradicate. A computer virus is a piece of executable code with the unique ability to replicate. They can attach themselves to many types of files and are spread as files are copied and sent from individual to individual. Some varieties mass-mail themselves out and infect the computers of friends, customers and colleagues. Real-world global virus outbreaks like W97M_MELISSA, VBS_LOVELETTER, and JOKE_NAKEDWIFE.A have shown how effective malicious code technology can be and how destructive.

The storage system market is rapidly expanding with the revenue from disk storage systems expected to grow to \$6.57 billion by 2003. Already there has been a significant increase from \$540 million in 1998. Network-attached storage systems are designed to focus their processing power on data access and file storage, and therefore separate storage resources are different from general-purpose servers (e.g. network and application servers). Storage systems increase the overall productivity in a way that simplifies storage management and improves the reliability, performance and efficiency of the network.

However, storage systems are also vulnerable to virus attacks. A virus-infected file in a storage system, such as the Network Appliance filers, can be exchanged among storage users and infect large amounts of data, resulting in a disastrous breakdown of storage services and data management and eventually spread to a number of client systems.

Security and data integrity for a storage system are very important. Users of storage systems are actively driving their requirements for an antivirus product for their storage devices. Trend Micro has been closely working with Network Appliance to provide virus protection for Network Appliance filers.

ServerProtect for Network Appliance filers

Trend Micro's ServerProtect for Network Appliance filers offers a comprehensive antivirus solution for Network Appliance filers. Managed through an intuitive, portable console, the software provides centralized virus scanning, pattern updates, event reporting and antivirus configuration. Virus scanning takes place on separate scan servers running Windows 2000/NT. Multiple ServerProtect scan servers can be registered with one filer to provide better scan performance.

Management of ServerProtect for Network Appliance filers can be done with limited resources and budget. Administrators can easily direct such virus maintenance tasks as configuring scanning, pattern and program file updates, compiling virus logs and setting parameters for real-time scanning. Because the connection between ServerProtect scan servers and the filer is monitored, they are able to reconnect automatically should a disconnection occur.

Virus scanning takes place in on-access mode and on one or more separate scan servers running Windows 2000 or NT 4.0. For this purpose, the filer must have Network Appliance proprietary

operating system Data ONTAP 6.1 or above, to interact with the scan servers of ServerProtect for Network Appliance filer. Figure 1 presents basic ideas on how data in a filer is protected from virus infections.

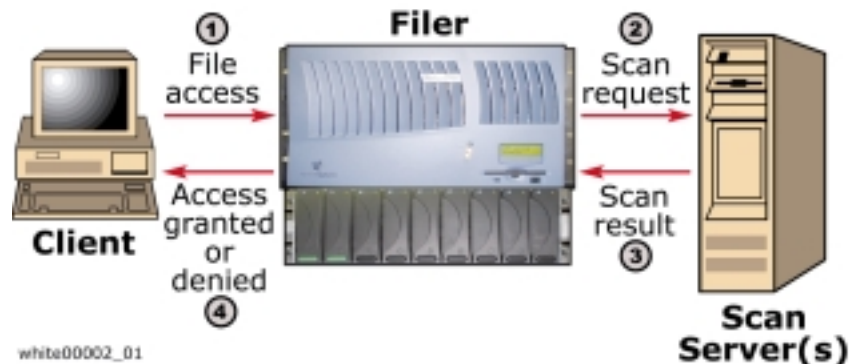


Figure 1: The Work Flow of Virus Scanning

When a client seeks access to a file in the filer or store a new file, the filer will be triggered to perform a virus check. If the filename extension appears on the extension list of file types, predetermined by the Administrator, and the file has not been previously scanned; then the filer will make a scan request to one of the registered scan servers. The result of the scan will then be passed back to the filer from the scan server and the user is, according to the scan result, either allowed access or denied access to the file. The administrator can manually add filename extensions by using the Vscan command line.

