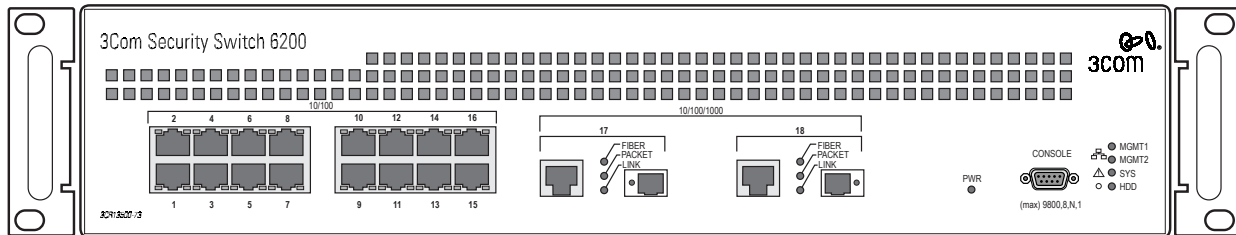




Security Switch 6200 Applications Software | Installation



December 2003

© Copyright © 2003, 3Com Corporation. All rights reserved.

No part of this documentation may be reproduced in any form or by any means or used to make any derivative work (such as translation, transformation, or adaptation) without written permission from 3Com Corporation.

3Com Corporation reserves the right to revise this documentation and to make changes in content from time to time without obligation on the part of 3Com Corporation to provide notification of such revision or change.

3Com Corporation provides this documentation without warranty, term, or condition of any kind, either implied or expressed, including, but not limited to, the implied warranties, terms or conditions of merchantability, satisfactory quality, and fitness for a particular purpose. 3Com may make improvements or changes in the product(s) and/or the program(s) described in this documentation at any time.

If there is any software on removable media described in this documentation, it is furnished under a license agreement included with the product as a separate document, in the hard copy documentation, or on the removable media in a directory file named LICENSE.TXT or !LICENSE.TXT. If you are unable to locate a copy, please contact 3Com and a copy will be provided to you.

UNITED STATES GOVERNMENT LEGEND

If you are a United States government agency, then this documentation and the software described herein are provided to you subject to the following:

All technical data and computer software are commercial in nature and developed solely at private expense. Software is delivered as "Commercial Computer Software" as defined in DFARS 252.227-7014 (June 1995) or as a "commercial item" as defined in FAR 2.101(a) and as such is provided with only such rights as are provided in 3Com's standard commercial license for the Software. Technical data is provided with limited rights only as provided in DFAR 252.227-7015 (Nov 1995) or FAR 52.227-14 (June 1987), whichever is applicable. You agree not to remove or deface any portion of any legend provided on any licensed program or documentation contained in, or delivered to you in conjunction with, this User Guide.

Unless otherwise indicated, 3Com registered trademarks are registered in the United States and may or may not be registered in other countries.

3Com, SuperStack, and Transcend are registered trademarks of 3Com Corporation. The 3Com logo and CoreBuilder are trademarks of 3Com Corporation.

Intel and Pentium are registered trademarks of Intel Corporation. Microsoft, MS-DOS, Windows, and Windows NT are registered trademarks of Microsoft Corporation. Novell and NetWare are registered trademarks of Novell, Inc. UNIX is a registered trademark in the United States and other countries, licensed exclusively through X/Open Company, Ltd.

Netscape Navigator is a registered trademark of Netscape Communications.

JavaScript is a trademark of Sun Microsystems

All other company and product names may be trademarks of the respective companies with which they are associated.

ENVIRONMENTAL STATEMENT

It is the policy of 3Com Corporation to be environmentally-friendly in all operations. To uphold our policy, we are committed to:

Establishing environmental performance standards that comply with national legislation and regulations.

Conserving energy, materials and natural resources in all operations.

Reducing the waste generated by all operations. Ensuring that all waste conforms to recognized environmental standards.

Maximizing the recyclable and reusable content of all products.

Ensuring that all products can be recycled, reused and disposed of safely.

Ensuring that all products are labelled according to recognized environmental standards.

Improving our environmental record on a continual basis.

End of Life Statement

3Com processes allow for the recovery, reclamation and safe disposal of all end-of-life electronic components.

Regulated Materials Statement

3Com products do not contain any hazardous or ozone-depleting material.

