# Contents

**Preface**  
Overview ................................................................. vii  
How to Use Proventia Network ADS Documentation .......................... viii  
Conventions Used in this Guide ........................................... ix  
Getting Technical Support ................................................. x  

**Chapter 1: Introduction to Proventia Network ADS**  
Overview ................................................................. 13  
Appliances and Deployment Modes ........................................ 14  
Analyzer Ports Diagram ................................................ 16  
Collector Ports Diagram ................................................. 17  
Recommended Firewall Port Configuration ............................... 19  

**Chapter 2: Using the Command Line Interface (CLI)**  
Overview ................................................................. 21  
Connecting the Serial Cable for CLI Setup .............................. 22  
Ports Used by Proventia Network ADS .................................. 24  
Using CLI Commands .................................................... 26  

**Chapter 3: Upgrading and Reinstalling Proventia Network ADS**  
Overview ................................................................. 29  
Reinstallation Requirements .............................................. 30  
Reinstalling an Appliance ............................................... 31  
Upgrading Appliances to Proventia Network ADS Version 3.6.1 ...... 34  

**Chapter 4: Configuring External Flow Storage**  
Overview ................................................................. 37  
About Proventia Network ADS External Flow Storage .................. 38  
Configuring the External Disk .......................................... 39  
Removing a Fibre Channel Disk ......................................... 41  

**Chapter 5: Configuring DHCP for Identity Tracking**  
Overview ................................................................. 43  
About Identity Tracking with DHCP .................................... 44  
Configuring DHCP for Identity Tracking ............................... 45  

**Chapter 6: Configuring TACACS+ and RADIUS**  
Overview ................................................................. 47  
Configuring TACACS+ Integration ...................................... 48  
Configuring RADIUS Integration ....................................... 50  
Setting the Method for TACACS+ and RADIUS ....................... 52  

**Chapter 7: Configuring Flow**  
Overview ................................................................. 55  
Configuring Flow on Collectors ........................................ 56  
Configuring NetFlow for Cisco IOS ..................................... 57  
Configuring Cflowd for JunOS ......................................... 59  
Configuring sFlow ..................................................... 63  
Configuring SNMP Polling on Collectors .............................. 65
Chapter 8: Configuring NetScout Integration
Overview ........................................................................................................... 67
Configuring NetScout Probes ........................................................................... 68
Configuring Proventia Network ADS ............................................................... 69
Testing and Viewing the NetScout Probe Flow Collection ............................... 70

Chapter 9: Creating User Groups
Overview ........................................................................................................... 71
About User Groups .......................................................................................... 72
Creating User Groups ...................................................................................... 73
Editing User Groups ....................................................................................... 74
Deleting User Groups ..................................................................................... 78
Adding Users to User Groups ......................................................................... 79

Chapter 10: Configuring ATF Settings
Overview ........................................................................................................... 81
About ATF Behaviors ...................................................................................... 82
Setting a Proxy Server ..................................................................................... 83
Enabling and Updating the Poll Interval ........................................................ 84
Manually Updating the ATF Data .................................................................... 85

Chapter 11: Configuring Check Point for Safe Quarantine
Overview ........................................................................................................... 87
About Check Point Integration ........................................................................ 88
Configuring the Check Point Console ............................................................. 89
Preparing to Configure Check Point on the Proventia Network ADS Analyzer ................................................................................................. 96

Chapter 12: Using the CLI to Capture Flow Data
Overview ........................................................................................................... 97
Watching Flows ............................................................................................... 98
Viewing Flow Summaries ............................................................................. 99
FCAP Flow Filters .......................................................................................... 102

Chapter 13: Manually Installing Proventia Network ADS on your Appliances
Overview ........................................................................................................... 103
Task Overview for Manual Installation ........................................................... 104
Determining the Mode and Setting Up Communication ................................... 106
Configuring Interfaces ................................................................................... 108
Setting the System Name and Default Route ................................................ 110
Setting up Services for Remote Access ........................................................ 111
Configuring Access Rules ............................................................................ 112
Setting up Domain Name Services and SMTP .............................................. 113
Changing the Administrative Password ....................................................... 114
Setting System Time ..................................................................................... 115
Saving the Configuration Changes and Starting Proventia Network ADS . . . 117
Configuring Additional Optional Settings .................................................... 118

Appendix A: Notification Formats
Overview .......................................................................................................... 121
Email Notification Examples .......................................................................... 122
Syslog Notifications ...................................................................................... 125

Appendix B: Commands in the /services/ads Menus
Overview .......................................................................................................... 127
Commands in the /services/ads Menu ............................................................ 128
Subcommands in the /services/ads Menu ...................................................... 129
Preface

Overview

Introduction
This guide includes instructions for additional optional configuration for your Proventia Network ADS Analyzer and Collectors. For initial installation instructions, see the Proventia Network ADS 3.6 Quick Start Card.

