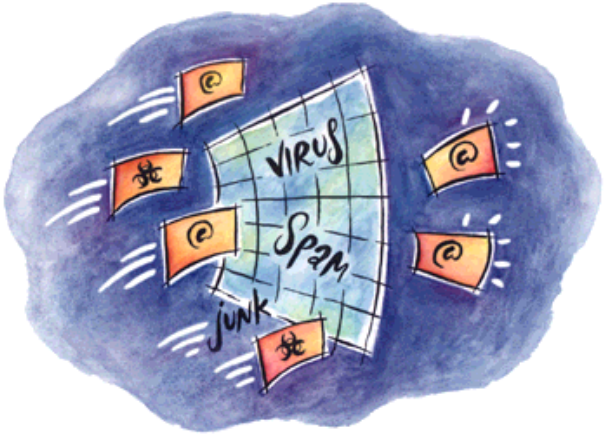
TREND INTERSCAN® VIRUSWALL® 3.6



Quick Start Guide

For Solaris, HP-UX, and Linux

What This Document Covers

Use this Quick Start Guide to install InterScan VirusWall 3.6 for Solaris, HP-UX, and Linux. The Quick Start Guide contains instructions for installing the *Standard Edition*, *CVP Edition,* and *Sendmail Switch Edition* of InterScan VirusWall.

Trend InterScan VirusWall 3.6

Trend InterScan VirusWall® is a suite of antivirus programs that work at the Internet gateway to detect and clean virus-infected files before they can enter your network. It is available for the Solaris, HP-UX, and Linux platforms.

- *E-mail VirusWall* monitors all inbound and outbound email messages for viruses, including macro viruses. *E-mail VirusWall* also supports the *sendmail* anti-relay and anti-spam functions.
- *Web VirusWall* monitors all HTTP traffic and checks for viruses, as well as malicious Java and ActiveX applets. It also provides enterprise-wide Java and Authenticode standards.
- *FTP VirusWall* protects against viruses entering your corporate network through FTP file transfers.

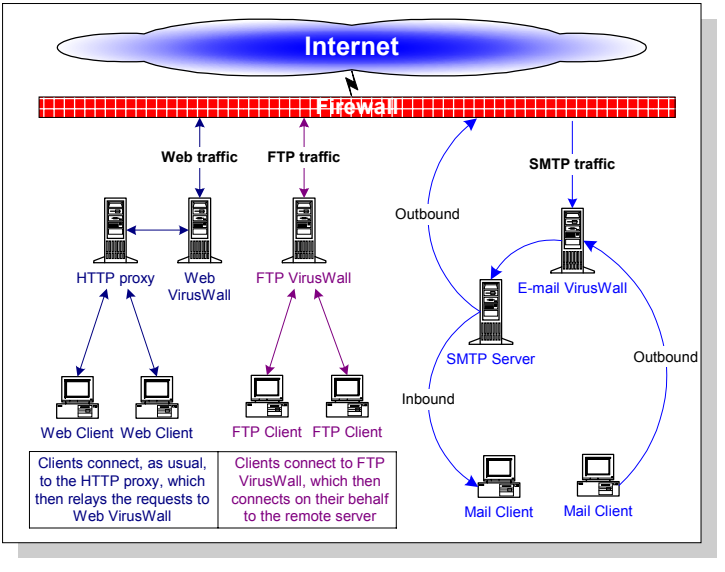


Figure 1. The diagram shows the *standard* versions of Web, FTP, and E-mail VirusWall installed on a network.

Which Version Should I Install?

InterScan VirusWall comes in two editions, either of which can be installed from the Setup package.

- **InterScan VirusWall *Standard Edition*** can be installed in any network topology and supports most firewalls. The Standard Edition works with Solaris, HP-UX, and Linux.
- **InterScan VirusWall *CVP Edition*** includes support for Check Point Software's *Content Vectoring Protocol*. Install this version if you use FireWall-1 (v. 3.0b, build 3064 or later) and want InterScan to act as a CVP server. **Solaris only**.
- **InterScan VirusWall Sendmail Switch Edition** is a plug-in that takes advantage of the Sendmail Switch Content Management API for mail filtering. For Sendmail Switch users, InterScan Sendmail Switch Edition simplifies deployment, reduces management cost, and provides better security. **Solaris only**.

InterScan VirusWall with eManager

Trend InterScan eManager is a part of the InterScan suite of products. Used in conjunction with InterScan VirusWall, eManager provides additional security and management features to an Internet gateway security solution. InterScan E-mail VirusWall scans SMTP traffic passing between the corporate network and the Internet. eManager adds the ability to filter out spam mail and inappropriate content.

Processing Order

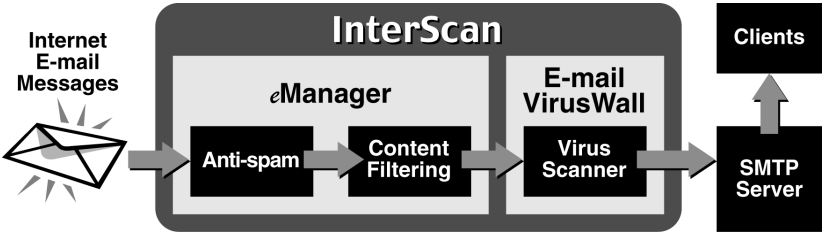


Figure 2. A graphic overview of the processing order of an incoming email.

On a network with an SMTP server, InterScan E-mail VirusWall, and one or more instances of Content Management installed, the processing order is as follows:

1. InterScan E-mail VirusWall receives inbound and/or outbound mail, and directs it to the content filter. This action occurs before virus scanning, and, before the SMTP server receives the message for processing.
2. In a quick operation, a spam/not-spam evaluation is performed.

   Message header information is compared to the user-defined list of current rules. Mail that violates a policy is **Deleted, Archived**, or **Quarantined**, as defined in the policy. The message is not compared further, nor is it forwarded to the E-mail VirusWall or SMTP server.
3. Next, the message text of all mail found not to be spam is evaluated against active user-defined policies in the content filter. Encoded attachments are not evaluated.
4. Mail that has not matched any of the content filter policies or spam filter rule-sets is forwarded. If another plug-in is installed, E-mail Management, for example, the mail is passed to it. Otherwise the message is passed to E-mail VirusWall where it will be checked for viruses.

5. Infected e-mail attachments are either **Cleaned**, **Quarantined**, **Deleted**, or **Passed** (infected files are not blocked), according to what is specified in the E-mail VirusWall configuration. Cleaned and uninfected messages are passed to the SMTP server for processing, as usual.
6. The SMTP server delivers the e-mail to the intended recipient(s). Results may vary greatly, but the spam and content filters can reduce the volume of e-mail that reaches the SMTP server by more than 10 percent.

Minimum System Requirements

Install InterScan on a system with at least the configuration indicated below. Be sure to read the **Important Notes**.