Environmental Statement about the Documentation

The documentation for this product is printed on paper that comes from sustainable, managed forests; it is fully biodegradable and recyclable, and is completely chlorine-free. The varnish is environmentally-friendly, and the inks are vegetable-based with a low heavy-metal content.

Contents

1	Installing Applications on Your system	1-1
2	Installing the CheckPoint FireWall-1 NG FP3 and NG AI Software Onto Your System	2-1
3	Installing the Trend Micro VirusWall, eManager, and IMSS Software onto Your System	3-1
4	Installing the Enterasys Dragon Intrusion Detection Software Onto Your System	4-1
5	Installing the Internet Security Systems RealSecure Network Software onto Your System	5-1
6	Installing the Snort Software Onto Your System.....	6-1
7	Installing the WebSense Enterprise Software Onto Your System ...	7-1
8	Installing the Squid Software Onto Your System	8-1
9	Installing the Secure Computing's SmartFilter Software Onto Your System.....	9-1
10	Installing the eSafe Software Onto Your System	10-1

1

Installing Applications on Your system

The following sections describe how to install applications onto your system. For further information on the applications installation, refer to the *3COM Security Switch 6200 Hardware and Software Users Guide*.

The following applications are described in this guide.

NOTE: The following information contained in this guide assumes that you have already downloaded the system image and completed the system level configuration. If you have not completed these, please do so now.

- Check Point™ FireWall-1® (pre-installed)
- Trend Micro VirusWall, eManager, and IMSS
- Enterasys™ Dragon®
- Internet Security Systems™ RealSecure®
- Snort
- Websense
- Squid Web Proxy Cache
- SmartFilter
- eSafe (CVP)

NOTE: Installation of non-OPSEC certified applications will void the “Secured By Check Point”.

2

Installing the CheckPoint FireWall-1 NG FP3 and NG AI Software Onto Your System

This chapter describes how to install the Check Point FireWall-1 NG FP3 and NG AI software onto your system.

Installing the Check Point FireWall-1 NG FP3 Software

To download and install the Check Point FireWall-1 NG FP3 software onto your system, complete the following.

NOTE: Steps 2, 3, and 4, of the following procedure may have already been performed by manufacturing.

- 1 Log into your system as root.
- 2 Locate the file `app-firewallng-FP3-x.x.x.x.7xCOS.i686.rpm`¹ and execute the following command:

```
[root@xxxxxx rpm]# rpm -i app-firewallng-FP3-  
x.x.x.x.7xCOS.i686.rpm
```

You must now install the application as specified by Check Point. The vendor files have been copied to `/usr/os/apps/CPFW-1_5_0`.

- 3 Change to the `/usr/os/apps/` directory, using the following command:

```
cd /usr/os/apps/CPFW-1_5_0
```

The following rpms and hotfixes are contained in this directory:

```
CPdtps-50-03.i386.rpm  
CPfw1-50-03.i386.rpm  
CPrtm-50-03.i386.rpm  
CPshrd-50-03.i386.rpm  
SHF_HFA_311.tar
```

¹ Refer to the 3COM Security Switch 6200 Product Release Notes for the correct software version and rpm file name.

- 4 To install FireWall-1, enter the following commands:

```
rpm -i CPshrd-50-03.i386.rpm
rpm -i CPfw1-50-03.i386.rpm
```

- 5 Untar and install hotfixes. Refer to the Check Point website for the latest hotfixes.
- 6 Run `cpconfig` and step through the Firewall-1 configuration. For SecureXL, answer “yes”. The VPN acceleration driver is automatically installed if an accelerator card is installed.

For further information about the Check Point FireWall-1 installation, refer to the Check Point FireWall-1 documentation.

Installing the Check Point FireWall-1 NG AI Software

To download the Check Point FireWall-1 NG AI software onto your system, complete the following.

NOTE: Steps 2, 3, and 4, of the following procedure may have already been performed by manufacturing.

- 1 Log into your system as root.
- 2 Locate the file `app-firewallng-AI-x.x.x.x.7xCOS.i686.rpm1` and execute the following command at the root prompt:

```
[root@xxxxxx rpm]# rpm -i app-firewallng-AI-
x.x.x.x.7xCOS.i686.rpm
```

You must now install the application as specified by Check Point. The vendor files have been copied to `/usr/os/apps/CPFW-1_5_0`.

