



ADF V3.4 Security Services Switch Release Notes

Copyright © 2005, 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

1.0 Prerequisites.....	1
2.0 What's New	1
3.0 Application RPMs and Revision Levels.....	3
4.0 Configuration Considerations.....	4
4.1 ISS RealSecure Network Sensor	4
4.2 Check Point FireWall-1 and eConsole	4
5.0 Corrected Issues.....	5
5.1 V3.4.0	5
5.2 V3.3.0	5
5.3 V3.2.1	5
5.4 V3.2.0	5
6.0 Limitations.....	6
6.1 COS Security Services Switch	6
6.2 XOS Security Services Switch	6
6.3 Check Point Firewall-1	6
6.4 ISS RealSecure Network Sensor	6
6.5 Aladdin eSafe Security Solution	7
6.6 Secure Computing SmartFilter	8
6.7 Trend Micro IMSS	9
6.8 Trend Micro IWSS	9
6.9 Trend Micro VirusWall	9

ADF V3.4 Release Notes

This document provides important information about this release of the Applications Development Framework (ADF). Specifically, this document identifies the applications and system features which are supported on a full or partial basis, and also provides a list of known restrictions that exist with these applications.

1 Prerequisites

The applications in this ADF release can be installed on a Security Services Switch running the following versions of XOS or COS:

- XOS 5.1.x and 6.0.x
- COS 3.0.x

NOTE: COS 2.1.x must use ADF 2.6.x or below.

2 What's New

V3.4.0

The following applications have been updated to a newer version for the ADF 3.4.0 release. These applications are available on both COS and XOS systems.

- Websense Enterprise URL Filtering Version 5.5, which has the new option to be configured as a stand-alone product (called a Network Agent).
- SmartFilter V4.0, which contains the Squid application. If installing SmartFilter, you need to uninstall any existing version of Squid first.
- InterSpect V1.5, which is identical to InterSpect V1.5 on ADF 3.3, except that this release supports the Application Processor Module 8400 (APM4) released with XOS 6.0.0. Refer to the *Check Point InterSpect V1.5 for ADF 3.4 Release Notes*.

NOTE: Check Point VPN-1/Firewall-1 NG with Application Intelligence R55W (COS and XOS) was removed from ADF 3.4.

V3.3.0

The following items are supported in the 3.3.0 release:

- Check Point InterSpect V1.5 (XOS)
NOTE: The InterSpect application has its own set of documentation and release notes.
- Check Point VPN-1/Firewall-1 NG with Application Intelligence R55W (COS and XOS)
- Check Point VPN-1/Firewall-1 GX (COS and XOS)
- Ability to install multiple versions of FW1 (XOS)
- Trend Micro Anti-Virus IWSS Version 1.0. (COS)
- Added **Configure Check Point fwkern.conf file** to the Check Point Firewall-1 Configuration Options menu. This option allows you to edit a copy of **fwkern.conf** and save the change to each copy on each vAP.

NOTE: Check Point VPN-1 VSX NG with Application Intelligence is part of XOS and not ADF, beginning with XOS 5.1.4. To upgrade from VSX 2.0.1, refer to the VSX Installation Guide provided with the XOS release.

V3.2.1

The following items are either new or changed in the 3.2.1 release:

- VPN Accel RPM to COS for BroadCom driver
- VirusWall 3.8.1

V3.2.0

The following items are either new or changed in the 3.2.0 release:

XOS

- Check Point FireWall-1 NG AI R55 - minor fixes
- Snort 2.1.2 - updated version
- Secure Computing SmartFilter 3.2.1
- Squid - updated version and ICAP support
- eSafe - General Availability for NitroInspection and CVP mode
- Permeo 5.0.2 - General Availability
- Trend Micro's IMSS 5.5
- Trend Micro's IWSS 1.0.

COS

- Check Point FireWall-1 NG AI R55 - minor fixes
- Snort 2.1.2 - updated version
- Secure Computing SmartFilter 3.2.1.
- Squid - updated version and ICAP support
- Trend Micro IMSS 5.5
- eSafe - CVP General Availability (NitroInspection Not Supported)

3 Application RPMs and Revision Levels

This ADF revision uses the application RPMs and software revision levels listed in [Table 1](#) and [Table 2](#).