Solaris Version

- Solaris 2.6 or later on Sun SPARC platform (InterScan VirusWall Sendmail Switch edition has only been tested with Solaris 2.6 and 2.7)
- 256 MB main memory (DRAM)
- swap space should be 2 to 3 times the main memory
- 20 MB disk space for InterScan only, 50 MB if including eManager plug-in
- At least 9 GB disk space for operation (processing emails)

HP-UX Version

- HP-UX 10.20 or later
- 128 MB RAM
- swap space should be 2 to 3 times the main memory
- 20 MB disk space for InterScan

- At least 9 GB disk space for operation (processing emails)

Linux Version

- IBM/AT compatible PC with Intel Pentium 133MHz or faster
- Memory: 128 MB or more
- Swap space should be 2 to 3 times the main memory
- 20 MB disk space for InterScan
- At least 9 GB disk space for operation (processing emails)
- OS : Linux kernel 2.2.x ONLY, glibc 2.1.x ONLY (*2)
- *2: We have tested on these Linux distributions.
  - RedHat Linux 6.1
  - RedHat Linux 6.2
  - TurboLinux Server 6.1 Japanese version (*3)
- *3: C++ standard shared library (libstdc++) package needs to be installed. For more details about its installation, please refer to the manuals of your OS.
- Package name: libstdc++-compat

Important Notes

- Check Point Software's FireWall-1 version 3.0b) build 3064 or later) is required for the InterScan *CVP Edition*
- The HP-UX and Linux versions of InterScan VirusWall do not contain a CVP Edition.
- The InterScan Sendmail Switch Edition requires Sendmail Switch 2.1.2 or later to be installed on the network. Sendmail Switch Edition has only been tested with Solaris 2.6 and 2.7.

- *open source sendmail* users: Trend recommends using InterScan on platforms that bundle version 8.8.8 or later
- The InterScan E-mail (SMTP) VirusWall "temp" directory should be configured to 4 (ISVW only) or 5 (including eManager) times the total number of connections (max_proc times thr_per_proc) configured. For example:

  max_proc = 25
  thr_per_proc = 5
  Average email size = 50K

  (25X5X50) X 4 = 25MB (InterScan only)

  (25X5X50) X 5 = 31.25MB (InterScan with eManager)

Note: Insufficient temporary disk space may lead to program performance problems, up to and including program failure.

New Features and Enhancements

- **InterScan Sendmail Switch Edition**—The InterScan Sendmail Switch Edition is specifically designed to work with Sendmail Switch products (2.1.2 version or later) based on the 8.11.3 version open source code in a Solaris environment. The InterScan Sendmail Switch Edition takes advantage of the Content Management API for mail filtering, increasing ease of deployment, administration, and security.
- **Plug-In Support—**InterScan now supports additional plug-ins. The first plug-in available is InterScan eManager. InterScan eManager blocks spam and filters email content. (Standard Edition only)
- **Purge log and pattern files automatically—**From the Administration page in the InterScan web console, you can configure InterScan to automatically delete old log and pattern files.
- **Automatically run sendmail daemon with "-bd" switch**— InterScan can now be configured to run sendmail with the "-bd" switch from the web GUI. This feature can only invoke original sendmail in local host, it does not support invoking remotely.
- **Configurable notification message head/tail**— A number of parameters and message were added into intscan.ini in order to make the message head/tail to be configurable. This feature is only configurable by modifying the `intscan.ini` file. See `readme.txt` or `intscan.ini` for configuration details.
- **Configurable notification server—** This parameter allows you to define which server to use to send notification messages. To define the notification server using the Web Configuration menu, click on the Administration link and enter the server name (or IP address) and port number of the notification server.

- **Hourly pattern update support—** InterScan can now be configured to send hourly pattern updates. This is useful during a virus outbreak.
- **Check Point OPSEC Certified—**InterScan 3.6 CVP passed the OPSEC CVP certification with Check Point FireWall-1.

Installing InterScan Standard Edition

Before Installing InterScan

Important: Before Installing InterScan, you must completely remove any existing version you may have. When you remove InterScan, the `intscan.ini` file will be temporarily saved in the following directory: `/tmp/iscan_old.`

> **Note:** If the `tmp` directory is deleted prior to reinstalling InterScan VirusWall, you will lose your previous customized values.

To remove InterScan, follow the installation instructions below. When the main menu appears, choose **Option 2**: **Remove InterScan VirusWall sub-system**. Then choose **Remove All InterScan VirusWall System**.

During the Base System installation, the script will create a new `intscan.ini` and save your old `intscan.ini` file to the following directory: `/etc/iscan/old_log_ini`. The new intscan.ini file will contain default installation values. **It will not save your previous values**.

To retain your customized `intscan.ini` values, you must manually replace the default values in the new `intscan.ini` file with your customized values. We recommend that you print out the old `.ini` file and use it to review each value in the new `.ini` file. Use any text editor to restore the old settings and save the new `.ini` file. When finished, start the InterScan services.

Installing InterScan

The InterScan setup includes scripts requiring superuser permission—log on as **root** before installing InterScan.

Note: If you are installing the HP-UX or Linux versions of InterScan, the installation will differ somewhat from the description based on the Solaris platform.

1. If you are installing from the Trend Enterprise Solutions CD, you need to mount Solutions CD #2 onto a Windows NT server, locate the directory where the files are located,

   `PROGRAMS/ISVWSOL`, for Solaris
   `PROGRAMS/ISVWHP`, for HP-UX
   `PROGRAMS/ISVNUX`, for Linux

2. Choose the English or Japanese version. FTP the program files to a UNIX server and untar them.
3. From the directory containing the InterScan installation files, type `./isinst` and press ENTER.
4. You are prompted to select which edition of InterScan you want to install, the *Standard* or *CVP Edition*.
   - Choose **InterScan VirusWall for FTP, SMTP, HTTP** to install the *Standard Edition* of InterScan.
5. The **Main Menu** appears, displaying the current system configuration.
   - **Yes** means the package is not installed. This is the typical value for first time installations.
   - **No** means the package exists on the server. Before installing the current version, be sure to uninstall any previous version.
6. Choose **Option 1** to install InterScan.

7. By default, InterScan will install all available systems to subdirectories of `/opt/trend`. If you want to install to a different directory, type in the path and press `ENTER`.

Note: the **Trend Virus Control System (TVCS) Agent** is not installed by default, *see* Chapter 12, "Trend Virus Control System," for more information).

---

8. Choose **Option 8, Start Installation** to start the installation.

   a. Enter **y** and press **Enter** as prompted to install the BASE system and CGI Admin (interface).

      The BASE and CGI Admin are required for each computer that you will install a VirusWall on.

9. Continue to follow the screen prompts to complete the installation.

10. Once the InterScan Base and Admin systems are installed you are prompted to enter a serial number.

    Press **Enter** without entering a serial number to install the 30-day trial version. This version of InterScan is fully functional but will expire after 30 days, at which time it should be upgraded or removed. For information on how to buy, please refer to the following URL:

    `http://www.antivirus.com/buy`

11. To install HTTP, SMTP, and FTP VirusWall, press **y** and **Enter** as prompted. To install only one VirusWall, enter **n** when prompted to install the additional VirusWall(s).

12. Once you have completed the installation, select **Exit**. InterScan will then ask if you want to start the services. If you choose **yes**, the services will start with new `interscan.ini` settings. **Please read the following section before starting the services**.

Opening the Web Console

After installation, InterScan automatically stops and restarts your *sendmail* and/or other daemons. Although InterScan is configured to run on a robust set of default values, you should at least open the InterScan console and confirm the settings.

Open a web browser, then enter the InterScan URL followed by the port (**:1812)**. The IP address can be either the domain name or number of the InterScan computer. The port used for the Web Console is also user-configurable. For example,

```
http://domain:port/interscan
http://isvw.widget.com:1812/interscan
http://123.12.123.123:1812/interscan
```

The InterScan console is password protected. By default, both the Username and Password are **admin**.

