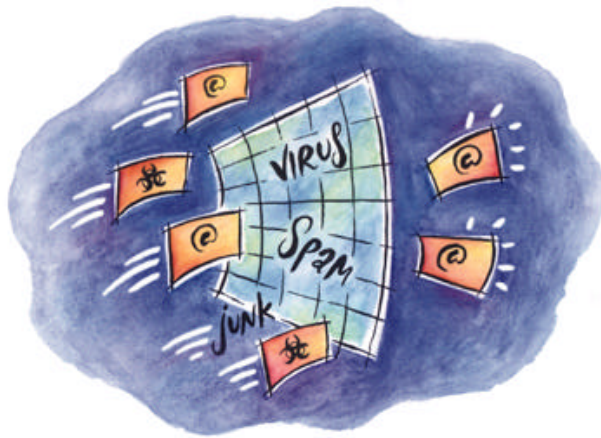


TREND INTERSCAN[®] VIRUSWALL[®] 3



Quick Start Guide
For Solaris, HP-UX, and Linux

What This Document Covers

Use this **Quick Start Guide** to install InterScan VirusWall 3 for Solaris, HP-UX and Linux. Chapter 1 contains instruction for installing the *Standard* Edition of InterScan (Solaris, HP-UX, and Linux). Chapter 2 contains instructions for installing the *CVP* Edition of InterScan, which is specially designed for use with CheckPoint FireWall's FireWall-1 (Solaris only).

InterScan VirusWall	1-1
Which Version Should I Install?.....	1-2
Important Changes to Release 3	1-2
Where Should I install?	1-3
System Resources	1-3
Minimum System Requirements	1-4
New Features	1-5
Installing InterScan	1-6
Configure E-mail VirusWall.....	1-9
Configure Anti-Relay Feature	1-11
Configure Anti-Relay Feature for Sendmail.....	1-11
Opening the InterScan Console	1-24
InterScan VirusWall CVP Edition.....	2-1
Minimum System Requirements	2-3
Installing the CVP Edition.....	2-4
After Installing the CVP Edition... ..	2-6
On the InterScan side.....	2-6
On the FireWall-1 side.....	2-8
Optional: Setting up OPSEC Authentication.....	2-14
Opening the InterScan Console	2-16
Testing InterScan	2-16

Trend InterScan VirusWall 3

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 corporate network. It is available for both 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* can also support anti-relay. Anti-relay is a new feature available in this release.
- *Web VirusWall* monitors all HTTP traffic and checks for viruses, malicious Java & ActiveX applets. It also provides enterprise-wide Java and Authenticode standards.
- *FTP VirusWall* protects against viruses entering your corporate network through FTP file transfers. Or, it can exclusively protect a given server.

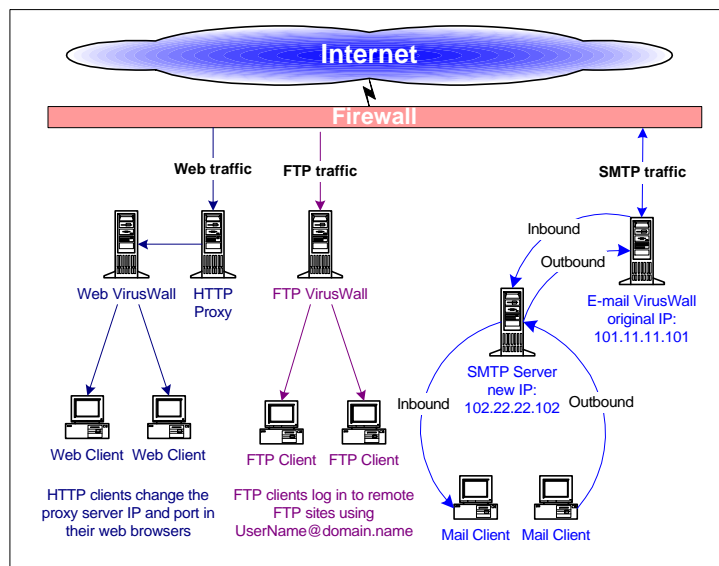


Figure 1. The illustration shows the *standard* versions of Web, FTP, and E-mail VirusWall installed on a corporate network.

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**.

Note: See the next chapter if you are installing the CVP Edition.

Important Changes to Release 3

The Plugin Edition has been removed from the program. The Standard Edition of E-mail VirusWall can be configured to support the Sendmail anti-relay and anti-spam features. See detailed instructions later in this chapter.

InterScan VirusWall 3 has a new file-blocking type called "other_binary." Other_binary blocks non-executable binary data files. These files can be .com files.

Where Should I Install?

In a typical scenario, you install InterScan to sit logically between the clients and the server whose traffic InterScan will check.

Physically, this can be the same computer as the server (or proxy) or a different computer.

System Resources

In choosing where to install, the most important issue is almost always whether or not there are sufficient resources on the target computer to adequately handle the additional load.

Before installing InterScan, you should evaluate the peak and mean traffic loads handled by the server and compare the results to the overall capacity of that computer. The closer the two measurements are, the more likely it is that you will want to install InterScan on a dedicated computer. Additional factors to consider include network bandwidth, current CPU loads, CPU speed, total and available system memory, and the total amount of available swap space.