Table 1. XOS Switches

Application	Revision Level	rpm
Aladdin eSafe Security Solution (CVP or NitroInspection)	eSafe 4.0.420	app-esafe-4.0.420-3.2.0.6.7xXOS.i686.rpm
Argus Flow Monitor	Argus 2.0	app-argus-2.0-3.0.0.7.7xXOS.i686.rpm
Check Point Firewall-1 NG Feature Pack 3 and VPN-1	NG FP3	app-firewallng-FP3-2.2.2.14.7xXOS.i686.rpm
Check Point VPN-1/FireWall-1 NG AIR55	R55	app-firewallng-AIR55-1-3.4.0.*.7xXOS.i686.rpm
Check Point VPN-1/FireWall-1 GX	GX 2.5	app-firewall-GX-2.5-3.4.0.*.7xXOS.i686.rpm
Check Point InterSpect	InterSpect 1.5	app-InterSpect-1.5-3.4.0.*.7xXOS.i686.rpm
Enterasys Dragon IDS	Dragon 6.1.1	app-Dragon-6.1.1.B304-3.0.0.7.7xXOS.i686.rpm
Internet Security Systems RealSecure Network Sensor	ISS 7.0	app-ISS-7.0.2003.167-3.3.0.31.7xXOS.i686.rpm
Permeo	Permeo 5.0.2	app-permeo-5.0.2-3.2.0.6.7xXOS.i686.rpm
Secure Computing SmartFilter	SmartFilter 4.0	app-smartfilter-4.0-3.4.0.*.7xXOS.i686.rpm
Squid Web Proxy Cache	Squid 2.5	app-squid-2.5-3.4.0.*.7xXOS.i686.rpm
Snort Network Intrusion Detection System	Snort 2.1.2	app-Snort-2.2.0-3.4.0.*.7xXOS.i686.rpm
Trend Micro Anti-Virus VirusWall	Trend 3.8.1	app-VirusWall-3.81-3.2.1.6.7xXOS.i686.rpm
Trend Micro InterScan Messaging Security Suite (IMSS)	IMSS 5.5	app-IMSS-5.5-3.2.0.6.7xXOS.i686.rpm
Trend Micro InterScan Web Security Suite (IWSS)	IWSS 1.0	app-IWSS-2.0-3.4.0.*.7xXOS.i686.rpm
Websense Enterprise URL Filtering	Websense 5.5	app-Websense-5.5-3.4.0.*.7xXOS.i686.rpm

Table 2. COS Switches (Requires COS 2.3.x or Higher)

Application	Revision Level	rpm
Aladdin eSafe Security Solution (CVP only)	eSafe 4.0.420	app-esafe-4.0.420-3.2.0.6.7xCOS.i686.rpm
Check Point Firewall-1 NG Feature Pack 3 and VPN-1	NG FP3	app-firewallng-FP3-2.2.2.14.7xCOS.i686.rpm
Check Point VPN-1/FireWall-1 NG AIR55	R55	app-firewallng-AIR55-1-3.4.0.*.7xCOS.i686.rpm
Check Point VPN-1/FireWall-1 GX	GX 2.5	app-firewall-GX-2.5-3.4.0.*.7xCOS.i686.rpm
Enterasys Dragon IDS	Dragon 6.1.1	app-Dragon-6.1.1.B304-3.0.0.7.7xCOS.i686.rpm
Internet Security Systems RealSecure Network Sensor	ISS 7.0	app-ISS-7.0.2003.167-3.3.0.31.7xCOS.i686.rpm
Secure Computing SmartFilter	SmartFilter 4.0	app-smartfilter-4.0-3.4.0.*.7xCOS.i686.rpm
Squid Web Proxy Cache	Squid 2.5	app-squid-2.5-3.4.0.*.7xCOS.i686.rpm
Snort Network Intrusion Detection System	Snort 2.1.2	app-Snort-2.2.0-3.4.0.*.7xCOS.i686.rpm
Trend Micro Anti-Virus VirusWall	Trend 3.8.1	app-VirusWall-3.81-3.2.1.6.7xCOS.i686.rpm
Trend Micro InterScan Messaging Security Suite (IMSS)	IMSS 5.5	app-IMSS-5.5-3.2.0.6.7xCOS.i686.rpm
Trend Micro InterScan Web Security Suite (IWSS)	IWSS 1.0	app-IWSS-2.0-3.4.0.*.7xCOS.i686.rpm (Requires COS 3.0.0 or Higher)
Websense Enterprise URL Filtering	Websense 5.5	app-Websense-5.5-3.4.0.*.7xCOS.i686.rpm

4 Configuration Considerations

4.1 ISS RealSecure Network Sensor

When installing the ISS Gigabit driver, included with ISS RealSecure Network Sensor, the following configuration considerations must be used.