Configuring Web VirusWall

Depending on how your system is set up, you need to choose either **InterScan acts as a proxy itself:** or **Original HTTP server location** and specify a port (typically 80) in the **InterScan HTTP Proxy port (connects to browser):** field.

> **Note:** To have Web VirusWall handle FTP scanning, have your clients configure their web browsers to use Web VirusWall as their FTP proxy.

Original HTTP server location

In the **Main service port** field, enter the port Web VirusWall will use to listen for new client connections. Typically, this number is 80. If Web VirusWall and the HTTP proxy are on the same

machine, you can change the proxy's port and give Web VirusWall port 80.

You also need to choose either **InterScan acts as a proxy itself:** or **Other (Server and port)** and specify a location and port, explained below.

InterScan acts as proxy itself:

Choose this option if there is no HTTP proxy on the network and you want Web VirusWall to serve as the system's HTTP proxy, or if you will place Web VirusWall (logically) between the Internet and proxy.

Other (Server and port)

Choose this option if there is an existing HTTP proxy server on the system and enter the location *and* port of this server. Web VirusWall will scan all HTTP traffic to and from the machine identified in this field.

Testing: Use Telnet (or a similar program) to Telnet to the InterScan IP and port you have specified. By observing the response, you can solve most configuration issues.

If the HTTP proxy server and Web VirusWall are on the same machine...

1. In **Other (server and port),** enter the local path of your HTTP daemon. For example,

   ```
   /usr/sbin/in.httpd
   ```

2. Note that there is no need to specify a port.

If the HTTP proxy server and Web VirusWall are on different machines...

1. In **Other (server and port),** enter the domain name or IP address of the machine running the HTTP daemon (`in.httpd`). For example,

   ```
   proxy.yourcompany.com 80
   123.12.13.123 80
   ```

2. Because the proxy is on a different machine, you need to specify a port.

Configuring FTP VirusWall

The FTP server location and port you specify in the **FTP Service** fields depends on which edition of FTP VirusWall you are running: *Standard* or *CVP*.

For the Standard Edition, server location and port are also determined by your set up configuration, in particular whether FTP VirusWall will serve as its own proxy, or, if installed in conjunction with an existing FTP server, whether it is installed on the same machine or a different one.

Original FTP server location

In the **Main service port** field, enter the port FTP VirusWall will use to listen for new client connections. Typically, this is port 21.

You also need to choose either **Use user@host** or **Server location** (for the latter, specify the FTP server's location and port).

Use user@host

Choose **Use user@host** if there is no existing FTP server on the network and you want FTP VirusWall to serve as the system's FTP server. Clients will *always* FTP to InterScan, which will then open a tandem connection with the requested site. When prompted for a

user name and password, clients must be sure to append the target domain to their username.

For example, to FTP *widgets.com* through FTP VirusWall, user John would open an FTP session to FTP VirusWall. When prompted, John enters his *Widgets* user name, modified by the *widgets.com* domain, and password.

- Without FTP VirusWall:

```
username: john
password: opensesame
```

- With FTP VirusWall:

```
username: john@widgets.com
password: opensesame
```

Server location

Choose **Server location** if there is an existing FTP server on the system. Enter the location and port of the server in the Server Location field. FTP VirusWall will scan all FTP traffic to and from the machine identified in this field.

If FTP server and FTP VirusWall are on the same machine...

1. In **Main service port**, enter the port used to connect to the FTP server, typically 21.
2. In **Server location,** enter the local path of your FTP daemon. For example,

```
/usr/sbin/in.ftpd
```

If FTP server and FTP VirusWall are on different machines...

1. In **Main service port**, enter the port used to connect to the FTP server, typically 21.

2. In **Server location,** enter the domain name (or IP address) *and path* of the FTP server. For example,

```
ftp-server.yourcompany.com 21
123.12.13.123 21
```

Testing: Use Telnet (or a similar program) to Telnet to the InterScan IP and port you have specified for these fields. By observing the response, you can identify and then eliminate most configuration issues.

Configuring E-mail VirusWall

E-mail VirusWall can be installed onto the same machine as your Sendmail program or a different one. It also supports running with another SMTP server, installed either on the same machine or a different one. How you configure **E-mail VirusWall** depends upon the installation topology you have selected.

E-Mail Scan Configuration

Email routing

On the E-mail Scan Configuration page, you define the path that email takes to get to the client after it enters through the gateway and the resources used to make the journey. The path is from the firewall, through InterScan, then to the client. The resources are the ports used, email servers and services that aid the journey. The following parameters need to be set to create the email routing path.

Main service port

The main service port is the port InterScan uses to receive SMTP traffic. The default value is 25: the standard SMTP port specification. This value is configurable, but in most circumstances it should not be changed.

Original SMTP server location

The Original SMTP server is the server that will deliver the message after it has been scanned for viruses. InterScan VirusWall for UNIX is not an MTA, therefore it needs to send the mail to an SMTP server after scanning. The Original SMTP server can also be thought of as the "delivery" SMTP server.

If you choose to have a local server deliver the mail, you have two configuration options: Command mode and Daemon mode.

- Command mode is used only when the MTA is on the local server. The MTA can be sendmail or any other SMTP server program. Each time a message is delivered, an instance of sendmail (or other MTA) is opened to deliver the message. Once the message is delivered, sendmail automatically closes. This process is repeated for each message that needs to be delivered.
- Daemon mode has the SMTP server program running continuously in the background. If you decide to run the SMTP server program in daemon mode, you choose the port that it will run on. The program will automatically start when InterScan starts up.

If you choose to have a remote server deliver the messages after scanning, you will only be able to configure it in daemon mode.

Using Sendmail

If E-mail VirusWall and Sendmail are on the same machine,

1. From the **Configuration | E-mail Scan** page, specify the port on which E-mail VirusWall will listen for SMTP connections (e.g., 25) in the **Main service port** field.
2. Specify the location of your Sendmail program in the **Original SMTP server location:** field. Choose either Daemon mode or Command mode. For example, if you intend to run sendmail in command mode, you would

select **Command mode** and type the following in the field provided:

```
/usr/lib/sendmail -bs
```

Note: Only the *Standard* Edition uses the **-bs** flag (formats scanned messages for delivery to the SMTP server).

Using another SMTP server

If E-mail VirusWall and your original SMTP server are on the same machine,

1. In the **Main service port** field, specify port 25 (the port E-mail VirusWall will use to listen for new SMTP connections).
2. Change your SMTP server to use another port, for example 5000.
3. In the **Original SMTP server location:** field, enter the location of your SMTP server followed by the new port that it will use. For example, a typical command mode setting for a local server would look like the following:

   ```
   localhost 5000
   ```

   Testing: Use Telnet (or a similar program) to Telnet to the InterScan IP and port and/or the SMTP server IP and port you have specified for these fields. By observing the response, you can identify and then eliminate most configuration issues.

If E-mail VirusWall and your original SMTP server are on different machines,

1. In the **Main service port** field, specify port 25 (the port E-mail VirusWall will use to listen for new SMTP connections).

2. In the **Original SMTP server location:** field, choose **Remote server** and specify the hostname (or IP address) and port of your SMTP server.

InterScan VirusWall *CVP* Edition

In the *CVP* Edition, InterScan acts as a CVP server to your FireWall-1 (v. 3.0b build 3064 or later) computer and provides real-time virus scanning for SMTP, HTTP, and FTP file transfers. It is not available with the HP-UX and Linux versions of InterScan.