If you are planning to install InterScan on a dedicated computer, consider the impact of your choice on overall network bandwidth. Installing InterScan onto a dedicated computer, although less resource intensive, will consume more network bandwidth than installing InterScan on the same computer as the server it is scanning for.

- **Same Computer.** If you install InterScan on the same computer as the original server, you will probably need to change the original server port—give InterScan the default, typically, FTP: 21, SMTP: 25, and HTTP: 80.
- **Dedicated Computer.** If InterScan is installed on different computer than the server it will scan for, you do not need to change the port of the original server. You may, however, need to modify the clients to reflect the new IP address (or hostname) of the InterScan computer.

Minimum System Requirements

Install InterScan on a system with at least the configuration indicated below. If you are installing the *CVP* Edition, be sure to read the **Important Notes** below.

Solaris Version

- Solaris 2.5 or above *see note
- 128 MB RAM
- 256 MB swap space
- 15 MB disk space for program files

HP-UX Version*

- HP-UX 10.10 or later *see note
- 128 MB RAM
- 256 MB swap space
- 15 MB disk space for program files

Linux Version*

- Linux Red Hat 5.2 OS Only *see note
- At least PII 266 MHz
- 128 MB RAM
- 2 GB hard drive

* Important Notes

- Check Point Software's FireWall-1 version 3.0b build 3064 or later is required for the InterScan *CVP* Edition
- Systems supporting more than 1,000 email accounts require at least a server-class computer.
- The HP-UX and Linux versions of InterScan VirusWall do not contain a CVP Edition.

New Features

Version 3

- **Linux Edition**—InterScan now supports the Linux version of UNIX. InterScan VirusWall version 3 was tested with RedHat Linux 5.2
- **New File-Blocking Type—Other_binary** blocks non-executable binary data files. These files can be .com files.
- **Anti-relay support**—InterScan can be configured accept email addressed to specific domains.
- **Sendmail anti-spam support**—To address the issue of rampant spam, InterScan E-mail VirusWall supports the anti-spam filtering capacity of Sendmail version 8.8.6 and later.
- **Uniform tagline or disclaimer**—E-mail VirusWall supports adding corporate slogans or a uniform disclaimer to all outbound mail, for example, "Visit <http://www.widgets.com> for a world of widget wonders."
- **MIME encoding**—In addition to supporting 19 types of compression (up to 20 layers deep), E-mail VirusWall also decodes three types of encoding: UUencoding, MIME, BinHex (messages received in BinHex are re-coded for delivery using UUencode).
- **Enhanced logging**—In addition to logging all virus events and virus pattern downloads, InterScan now provides the option to track all HTTP and FTP transactions.
- **Year 2000 compliance**—All components of InterScan VirusWall 3 are guaranteed to be year 2000 compliant. Please visit www.antivirus.com for details on what this guarantee entails.

Installing InterScan

Before Installing InterScan, you must completely uninstall any existing version you may have. Because there are numerous new parameters, it is not possible to preserve your existing settings by saving your `intscan.ini` file

Note: If you are installing the HP-UX or Linux versions of InterScan, the installation will differ somewhat from what is described below.

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

From the directory containing the InterScan installation files, type `./isinst` and press ENTER.

1. 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
 - Choose **InterScan VirusWall for CVP** if you will be installing onto a FireWall-1 network and you want InterScan to act as a CVP server. Switch to Chapter 2 of this Install Guide for the CVP installation instructions.
2. The **Main Menu** appears, displaying the current system configuration.
 - **None** means the package is not installed. This is the typical value for first time installations.
 - **Installed** means the package exists on the server. Before installing the current version, be sure to uninstall any previous version.
Choose **Option 1** to install InterScan.

3. By default, InterScan will install all available systems to sub-directories of /opt/trend (with the exception of the **Trend Virus Control Agent**, as explained in Chapter 11 of the Administrator's Guide).

InterScan VirusWall 3.0 Setup Script

```

Install InterScan Base System-----[ YES ]
Installation Path          /opt/trend/ISBASE

Install InterScan CGI Admin -----[ YES ]
Installation Path          /opt/trend/ISADMIN

Install InterScan for FTP -----[ YES ]
Installation Path          /opt/trend/ISFTP

Install InterScan for HTTP -----[ YES ]
Installation Path          /opt/trend/ISHTTP

Install InterScan for SMTP -----[ YES ]
Installation Path          /opt/trend/ISSMTP

Install TVCS Agent for InterScan --[ NO ]
Installation Path          /opt/trend/ISTVCS

```

1. Modify option for BASE.
2. Modify option for ADMIN.
3. Modify option for FTP.
4. Modify option for HTTP.
5. Modify option for SMTP.
6. Modify option for TVCS.
7. Start installation.
8. Back to Main Menu.

Select a number [7]

To modify the Install status or path of a system,

- a. Specify the option you want to change and press **Enter**.
 1=**Base** (required), 2=**CGI Admin** interface (required),
 3-5 are the **VirusWalls**, and 6=**Trend VCS Agent**.