- AP modules that run the ISS Gigabit driver must have at least 512 MB RAM.

4.2 Check Point FireWall-1 and eConsole

When a FireWall-1 application is between the eSafe gateway and the system running the eConsole, the connection may be dropped by the FireWall if there is no activity on the connection. To avoid this problem, do not setup your FireWall to be between the eSafe gateway and the system running the eConsole.

5 Corrected Issues

The following sections lists the issues that were corrected in each release.

5.1 V3.4.0

The following issues have been corrected in the 3.4.0 release.

When installing the Check Point NG AI R55 RPM file to XOS after FP3 is installed, R55 is considered an older version than FP3.	4286
When uninstalling a Check Point Firewall-1 application, the installation program may not prompt the user to reboot.	4686
Postfix does not start after installing IMSS. The vAP group or COS switch needs to be rebooted.	4740
Changing the SmartFilter password on an XOS system using the XOS CLI leaves the wrong ownership of the <code>/etc/squid/etc/sfagent.txt</code> file. To change the password, run the <code>sfagent -p <newpass></code> command directly on the vAP.	4744
The COS installation program installs Performance Pack for a Check Point Firewall-1 application when it should not.	4859
The COS installation program asks for the directory from where it can install applications, even when the user wants to uninstall an application.	5428

5.2 V3.3.0

The following issues have been corrected in the 3.3.0 release.

Using Firewall-1 in a High Availability configuration causes mis-matched MAC errors.	3281
Using Firewall-1 NG with Application Intelligence in a Dual Box High Availability configuration, the sync over external interface does not work.	3957
Firewall-1 NG with Application Intelligence R55 does not start SXL. When started manually, it disables the templates.	4020
The COS installation does not install the latest SXL and PPak RPMs.	4048
ISS will not install on COS.	4054
The COS turn-key solution does not uninstall the Squid package.	4946
The XOS installation script for ISS does not prompt for the Gig driver installation.	5242

5.3 V3.2.1

The following issues have been corrected in the 3.2.1 release.

<code>cos_apps_install.sh</code> does not copy <code>vpn_accel.conf</code> to the fw boot dir.	5049
<code>cos_apps_install.sh</code> needs to add support for FP3 to install <code>CPacc2-10-00.i386.rpm</code> .	5056

5.4 V3.2.0

The following issues have been corrected in the 3.2.0 release.

VPN (FP3) does not work with SecureXL.	2835
--	------

The fwaccel conns command brings down Firewall-1 FP3.	3372
eSafe startup script may cause a system hang.	3849
Squid application does not configure the local disk automatically	3968
The application-update command fails when multiple applications are installed on a vAP group.	4037
Check Point processes may hang when a vAP is reset.	4217

6 Limitations

6.1 COS Security Services Switch

When installing any application, the COS Installation program will reinstall any application that has already been installed. Before installing an application, move the rpm file of each application that is currently installed to another directory. You can move the files back once you have completed the installation.

6.2 XOS Security Services Switch

If AP modules are reset by pulling them from the chassis or by hitting the reset button, it sometimes results in the magic number corruption in certain files. This is visible in the FireWall-1 log, or when you stop/start the FireWall. The workaround is to remove the file causing the problem and restart FireWall-1.

6.3 Check Point Firewall-1

The following items only apply when running on an XOS system.

- When eth0 is used for FireWall-1 synchronization there is a chance of a loss of heartbeats which may lead to AP and NP module reboots. To correct this problem, use the XOS switch's data plane internal or external interfaces as the sync network.
- When a configuration is set to have packets from the PIM Source be NAT'd behind the IP of the FireWall, the NATing does not occur. There is no workaround.
- The Expect script (used to configure Check Point FireWall-1 for vAP) does not allow installation of the same version of FireWall on different vAP groups simultaneously. You must install the applications one at a time.

6.4 ISS RealSecure Network Sensor

When install on an XOS system, the ISS Gigabit driver prevents Killer packets from being sent. To correct this problem send the Killer packets over one of the VND that sits over the SDP. For example:

```
Selected Adapter:
RealSecure(R) PRO/1000 High Performance Driver [ISSE1000_S_1]

Adapter to send kills:
Linux Ring-buffer High Performance Driver [vnd1032-p]
```

6.5 Aladdin eSafe Security Solution

CVP

- The Firewall-1 application cannot connect to the eSafe CVP server on an XOS system, since the CVP process is listening on the wrong interface. To correct this problem:
 - a. Stop eSafe by running the following CLI command:


```
application esafe vap-group <vap-group-name> stop
```
 - b. On each vAP, edit the `/opt/eSafe/eSafeCR/esafecfg.ini` file and change the following line:


```
CVP Server IP Address=  
CVP Server IP Address=3.0.0.100
```

 Where "3.0.0.100" is the IP address of the interface you wish to use.
 - c. Restart eSafe by running the following CLI command:


```
application esafe vap-group <vap-group-name> start
```

NitroInspection Router

These limitations only occur on an XOS system.