ServerProtect for Network Appliance Filer communicates with the filer via Remote Procedure Call (RPC). The scan server performs the following functions:

- Registers itself with the filer as a scan server to inform the filer of the availability and whereabouts of a virus scan server
- Watch for the filer's requests for file scanning
- Return scan results to the filer
- Answer any queries from filer
- Inform filer of any pattern file or scan engine updates
- Communicate with the filer to check the connection between the scan server and the filer

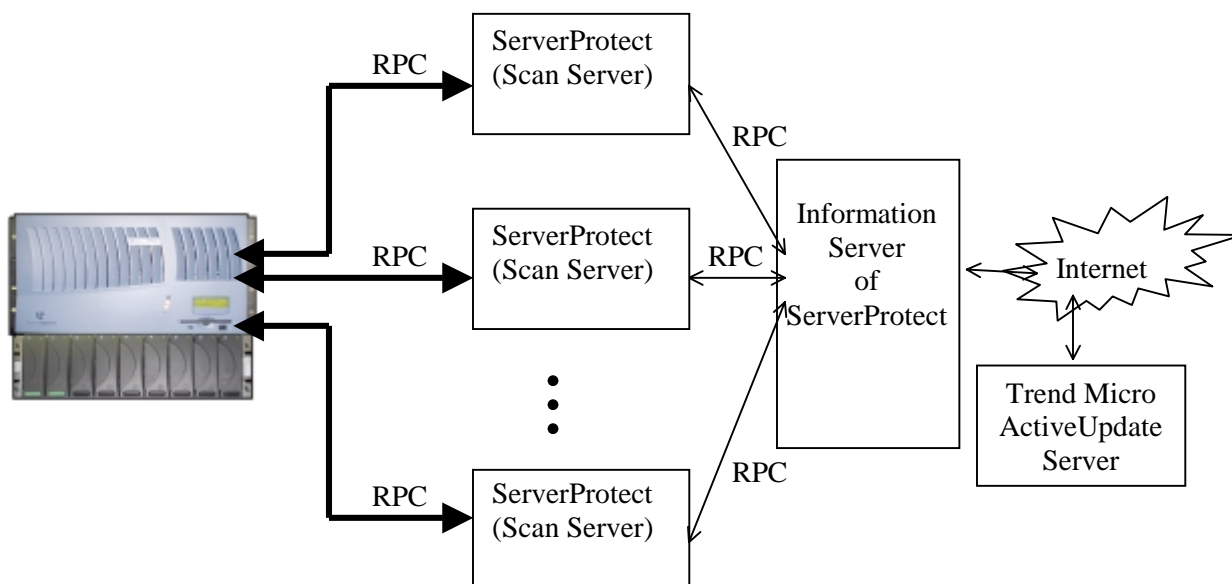


Figure 2. Architecture of ServerProtect for Network Appliance filers

The Information Server is a communication hub for coordinating antivirus activities within its domains. Each scan server is dedicated to a single filer; however, one filer can be registered with multiple scan servers. Because system administrators are provided with a single point of management for the scan servers assigned to the filer, the tedious task of directly communicating with each individual scan server is eliminated.

The filers' processing power will not be consumed by virus scanning, because scanning is done on a separate scan server rather than on the filers. There is constant communication between the filers and the scan server to monitor the connection, handle scan requests and return the scan results. To optimize the performance, the design works to minimize the traffic and speed up the scan performance with the following features:

- Administrators can configure the filers to send files of specified extensions to the scan server for virus checking in order to best-use available bandwidth
- Files in the filers will be marked as *clean* if it has been scanned before and required no modification. Files marked as *clean* won't be sent to any scan server. A gigabit connection between the filer and the scan server is recommended
- More scan servers can be added and registered with the filer at any time, so that the filer can send scan requests to the scan servers in round robin for scalability, i.e. if the first scan server is busy, the scan request is sent to the next available scan server
- Files after being scanned in the scan server won't be passed back to the filers. Only the scan results and disinfected files will be returned to the filers

Note: If a new virus pattern file becomes available in the scan servers, the administrator can reset the cached information on the filers to force it to scan all applicable files including those that were scanned with the old virus pattern file.

The key benefits of ServerProtect for Network Appliance filers include:

- Scalability and High-Performance

To increase scalability and raise performance levels, multiple ServerProtect scan servers can be registered with one filer at any time. An increased number of scan servers will increase the scan performance for the filer. Once a ServerProtect scan server is registered to a filer, connection and reconnection between that server and the filer are maintained automatically.