Audience
This guide is intended for network operators who use Proventia Network ADS to secure their network. Users should have working knowledge of their network security policies and network configuration.

Scope
This guide supports the 3.6.1 release for the Proventia Network ADS Analyzer and Collector appliances.
How to Use Proventia Network ADS Documentation

Using this guide: Please read this guide before you install or operate this product. An overview of the setup process and a checklist is provided to help you gather and record required information. ISS recommends that you review the network deployment diagrams, prerequisites, and considerations before you begin the setup process.

Related publications: For more information, see the following:

<table>
<thead>
<tr>
<th>Document</th>
<th>Contents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proventia Network ADS User Guide</td>
<td>Instructions for and information about using your Proventia Network ADS appliances in the Web user interface.</td>
</tr>
<tr>
<td>Proventia Network ADS Quick Start Card</td>
<td>Instructions for and information about connecting, starting, and setting up your appliances using the Setup Wizard.</td>
</tr>
</tbody>
</table>

Table 1: Related documents

Additional documentation: Additional ISS documentation is available on the ISS Web site:

http://www.iss.net/support/documentation
Conventions Used in this Guide

Introduction
This topic explains the typographic conventions used in this guide to make information in procedures and commands easier to recognize.

In procedures
The typographic conventions used in procedures are shown in the following table:

<table>
<thead>
<tr>
<th>Convention</th>
<th>What it Indicates</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bold</td>
<td>An element on the graphical user interface.</td>
<td>Type the computer’s address in the IP Address box.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Select the Print check box.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Click OK.</td>
</tr>
<tr>
<td>SMALL CAPS</td>
<td>A key on the keyboard.</td>
<td>Press ENTER.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Press the PLUS SIGN (+).</td>
</tr>
<tr>
<td>Constant width</td>
<td>A file name, folder name, path name, or other information that you must type exactly as shown.</td>
<td>Save the User.txt file in the Addresses folder.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Type IUSR_SMA in the Username box.</td>
</tr>
<tr>
<td>Constant width italic</td>
<td>A file name, folder name, path name, or other information that you must supply.</td>
<td>Type Version number in the Identification information box.</td>
</tr>
<tr>
<td>➔</td>
<td>A sequence of commands from the taskbar or menu bar.</td>
<td>From the taskbar, select Start ➔ Run.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>On the File menu, select Utilities ➔ Compare Documents.</td>
</tr>
</tbody>
</table>

Table 2: Typographic conventions for procedures

Command conventions
The typographic conventions used for command lines are shown in the following table:

<table>
<thead>
<tr>
<th>Convention</th>
<th>What it Indicates</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Constant width bold</td>
<td>Information to type in exactly as shown.</td>
<td>md ISS</td>
</tr>
<tr>
<td>Italic</td>
<td>Information that varies according to your circumstances.</td>
<td>md your_folder_name</td>
</tr>
<tr>
<td>[ ]</td>
<td>A set of choices from which you must choose one.</td>
<td>% chmod {u g o a}={r w x} file</td>
</tr>
</tbody>
</table>

Table 3: Typographic conventions for commands
Getting Technical Support

Introduction

ISS provides technical support through its Web site and by email or telephone.

The ISS Web site

The Internet Security Systems (ISS) Resource Center Web site (http://www.iss.net/support/) provides direct access to frequently asked questions (FAQs), white papers, online user documentation, current versions listings, detailed product literature, and the Technical Support Knowledgebase.

Support levels

ISS offers three levels of support:

- Standard
- Select
- Premium

Each level provides you with 24-7 telephone and electronic support. Select and Premium services provide more features and benefits than the Standard service. Contact Client Services at clientservices@iss.net if you do not know the level of support your organization has selected.