- 3 Change to the `/usr/os/apps/` directory, using the following command:

```
cd /usr/os/apps/CPFW-1_5_0
```

The following rpms and hotfixes are contained in this directory:

```
CPdtps-50-04.i386.rpm
CPfw1-50-04.i386.rpm
CPrtm-50-04.i386.rpm
CPshrd-50-04.i386.rpm
```

- 4 To install FireWall-1 NG AI, complete the following:

```
rpm -i CPshrd-50-04.i386.rpm
rpm -i CPfw1-50-04.i386.rpm
```

- 5 Run `cpconfig` and step through the Firewall-1 NG AI configuration. For SecureXL, answer “yes”. The VPN acceleration driver is automatically installed if an accelerator card is installed.

For further information about the Check Point FireWall-1 NG AI installation, refer to Check Point FireWall-1 NG AI documentation.

¹ Refer to the 3COM Security Switch 6200 Product Release Notes for the correct software version and rpm file name.

3

Installing the Trend Micro VirusWall, eManager, and IMSS Software onto Your System

This chapter describes how to install the Trend Micro VirusWall, eManager, and IMSS software onto your system.

Installing the Trend Micro VirusWall and eManager Software

Trend Micro's VirusWall provides real-time virus detection and cleanup for the following Internet traffic.

- SMTP protection works with your mail server to scan all inbound and outbound SMTP traffic for viruses.
- HTTP protection keeps infected files from being downloaded and allows you to set uniform, system-wide security standards for Java and Authenticode. It also protects against malicious Java and ActiveX programs.
- FTP protection works transparently to ensure that infected files are not downloaded from unsecured remote sites.

The VirusWall software is compatible with most firewalls and is fully integrated with major firewalls, such as Check Point FireWall-1, and can be updated weekly from Trend Micro's website.

VirusWall can be configured to respond to virus detection and security violation incidents either alone or in combination, and responds as follows:

- Alerts the system administrator.
- Isolates the infected file for later cleaning or other action.
- Deletes the infected file.
- Allows you to download the file under certain strictly-controlled conditions.

VirusWall maintains a comprehensive activity log that details the following for each infected file or attempted security violation:

- Origin, name, and destination of the file.
- Date the file was received.
- Identity of the virus found.
- Action taken.

This allows you to track the source of the problem and to take the appropriate action.

Installing the VirusWall Software

The VirusWall software is unchanged from the tar files found on Trend Micro's website. Refer to Trend Micro's website for all VirusWall documentation.

NOTE: The VirusWall software requires a license from Trend Micro.

Downloading the VirusWall and eManager Software onto Your system

To download the VirusWall software onto your system, complete the following:

- 1 Log into your system as root.
- 2 Locate the file `app-VirusWall-x.x.x.x.x.7xCOS.i686.rpm1` and execute the following command:

```
[root@xxxxxx rpm]# rpm -i app-VirusWall-x.x-x.x.x.7xCOS.i686.rpm
```

You must now install the application as specified by Trend Micro. The vendor files have been copied to `/usr/os/apps/VirusWall`.

- 3 Change to the `/usr/os/apps/` directory, using the following command:

```
cd /usr/os/apps/VirusWall
```

- 4 Locate the following tarball files:

```
VirusWall: isvw_v38build1080_linux.tar  
Emanager: isem_lx_37_1008.tar.gz
```

- 5 To install VirusWall, complete the following:

- a Execute the tar command on the following tar file:

```
tar -xvf isvw_v38build1080_linux.tar
```

- b Change to the following directory:

```
cd /usr/os/apps/VirusWall/build_1080
```

- c Step through the VirusWall configuration, using the following command:

```
./isinst
```

- 6 To install eManager, complete the following:

- a Change to the VirusWall directory, using the following command:

¹ Refer to the 3COM Security Switch 6200 Product Release Notes for the correct software version and rpm file name.

```
cd /usr/os/apps/VirusWall/1008
```

b Execute the tar command on the following tar file:

```
tar -zxvf isem_lx_37_1008.tar.gz
```

c Execute the following command:

```
./install.sh
```

For further information on the VirusWall and eManager configurations, refer to the Trend Micro documentation.