The *CVP* Edition works by receiving inbound and/or outbound network traffic from the FireWall-1 server, scanning it, and then routing it back to the FireWall-1 computer for delivery as usual. All three VirusWalls are installed as a single daemon. You can turn each VirusWall on or off individually.

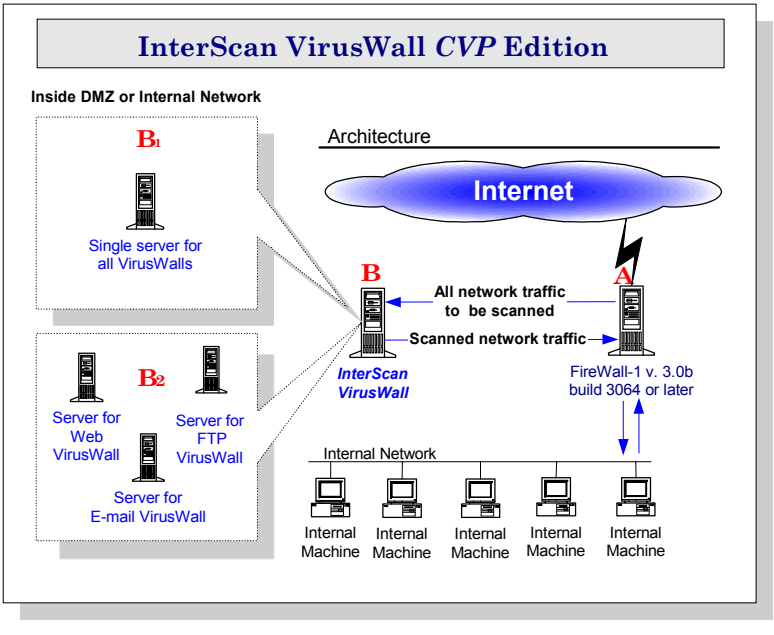


Figure 3. InterScan must receive network traffic from FireWall-1. Possible installation points for InterScan VirusWall are indicated by the letters A (the FireWall-1 computer) and B (another server).

When deciding where to install InterScan, consider first whether you want it inside the DMZ or inside the internal network. Next, consider your network traffic load and available resources. If you are installing onto an existing server that is already running programs, consider available CPU, memory, and disk space. If network traffic is light, you may, for example, want to install InterScan onto the server it will scan for. If network traffic is heavy, consider using one or more dedicated servers.

Choosing the best place to install depends on your network's traffic available resources. Installing on the FireWall-1 server, for example, can be faster but is resource intensive. InterScan can also be installed on a single server (Point B1 in the illustration below) or each VirusWall onto a different server (Point B2 in the illustration below).

- **Point A**. Installing InterScan VirusWall onto the same server as FireWall-1 is preferable for light network loads. It can be faster than transferring all traffic back and forth to the FireWall-1 computer, but expect that running InterScan in addition to FireWall-1 will place a high demand on resources.
- **Point B1**. Installing InterScan VirusWall onto a single, dedicated Solaris server (located in the DMZ or internal network) is recommended for systems with moderate to light traffic loads.
- **Point B2**. Installing InterScan VirusWall onto one or more existing servers running other software is another possibility for networks with moderate network traffic loads. Of course, a lot will depend on how resource intensive the other programs are.

Note: You can use the *Trend Virus Control System* (Trend VCS) to consolidate InterScan configuration tasks among the three computers. *See* Chapter 11 of the Administrator's Guide for details.

Installing the *CVP* Edition

To install InterScan VirusWall *CVP* Edition, you must be logged on to the target server as **root**. Installation takes about ten minutes and does not require you to restart the server.

1. If you are installing from the Trend Enterprise Solutions CD, you need to mount Solutions CD #2 onto a Windows NT server, locate the directory where the files are located, `PROGRAMS/ISVWSOL`, choose the English or Japanese version. FTP the program files to a UNIX server and untar them.
2. From the directory containing the InterScan installation files, type `./isinst` and press ENTER.
3. Choose **InterScan VirusWall for CVP** to install onto a FireWall-1 network and have InterScan act as a CVP server.
4. A **Setup** menu appears showing the current InterScan system configuration. **Yes** indicates that the package is not installed. **No** indicates that the package is installed.

   Note: If any systems or sub-systems are installed, remove them (**Option 2**) before proceeding with Setup.

   Choose **Option 1** to install InterScan.
5. By default, InterScan will install all available systems to subdirectories of `/opt/trend`. If you want to install to a different directory, type in the path and press ENTER.

Installing selected VirusWalls

Unlike the InterScan *Standard* Edition, all three protocols (SMTP, HTTP, FTP) for the *CVP* Edition are installed as a single daemon; FireWall-1 controls which protocol is scanned.

Note: To run each VirusWall on a dedicated computer, you need to install the **InterScan Base, CGI Admin**, and the VirusWall daemon onto each computer.

6. Choose **Start Installation** at the Setup Script menu to start the installation. Enter **y,** then **ENTER**, as prompted to continue installation.
7. Once the **InterScan Base** and **Admin** systems are installed you are prompted to enter a serial number to continue with the installation of the VirusWall.

   Press **Enter** without entering a serial number to install the 30-day trial version. This version of InterScan is fully functional but will expire after 30 days, at which time you should either obtain a serial number and register the product, or uninstall it and re-route your protocol traffic so InterScan is no longer a destination. To upgrade visit our web site:

   `http://www.antivirus.com/buy`
8. Follow the prompts to complete the Setup.

Opening the CVP Web Console

After installation, InterScan will automatically start CVP to initiate scanning. Although InterScan is configured to run on a robust set of default values, it's a good idea to open the configuration console to confirm or modify the settings to fit you particular needs.

1. Open a web brower and enter the URL of the InterScan computer. For example,

   `http://IP Address:port/interscan`

The IP address can be either the domain name or number of the InterScan computer. The port is 1812.

```
http://209.76.213.256:1812/interscan
http://av.widgets.com:1812/interscan
```

2. The InterScan configuration is password protected. By default, both the username and password are **admin.**

After Installing the *CVP* Edition...

After installing the InterScan program files, you need to configure InterScan and your FireWall-1 to work together. The main tasks are identified below, followed by the step-by-step instructions.

On the InterScan Side...

There are three things on the InterScan side that need to be in place for scanning to work:

- The port specified as InterScan's **Main service port** must match that set for FireWall-1's FW1_cvp service; this port is typically set to 18181, and you can set InterScan's port first, then add the port used when setting your FireWall-1 rules
- If you use Check Point Software's OPSEC Authentication, enable this option in the InterScan configuration
- InterScan must be turned **ON** (when **OFF**, network traffic does not pass through InterScan and, unless re-routed, network traffic for that protocol will stop)

A. Setting The Main Service Port

1. From the FireWall-1 rule base editor, click the **Services** check box and select FW1_cvp from the list of **Services**

Objects. Double click FW1_cvp to see which port it is using (18181).

2. Next, from the InterScan configuration page, click **Configuration** in the left window frame and then the **CVP Configuration** button.
3. In the Main Service Port field, enter the port number that the FW1_cvp is using.

B. OPSEC Authentication Users

If you are using OPSEC Authentication,

1. Bring up the InterScan configuration page and click **Configuration**, then the ISCVP **Configuration** button.
2. Choose **ON** for the **Authentication Port** option.