- Comprehensive Log Reports

ServerProtect provides comprehensive log reports that enable the user to track and manage a large number of antivirus events, including: virus infection, pattern or program updates, virus alerts, running tasks, scan activity and modifications to a single console. This will simplify tasks of virus management and product configuration for administrators.

- Centralized Management via Information Server

The ServerProtect Information Server provides simple management of multiple Windows 2000/NT scan servers from a single portable management console. The multiple scan servers can be grouped into a logical domain, but assigning scan servers for one filer into one domain is recommended. The ServerProtect management console enables administrators to configure servers in the same domain simultaneously and generate integrated virus incident reports from all scan servers. This consolidates status information when there are multiple filers and multiple scan servers for each filer.

- Scan engine and Virus Pattern Updates

Saving time and preserving network bandwidth, the Information Server can be configured to automatically download virus pattern file and scan engine updates. Using an incremental update mechanism for the distribution of a new pattern file requires only one server to download the new virus signatures added since the last update from Trend Micro's ActiveUpdate server and distribute them to designated scan servers.

- Virus Scanning to Ensure Data Integrity

ServerProtect uses the latest Trend Micro proprietary scan engine using both rule-based and pattern recognition technology to detect and remove both known and unknown viruses, including all of the in-the-wild viruses. The engine recursively scans inside files compressed with the following compression algorithms: PKZIP, PKZIP_SFX, LHA, LHA_SFX, ARJ, ARJ_SFX, CABANET, TAR, GUN ZIP, RAR, PKLITE, LZEXE, DIET, MSCOMPRESS, UNIX, PACKED, UNIX COMPACTED, UNIX LZW, UUENCODE, BINHEX, BASE64 and others.

- Configurable Actions for Infected Files

The Information Server provides GUIs for users to configure what action a scan server takes on an infected file. Choices include:

- Quarantine the infected file
 - Perform clean with a backup for cleanable viruses
 - Perform clean without a backup
 - Delete the infected file
-
- Notification of Program Events

ServerProtect for Network Appliance filer sends alerts to administrators with regard to potentially serious situations within their system. Alerts can be sent via a message box, pager, printer, Internet email, SNMP trap and/or written to the Windows NT event log. An alert will be issued in response under the following conditions: virus infections and an out-of-date virus pattern, or any problems with pattern/engine file distributions.

- Comprehensive Built-in Support

ServerProtect provides intelligent help that recommends solutions to virus-related problems and Trend Micro's online virus encyclopedia provides detailed descriptions of thousands of viruses.

System Requirements

Scan Server

- Windows 2000 (Service Pack 1) or NT Server 4.0 (Service Pack 3 or above)
- Intel Pentium II 500 MHz or faster (or equivalent)
- 50MB free disk space

Information Server

- Windows 2000 (Service Pack 1) or NT Server 4.0 (Service Pack 3 or above)
- Intel Pentium II 500 MHz or faster (or equivalent)
- 64MB RAM or above recommended
- 50MB free disk space

Management Console

- Windows 2000 (Service Pack 1) or NT Server 4.0 (Service Pack 3 or above)
- Intel Pentium II 500 MHz or faster (or equivalent)
- 64MB RAM or above recommended
- 50MB free disk space

Network Appliance Filers

- The filer must have Network Appliance proprietary OS Data ONTAP 6.1 or above.

Installation

Installing ServerProtect 5.3 for Network Appliance filers constitutes your acceptance of the terms and conditions of the license agreement that accompanies each evaluation copy of Trend Micro's software. Please review the license agreement carefully before installing the software. In addition, please note that as a product reviewer, you may only install and use an evaluation copy of ServerProtect for Network Appliance filers for the purpose of evaluation. You may not use ServerProtect for Network Appliance filers in a production environment. Any use of an evaluation copy of the software in a production environment violates the terms and conditions of the license agreement.

Before installing ServerProtect for Network Appliance filers (SPNAF) 5.3 you must delete all connections between scan servers and the filers.