Verifying the VirusWall and eManager Installation

To verify the VirusWall and eManager installations, follow the instructions given by Trend Micro for using HTTP to manage this application.

Installing the Trend Micro IMSS Software

Trend Micro's InterScan Messaging Security Suite (IMSS) software, using internal filters, can detect email-born threats at the Internet gateway before they penetrate your network. The IMSS software includes filters that protect against the following:

- Viruses
- Unwanted message attachments
- Large messages
- Inappropriate content
- SPAM mail

In addition, the IMSS software includes a filters that can add disclaimers to all processed messages and maintain compatibility with previous versions.

The IMSS software also permits you to apply different policies to different groups in your organization, allowing you to decide on the appropriate level of protection for each user.

Downloading and Installing the IMSS Software

NOTE: The software used in this release is unchanged from the tar files found on Trend Micro's WEB site: <http://www.trendmicro.com>. Refer to this site for all IMSS documentation.

Also, the Trend Micro IMSS software requires a license from Trend Micro.

To download and install the IMSS software onto your system, complete the following:

- 1 Log into your system as root.
- 2 Locate the file `app-IMSS-x.x-x.x.x.x.7xCOS.i686.rpm1` and execute the following command:

```
[root@xxxxxx rpm]# rpm -i app-IMSS-x.x- x.x.x.x.7xCOS.i686.rpm
```

3-4 Installing the Trend Micro VirusWall, eManager, and IMSS Software onto Your System

You must now install the application as specified by Trend Micro. The vendor files have been copied to /usr/os/apps/IMSS.

- 3 Change to the /usr/os/apps/ directory, using the following command:

```
cd /usr/os/apps/IMSS
```

- 4 Locate the following zipped tar-ball file:

```
imss_v5.1en_b1300_linux.tar.gz
```

- 5 To install IMSS, complete the following:

- a Execute the gzip and tar commands on the following zipped tar file:

```
tar -zxvf imss_v5.1en_b1300_linux.tar.gz
```

- b Change to the following directory:

```
cd /usr/os/apps/IMSS/build_LINUX_1300
```

- c Step through the IMSS configuration, using the following command:

```
./isinst
```

Editing the IMSS Postfix Configuration

After you have installed the IMSS software you need to change the IMSS Postfix configuration to enable the content filter interface to the InterScan MSS for Unix scanning daemon. To do this, complete the following:

- 1 Change to the /etc/postfix directory and open the main.cf file.
- 2 Insert or modify the following settings within the main.cf file, as follows.

```
mydomain = your.domain.name
myhostname = your.hostname.domainname
mydestination = $myhostname, localhost.$mydomain, $mydomain

default_process_limit=200
imss_timeout=10m
imss_connect_timeout=1s
content_filter = imss:localhost:10025
imss_destination_recipient_limit=200
imss_destination_concurrency_limit=20
```

- 3 Close the previous file and then open the master.cf file.
- 4 Insert the following settings into the master.cf file.

```
#InterScan MSS: content filter smtp transport imss for
InterScan MSS

imss unix - - n - - smtp
disable_dns_lookups=yes
smtp_connect_timeout=$imss_connect_timeout
smtp_data_done_timeout=$imss_timeout

#InterScan MSS: content filter loop back smtpd
localhost:10026 inet n - n - 20 smtpd
```

- 1 Refer to the 3COM Security Switch 6200 Product Release Notes for the correct software version and rpm file name.

```
content_filter=  
smtpd_timeout=$imss_timeout  
local_recipient_maps=  
myhostname=localhost.$mydomain
```

5 Save all changes.

Verifying the IMSS Installation

To verify the IMSS installation, follow the instructions given by Trend Micro for using HTTP to manage this application.

3-6 Installing the Trend Micro VirusWall, eManager, and IMSS Software onto Your System

4

Installing the Enterasys Dragon Intrusion Detection Software Onto Your System

This chapter describes how to install the Enterasys Dragon Intrusion Detection software onto your system.

Installing the Enterasys Dragon Intrusion Detection Software

The Enterasys™ Dragon® Network Intrusion Detection System (NIDS) (Dragon) software detects network attacks by monitoring network traffic as it passes over the IT infrastructure. Dragon Sensor analyzes the network traffic at the protocol and application level, employing both signature and anomaly based techniques to identify network misuse, attack, and denial of service efforts.