C. Enable Virus Scanning

Upon installation, SMTP, HTTP, and FTP virus scanning are enabled and do not require subsequent configuration. To check your settings, open the web browser:

1. Bring up the InterScan configuration page and click **Turn On/Off InterScan**.

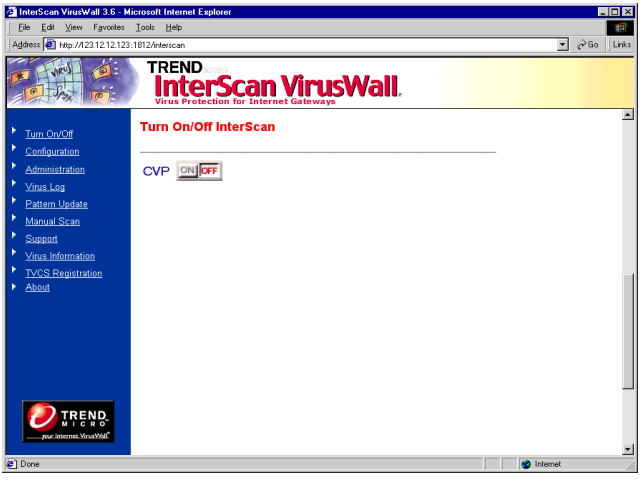


Figure 4. Be sure that each service is ON.

2. InterScan can be turned ON or OFF.
3. Click **On** to enable scanning if the current status is CVP OFF, or **Off** to disable scanning it the status is CVP ON.

On the FireWall-1 Side...

Note: Each FireWall-1 procedure is illustrated with a "screen shot" from version 4.1 that shows the Windows/Motif user interface. If you use OpenLook, some screen arrangements may look different.

FireWall-1 operates at the packet level, distributing the individual packets it receives on the basis of protocol type and the policies that are defined in the FireWall-1 rule base. In order for InterScan to receive these packets from FireWall-1, Server and Resource objects representing InterScan must be defined in the rule base and a policy describing their use engaged.

There are two main tasks for adding InterScan to FireWall-1:

1. Create the necessary objects and add the InterScan rules to the rule base:
   - Create a **Network** workstation object for each computer with InterScan VirusWall installed
   - Create a **CVP Server** object (one for each protocol if InterScan is installed on multiple computers)
   - Create a **Resource** (one for each protocol if InterScan is installed on multiple computers)
   - Add and install your scanning rules to the **rules base**
2. *If you are using Check Point's OPSEC Authentication*, set up the OPSEC authentication between the InterScan computer with FireWall-1 prior to enabling authentication in the InterScan configuration interface.

Note: InterScan does not support **Read Only** (or **Check**) mode of CVP and needs to be configured at the FireWall-1 Security Policy Editor in **Read/Write** mode (or **Cure**). See your FireWall-1 documentation for complete configuration details.

A. FireWall-1: Create a Network Object

1. In the FireWall-1 configuration page, click **Manage | Network Objects...**
2. Click **New**, then choose **Workstation** (or choose an existing Network object representing the InterScan computer).
   - If you installed the InterScan onto the FireWall-1 computer, a Network Object may already exist.
   - If you installed one instance of InterScan, create only one Network Object.
   - If you installed multiple instances of InterScan, create a different Network Object for each computer.
3. In the **General** tab, enter the name of the computer where InterScan is installed in the **Name:** field. For example,

Paris

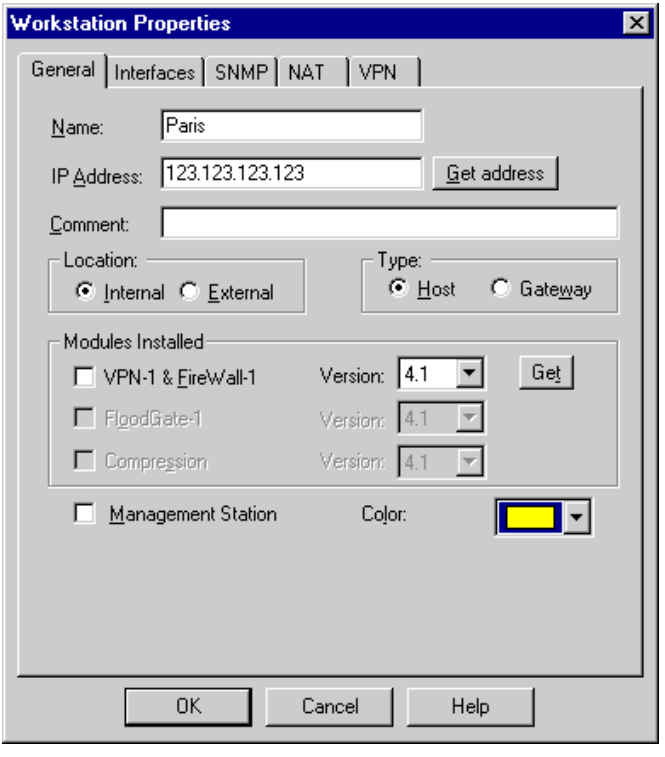


Figure 5. Create a **Network Object** for each of the VirusWalls.

4. In the **IP Address:** field, enter the IP address of this server or click **Get address** to have FireWall-1 resolve it automatically.
5. Fill out the rest of the page, for example, **Location** (Internal, External) and **Type** (Host, Gateway) as appropriate for your circumstances.

   No particular settings are required for InterScan, and none of the other pages are directly relevant to this setup.
6. Click **Close** when you have finished.

B. FireWall-1: Create a CVP Server Object

1. In the FireWall-1 configuration page, click **Manage | Servers...**
2. Click **New...**, then choose **CVP** from the drop down menu.
3. Enter a name for the Server in the **Name:** field, for example, **E-mail-Anti-Virus**.

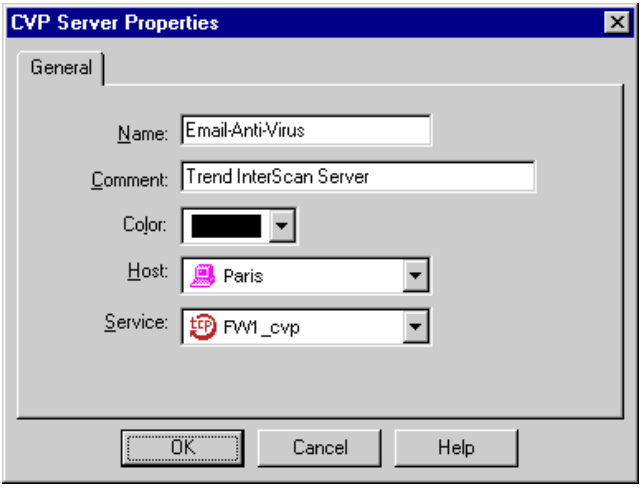


Figure 6. Define a **Server Object** for each of the VirusWalls.

4. Next, click the **Host** drop-down box and select from the list that appears the *Network Object* you created in task A, **`Paris`** in our example.
5. Accept the **Service:** type already specified, i.e., *FW1_cvp*.
6. Click **OK**, then **Close**. You have just finished creating the SMTP object.Repeat these steps for each additional InterScan service you will add (HTTP and/or FTP).