- b.** Enter **y** to install the system or change the Install path, **n** to remove it from the list. The install script is case sensitive. Use lower case.
 - c.** Specify the new path or press **Enter** to accept the default, for example, `/opt/trend/ISBASE`.
- 4.** Choose **option 7, 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.
 - b.** During the CGI Admin installation, InterScan will create a group and user account on your system: Group—**iscan**, User—**iscan**. You will then be able to execute the web based configuration utility. The user name and password for configuration utility is **admin**.
 - c.** During the installation of the Virus Walls, the program will ask you to enter a port number for the web-enabled Configuration Console. Accept the default or choose an available port.
- 5.** Continue to follow the screen prompts to complete the installation.

Installing the 30-day trial version

- 6.** 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/index.htm>

7. 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).

Configure E-mail VirusWall

E-mail VirusWall can be set up in a number of different configurations depending on your network environment. There are two main types of configurations that you need to consider for your installation.

- Configure E-mail VirusWall to use its own built-in anti-relay feature (or not). If you are using a SMTP server other than Sendmail, or do not wish to use the Sendmail anti-spam feature, you can perform the standard installation and configuration. Then you can choose whether or not to use the InterScan anti-relay feature.
- Configure E-mail VirusWall to use the Sendmail anti-spam feature. There are three specific configurations available if you want to support sendmail's anti-spam feature. (See **Configure E-mail VirusWall to support the Sendmail Anti-Spam feature**).

E-mail VirusWall can be installed onto the same computer as your SMTP server or a different computer. **Important:** how you configure the **Main Service port** option in the E-mail Scan page depends on the installation topology you have chosen. See Chapter 2 of the Administrator's Guide for illustrated examples.

Note: Sendmail users see section specific to Sendmail if you intend to use the Sendmail anti-relay and anti-spam features.

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

1. Open a web browser, then enter the InterScan URL followed by the port and file name(**:1812/interscan**). The

InterScan console is password protected. By default, both the user name and password are **admin**.

2. In the **Main service port** field, specify port 25 (the port E-mail VirusWall will use to listen for new SMTP connections).
3. Change your SMTP server to use another port, for example 5000.
4. 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,

```
localhost 5000  
yourcompany.com 5000  
mailserver.yourcompany.com 5000
```

How it works: E-mail VirusWall receives SMTP traffic on port 25, scans it, and then forwards it to the SMTP server identified in the **Original SMTP server location** field using the port specified (in this case, 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 computers,

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, specify the hostname (or IP address) *and port* of your SMTP server. This port is often 25. For example,

```
mailserver 25  
mailserver.yourcompany.com 25  
123.12.12.123 25
```

How it works: E-mail VirusWall receives SMTP traffic on port 25, scans it, and then routes it to the SMTP server specified for **Original SMTP server location** using the port specified, in this case, 25.

Configure Anti-Relay Feature

1. Scroll to the bottom of the **SMTP Scan Configuration** page.
2. Click **Outbound Mail**.
3. To enable anti-relay, you must choose **Enable outbound mail blocking, disclaimer and relay processing** at the top of the page (Required).
4. Specify the local domain.
5. Choose **Enable Anti-Relay**.
6. Type in the names of the domains for which you will accept incoming mail. Separate by space, comma, or tab. The local domain is automatically included in this field.
7. Click **Apply**.

Configure E-mail VirusWall to support the Sendmail Anti-Spam feature

To configure E-mail VirusWall to support the Scanmail anti-spam feature, you must use one of the following three topologies:

1. E-mail VirusWall and Sendmail are installed on the same box. Only one Sendmail daemon is running alongside of E-mail VirusWall. For light network traffic only.

2. Sendmail is running on two different Unix boxes. This is the preferred configuration for relatively heavy mail traffic.
3. E-mail VirusWall and Sendmail are installed on the same box. Two Sendmail daemons are spawned to enhance performance. For medium to heavy network traffic.

1. Sendmail and E-mail VirusWall on one box—spawn one daemon

The following instructions provide the details to setup InterScan and Sendmail on a single Unix box. Only one Sendmail daemon runs alongside InterScan.

This configuration will have reduced server performance when InterScan delivers mail after scanning. The reduced server performance occurs when InterScan starts the Sendmail program to deliver the mail. The performance hit is directly proportional to the time and resources required to execute a Sendmail program. Not recommended for systems with heavy mail traffic.

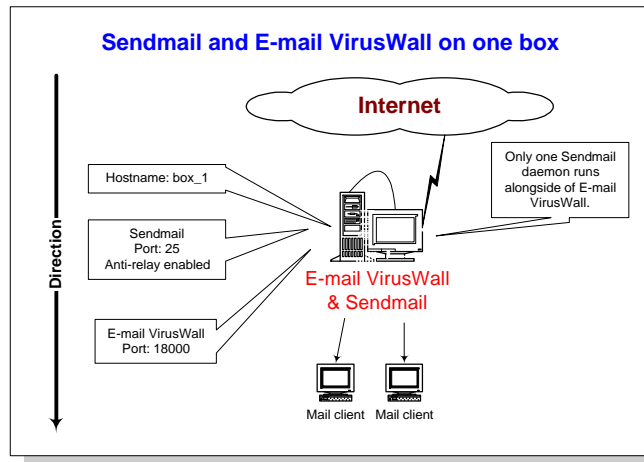


Figure 2. Illustration shows a sendmail daemon and InterScan running of the same machine.