To download the Dragon software onto your system, complete the following:

- 1 Log into your system as root.
- 2 Locate the file `app-Dragon-x.x-x.x.x.x.7xCOS.i686.rpm`¹ and execute the following command:

```
[root@xxxxxx rpm]# rpm -i app-Dragon-x.x-x.x.x.x.7xCOS.i686.rpm
```

You must now install the application as specified by Enterasys. The vendor files have been copied to `/usr/os/apps/Dragon`.

- 3 Change to the `/usr/os/apps/` directory, using the following command:

```
cd /usr/os/apps/Dragon
```

This directory contains the following tarball file:

```
Dragon-6.0.2-Linux-i686-BUILD215.tar.gz
```

1 Refer to the 3COM Security Switch 6200 Product Release Notes for the correct software version and rpm file name.

4-2 Installing the Enterasys Dragon Intrusion Detection Software Onto Your System

- 4 To install the Dragon software, unzip, and untar the above file, using the following command:

```
tar -zxvf Dragon-6.0.2-Linux-i686-BUILD215.tar.gz
```

- 5 Change to the following directory:

```
cd Dragon-6.0.2-Linux-i686-BUILD215
```

- 6 Step through the Dragon configuration, using the following command:

```
./install.pl
```

For further information on the Dragon configuration, refer to the Enterasys Dragon documentation.

5

Installing the Internet Security Systems RealSecure Network Software onto Your System

This chapter describes how to install the Internet Security Systems™ RealSecure® Network software onto your system.

Installing the ISS Real Secure Software

The Internet Security Systems™ RealSecure® Network software protects critical assets using sophisticated intrusion prevention techniques on a single, high availability, configurable multi-segment application platform. RealSecure Network's proven accuracy and performance combined with the switch's advanced control technology comprehensively protects high-speed networks while simplifying the infrastructure, resulting in more effective use of network resources, across-the-board fault tolerance, and increased network integrity.

To download the ISS software onto your system, complete the following:

- 1 Log into your system as root.
- 2 Locate the file `app-ISS-x.x-x.x.x.x.7xCOS.i686.rpm`¹ and execute the following command:

```
[root@xxxxx rpm]# rpm -i --nodeps app-ISS-x.x-  
x.x.x.x.7xCOS.i686.rpm
```

You must now install the application as specified by ISS. The vendor files have been copied to `/usr/os/apps/ISS`.

- 3 Change to the `/usr/os/apps/` directory, using the following command:

```
cd /usr/os/apps/ISS
```

¹ Refer to the 3COM Security Switch 6200 Product Release Notes for the correct software version and rpm file name.

This directory should contain the following rpms file:

```
ISS-RealSecure-common-lib-7.0-2003.167.i386.rpm  
ISS-RealSecure-ns-daemon-7.0-2003.167.i386.rpm  
ISS-RealSecure-ns-sensor1-7.0-2003.167.i386.rpm
```

4 To install the ISS software, install the above rpms, using the following command:

```
rpm -i --nodeps ISS-RealSecure-common-lib-7.0-2003.167.i386.rpm  
rpm -i --nodeps ISS-RealSecure-ns-daemon-7.0-2003.167.i386.rpm  
rpm -i --nodeps ISS-RealSecure-ns-sensor1-7.0-2003.167.i386.rpm
```

5 Change to the following directory:

```
cd /opt/ISS/issSensors/network_sensor_1
```

6 Step through the ISS configuration, using the following command:

```
./setup.sh
```

For further information on the ISS RealSecure configuration, refer to the ISS documentation.

6

Installing the Snort Software Onto Your System

This chapter describes how to install the Snort software onto your system.

Installing the Snort Software

Snort is a Network Intrusion Detection System (NIDS) that performs real-time traffic analysis and packet logging on IP networks. Snort performs protocol analysis, content searching/matching and is used to detect a variety of attacks and probes, such as buffer overflows, stealth port scans, CGI attacks, SMB probes, OS fingerprinting attempts, and so on. Snort uses a flexible rules language to describe traffic that it should collect or pass, as well as a detection engine that utilizes a modular plug-in architecture. Snort has a real-time alerting capability as well, incorporating alerting mechanisms for syslog, a user specified file, a UNIX socket, or WinPopup messages to Windows clients using Samba's smbclient.