C. FireWall-1: Create a Resource Object

1. In the FireWall-1 configuration page, click **Manage | Resources...**
2. Click **New...**, then choose the appropriate protocol from the drop down menu.
   - Choose **SMTP** for the E-mail VirusWall
   - Choose **URI** for the Web VirusWall
   - Choose **FTP** for the FTP VirusWall

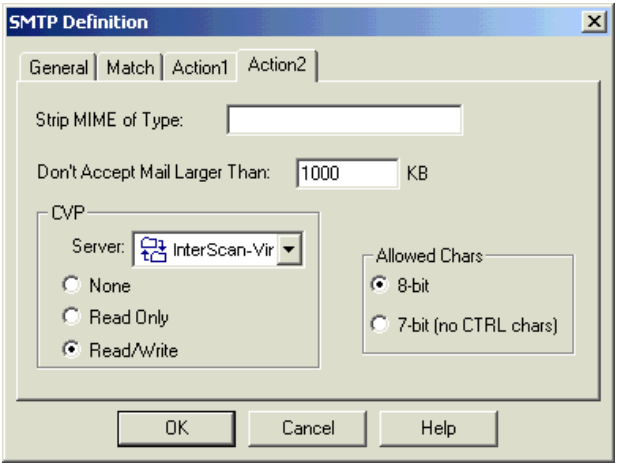


Figure 7. Define a **Resource Object** for each VirusWall.

3. In the **General** tab, enter a name for the Resource in the **Name:** field, for example, **E-mail_VirusWall_Resource**.

For SMTP scanning

a. For the E-mail VirusWall, make the **Action2** tab active and, from the **Server:** drop-down box, select the *Server* you created in task B.

b. Click **Read/Write** to enable virus scanning and cleaning (step **b**, above).

For HTTP and FTP scanning

a. Make the **Action** tab active and, in the **Server:** drop-down box, select the *Server* you created in task B, `Anti-virus` in our example.

b. Click **Read/Write**, the only valid option with InterScan, to enable virus scanning and cleaning. (The **None** option is not supported by InterScan—instead, disable virus scanning via InterScan side. InterScan does not support the **Check** option.)

c. For the FTP service, you must select either **Get**, or **Push**, or both on the **Match** tab in order to create the FTP Resource Object.

4. Click **OK**, then **Close**.

D. FireWall-1: Add Rule to the Rule Base

1. In the FireWall-1 configuration page menu, click **Edit | Add Rule | Top** to create a new rule.
2. Next, right-click the **Service** column of the rule and choose **Add With Resource...**.
3. From the list of **Services** that appears, select the resources from task C, SMTP, for instance.

4. Right-click the **Action** column of the rule and choose **accept** from the menu that appears.

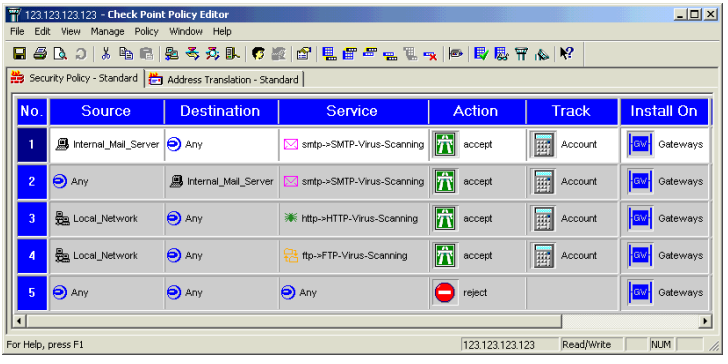


Figure 8. InterScan's scanning services are added to the CVP rule base.

5. Optionally, right-click the **Track** column of the rule and choose **Long** from the menu to enable logging.

Installing the Rule

1. From the FireWall-1 configuration page menu, click **Policy | Install**.
2. Highlight the FireWall-1 server where you want this policy installed, and click **OK**.
3. Click **Close** to complete the operation.

Rule Base Order

FireWall-1 examines the rule base sequentially, from top to bottom, until a rule successfully matches the type of traffic being examined. We recommend that you place the InterScan CVP rules accepting HTTP, SMTP, and FTP connections *before* any other rules which accept these services to prevent unwanted traffic from entering the network.

For example, if you define a rule allowing all HTTP connections but place this rule ahead of one specifying CVP scanning on a URI Resource, *the CVP rule will never be executed*.

Optional: Setting up OPSEC Authentication

As an option, the connection between InterScan and FireWall-1 can be authenticated at the transport layer using Check Point's proprietary authentication algorithm. Prior to enabling the FireWall-1 authentication port in InterScan, do the following:

- Establish an authentication key for communication between the computers. The computers identify themselves using the authentication key.
- Establish authenticated communication between the Client process (FireWall-1) and the Server process (InterScan).

For example, say there are two computers: "**FireWall-1**" and "**InterScan**".

1. On **FireWall-1**, go to the `/bin` directory and type the following at the command line prompt:

   ```
   fw putkey -opsec InterScan
   ```

   where InterScan represents the host name of the computer where InterScan is installed. You are prompted (twice) to enter the authentication key.

2. Next, on **InterScan**, go to the `etc/iscan` directory and type the following at the command line prompt:

   ```
   opsec_putkey FireWall-1
   ```

   where FireWall-1 represents the host name of the computer where FireWall-1 is installed. You are prompted (twice) to enter the authentication key.

Enter the same key as entered in Step 1. Make sure the `authkeys.C` and `rand.C` files were created in the `etc/iscan` directory.

Note: `Putkey` must be run first on the firewall before it is run from the CVP server.

3. On **FireWall-1**, change `$FWDIR/conf/fwopsec.conf` as follows:

   ```
   server 127.0.0.1 18181 auth_opsec
   ```

   should be changed to

   ```
   server InterScan 18181 auth_opsec
   ```

   where **InterScan** represents the hostname of the CVP server.

4. Next, from the InterScan's configuration console, enable the **Authentication** port by clicking **Yes**.
5. Click **Apply** to save your changes and restart the daemons.

SSL Configuration for the Web Console

Overview

The InterScan VirusWall for UNIX Web Console uses HTTP 1.0 Basic authentication. The password typed from the browser is encoded by Base64 and sent to the server. However, since Base64 does not implement an encryption algorithm, there is a risk of the password being stolen by analyzing data packets using packet filtering software.

The following explains the steps to enable a SSL (Secure Socket Layer) connection between the ISVW web console and a web browser.

Configuration

To configure SSL (Secure Socket Layer) communication, do the following:

1. Install ssleay-0.9.0b. You can download ssleay-0.9.0b from the following URL:

   ```
   http://www2.psy.uq.edu.au/~ftp/Crypto/ssleay/
   ```

2. Create a RSA private key. Type the following command:

   ```
   % /usr/local/ssl/bin/ssleay genrsa -rand .rnd > key.pem
   ```

3. Create the certification. Type the following command:

   ```
   % /usr/local/ssl/bin/ssleay req -new -x509 -nodes -key key.pem -out dummy.pem
   ```

4. Prepare the certification for stunnel. Type the following command:

   ```
   % echo "" > dummy.txt
   ```

   ```
   % cat key.pem dummy.txt dummy.pem dummy.txt > ca.pem
   ```

   If stunnel is not installed on your system, you must intall it after downloading from the following site:

   ```
   http://www.stunnel.org/download/source.html
   ```

   Start stunnel by typing the following command:

   ```
   % stunnel -p ca.pem -d 443 -r localhost:1812
   ```

5. Open "https://ISVWhost/interscan" in your web browser and authenticate the certificate.

Additional Information

After the configuration, you can use both the existing web console connection via TCP port 1812 and SSL connection simultaneously.