Configure Sendmail,

1. Make a copy of sendmail.cf file called sendmail.cf.delivery.
2. Change the A option in Sendmail.cf for Msmtp, Mesmtp, Msmtp8, and Mrelay from “IPC \$h” to “IPC localhost 18000” where 18000 is an arbitrary free port on box_1.

Note: Port 18000 is an arbitrary port number. Please select a free port when doing the configuration below. Port 25 is the standard SMTP port. This should not be changed.

3. Add the k flag to the F option for Msmtp, Mesmtp, Msmtp8, and Mrelay in sendmail.cf.

For example, the changes for Msmtp should look as follows:

Before:

```
Msmtp, P=[IPC],F=mDFMuX,S=11/31,R=21,E=\r\n,L=990,
T=DNS/RFC822/SMTP,
A=IPC $h
```

After:

```
Msmtp, P=[IPC],F=kmDFMuX,S=11/31,R=21,E=\r\n,L=990,
T=DNS/RFC822/SMTP,
A=IPC localhost 18000
```

4. Replace the local mailer with [IPC] for Mlocal in sendmail.cf.
5. Change the A option to “IPC localhost 18000” for Mlocal in sendmail.cf.
6. Add the k flag to the F option for Mlocal in sendmail.cf.

For example, the changes for Msmtp should look as follows:

Before:

```
Mlocal,P=/usr/lib/mail.local, F=lsDFMAw5:/|@qfSmn9,
S=10/30, R=20/40,
```

```
T=DNS/RFC822/X-Unix,  
A=mail.local -d $u
```

After:

```
Mlocal,P=[IPC], F=kl$DFMAw5:/|@q$mn9, S=10/30,  
R=20/40,  
T=DNS/RFC822/X-Unix,  
A=IPC localhost 18000
```

Note: Make sure the F option of Mlocal does **not** include the 'f' flag. This flag is standard on Solaris 7 distribution of Sendmail and needs to be removed.

Configure the delivery mail queue used by InterScan,

1. Change the mail queue to a different directory in sendmail.cf.delivery.

Before:

```
O QueueDirectory=/var/spool/mqueue
```

After:

```
O QueueDirectory=/var/spool/mqueue1
```

2. Create the directory /var/spool/mqueue1 and make sure it has the same ownership and permission as the original in /var/spool/mqueue.
3. Add the k flag to the F option for Mlocal, Msmtplib, Mesmtplib, Msmtplib8, and Mrelay in sendmail.cf.delivery.

Configure InterScan,

1. Make sure the standard version of ISVW is installed.
2. Edit intscan.ini and change the InterScan SMTP service port to 18000.

3. In `intscan.ini`, change the original SMTP server location to include “`-C /etc/mail/sendmail.cf.delivery`” where the `sendmail.cf.delivery` file is assumed to be in `/etc/mail`.

Under `[smtp]`,

Before:

```
svcport=25
original=/usr/lib/sendmail -bs
```

After:

```
svcport=18000
original=/usr/lib/sendmail -bs
-C/etc/mail/sendmail.cf.delivery
```

4. Restart InterScan SMTP by “`/etc/iscan/sendmail`”.
5. Restart a new Sendmail daemon to process the new mail queue by “`/usr/lib/sendmail -q1h -C/etc/mail/sendmail.cf.delivery`”
6. Restart Sendmail to handle SMTP traffic on port 25 by “`/usr/lib/sendmail -bd -q1h`”.

Note: Although there is a second Sendmail daemon running, this daemon’s only responsibility is to process any mail that has been queued up. If this second daemon is not running, then the user will need to manually and periodically flush the queue.

The `S88sendmail` rc script must be modified to correctly start the mail servers: The start script should now start 3 daemons (started in steps 12, 13, and 14).

Under start section of the script,

Before:

```
/etc/iscan/sendmail; /usr/lib/sendmail -q1h
```

After:

```
/etc/iscan/sendmail; /usr/lib/sendmail -qlh  
-C/etc/mail/sendmail.cf.delivery;  
/usr/lib/sendmail -bd -qlh
```

2. Sendmail on one box, E-mail VirusWall on another box

The following instructions are applicable to those who are using two different Unix boxes to handle their mail traffic. This is the recommended configuration for relatively heavy mail traffic.

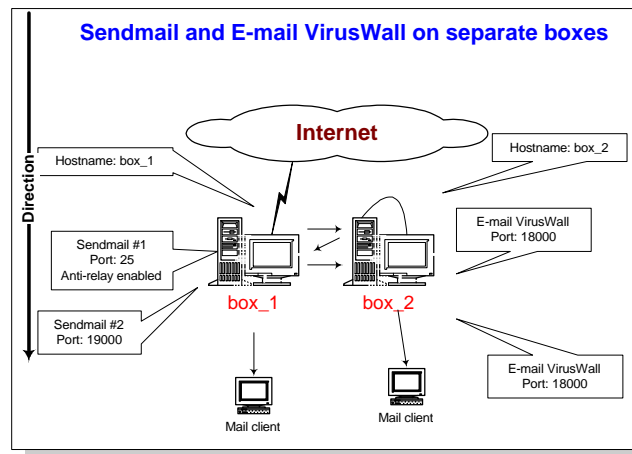


Figure 3. The illustration shows two Unix boxes configured to handle SMTP traffic. The arrows show the flow of traffic between boxes.