To download the Snort software onto your system, complete the following:

- 1 Log into your system as root.
- 2 Locate the file `app-Snort-x.x.x.x.x.7xCOS.i686.rpm`¹ and execute the following command:

```
[root@xxxxx rpm]# rpm -i app-Snort-x.x-x.x.x.7xCOS.i686.rpm
```

This installs Snort on your system. For further information about the Snort configuration, refer to www.snort.org website.

1 Refer to the 3COM Security Switch 6200 Product Release Notes for the correct software version and rpm file name.

7

Installing the WebSense Enterprise Software Onto Your System

This chapter describes how to install the Websense® Enterprise software onto your system.

Installing the Websense Enterprise Software

Websense® Enterprise, working with Check Point™ FireWall-1® allows you to transparently analyze, manage, and report on traffic flowing from your internal networks to the Internet. Using pass-through technology, it is tightly integrated with Check Point FireWall-1, giving you the most accurate, reliable and scalable Internet filtering solution available.

The version of Websense Enterprise software used by your system is unchanged from the tar files found on the Websense website:

<http://www.websense.com>

Refer to this site for all Websense documentation.

To download the Websense software onto your system, complete the following:

- 1 Log into your system as root.
- 2 Locate the file `app-Websense-x.x-x.x.x.7xCOS.i686.rpm`¹ and execute the following command at the root prompt:

```
[root@xxxxx rpm]# rpm -i app-Websense-x.x-x.x.x.7xCOS.i686.rpm
```

You must now install the application as specified by Websense. The vendor files have been copied to `/usr/os/apps/Websense`.

`WebsenseEIM_Lnx_5.0.1.tar.gz` has already been expanded in the subdirectory `x_x_x`.

1 Refer to the 3COM Security Switch 6200 Product Release Notes for the correct software version and rpm file name.

7-2 Installing the WebSense Enterprise Software Onto Your System

3 Change to the following directory:

```
cd 5_0_1
```

4 Step through the Websense configuration, using the following command:

```
./install.sh
```

For further information on the Websense configuration, refer to the Websense documentation.

8

Installing the Squid Software Onto Your System

This chapter describes how to install the Squid software onto your system.

Installing the Squid Web Proxy Cache Software

The Squid software is a high-performance proxy caching server for web clients, supporting FTP, gopher, and HTTP data objects. Unlike traditional caching software, Squid handles all requests in a single, non-blocking, I/O-driven process.

Squid keeps meta data and especially hot objects cached in RAM, caches DNS lookups, supports non-blocking DNS lookups, and implements negative caching of failed requests.

Squid supports SSL, extensive access controls, and full request logging. By using the lightweight Internet Cache Protocol, Squid caches can be arranged in a hierarchy or mesh for additional bandwidth savings.

Squid consists of a main server program `squid`, a Domain Name System lookup program `dnsserver`, some optional programs for rewriting requests and performing authentication, and some management and client tools. When `squid` starts up, it spawns a configurable number of `dnsserver` processes, each of which can perform a single, blocking Domain Name System (DNS) lookup. This reduces the amount of time the cache waits for DNS lookups.

Installing the Squid Software

To install the Squid software onto your system, complete the following:

- 1 Log into your system as root.
- 2 Locate the file `app-squid-x.x-x.x.x.7xCOS.i686.rpm`¹ and execute the following command at the root prompt:

```
[root@xxxxxx root]# rpm -i app-squid-x.x-x.x.x.7xCOS.i686.rpm  
  
You must now install the application as specified by the vendor.  
The vendor files have been copied to /usr/os/apps/Squid.
```

- 3 Display the contents of the `/usr/os/apps/Squid` directory, using the following command, and locate the rpm file `squid-2.5.STABLE3-0.i386.rpm`:

```
[root@xxxxxx root]# ls /usr/os/apps/Squid/  
  
squid-2.5.STABLE3-0.i386.rpm
```

- 4 Change to the Squid directory, using the following command:

```
[root@xxxxxx root]# cd /usr/os/apps/Squid/
```

- 5 Install the Squid software, using the above rpm:

```
[root@xxxxxx Squid]# rpm -i squid-2.5.STABLE3-0.i386.rpm
```

For further information on the Squid Web Proxy Cache software configuration, refer to the Squid documentation.