Hours of support

The following table provides hours for Technical Support at the Americas and other locations:

<table>
<thead>
<tr>
<th>Location</th>
<th>Hours</th>
</tr>
</thead>
<tbody>
<tr>
<td>Americas</td>
<td>24 hours a day</td>
</tr>
<tr>
<td>All other locations</td>
<td>Monday through Friday, 9:00 A.M. to 6:00 P.M. during their local time, excluding ISS published holidays</td>
</tr>
</tbody>
</table>

Note: If your local support office is located outside the Americas, you may call or send an email to the Americas office for help during off-hours.

Table 4: Hours for technical support

Contact information

The following table provides electronic support information and telephone numbers for technical support requests:

<table>
<thead>
<tr>
<th>Regional Office</th>
<th>Electronic Support</th>
<th>Telephone Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>North America</td>
<td>Connect to the MYISS section of our Web site: <a href="http://www.iss.net">www.iss.net</a></td>
<td>Standard: (1) (888) 447-4861 (toll free) (1) (404) 236-2700</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Select and Premium: Refer to your Welcome Kit or call your Primary Designated Contact for this information.</td>
</tr>
<tr>
<td>Latin America</td>
<td><a href="mailto:support@iss.net">support@iss.net</a></td>
<td>(1) (888) 447-4861 (toll free) (1) (404) 236-2700</td>
</tr>
</tbody>
</table>

Table 5: Contact information for technical support
### Regional Office

<table>
<thead>
<tr>
<th>Regional Office</th>
<th>Electronic Support</th>
<th>Telephone Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Europe, Middle East, and Africa</td>
<td><a href="mailto:support@iss.net">support@iss.net</a></td>
<td>(44) (1753) 845105</td>
</tr>
<tr>
<td>Asia-Pacific, Australia, and the Philippines</td>
<td><a href="mailto:support@iss.net">support@iss.net</a></td>
<td>(1) (888) 447-4861 (toll free) (1) (404) 236-2700</td>
</tr>
<tr>
<td>Japan</td>
<td><a href="mailto:support@isskk.co.jp">support@isskk.co.jp</a></td>
<td>Domestic: (81) (3) 5740-4065</td>
</tr>
</tbody>
</table>

**Table 5: Contact information for technical support (Continued)**
Chapter 1

Introduction to Proventia Network ADS

Overview

Introduction

This guide assumes that you have already configured the basic settings on your Proventia Network ADS Analyzer and covers only optional additional settings. This chapter provides background information you should review before you configure these optional settings in the CLI.

Reference: If you have not configured the basic settings on your appliances or using the Web-based Setup Wizard for initial installation, see the Proventia Network ADS Quick Start Card that was included in your appliance package.

In this chapter

This chapter contains the following topics:

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Appliances and Deployment Modes</td>
<td>14</td>
</tr>
<tr>
<td>Analyzer Ports Diagram</td>
<td>16</td>
</tr>
<tr>
<td>Collector Ports Diagram</td>
<td>17</td>
</tr>
</tbody>
</table>
Appliances and Deployment Modes

Introduction
The deployment mode you choose is based upon the number and types of appliances you are deploying. The main difference between the modes is that Standalone mode does not require Collector appliances, whereas Two-tier mode does.

Appliance types
The two types of Proventia Network ADS appliances are as follows:

- The Analyzer is a 2U appliance that stores network traffic databases, generates alerts, and provides the primary Web user interface.
- The Collectors are 1U appliances that accept and process network traffic data and report summary information to the Proventia Network ADS Analyzer appliance.

Standalone mode
Standalone mode is for smaller deployments in which an Analyzer collects network flow information without using a Collector. In this mode, the Analyzer collects data from up to three flow sources, and accepts raw packet data from network SPAN ports or TAPs.

Two-tier mode
Two-tier mode is for large deployments using both Analyzer and one or more Collector appliances. In this type of deployment, network flow information and raw packet data from SPAN ports or TAPs is directed to Collector appliances. The Collector appliances then forward consolidated traffic data to an Analyzer appliance.
The Collectors can collect information from a variety of flow sources, depending upon the Collector models and the number of Collectors deployed.

**Two-tier mode diagram**

An example of a two-tier mode deployment is shown in Figure 2:

---

**Figure 2:** Two-tier mode deployment
Chapter 1: Introduction to Proventia Network ADS

Analyzer Ports Diagram

Overview
This topic describes the Analyzer ports and includes a diagram of the back panel for reference.