- The XOS system cannot be upgraded while the eSafe NitroInspection Router application is installed. You must uninstall eSafe before you attempt the upgrade.
- If the eSafe NitroInspection Router application is over utilized it may crash. If more than one vAP is running eSafe, one crash may eventually cause all of the vAPs to reset. To avoid this problem, install the latest hot fix from eSafe.
- With eSafe NitroInspection installed on a vAP and high volumes of traffic being sent, the AP module resets. To correct this problem, execute the following command, at the UNIX prompt, on the AP module:


```
echo "1 7 1 7" >/proc/sys/kernel/printk
```
- With eSafe NitroInspection installed, the following error message occurs. This is an erroneous message and can be ignored.


```
sendmail: No such file or directory
```

CVP or NitroInspection Router

- The eSafe Nitro-Inspection and CVP applications do not run on XOS dual-CPU AP modules.
- The eSafe application using three simultaneous users fails and restarts (on either an XOS or COS system). To correct this, complete the following in the eConsole:
 - a. Go to **Options... Configuration... Administration... Updates**.
 - b. Enable the Service Pack checkbox, and enter "cr_hotfix_lin_0400420002.upd" in the text box.
 - c. Click on Update Now. It will take a few minutes to update and restart eSafe.
 - d. To confirm the update, go into eConsole and click on Help... Product And Registration Information and check the Currently Installed Hotfixes field.

- Executing eSafe’s Update Now program on either an XOS or COS system fails with no error message. To update the eSafe application:
 - a. Stop the eSafe service, using the following command:


```
/opt/eSafe/esgstop
```
 - b. Edit the file **/opt/eSafe/eSafeCR/esafecfg.ini**, making sure that all update types in the file are set to 0, with the exception of the “Update virus tables=1” and “Update restricted List=1”.


```
[PRODUCT UPDATE]
Update virus tables=1
Update restricted Lists=1
Update product=0
Update restricted URLs list=0
OS=0
HotFix=
root update module=0
scripts update module=0
report update check=0
```
 - c. Start the eSafe service, using the following command:


```
service /opt/eSafe/esgstart
```
 - d. Force an update through the Update Now option on eConsole.

NOTE: For XOS systems, each vAP group must be updated.

6.6 Secure Computing SmartFilter

- If Squid is installed when you install SmartFilter on the same AP local disk, Squid will start up and exit. Make sure that you completely uninstall Squid before installing SmartFilter. You may need to manually delete the Squid directory.
- If you require Transparent Authentication (also known as Integrated Authentication), you need to install Samba and its supporting libraries. Transparent Authentication means each time the user opens the browser they will not be prompted for the username and password. Contact Customer Support for the Samba and lib tar file. Once you have this file, perform the following:
 - a. FTP the `sambalibs.tar` file and untar it.


```
# tar -xvf sambalibs.tar
```
 - b. Install the individual rpms:


```
[root@xxxxxx bin]# rpm -Uvh krb5-libs-1.2.4-1.i386.rpm
[root@xxxxxx bin]# rpm -Uvh libjpeg-6b-19.i386.rpm
[root@xxxxxx bin]# rpm -Uvh libpng-1.0.12-2.i386.rpm
[root@xxxxxx bin]# rpm -Uvh libtiff-3.5.7-2.i386.rpm
[root@xxxxxx bin]# rpm -Uvh cups-libs-1.1.14-15.i386.rpm
[root@xxxxxx bin]# rpm -Uvh samba-3.0.10-1.i386.rpm
```

6.7 Trend Micro IMSS

IMSS does not start properly on a COS system. After installing the IMSS application, reboot your COS system.

6.8 Trend Micro IWSS

IWSS fails to start on boot on an XOS system. To avoid this problem, set the delay-flow to 240 seconds on each vAP group running IWSS, using the XOS CLI.

6.9 Trend Micro VirusWall

Trend Micro VirusWall SMTP on either an XOS or COS system is only supported with a remote server and not a local server.