If you need to disable an existing connection to use SSL exclusively, do the following:

1. Modify access.conf. If you have installed ISVW under the /opt/trend directory, please change the current directory as below, typing the following command:

   ```
   # cd  /opt/trend/ISADMIN/IScan.adm/conf
   ```

2. Add the following 5 lines (from <Directory /> to </Directory> below) to the header of the "access.conf" file. Type the following command and lines:

   ```
   # vi  access.conf


   <Directory />
   order deny, allow
   allow from 127.0.0.1
   deny from all
   </Directory>
   ```

3. Send the HUP signal to the parent process of "IScanWeb" to reflect the information ("ps" is command output, and the parent process "PPID" is "1").

   ```
   #  ps -eal | grep IScanWeb
   F SUIDPIDPPID


   8 S056881IScanWeb
   8 S057565688IScanWeb
   #  kill -HUP  5688
   ```

4. Access each of the following URLs, and confirm the status:

   - http://ISVWhost:1812/interscan: Confirm that the connection is refused.

- https://ISVWhost/interscan: Confirm that HTTPS connection is available.

Installing InterScan Sendmail Switch Edition

Overview

The InterScan VirusWall Sendmail Switch Edition scans SMTP traffic for viruses. The Sendmail Switch Edition is for the Sendmail Switch mail server version 2.1.2 or later. By using Sendmail's Content Management API architecture, InterScan is easily configured and installed. Security is also enhanced because of the tight integration with Sendmail Switch.

Note: InterScan Sendmail Switch Edition can also be used with the open source sendmail version 8.11.3. However, due to the complexity of configuring open source sendmail to work in this environment, Trend will not support any problems that may arise when setting up mail filtering in the open source environment.

InterScan receives inbound and/or outbound SMTP traffic from the Sendmail Switch program, scans it for viruses, and then routes it back to the same Sendmail Switch program for delivery as usual.

The InterScan Sendmail Switch Edition is designed to be installed on the same server as the Sendmail Switch product.

Installing the Sendmail Switch Edition

To install InterScan VirusWall Sendmail Switch Edition, you must be logged on to the target server as **root**. Installation takes about ten minutes and does not require you to restart the server.

1. If you are installing from the Trend Enterprise Solutions CD, you need to mount Solutions CD #2 onto a Windows

NT server, locate the directory where the files are located, `PROGRAMS/ISVWSOL`, and choose the English or Japanese version. FTP the program files to a UNIX server and untar them.

2. From the directory containing the InterScan installation files, type `./isinst` and press `Enter`.
3. If you have previously installed InterScan, the setup program will ask you to remove all packages before installing the Sendmail Switch Edition. Choose **yes** to remove all previous InterScan packages. You will be prompted to enter **Yes** for each package that needs to be removed.

Note: You **must** remove all InterScan packages to continue with the installation.

---

4. After removing all existing packages, a **Setup** menu appears showing the current InterScan system configuration. **None** indicates that the package is not installed. **Installed** indicates that the package is installed.

   Choose **Option 3** to install InterScan VirusWall Sendmail Switch Edition.

   By default, InterScan will install all available systems to subdirectories of `/opt/trend`.

5. Enter the serial number and hit `Enter`.

   Press `Enter` without typing in a serial number to install the 30-day trial version. This version of InterScan is fully functional but will expire after 30 days, at which time you should either obtain a serial number and register the product, or uninstall it and re-route your protocol traffic so InterScan is no longer a destination. To upgrade visit our web site:

   `http://www.antivirus.com/buy`

6. The installation script will show the packages to be installed and give you an opportunity to modify the installation options. By default, the Base System, CGI Admin, and Sendmail Switch Edition packages will be installed in English. If you wish to modify any of these options, choose one of the modification options from the menu. Choose option 7, **Start Installation**, and hit `Enter`.
7. If you want to install to a different directory, type in the path and press `Enter`.
8. Follow the prompts to complete the Setup. Once the setup is complete, return to the main menu and exit the program.

After Installing InterScan Sendmail Switch Edition...

After installing the InterScan program files, you need to install and configure Sendmail Switch for virus scanning to function properly. The following section describes how to install and configure Sendmail Switch.

Installing Sendmail Switch

The current instructions are for Sendmail Switch 2.1.2. Please consult your Sendmail Switch Installation Guide and Release Notes for the latest instructions.

Remove previous versions of Sendmail

It's a good idea to remove the previous versions of Sendmail before installing Sendmail Switch. Use the `pkgrm` first to remove the older version of sendmail. After using `pkgrm`, you can manually remove all of the following files (optional):

```
/etc/mail/sendmail*, /usr/lib/sendmail*,
/usr/sbin/sendmail*, /usr/local/sendmail*,
/etc/sendmail*, /etc/mail/*
```

Note: If you are currently a Sendmail Switch customer, you need to upgrade to version 2.1.2 or later, or apply the 2.1.2 patch in order to have the Content Management API support.

Install Sendmail Switch

1. Locate the new sendmail package and type the following command:

   ```
   pkgadd –d SMIswitch SMIswitch
   ```

   In the installation process, Sendmail Switch 2.1.2 will ask you where to install the base package. For example, if you enter `/usr/local`, then Sendmail Switch will create a sub directory called *sendmail* under the specified `/usr/local` to install the base, e.g., `/usr/local/`.

2. If you installed Sendmail Switch under /usr/local, then type:

   ```
   /usr/local/sendmail/smadmin-2.0.0/sbin/
   installer
   ```

   to install the Web-based configuration program.

   Ifyou installed the Sendmail Switch on a machine named `emailhost.yourcompany.com`, then point your browser at `https://emailhost.yourcompany.com:2048/gui` to configure Sendmail Switch.

   When you log into the Web configuration main menu for the first time, you should “create the new configuration”

(sendmail.cf) first in order to start sendmail. We recommend that you accept all the default settings first to see if Sendmail Switch is working properly.

3. Test Sendmail Switch to make sure it is working properly before continuing with the configuration.

Configuring Sendmail Switch

1. Open the Sendmail Switch's Web configuration program and log into
`https://[domain name or IP address]:8890/gui`

2. If you do not have a configuration, choose **New Configuration** and create a configuration before continuing.

3. Choose **Edit Existing Configuration**.

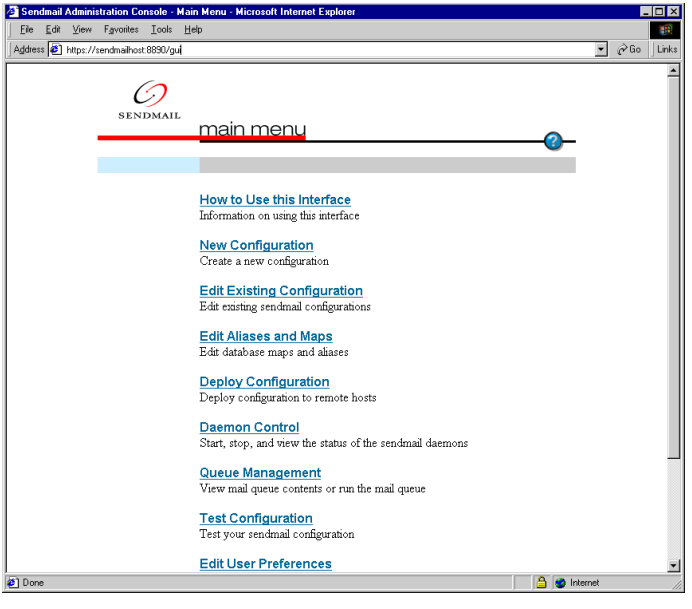


Figure 9. The Sendmail Switch main configuration page.