Analyzer back panel diagram
The back panel of the Proventia Network ADS Analyzer appliance is shown in Figure 3:

![Analyzer appliance back panel diagram](image)

Figure 3: Analyzer appliance back panel diagram

The back panel includes the following:

- Serial console port (RJ-45)
- Management/NetFlow Ethernet port
- Packet capture Ethernet port for Standalone mode
- two AC power connections

Analyzer interfaces and ports
Within the Proventia Network ADS application, the Ethernet ports are referenced by their hardware identifiers. Table 6 shows the correct correlation between the hardware identifiers and the appliance labels:

<table>
<thead>
<tr>
<th>Hardware Identifier</th>
<th>Back Panel Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>e3/4/0</td>
<td>Management/NetFlow port</td>
</tr>
<tr>
<td>e3/4/1</td>
<td>Packet capture port for Standalone mode</td>
</tr>
</tbody>
</table>

Table 6: Port representations
Collector Ports Diagram

Introduction

This topic describes the Collector ports and includes a diagram of the back panel for reference.

Collector back panel diagram

The back panel of the Proventia Network ADS Collector appliance is shown in Figure 4:

![Collector back panel diagram]

Figure 4: Back panel description of Collectors

The back panel includes the following:

- Serial console port (RJ-45)
- Management/NetFlow Ethernet port
- optional NetFlow Ethernet port
- four packet capture Ethernet ports
- AC power connection

Collector interfaces and ports

Within the Proventia Network ADS application, the Ethernet ports are referenced by their hardware identifiers. Table 7 shows the correct correlation between the hardware identifiers and the appliance labels:

<table>
<thead>
<tr>
<th>Hardware Identifier</th>
<th>Back Panel Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>e3/4/0</td>
<td>Management/NetFlow port</td>
</tr>
<tr>
<td>e3/4/1</td>
<td>Optional NetFlow port</td>
</tr>
</tbody>
</table>

Table 7: Port representations on the Collector appliances

Flow source limits

The number of flow sources you can have depends upon the Collector model you have purchased. Table 8 shows the maximum number of flow sources per Collector model:

<table>
<thead>
<tr>
<th>Model</th>
<th>Description and Maximum Number of Flow Sources</th>
</tr>
</thead>
<tbody>
<tr>
<td>AD3000</td>
<td>Packet Collector appliance (0 flow sources)</td>
</tr>
</tbody>
</table>

Table 8: Collector models
## Model Description and Maximum Number of Flow Sources

<table>
<thead>
<tr>
<th>Model</th>
<th>Description and Maximum Number of Flow Sources</th>
</tr>
</thead>
<tbody>
<tr>
<td>AD3007</td>
<td>Flow/Packet Collector (7 flow sources)</td>
</tr>
<tr>
<td>AD3014</td>
<td>Flow/Packet Collector (14 flow sources)</td>
</tr>
<tr>
<td>AD3020</td>
<td>Flow/Packet Collector (20 flow sources)</td>
</tr>
</tbody>
</table>

*Table 8: Collector models (Continued)*
Recommended Firewall Port Configuration

**Introduction**
If you have firewalls in between the appliances, you must open the ports on the firewall to ensure that your deployment of ADS is successful.

**Firewall ports diagram**
An example of a typical Proventia Network ADS deployment and the traffic that flows between the devices is shown in Figure 5. Use this diagram as a guide to configure access rules in any firewalls you may have in your network:

![Firewall ports diagram](image)

**Figure 5: Typical Proventia Network ADS port usage**

**Additional port information**
Proventia Network ADS might use additional ports in certain situations.

**Reference:** See Table 9 on page 24 for a list of the ports and how they are used.
Chapter 2

Using the Command Line Interface (CLI)

Overview

Introduction

This chapter provides the instructions for connecting to and using the CLI. Although ISS recommends using the Web-based setup wizard to complete the initial setup of your appliances, you might want to use the CLI to perform the following tasks:

- reinstalling an appliance
- moving and restarting an appliance
- configuring settings available only in the CLI

In this chapter

This chapter contains the following topics:

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connecting the Serial Cable for CLI Setup</td>
<td>22</td>
</tr>
<tr>
<td>Ports Used by Proventia Network ADS</td>
<td>24</td>
</tr>
<tr>
<td>Using CLI Commands</td>
<td>26</td>
</tr>
</tbody>
</table>
Connecting the Serial Cable for CLI Setup

Introduction
You can use the CLI to manually install an appliance or to configure additional settings after using the Web-based Setup Wizard.