To delete connections between scan servers and a filer,

from the command prompt type: `net use \\Filer-Machine\C$ /delete`

With the exception of one step, the installation procedure for SPNAF 5.3 is similar to the original Trend Micro ServerProtect. Refer to *Installation Planning* in the ServerProtect Administrator's Guide.

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

Before installing an SPNAF 5.3 scan server, you 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 (requiring 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 (see Figure 3).



Figure 3. Setup File Information screen

1. Select one of the following:
 - In the filer name or IP address text box, type the filer's name or the filer's 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 the filer logon credentials (this requires need filer backup operator or above privileges).
2. Click **Next** and follow the directions in the *Installing ServerProtect* section of the ServerProtect Administrator's Guide.

Verification

Verify the software is correctly installed and configured, perform one or both of the following two steps:

1. Use the filer command "**vsan scanners**" on the filer's console to list all of scan servers that have currently registered with the filer to do virus scanning.

If the IP address of the scan server listed, the scan server is successfully registered and ready to accept scan requests from filer.

2. Under the ServerProtect bar, click **Scan Now**.

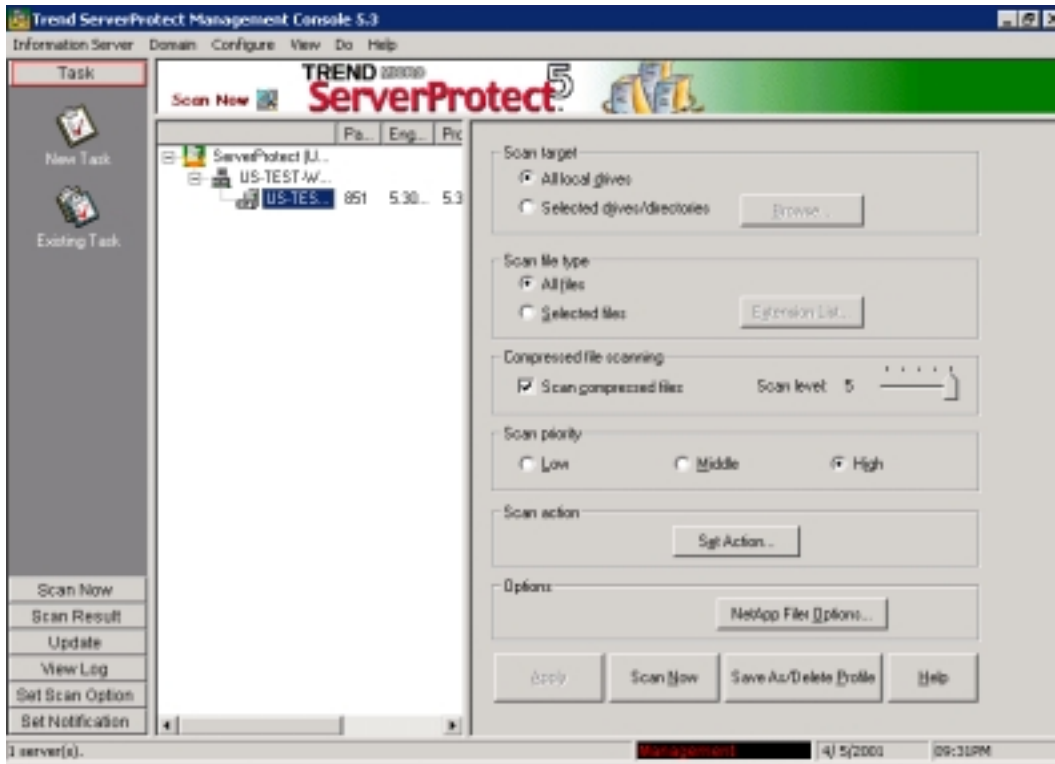


Figure 4. Management Console

Click **NetApp Filers Options**. The *Selected Filer* dialog box appears:

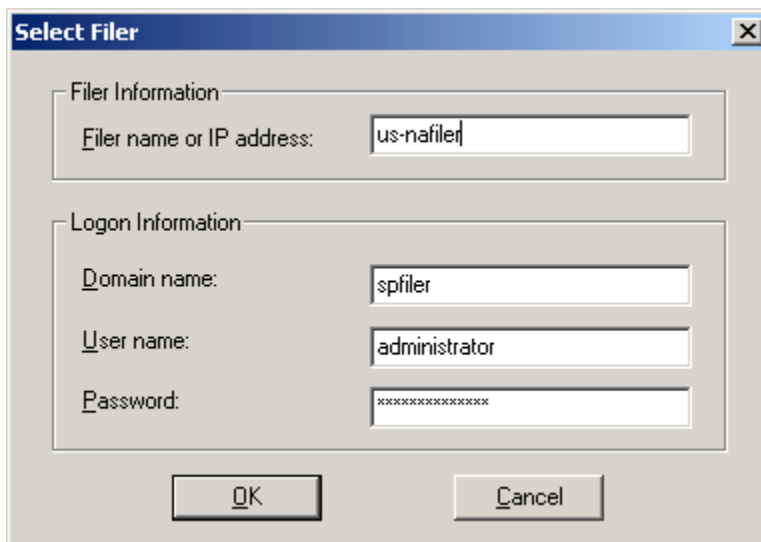


Figure 5. Modifying Filer Information

If the IP address of the filer, the scan server is successfully registered and ready to accept scan requests from the filer.

A Note About Virus Detection Testing

The antivirus marketplace is marred by a vast amount of hype and unsubstantiated claims, primarily in regard to virus detection rates. The following provides a guide for evaluating antivirus products:

1. The current hype persists due to the difficulty in testing detection rates. Depending on which variants are being defined as a new virus, experts estimate there are between 8,000 and 50,000 known viruses. Perhaps 300 of those are In-the-Wild, or known to be in the real world infecting computers. Testing antivirus software with a few dozen "pet" viruses is not statistically valid.
2. Many viruses infect boot sectors and master boot records and to run a valid test these need to be infected one at a time. Testing boot sector virus detection is a time-consuming, challenging process that doesn't begin to cover the full spectrum of in-the-wild viruses.
3. The best way to determine the quality of a product is to find out whether it has been certified by the International Computer Security Association (ICSA) and West Coast Labs (Checkmark). The ICSA creates test sets from the official published Wildlist compiled by the Wildlist Organization (www.wildlist.org). The resulting list inventories approximately 500 viruses which have shown up in the real world infecting computers. The ICSA and West Coast Lab also maintain a library of viruses known as the zoo which they use to test detection rates. Certification requires detection of 100% of In-the-Wild viruses and at least 90% of viruses in the Zoo.
4. Some vendors will distribute virus samples to reviewers which include rare samples they know their competitors will not detect. The best way to conduct a test is to contact independent organizations like ICSA or West Coast Labs or have these independent organizations perform the testing for you.
5. Many vendors claim to have the ability to detect unknown viruses without backing up their claims. The ability to detect unknown viruses is important simply because viruses are coming out faster than software or pattern files can be updated.

Additional Factors to Consider

Defining the Virus Threat

Some vendors focus solely on the threat posed by programs that only meet the technical definition of a computer virus. Obviously, a broader definition provides more protection. A complete antivirus solution should include protection from Trojans, malicious applets and related threats.

Cost of Ownership

Antivirus software is only as good as its last update. If updates are not automated then they require the Administrator to take time from other business activities to verify that each desktop has been updated. There are tools which make this process faster and more efficient and these include centralized management.

Updates are only part of hidden costs associated with deployment and updating of antivirus software. Consider the cost, in terms of time and resources, as well as how much training will be

necessary and are end users required to participate. Non-technical end users should not be required to update or perform maintenance operations for the antivirus solution to be effective.

Central logs of virus events should be available not just from one server, but from all servers so the administrator can work more efficiently. Centralized antivirus control offers the fastest response times and most effective defense against virus outbreaks.

Strength of Vision

Antivirus products require continued support and whether a vendor has its own true antivirus technology and virus research staff can become an issue when you really need support. Computer security is a highly dynamic market with new threats arising frequently. A company must have the vision to anticipate these threats and the technology to respond to them.