Configure the Mail Daemons,

On box_1...

1. Make a copy of sendmail.cf file called sendmail.cf.delivery.

2. Change the A option in sendmail.cf for Msmtp, Mesmtp, Msmtp8, and Mrelay from “IPC \$h” to “IPC box_2 18000” where box_2 is the hostname of the box running ISVW.

Note: Port 18000 and 19000 are arbitrary port number. Please select a free port when doing the configuration below. Port 25 is the standard SMTP port. This should not be changed.

3. Add the k flag to the F option for Msmtp, Mesmtp, Msmtp8, and Mrelay in sendmail.cf.

For example, the changes for Msmtp should look as follows:

Before:

```
Msmtp, P=[IPC], F=mDFMuX, S=11/31, R=21, E=\r\n, L=990,
T=DNS/RFC822/SMTP,
A=IPC $h
```

After:

```
Msmtp, P=[IPC], F=mDFMuX, S=11/31 R=21, E=\r\n, L=990,
T=DNS/RFC822/SMTP,
A=IPC box_2 18000
```

1. Replace the local mailer with [IPC] in sendmail.cf.
2. Change the A option to “IPC localhost 18000” for Mlocal in sendmail.cf.
3. Add the k flag to the F option for Mlocal in sendmail.cf.

For example, the changes for Mlocal should look as follows:

Before:

```
Mlocal, P=/usr/lib/mail.local, F=lsDFMAw5:/|@qfSmn9,
S=10/30, R=20/40,
T=DNS/RFC822/X-Unix,
A=mail.local -d $u
```

After:

```
Mlocal,P=[IPC], F=klsDFMAw5:/|@qSmn9, S=10/30,R=20/40,  
T=DNS/RFC822/X-Unix,  
A=IPC box_2 18000
```

Note: IMPORTANT: Make sure the F option of Mlocal does not include the 'f' flag. This flag is standard on Solaris 7 and needs to be removed.

4. Change the port to listen on 19000 in sendmail.cf.delivery.

Before:

```
#O DaemonPortOptions=Port=esmtplib
```

After:

```
O DaemonPortOptions=Port=19000
```

5. Change the mail queue to a different directory in sendmail.cf.delivery.

Before:

```
O QueueDirectory=/var/spool/mqueue
```

After:

```
O QueueDirectory=/var/spool/mqueue1
```

6. Create the directory /var/spool/mqueue1 and make sure it has the same ownership and permission as the original in /var/spool/mqueue.
7. Add the k flag to the F option for Mlocal, Msmtplib, Mesmtplib, Msmtplib8, and Mrelay in sendmail.cf.delivery.

On box_2...

1. Make sure the standard version of ISVW is installed.
2. Edit intscan.ini and change the InterScan SMTP service port to 18000.

3. In intscan.ini, change the original SMTP server location to box_1 port 19000 under [smtp] where box_1 is the hostname of the box running the 2 Sendmail daemons.

Under [smtp],

Before:

```
svcport=25
original=/usr/lib/sendmail -bs
```

After:

```
svcport=18000
original=box_1 19000
```

4. Restart one Sendmail on box_1 by “/usr/lib/sendmail -bd -qlh”.
5. Restart another Sendmail on box_1 by “/usr/lib/sendmail -C/etc/sendmail.cf.delivery -bd -qlh”. Replace “/etc/sendmail.cf.delivery” with the path where sendmail.cf.delivery is stored.
6. Restart ISVW on box_2.
7. Restart Sendmail on box_2 by “/usr/lib/sendmail -bd -qlh”.

The S88sendmail rc script must be modified to correctly start the mail servers: On box_1, two Sendmail daemons must now be started instead of one.

Under start section of the script,

Before:

```
/usr/lib/sendmail -bd -qlh
```

After:

```
/usr/lib/sendmail -bd -qlh; /usr/lib/sendmail
-C/etc/sendmail.cf.delivery -bd -qlh
```

8. On box_2, make the following changes.

Under start section of the script,

Before:

```
/etc/iscan/sendmail; /usr/lib/sendmail -qlh
```

After:

```
/etc/iscan/sendmail; /usr/lib/sendmail -bd -qlh
```

3. Sendmail and E-mail VirusWall on one box—spawn two daemons

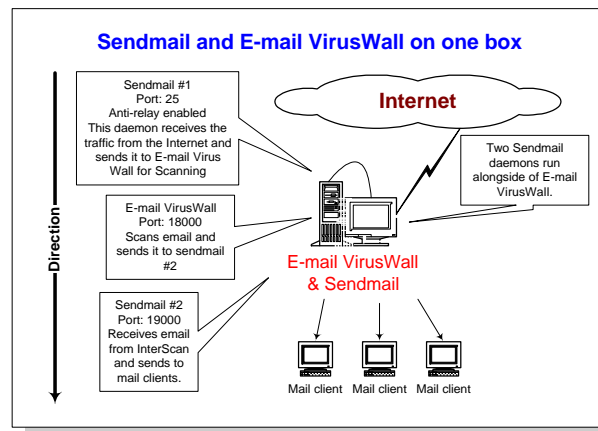


Figure 4. The illustration shows two Sendmail daemons and Inter-Scan on the same Unix box.

The instructions to configure the mail daemons for this configuration are as follows.