Using the correct serial cable
To use the serial console, you must connect the appliance to the console with a null modem (RJ-45) cable. This type of cable is not included in your appliance packages. If you do not have an RJ-45 serial cable, contact ISS to purchase one.

Terminal emulation
If you are configuring an appliance for the first time or reinstalling the software on a Proventia Network ADS Analyzer, you can either connect directly to the appliance or establish a connection to the appliance using a compatible terminal emulator, such as Hyperterminal.

Setting up terminal emulation
To set up terminal emulation and connect to the appliance:

1. In the Hyperterminal application, go to FileÆPropertiesÆSettings.
2. Select Emulation=AutoDetect.
3. Click OK.

Connecting the appliance to a computer or laptop
To connect the appliance to a computer or laptop:

1. Plug one end of the serial cable into the serial port on the back of the appliance.
   Reference: See Figure 3 on page 16 for the Analyzer appliance, and Figure 4 on page 17 for the Collector appliances.
2. Plug the other end of the serial cable into the serial port on your computer or laptop.
3. Plug the AC Power connector into the back of the appliance where indicated in Figure 3 on page 16, and then plug the other end into a standard AC receptacle.
4. Turn on the appliance, and then start your computer.
5. Use a terminal emulation program, such as Hyperterminal, to create a connection to the appliance with the following settings:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bits per second</td>
<td>9600</td>
</tr>
<tr>
<td>Data bits</td>
<td>8</td>
</tr>
<tr>
<td>Parity</td>
<td>None</td>
</tr>
<tr>
<td>Stop bits</td>
<td>1</td>
</tr>
<tr>
<td>Flow control</td>
<td>None</td>
</tr>
<tr>
<td>Communications Port</td>
<td>Typically COM1, but this depends on the computer you are using.</td>
</tr>
</tbody>
</table>

Note: If you are not using the Hyperterminal program, then your settings may be different. For more information, refer to the documentation for your program.

6. To connect to the network, connect an Ethernet cable between the Analyzer management port on the back panel of the Analyzer appliance and the network you will use to manage it.
Logging on

To log on to the appliance:

1. Turn on the appliance.
2. Start your terminal emulator.
3. At the login prompt, type admin for the user name, and then press ENTER.
4. Type admin for the password, and then press ENTER.
5. Proceed to Chapter 13, "Manually Installing Proventia Network ADS on your Appliances" for instructions about configuring or changing settings in the CLI.
Chapter 2: Using the Command Line Interface (CLI)

Ports Used by Proventia Network ADS

**Introduction**

Proventia Network ADS uses specific ports for each of the services it allows.

**Firewall port configuration**

If you have firewalls in between your appliances, you must open the ports on the firewall to ensure that your appliances can forward and receive data.

**Reference:** See Figure 5 on page 19 for a diagram of the ports that you can reference to configure access rules in any firewalls you have.

**Ports table**

The ports Proventia Network ADS uses are as follows:

<table>
<thead>
<tr>
<th>Services</th>
<th>Port/Protocol</th>
<th>Direction</th>
<th>Feature/Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTPS</td>
<td>TCP/443</td>
<td>• Browser→Analyzer</td>
<td>• Operation/administration</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Collector→Analyzer</td>
<td>• Flow</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Analyzer→ATF server</td>
<td>• Active Threat Feed</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Active Directory Authentication agent→Analyzer</td>
<td>• Identity Tracking</td>
</tr>
<tr>
<td>DHCP</td>
<td>UDP/67-68</td>
<td>• Collector monitors</td>
<td>Identity Tracking</td>
</tr>
<tr>
<td>HTTP</td>
<td>TCP/80</td>
<td>• Collector→File server</td>
<td>CLI file transfers</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Analyzer→File server</td>
<td>sys file https:// ...</td>
</tr>
<tr>
<td>NTP</td>
<td>UDP/123</td>
<td>• Collector→NTP server</td>
<td>Timestamps</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Analyzer→NTP server</td>
<td></td>
</tr>
<tr>
<td>RADIUS Authentication</td>
<td>UDP/1645</td>
<td>• Collector→RADIUS server</td>
<td>Administration of user authentication</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Analyzer→RADIUS server</td>
<td></td>
</tr>
<tr>
<td>RADIUS Accounting</td>
<td>UDP/1646</td>
<td>• Collector→RADIUS server</td>
<td>Administration of user accounting</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Analyzer→RADIUS server</td>
<td></td>
</tr>
<tr>
<td>SMTP</td>
<td>TCP/25</td>
<td>Analyzer→SMTP server</td>
<td>• System error reports</td>
</tr>
<tr>
<td>SNMP TRAPs</td>
<td>UDP/162</td>
<td>Analyzer→Network management service</td>
<td>• Security reports</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Security notifications</td>
</tr>
<tr>
<td>SNMP polls</td>
<td>TCP/161</td>
<td>• Network management service→Analyzer</td>
<td>• Analyzer status</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Network management service→Collector</td>
<td>• Collector status</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Analyzer or Collectors→routers</td>
<td>• Router status</td>
</tr>
</tbody>
</table>