Development of new technologies and problem solving scenarios is important to meeting the changing needs of business. A good antivirus product should be able to scan compressed files, but caution should be used when dealing with recursively-compressed files. One firm was sent an infected document, which had been zipped 2000 times over. Their email virus scanner attempted to recursively unzip the file 2000 layers deep. Not surprisingly, it ran out of memory and crashed the email server. The lesson here is the product should have been developed to scan a limited number of layers.

The product must also have the ability to expand with the enterprise as it grows. The Internet presents a number of new business opportunities and an antivirus solution should be able to fully protect the enterprise at every entry point. Protection should be about prevention and not rely solely on response.

Testing

Testing scalability and high performance

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 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. The next 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: A scan server can only be registered to a single filer.

Virus protection for Network Appliance filers

When Windows-based clients try to open, create or change a file in the filers, it will be triggered to send a scan request to one of the ServerProtect Scan servers if the file meets the following criteria:

- The file extension listed among file types to watch for
- The file has NOT been marked as previously scanned

After the scan server receives the scan request, the scan server will scan the file for viruses. The scan result will then be passed back to the filers and therefore the user's operation on the file is either granted or denied based on the scan result.

For information on acquiring a virus test sample, see Appendix A.

- 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.
- The connection between a registered Scan Server and the filer is a trusted one. If a file is sent to the filer from a scan server, the file will not be requested for a scan. Setting the real-time scan of ServerProtect to **Incoming+Outgoing** is recommended.
- When the filer finds a scan request time-out, it will ignore this scan request and then send the same scan request to the next available scan server until a scan is completed before the timeout or all of the scan servers have been tried.
- Some additional registry values which users can set for ServerProtect for Network Appliance filers include:
 - HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ServerProtect\CurrentVersion\Engine*
 - ScanFilerTimeOut** (DWORD) -- unit in second; this is the timeout value for the Scan Server to scan a file
 - ScanTimeOutLog** (DWORD) -- 1 or 0; 1 enables the Scan Server to log for file scan request that is not scanned due to timeout; 0 disables this.
- Actions over viruses can be configured via **Scan Now** button on the side bar. Actions include **Clean, Rename, Delete, Move** and **Leave Alone**.

Remote installation, maintenance, upgrades, and un-installation of ServerProtect software throughout the network from a single console

The ServerProtect Management Console is a portable console giving network administrators centralized control of multiple network servers and domains. The Console enables you to simultaneously configure servers in the same domain and generate integrated virus incident reports for all servers. The Console has four parts: Main menu, Side bar (Shortcut bar), ServerProtect domain browser tree and Configuration data area.

The ServerProtect domain browser tree shows all the ServerProtect servers installed on Windows NT/2000 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 etc. The administrator can configure how all this data is displayed. The figure below provides a diagram of the three-tier architecture.

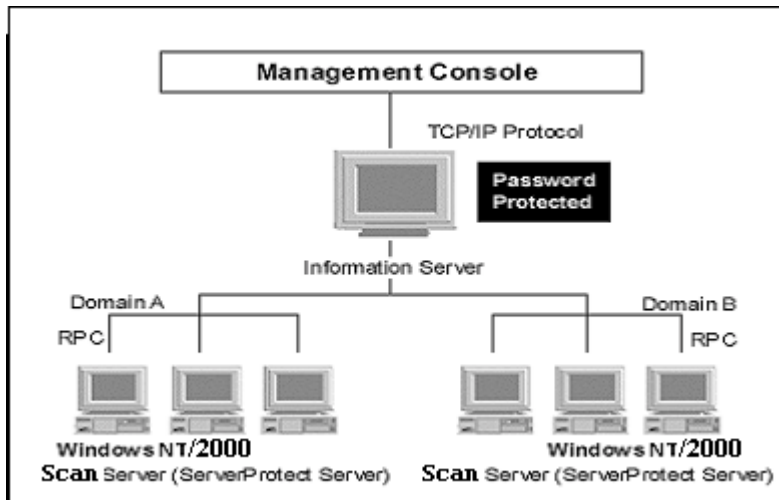


Figure 6. Architecture for Server Protect for Network Appliance filers

Scan Server is the server providing virus protection for the registered filer and is where all the action happens. These servers perform the actual antivirus functions and are managed by an Information Server.