Configure Sendmail #1,

1. Make a copy of sendmail.cf file called sendmail.cf.delivery.
2. Change the A option in Sendmail.cf for Msmtp, Mesmtp, Msmtp8, and Mrelay from "IPC \$h" to "IPC localhost 18000" where 18000 is an arbitrary free port on box_1.

Note: Note: Port 18000 and 19000 are arbitrary port numbers. Please replace with free ports when doing the configuration below. Port 25 is the standard SMTP port. This should not be changed.

3. Add the k flag to the F option for Msmtp, Mesmtp, Msmtp8, and Mrelay in sendmail.cf.

For example, the changes for Msmtp should look as follows:

Before:

```
Msmtp, P=[IPC],F=mDFMuX,S=11/31,R=21,E=\r\n,L=990,
T=DNS/RFC822/SMTP,
A=IPC $h
```

After:

```
Msmtp, P=[IPC],F=kmDFMuX,S=11/31,R=21,E=\r\n,L=990,
T=DNS/RFC822/SMTP,
A=IPC localhost 18000
```

4. Replace the local mailer with [IPC] for Mlocal in sendmail.cf.
5. Change the A option to “IPC localhost 18000” for Mlocal in sendmail.cf.
6. Add the k flag to the F option for Mlocal in sendmail.cf.

For example, the changes for Mlocal should look as follows:

Before:

```
Mlocal,
P=/usr/lib/mail.local,F=lsDFMAw5:/|@qfSmn9,S=10/30,R=20/40,
T=DNS/RFC822/X-Unix,
A=mail.local -d $u
```

After:

```
Mlocal,P=[IPC],F=klsDFMAw5:/|@qfSmn9,S=10/30,R=20/40,
```

```
T=DNS/RFC822/X-Unix,  
A=IPC localhost 18000
```

Note: IMPORTANT: Make sure the F option of Mlocal does not include the 'f' flag. This flag is standard on Solaris 7 distribution of Sendmail and needs to be removed.

Configure Sendmail #2,

1. Change the port to listen on 19000 in sendmail.cf.delivery.

Before:

```
#O DaemonPortOptions=Port=esmtip
```

After:

```
O DaemonPortOptions=Port=19000
```

2. Change the mail queue to a different directory in sendmail.cf.delivery.

Before:

```
O QueueDirectory=/var/spool/mqueue
```

After:

```
O QueueDirectory=/var/spool/mqueue1
```

3. Create the directory /var/spool/mqueue1 and make sure it has the same ownership and permission as the original in /var/spool/mqueue.
4. Add the k flag to the F option for Mlocal, Msmtp, Mesmtip, Msmtp8, and Mrelay in sendmail.cf.delivery.

Configure InterScan,

1. Make sure the standard version of ISVW is installed.

2. Edit intscan.ini and change the InterScan SMTP service port to 18000.
3. In intscan.ini, change the original SMTP server location to “localhost 19000”.

Under [smtp],

Before:

```
svcport=25
original=/usr/lib/sendmail -bs
```

After:

```
svcport=18000
original=localhost 19000
```

4. Restart InterScan SMTP by “/etc/iscan/sendmail”.
5. Restart a Sendmail daemon to handle SMTP traffic on port 25 by “/usr/lib/sendmail -bd -qlh”.
6. Restart another Sendmail daemon to receive SMTP traffic from InterScan by “/usr/lib/sendmail -bd -qlh -C/etc/mail/sendmail.cf.delivery”.

The S88sendmail rc script must be modified to correctly start the mail servers: The start script should now start 3 daemons (started in steps 14, 15, and 16).

Under start section of the script,

Before:

```
/etc/iscan/sendmail; /usr/lib/sendmail -qlh
```

After:

```
/etc/iscan/sendmail; /usr/lib/sendmail -bd -qlh;
/usr/lib/sendmail -bd -qlh
-C/etc/mail/sendmail.cf.delivery
```

Opening the InterScan 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.

1. 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. For example,

`http://domain:port/interscan`
`http://isvw.widget.com:1812/interscan`
`http://123.12.123.123:1812/interscan`
2. The InterScan console is password protected. By default, both the user name and password are **admin**.

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, and you can toggle on/off scanning for any of the individual VirusWalls.

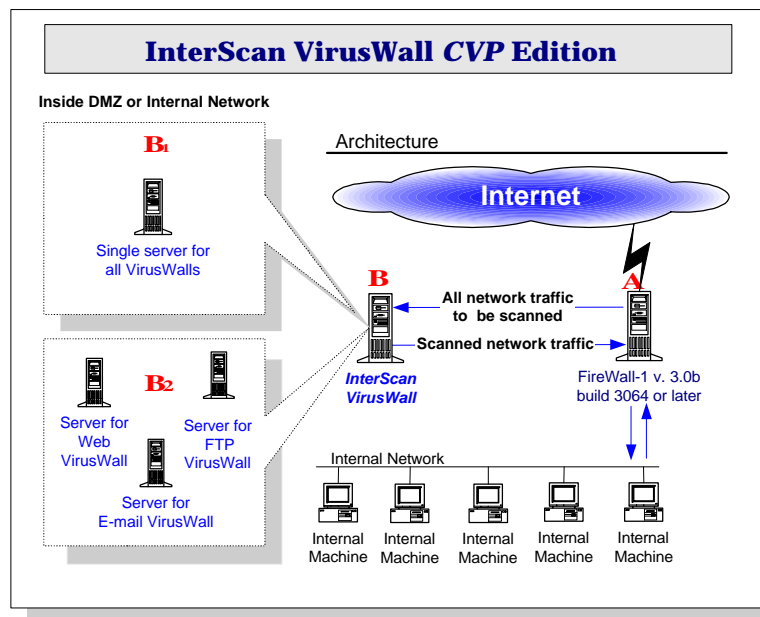


Figure 1. InterScan must receive network traffic from FireWall-1. Possible installation points for InterScan VirusWall are indicated by the letters A (the FireWall-1 computer) and B (another server).