*Table 9: Ports used by Proventia Network ADS*
<table>
<thead>
<tr>
<th>Services</th>
<th>Port/Protocol</th>
<th>Direction</th>
<th>Feature/Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSH</td>
<td>TCP/22</td>
<td>• Administrator→Analyzer</td>
<td>• Configuration and advanced administration (can also use Telnet)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Administrator→Collector</td>
<td>• ACL transfer for enforcing worm rules</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Analyzer→Cisco CAT6k</td>
<td></td>
</tr>
<tr>
<td>SSH/SCP</td>
<td>TCP/22</td>
<td>• Collector→File server</td>
<td>• CLI file transfer</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Analyzer→File server</td>
<td>• sys file scp://...</td>
</tr>
<tr>
<td>TACACS</td>
<td>TCP/49</td>
<td>• Collector→TACACS server</td>
<td>Administering user authentication and accounting</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Analyzer→TACACS server</td>
<td></td>
</tr>
<tr>
<td>Telnet</td>
<td>TCP/23</td>
<td>• Administrator→Analyzer</td>
<td>• Configuration and advanced administration (can also use SSH)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Administrator→Collector</td>
<td>• ACL transfer for enforcing worm rules</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Analyzer→Cisco CAT6k</td>
<td></td>
</tr>
<tr>
<td>FTP (PASV)</td>
<td>TCP/20-21</td>
<td>• Collector→FTP server</td>
<td>sys file scp://...</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Analyzer→FTP server</td>
<td></td>
</tr>
<tr>
<td>SYSLOG</td>
<td>UDP/514</td>
<td>Analyzer→Syslog server</td>
<td>Syslog messages</td>
</tr>
</tbody>
</table>

**Table 9:** Ports used by Proventia Network ADS (Continued)
Using CLI Commands

Introduction

This topic provides basic information about navigating and using the CLI.

Starting and logging on to Proventia Network ADS

To start the appliance and log on to the CLI:

1. Place the Proventia Network ADS CD-ROM in the CD drive, and then turn on the appliance.
2. Press any key when the system displays the “Press any key to continue” message.
   Proventia Network ADS runs its initial system diagnostics and displays boot loading messages, and then the boot menu when it finishes loading.
3. Select one of the following menu options:
   - disk to boot from hard disk
   - cdrom to boot from CD-ROM
   - (re)install to boot from cdrom and run the installation setup
     **Caution:** If you choose to reinstall, Proventia Network ADS writes over the current configuration.
     **Note:** If you do not press a key within five seconds, the system attempts to boot automatically, first from the disk, then from CD-ROM.
4. After the login prompt appears, type admin as the user name.
5. Type admin as the default password.
   You should customize this to maintain security.
   **Reference:** See “Changing the Administrative Password” on page 114 for these instructions.

Edit and disabled modes

The command shell runs in one of the following operating modes:

<table>
<thead>
<tr>
<th>Mode</th>
<th>Description</th>
<th>Command prompt</th>
</tr>
</thead>
<tbody>
<tr>
<td>Edit</td>
<td>Allows all configuration changes. The system starts in edit mode automatically when an administrator logs on to Proventia Network ADS, they do not need to enter a password to access edit mode</td>
<td>Hash mark (#)</td>
</tr>
<tr>
<td>Disabled</td>
<td>Allows read-only access and minimal configuration changes. Users without administrative privileges must enter edit mode to make configuration changes.</td>
<td>Percent sign (%)</td>
</tr>
</tbody>
</table>

**Table 10:** CLI modes

Switching to edit mode

Regular users must switch to edit mode to make configuration changes. To switch to edit mode:

1. At the login prompt, type `edit`.
2. Type the `administrator password`.
   The command prompt changes from % to # to indicate edit mode.
About the CLI command hierarchy

After you log on to Proventia Network ADS, the system displays the banner and the command prompt. Commands are arranged in a hierarchical manner, similar to a file system. The root menu is also known as / (slash). You can enter a / at any prompt to return to the root menu. Entering .. (dot-dot) moves you one level up in the command hierarchy.