Information Server acts as a communications hub for coordinating antivirus activities within its domains. It provides systems administrators with a single point of contact for the Scan Servers assigned to it, thus relieving them of the tedious task of directly communicating with each individual Scan Server.




Note: Theoretically, the number of scan servers that an Information Server can manage is only determined by the available bandwidth.

Domains are virtual groupings of Scan Servers on the ServerProtect to simplify their identification and management. Create, rename, or delete domains according to the needs of the network. Scan Servers in a domain can be assigned to one Information Server. Information Servers, on the other hand, can provide protection to more than one domain.

Note: Credentials for logon to the filer need to have privilege of the backup operator or above while doing a master installation. While doing a remote installation, the filer information will be copied from a source Scan Server to the target Scan Server.

Log reports track on Management console.

1. Open the *Management Console*. Select **View Log** menu from the sidebar on left side.
2. Click **View Log**. Select **Create**.
3. On ServerProtect domain browser tree, select which server should be shown. Each virus event log is listed on the right side.

4. Click any event log to view a more detailed description. There 3 different icons which represent different meanings: the  icon means **Task** event, the  icon means **Virus** event, and the  icon means an **Alert** event.

Active Update functions

Verify the network connection is working. The ServerProtect server will download the updated files from Trend Micro ActiveUpdate server via HTTP. Check the Internet connection and proxy setting on both the Web browser and ServerProtect Management console.

Updating ServerProtect requires a two-step process:

1. Downloading updates from the Trend Micro ActiveUpdate server
2. Deploying the downloaded updates to other servers on the network.

This highly efficient approach saves download time and minimizes network bandwidth. This process can be automated through the scheduled Update Task.

Downloading update files

ServerProtect displays the version of the virus pattern, scan engine, and program files currently used by an Information Server. Perform the steps below:

1. Choose one of the following:
 - Select **Update | Update** from the sidebar.
 - Select **Do | Update** from the main menu.
2. The **Update** main screen will then display.

All the version and release date information for the virus pattern, scan engine, and program files used by the system are shown on the upper part of the **Update** page.

After installing ServerProtect for the first time, the version fields are blank. They only show updates which have been cached in the Information Server. New information will be displayed after performing a successful update by pressing the **Download Now** button to download the latest updates from the Trend ActiveUpdate server.

Setting for *Download Now*

To initiate an immediate download of the latest virus pattern file, from either Trend Micro's ActiveUpdate server or another Information Server on the network:

1. From the **Update** main screen, click the **Download Now** button. To configure settings, click the **Configure** button on the **Update** main screen. The **Registration Notice** dialog box will appear offering online registration.
2. Click **OK** to register. Click **Cancel** to start downloading the updates from Trend Micro's ActiveUpdate server. A progress bar appears to show the time remaining till completion of the update.

Note: If you are using ServerProtect for the very first time, and have not yet configured the download settings, you may encounter an "HTTP generic failure" or "HTTP authentication failure" message when you click **Download Now**. See the *Configuring Download Setting* section below.

Setting for Configuring Download

The following steps describe how to download the latest update files efficiently:

1. From the *Update* main screen, click **Configure** to change the download configuration. The **Download Option** dialog box will appear.
2. Select the location the updates will be downloaded from.
 - Select the **Internet** icon to download the files from the Internet. Choose one of the following default download URLs that link to Trend ActiveUpdate server:
 - <http://serverprotect.trendmicro.com/activeupdate>
 - <http://activeupdate.trendmicro.com/activeupdate>
 - Select **From a local or network drive** to download the update files from another server on the network. Use the UNC format, rather than mapped drive format, to identify the update source server.
3. Do the following:
 - Enter the *UNC path* where the files are being kept. For example:
\\servername\foldername
 - Enter the **User name** and **Password** to access that resource

Before downloading from a local or network drive, a download source must be created:

1. Execute an update from the Internet by clicking the **Download Now**
2. After successfully downloading the updates, create a shared folder on any network server
3. Copy the SpntShare folder located under the \Program Files\Trend\Sprotect\ directory to the shared folder
4. Save the newly downloaded server.ini file in the shared folder

Note: Before attempting to download update files from another server, make sure the source server ALREADY HAS the updated files.

