Release Notes:
ProCurve Network Immunity Manager Version 1.05, Update 1

ProCurve Network Immunity Manager (NIM) version 1.05, Update 1 supports these products:

- J9060A ProCurve Network Immunity Manager 1.0 - 50-device license
- J9061A ProCurve Network Immunity Manager 1.0 - +100-device license
- J9062A ProCurve Network Immunity Manager 1.0 - unlimited device license

Network Immunity Manager is an add-on module to PCM+ 2.2 or later. If you are using a version of PCM or PCM+ earlier than PCM 2.3, you must first upgrade to PCM 2.3 and install PCM 2.3 Auto Update 2 before you can apply the fixes included in this update.

These release notes include information on the following:

Related Publications

For the latest version of any of the publications listed below, visit the ProCurve Networking Web site at **http://www.procurve.com**. Click on **Technical support**, then **Product manuals**.

- ProCurve Network Immunity Manager
- Read Me First for the ProCurve Manager, Version 2.3
- ProCurve Network Management Getting Started Guide
- ProCurve Manager Plus 2.3 Network Administrator's Guide

Publication Number

5991-8587
March 10, 2008

Applicable Products

- J9060A ProCurve Network Immunity Manager 1.0 - 50-device license
- J9061A ProCurve Network Immunity Manager 1.0 - +100-device license
- J9062A ProCurve Network Immunity Manager 1.0 - unlimited device license

Trademark Credits

Microsoft®, Windows®, and Windows NT® are US registered trademarks of Microsoft Corporation. Adobe® and Acrobat® are trademarks of Adobe Systems Incorporated. Java™ is a US trademark of Sun Microsystems, Inc.

Software Credits

SSH on ProCurve Switches is based on the OpenSSH software toolkit. This product includes software developed by the OpenSSH Project for use in the OpenSSH Toolkit. For more information on OpenSSH, visit

http:// www.openssh.com.

SSL on ProCurve Switches is based on the OpenSSL software toolkit. This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. For more information on OpenSSL, visit

http://www.openssl.org.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com)

Disclaimer

HEWLETT-PACKARD COMPANY MAKES NO WARRANTY OF ANY KIND WITH REGARD TO THIS MATERIAL, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. Hewlett-Packard shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this material.

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Hewlett-Packard assumes no responsibility for the use or reliability of its software on equipment that is not furnished by Hewlett-Packard.

Warranty

See the Customer Support/Warranty booklet included with the product.

A copy of the specific warranty terms applicable to your Hewlett-Packard products and replacement parts can be obtained from your HP Sales and Service Office or authorized dealer.

Hewlett-Packard Company
8000 Foothills Boulevard, m/s 5551
Roseville, California 95747-5551
www.procurve.com

Software Management – NIM 1.05 Update 1

ProCurve Manager 2.3 Update 2 must be installed before installing this ProCurve Network Immunity Manager 1.05 update. Once you have installed the ProCurve Manager update, you can install this update using the "Automatic Update" feature in PCM+, or you can install it manually.

To verify if the Update has already been installed, look in the Update History window under the PCM Global Preferences:

[Tools->Preferences->Automatic Updates->Update History]

Using the PCM Automatic Update to Install

1. Open the Preferences panel in the PCM Client and select the **Automatic Updates** node.
2. Click the **Check Now** button. A dialog appears with a list of the available update(s).
3. Select the update, ensure that the **install** checkbox is enabled and click the **Next** button.
4. A warning message appears, advising you that any PCM clients will be disconnected. Click **OK** to continue.
5. After the update package is downloaded, you will be prompted to close the PCM Client. Click **OK** to close the pop-up, then close the Preferences window and exit PCM.

The update will be applied and the PCM services restarted. Once this is done you can reconnect with the PCM client and begin using the updated version of Network Immunity Manager.

Using the Manual Process to Install

1. Copy the nim_1_0_5_update_1.zip file to the \PNM\server\data\download\autoupdate directory.* (Do not unzip the file.)
2. Open the Preferences panel in the PCM Client and select the **Automatic Updates** node to display the Global:Automatic Updates panel.
3. Click the **Check Now** button at the bottom of the panel to display the **Select update mode:** dialog.
4. Select the **Check for updates in PCM's download folder** option and press **Next**.
5. You should see the new auto-update presented for installation, and you can continue with the Update installation (steps 3 through 5 above).
6. Restart the client and verify that the update was applied by checking the **Update History** node located under the Automatic Updates preference node.

* The default PCM server installation directory is: C:\Program Files\Hewlett-Packard\PNM\server on the workstation where PCM was initially installed.

NIM 1.05 Enhancements

Update 1 Enhancements

- AntiVirus (AV) and Intrusion Prevention Service (IPS) support for the SonicWALL E-Class Network Security Appliance (NSA) series, version 5.0.0.7-44o of the SonicOS Enhanced firmware. This support gives PCM and Network Immunity Manager the ability to process AV and IPS SonicWALL traps and take action, as configured by the user. These appliances prevent damaging, content-based threats from email and web traffic such as viruses, worms, intrusions, and inappropriate web content. For additional SonicWALL support information, see the Network Immunity Manager Implementation Guide (accessible by registering at my.procurve.com).

  SonicWALL appliances are automatically discovered by PCM. However, you must configure the following PCM setting for proper operation:

  - If the UTM is configured with a unique read and write community name (other than PCM's default of public), configure the community names in PCM.
  - Configure the switch port connected to the UTM as a member of each VLAN where attacker or victim traffic might originate.

Note: All discovered UTMs, regardless of vendor, are placed in the UTM folder in the PCM navigation tree. Although PCM discovers SonicWALL appliances, they are not included in Network Maps. Instead, they appear in the unmapped devices section.

Software Fixes in NIM Updates

Update 1

The following Network Immunity Manager problems were resolved in Network Immunity Manager Update 1

- **Policies (PR_1000769295)** — NIM policies do not activate for null IP addresses.

Known Issues for NIM 1.05 Update 1

General

- Extremely long policy names are truncated in reports.
- Pressing the Ctrl (control) key while a PCM or Network Immunity Manager report is displayed causes a java script error.