Menu navigation example

The following example shows how to navigate up the menu hierarchy:

```
admin@mariner2.sea:/# system files
admin@mariner2.sea:/system/files# ..
admin@mariner2.sea:/system#..
admin@mariner2.sea:/# ip interfaces
admin@mariner2.sea:/ip/interfaces# /
admin@mariner2.sea:/#
```

Command types

The two types of commands are as follows:

<table>
<thead>
<tr>
<th>Command type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sub commands</td>
<td>Specific to the current menu.</td>
</tr>
<tr>
<td>Global</td>
<td>Available anywhere in the command hierarchy.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>help</td>
<td>Shows a list of the available choices within a menu.</td>
</tr>
<tr>
<td>?</td>
<td>Shows a list of the available choices within a menu.</td>
</tr>
<tr>
<td>help global</td>
<td>Shows a list of commands available in all menus.</td>
</tr>
</tbody>
</table>

Using Help

There are three types of Help commands:
Help examples

The following shows an example of a help and help global menu:

```
admin@mariner2.sea:/# help
Sub commands:
ip/          IP and network configuration
services/     System services
system/       System configuration
```

```
admin@mariner2.sea:/# help global
Global commands:
..           Return to previous menu
/            Return to root menu
clock        Show or set the system clock
config       Show or save the system configuration
edit         enter configuration mode
help/?       Show available commands
ping         Ping a network host
quit/exit    Exit the command shell
reload       Reload the system
shutdown     Shutdown the system
traceroute   Trace route to a network host
users        Show user login summary
```

Viewing the current configuration

From most menus within the CLI, you can view the configuration by typing the `show` command. Some menus show the configuration automatically when you press ENTER.

Saving the configuration

It is important to save the configuration whenever you make changes. Saving configuration ensures that if the system is restarted, it reloads with the most current configuration.

To save the configuration:

- Type `config write`.
  
  This is a global command, so you can enter it from any menu within the CLI.
Chapter 3

Upgrading and Reinstalling Proventia Network ADS

Overview

Introduction

This chapter describes the process and procedures for reinstalling the Proventia Network ADS Analyzer and Collector appliances.

Important: Reinstalling the appliance software clears the appliance’s current configuration settings and all data stored on the appliance. You must reconfigure all settings through the Proventia Network ADS Setup Wizard.

What you need

To reinstall an appliance, you need the following:

- a computer to use as your configuration interface
- a Proventia Network ADS Appliance Recovery CD

In this chapter

This chapter contains the following topics:

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reinstallation Requirements</td>
<td>30</td>
</tr>
<tr>
<td>Reinstalling an Appliance</td>
<td>31</td>
</tr>
<tr>
<td>Upgrading Appliances to Proventia Network ADS Version 3.6.1</td>
<td>31</td>
</tr>
</tbody>
</table>
Chapter 3: Upgrading and Reinstalling Proventia Network ADS

Reinstallation Requirements

Introduction
You can use a Proventia Network ADS Appliance Recovery CD to reinstall an appliance (Analyzer or Collector).

Caution: Reinstalling the appliance means erasing all data from the system and returning it to its factory state. This should only be done in an emergency situation and under the direction of ISS technical support.

Reinstallation process task overview
To reinstall the software, you must complete the following tasks:

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Reinstall the appliance.</td>
</tr>
<tr>
<td>2</td>
<td>Configure the appliance settings using the Setup Wizard.</td>
</tr>
<tr>
<td>3</td>
<td>Apply your settings and restart the appliance.</td>
</tr>
</tbody>
</table>

Table 13: Reinstallation process

Before you begin
Before you reinstall the appliance, verify you have all of the information you need.

Reference: See the checklists for both appliance types on the Quick Start Cards for the complete list of the information you need.
Reinstalling an Appliance

Introduction

Use the following procedure to reinstall the Proventia Network ADS Analyzer or Collector appliance software.