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 will be 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 (B1 in the illustration below) or each VirusWall onto a different server (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.

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 2.5 or above *see note
- 128 MB RAM
- 256 MB swap space
- 15 MB disk space for program files

Important Notes

- Check Point Software's FireWall-1 version 3.0b build 3064 or later is required for the InterScan *CVP* Edition
- CVP version of E-mail VirusWall's does not support anti-relay
- Systems supporting more than 1,000 e-mail accounts require at least a server-class computer.
- The HP-UX and Linux versions of InterScan VirusWall does not include a CVP Edition.

Installing the CVP Edition

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

1. From the directory containing the InterScan installation files, type `./isinst` and press ENTER.
2. You are prompted to select which "flavor" of InterScan you want to install, the *CVP* or *Standard* Edition.
 - Choose **InterScan VirusWall for CVP** if you are installing onto a FireWall-1 network and you want InterScan to act as a CVP server.
 - Choose **InterScan VirusWall for FTP, SMTP, and HTTP** to install the Standard Edition of InterScan. Also, switch now to Chapter 1 of this manual for special installation instructions.
3. A **Setup** menu appears showing the current InterScan system configuration. **None** indicates that the package is not installed. If any systems or sub-systems are **Installed**, remove them (**Option 2**) before proceeding with Setup.
Choose **Option 1** to install InterScan.
4. By default, InterScan will install all available systems to sub-directories of `/opt/trend`

```
InterScan VirusWall 3 Setup Script

Install InterScan Base System----[ YES ]
Installation Path      /opt/trend/ISBASE

Install InterScan CGI Admin-----[ YES ]
Installation Path      /opt/trend/ISADMIN

Install InterScan CVP System-----[ YES ]
Installation Path      /opt/trend/ISCVF
```

```
Install InterScan VirusWall TVCS--[ NO ]
Installation Path      /opt/trend/ISTVCS
```

1. Modify option for BASE.
2. Modify option for ADMIN.
3. Modify option for CVP.
4. Modify option for TVCS.
5. Start installation.
6. Back to Main Menu.

```
Select a number [ 5 ]
```

To modify the Install status or path of a system,

- a. Specify the option you want to change and press Enter.
1=Base (required), 2=Administration interface
(required), 3=CVP VirusWall, 4=Trend VCS Agent.
- b. Enter **y** to install the system or change the Install path,
or **n** to remove it from the list.
- c. Specify the new path or press Enter to accept the
default, /opt/trend/[SYSTEM].

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 will 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.

5. Choose **Start Installation** at the Setup Script menu to start the installation. Enter **y** as prompted to continue installation.

6. 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(s).

Installing the 30-day trial version

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/usc.htm>

7. Follow the prompts to complete the Setup.

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 thru 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 you have determined 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 **ISCVS 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**.

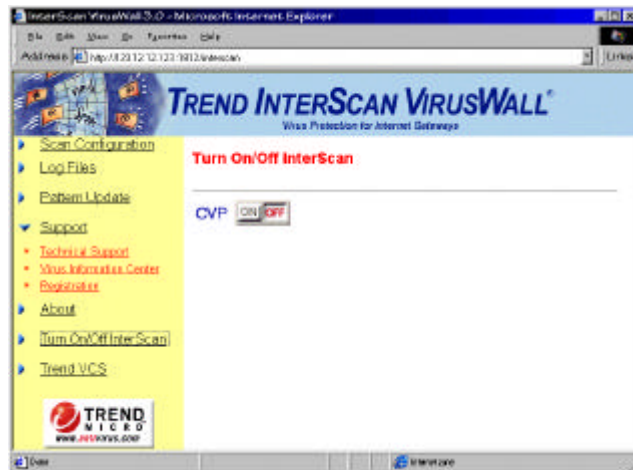


Figure 2. Be sure that each service is ON.

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 if the status is CVP ON.

On the FireWall-1 side...