5. Click the **Proxy Setting** tab to continue.
6. If using a proxy server to access the Internet, select **Connect to Internet through a proxy server** and enter the *Proxy server*, *Port no.*, *User name* and *Password*. When necessary, choose to specify the protocol type used for the download. The protocols supported are: *HTTP* and *Socks 4*

7. Click **Schedule Setting** to set when to perform the download. It is now possible to schedule ServerProtect to automatically download the latest update files from Trend Micro or another server on the network.

Deploying Updates

Files downloaded to a ServerProtect Information Server can be shared with ServerProtect Scan Servers throughout the network. This minimizes the bandwidth usage because an update necessitates only one connection to Trend's Web site. When an Information Server deploys updates to Scan Servers, it first sends commands to each Scan Server, asking them to obtain a copy of the updates. ServerProtect records both the connection and deployment process in a log file. This log verifies whether or not the deployment and update were successful.

Setting for *Deploy Now*

The **Deploy Now** function is used to immediately deploy the updates saved in an Information Server to other Scan Servers.

1. From the Update main screen (see Figure 13-1), click the **Deploy Now** button to invoke the **Deploy** window of the ActiveUpdate console.
2. A list of servers and components are shown in a server tree. Choose the Scan Server components to be updated by clicking on their checkboxes. To update all components in a Scan Server, click the server's checkbox.
3. Click the **Deploy** button to activate the deployment process. Or click **Cancel** to discontinue.

Summary

Security and data integrity for a storage system are very important. A storage system such as Network Appliance filers will be vulnerable to virus attacks if the storage device is without virus protection. Moreover, a virus-infected filer can become a source of infection for other clients systems as files are retrieved by users.

With the growing market of storage systems, Trend Micro proactively works out comprehensive solutions to virus protection for storage devices. In addition, storage system customers are also actively driving their requirements for an antivirus product for their storage devices. Trend Micro has been closely working with Network Appliance to provide virus protection for Network Appliance filers.

ServerProtect for Network Appliance filers is to provide a comprehensive antivirus solution for Network Appliance filers. Managed through an intuitive, portable console, the software provides centralized virus scanning, pattern updates, event reporting and antivirus configuration. Virus scanning takes place on separate scan servers running Windows 2000/NT. Multiple ServerProtect scan servers can be registered with one filer to provide better scan performance.

Appendix A: Virus Test Files

When you are testing antivirus software, you want to verify the product is working correctly. The problem is how to verify the product without introducing a real virus into your network. Testing virus detection using a real virus is a like catching the flu to see if the flu medicine works.

Since it is unacceptable to use a real virus to do testing, the European Institute of Computer Anti-virus Research (EICAR) has developed, along with antivirus vendors, a test file to assist users in testing their installations of antivirus software.

The EICAR file is not a virus. The file is a test file which may be used to test antivirus software. It is safe to pass around, because it is not a virus, and does not include any fragments of viral code. Most products react to it as if it were a virus, but in fact the file is a legitimate DOS program. The code is harmless and when detected properly the virus scanner will display the following message:
EICAR-TEST-FILE

You can download the EICAR test script from the following URLs:

- <http://www.antivirus.com/vinfo/testfiles/>
- http://www.eicar.org/anti_virus_test_file.htm

If the installed software is working correctly, tests should result in a notification message and log entry that a virus was detected.

Appendix B: About Trend Micro

Trend Micro provides centrally controlled server-based virus protection and content-filtering products and services. By protecting information that flows through Internet gateways, email servers, and file servers, Trend Micro allows companies and service providers worldwide to stop viruses and other malicious code from a central point before they ever reach the desktop. Trend Micro's corporate headquarters is located in Tokyo, Japan, with business units in North and South America, Europe, Asia, and Australia. Trend Micro's North American headquarters is located in Cupertino, CA. Trend Micro's products are sold directly and through a network of corporate, value-added resellers and service providers. Evaluation copies of all of Trend Micro's products may be downloaded from its award-winning Web site, <http://www.trendmicro.com/> or <http://www.antivirus.com/>