4. Load the configuration file. For example, `sendmail_switch.m4`

5. Scroll down to the bottom of the page and click **Mail Filtering** on the sidebar menu.

6. Click **Add** to add the filter.

   There are 2 input fields: one is **Filter Name** and the other is **Filter Equates**.

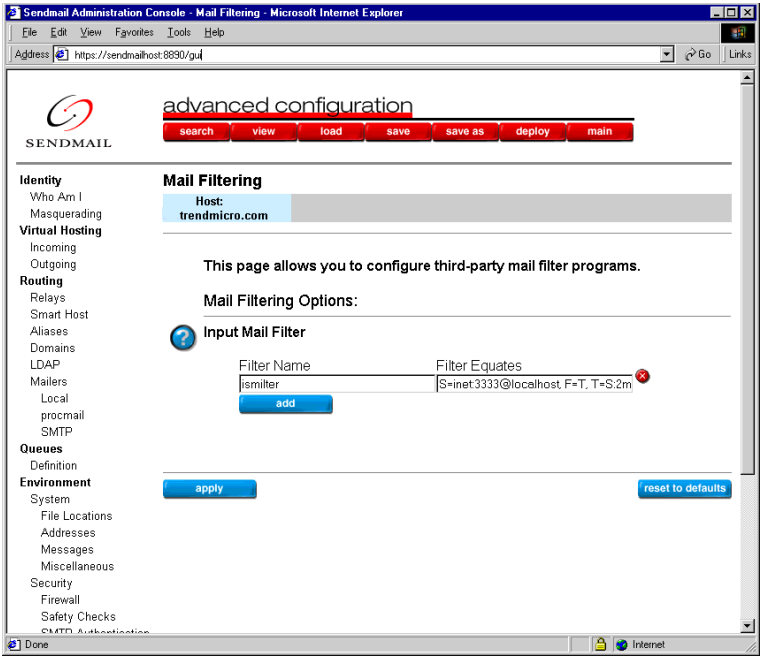


Figure 10. Mail filter options are set on this page.

7. Type `ismilter` into the **Filter Name** field and `S=inet:3333@localhost,F=T,T=S:2m;R:2m;E:5m` into the **Filter Equate** field. This is the recommended configuration for the **Filter Equates** field..

8. Click **Apply.** Once the changes are applied, you will need to "deploy" the changes to the `sendmail.cf` file for the changes to take effect.

9. Click **Deploy** on the top menu bar.

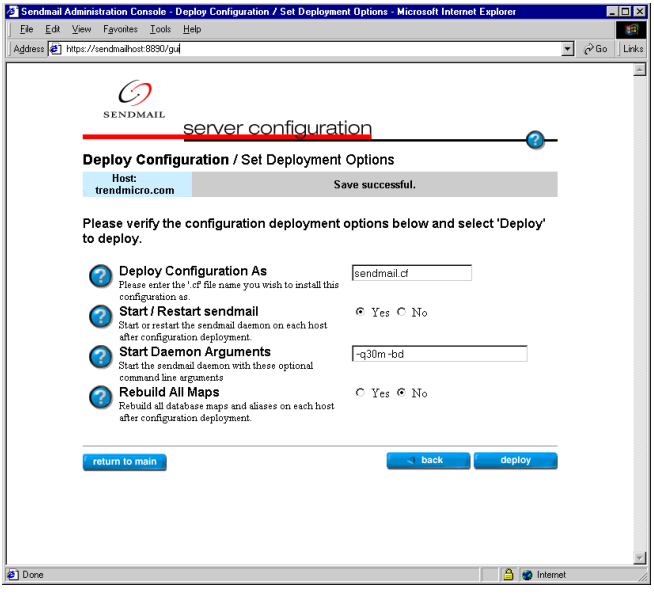


Figure 11. The picture shows the general deployment options.

10. Click the **Deploy** button at the lower right hand side of the page. Once finished, a confirmation page shows the results of the deployment.

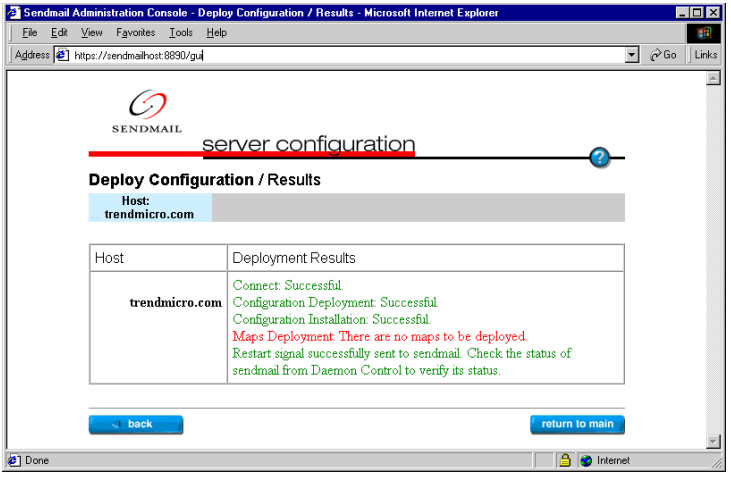


Figure 12. The deployment configuration results will be displayed after the deployment.

Filter Equates Explanations:

The Sendmail uses an IPv4 socket on port 3333 of localhost (S=inet:333). The current flags (F=) are:

R= Reject connection if filter is unavailable
T= Temporary fail connection if filter is unavailable

You can override the default timeouts used by Sendmail Switch when talking to the filters using the T= equate. There are three fields inside of the T= equate:

S = Timeout for sending information from the MTA to a filter
R= Timeout for reading reply from the filter
E = Overall timeout between sending end-of-message to filter and waiting for the final acknowledgment

T=S:2m;R:2s;E:5m where ‘s’ is seconds and ‘m’ is minutes. These are the recommended timeout settings.

Configuring InterScan Sendmail Switch Edition

By default, InterScan VirusWall Sendmail Switch Edition will create the following parameters in the [ismilter] section of the `intscan.ini` file:

```
svcport=inet:3333
logfile=/etc/iscan/log
```

Email scanning services will start automatically after the installation with the default configuration.

Note: If you change the default values in the `sendmail.cf` file, you will need to modify the values in the `intscan.ini` file and restart the InterScan service.

Testing InterScan

Once Trend VirusWall has been installed, we recommend that you test it to get familiar with the configuration and see how it works. The European Institute of Computer Antivirus Research, along with antivirus vendors, has developed a test file that can be used for checking your installation and configuration.

The file is not an actual virus; it will cause no harm and it will not replicate. Rather, it is a specially created file whose signature has been included in the virus pattern file. You can download the file from Trend at:

`www.antivirus.com/vinfo/testfiles`

Once on your computer, you can use the test virus in e-mail to test SMTP scanning, and also to check FTP and HTTP file transfers.

Trend Micro Incorporated
10101 N. De Anza Blvd., 2nd Floor
Cupertino, CA, 95014 USA
Internet: www.antivirus.com
Email: support@trendmicro.com
Toll Free: 1-800-228-5651
TEL: 1-408-257-1500
FAX: 1-408-257-2003

Trend InterScan VirusWall
for Solaris, HP-UX and Linux
Product Version: 3.6
Release Date: 03.05.2001