Note: Each FireWall-1 procedure is illustrated with a "screen shot" 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 **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*, register 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, **USS_Washington**

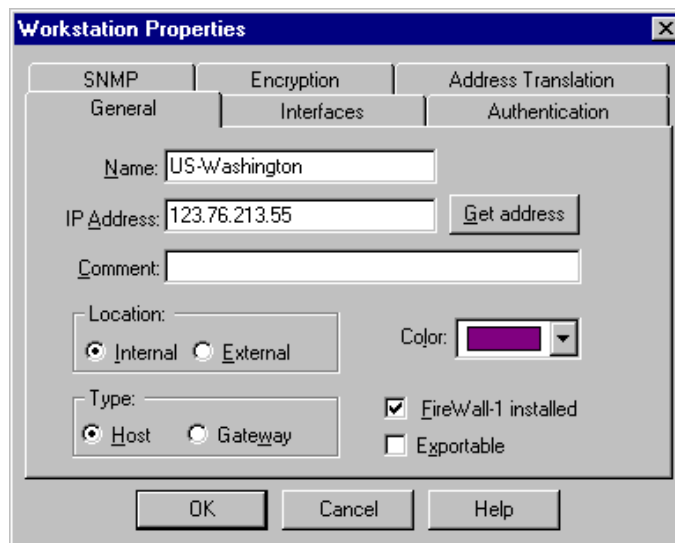


Figure 3. Create a **Network Object** for each of the VirusWalls.

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 set up.
6. Click **Close** when you have finished.

B.) FireWall-1: Create a 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, **Anti-virus**.

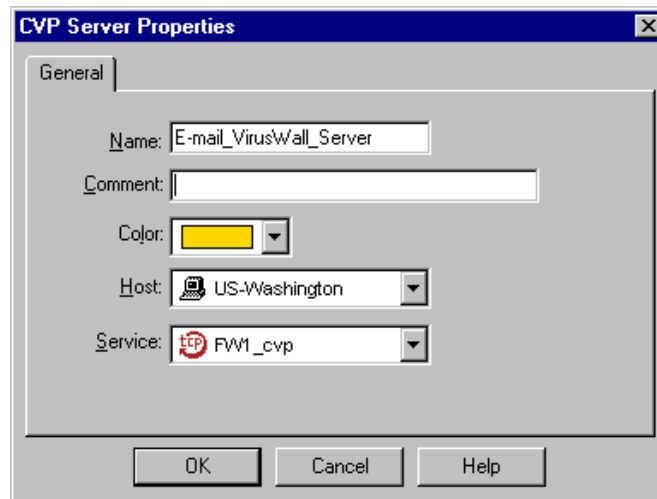


Figure 4. Define a **Server Object** for each of the VirusWalls.

4. Next, click the **Host** drop-down box and select from the list that appears the *Network Object* you created in task A, the **USS_Washington** in our example.
5. Accept the **Service:** type already specified, i.e., *FW1_cvp*.
6. Click **OK**, then **Close**. Repeat these steps for each InterScan service you will add (SMTP, HTTP, 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 that appears.
 - Choose **SMTP** for the E-mail VirusWall
 - Choose **URI** for the Web VirusWall
 - Choose **FTP** for the FTP VirusWall

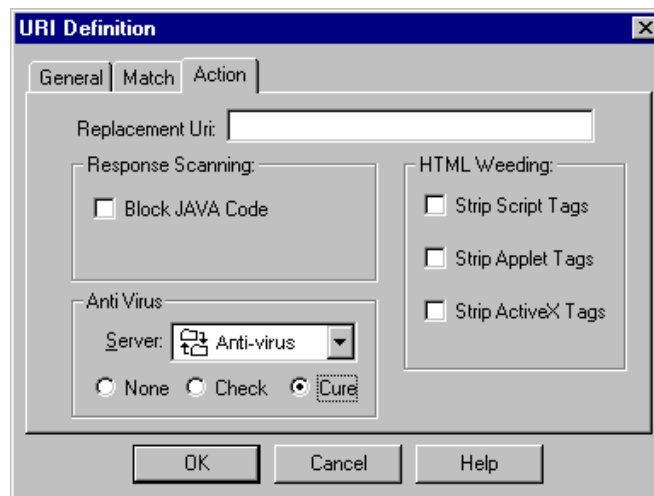


Figure 5. Define a **Resource Object** for each VirusWall.

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

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.)

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

No.	Source	Destination	Service	Action	Track
1	LocalNet	Any	ftp->AntiVirus-FTP http->AntiVirus-Web	accept	Account
2	MailServer	Any	smtp->AntiVirus-OutBoundMail	accept	Account
3	Any	MailServer	smtp->AntiVirus-InboundMail	accept	Account
4	Any	Any	Any	reject	Long

Figure 6. 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 appears 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

The connection between InterScan and FireWall-1 can *optionally* 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 OPSEC Client process (FireWall-1) and the OPSEC Server process (InterScan).

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

1. On **FireWall-1**, enter the following command:

```
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**, enter the following:

```
opsec_putkey FireWall-1
```

where **FireWall-1** represents the host name of the computer where FireWall-1 is installed. Again, you are prompted (twice) to enter the authentication key. Enter the same key as entered in Step 1.

Note: Putkey must be run first on the firewall before it is run from the CVP server. See **Running putkey** below.

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 enable **Authentication** port by clicking **Yes**.
5. Click **Apply** to save your changes and restart the daemons.

Opening the InterScan Console

After installation, InterScan will automatically stop and restart your daemons to initiate scanning. Although InterScan is configured to run on a robust set of default values, its a good idea to open the configuration console to confirm or modify the settings to fit you particular needs.

1. 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 user name and password are **admin**

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/testfile/index.htm`

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., Suite 400,
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 and HP-UX
Product Version: 3
Release Date: 3.15.99
Item Code: xxx-xxx-xxx