¹ Refer to the 3COM Security Switch 6200 Product Release Notes for the correct software version and rpm file name.

Editing the Squid Configuration File

After you have installed the Squid software you need to define several features within the Squid configuration file. To do this, complete the following:

- 1 Change to the `/etc/squid` directory and open the `squid.conf` (`vi squid.conf`) file.
 - 2 Execute a search for “`http_port`” and hit next until the default value of `http_port 3128` appears.
 - 3 Enter a new line with a port value with no comments, as follows:

```
http_port 8080
```
 - 4 Execute a search for “`visible_hostname`” and hit next until the default value of `none` appears.
 - 5 Enter a line with a Squid hostname with no comments, as follows:

```
visible_hostname <hostname>
```
 - 6 Execute a search for “`http_access`” and hit next until the default value of “`http_access deny all`” appears.
 - 7 Enter a line with `http_access` value with no comments, as follows:

```
http_access allow all
```
 - 8 Save all changes using the following command:

```
wqa
```
 - 9 From the root prompt, execute the following command to start the Squid Web Proxy if the Squid proxy is not running:

```
/etc/rc.d/init.d/squid start
```
- or if the Squid proxy is running:
- ```
/etc/rc.d/init.d/squid restart
```



# 9

## Installing the Secure Computing's SmartFilter Software Onto Your System

This chapter describes how to install the Secure Computing's SmartFilter<sup>®</sup> software onto your system.

---

### Installing the Secure Computing SmartFilter Software

Secure Computing's SmartFilter<sup>®</sup> is a URL filtering software that enables you to build and enforce sophisticated Web-usage policies. Specifically, you can control access to specific Web sites.

For a complete list of SmartFilter supported features and for further information on the SmartFilter software, refer to Secure Computing WEB site.

[www.securecomputing.com](http://www.securecomputing.com)

To load the SmartFilter software onto your system, complete the following:

- 1 Log in to your system as root using the following commands:

```
cbs# unix su
Password:
[root@xxxxxx admin]#
```

- 2 Change to the rpm directory within root and list the files within this directory.

```
[root@xxxxxx admin]# cd /usr/os/rpm/
[root@xxxxxx rpm]# ls
```

- 3 Locate the file `app-smartfilter-x.x.x-x.x.x.7xCOS.i686.rpm`<sup>1</sup> and execute the following command at the root prompt:

<sup>1</sup> Refer to the 3COM Security Switch 6200 Product Release Notes for the correct software version and rpm file name.

## 9-2 Installing the Secure Computing's SmartFilter Software Onto Your System

---

```
[root@xxxxxx rpm]# rpm -i app-smartfilter-x.x.x-
x.x.x.x.7xCOsi686.rpm

2003/10/02 17:20:08| Creating Swap Directories

sfagent starting.

SmartFilter installed and started.
```

For further information on the SmartFilter software configuration, refer to the SmartFilter documentation.

# 10

## Installing the eSafe Software Onto Your System

This chapter describes how to install the eSafe software onto your system.

---

### Installing the eSafe Security Solution Software

eSafe is a comprehensive gateway-based security solution that addresses all content security layers. Specifically:

- Proactive anti-virus and malicious code protection engine that is ICSA and Checkmark certified.
- Anti-spam module utilizing multiple spam control methods including real-time black lists (RBL), DNS lookup, header verification and keyword filtering to keep spam to a minimum.
- Optional URL filtering module to keep out unwanted web content.

To install the eSafe Security Solution software onto your system, complete the following:

- 1 Log into your system as root.
- 2 Locate the file `app-esafe-x.x.x-x.x.x.7xCOS.i686.rpm`<sup>1</sup> and execute the following commands at the root prompt:

```
rpm -i app-esafe-x.x.x-x.x.x.7xCOS.i686.rpm
```

```
You must now install the application as specified by the vendor.
The vendor files have been copied to
/usr/os/apps/esafe.
```

```
You must now execute the rpm -i --nodeps command on the eSafe
rpm that is presented from the previous command.
```

<sup>1</sup> Refer to the 3COM Security Switch 6200 Product Release Notes for the correct software version and rpm file name.

## 10-2 Installing the eSafe Software Onto Your System

---

For further information on the eSafe Security Solutions software configuration, refer to the eSafe documentation.