Procedure

To reinstall the appliance:

1. If there is a bezel cover on the front of the appliance, remove it.
2. Place the Proventia Network ADS Recovery CD in the CD-ROM drive.
3. Choose one of the following methods to connect the appliance to initiate recovery:
   - Connect a VGA monitor and keyboard to the appropriate ports on the back of the appliance.
   - Connect a serial cable from the serial console to the appliance.
4. Restart the appliance.
   You can manually turn the power off and on if the appliance is not responding.
5. Watch for the message that says “Press any key to continue.”
6. When you see this message, press any key to start the boot menu.
7. At the boot menu, select one of the following options:
   - (re) install (VGA) if you are using a monitor and keyboard.
   - (re)install (serial console) if you are using the serial method.
8. After the installation process is complete, remove the CD-ROM, and then restart the appliance.
9. Configure your settings by following the procedures listed on the Quick Start Card that was included in your appliance package contents.

Analyzer reinstallation configuration example

The following shows example configuration for reinstalling Proventia Network ADS on an Analyzer:

```
AdOS/4.1 (ados)
ados login: admin
Password:
Last login: Tue Jul 18 15:33:02 from 10.0.1.195

AdOS 4.1 (build 6ABC)
Welcome to AdOS

admin@ados:/> # reload
   Do you wish to proceed? [n] y
094: Rebooting the system..
Broadcast message Sending all processes the TERM signal...
Sending all processes the KILL signal...
Syncing hardware clock to system time
```
Chapter 3: Upgrading and Reinstalling Proventia Network ADS

Unmounting file systems:
Please stand by while rebooting the system...
Press any key to continue.
GNU GRUB  version 0.95  (633K lower / 3668864K upper memory)

| disk    (serial console) |
| cd      (serial console) |
| (re)install (serial console) |
| disk (VGA) |
| cd (VGA) |
| (re)install(VGA) |

Use the ^ and v keys to select which entry is highlighted.
Press enter to boot the selected OS, 'e' to edit the
commands before booting, or 'c' for a command-line.

Booting '(re)install (serial console)'

root (cd)
Filesystem type is iso9660, using whole disk kernel /boot/kernel-arbus-smp
console=ttys0,9600n8 root=/dev/ram0 randisk=24480 vdso=0 acpi=no
noht init=/linuxrc-install rw
[Linux-bzImage, setup=0xc00, size=0x3d21b4] initrd /boot/initrd.gz
[Linux-initrd @ 0x1fc73000, 0x37ca26 bytes]

.................................................................
.................................................................
INIT: version
2.85 booting
010: Using CD-ROM
018: No system configuration found
020: Configuring CD-ROM

Do you want to begin the install process?

Initializing filesystem "boot"...............done.
Initializing filesystem "system"...............done.
Initializing filesystem "data"...............done.
Probing devices to guess BIOS drives. This may take a long time.

Extracting package...done.
Changes to AdOS will take effect after the next reload.
Extracting package...done.
Upgrading Proventia Network ADS installation (this may take some
time)......done.
Extracting package...done.

INIT: Sending all processes the TERM signal...
Sending all processes the KILL signal...
Syncing hardware clock to system time
Unmounting file systems:
Please stand by while rebooting the system...
md: stopping all md devices.
md: md0 switched to read-only mode.
Restarting system.
Press any key to continue.

GNU GRUB  version 0.95  (633K lower / 366864K upper memory)

+---------------------------------------------------------+-
| disk    (serial console) |                     |
| cd      (serial console) |                     |
| (re)install (serial console) |                  |
| disk (VGA) |                         |
| cd (VGA) |                                       |
| (re)install(VGA) |                     |
|                 |                                         |
|                 |                                         |
|                 |                                         |
|                 |                                         |
+--------------------------------------------------------+-

Use the ^ and v keys to select which entry is highlighted.
Press enter to boot the selected OS, 'e' to edit the
commands before booting, or 'c' for a command-line.

The highlighted entry will be booted automatically in 1 seconds.

Booting 'disk    (serial console)'

root (hd0,0)
Filesystem type is ext2fs, partition type 0x83 kernel /boot/kernel-arbux-smp console=ttys0,9600n8 root=/dev/ram0 ramdisk=24480 vdso=0 acpi=noht rw init=/linuxrc-disk
[Linux-bzImage, setup=0xc00, size=0x3d21b4] initrd /boot/initrd.gz
[Linux-initrd @ 0x1fc73000, 0x37ca26 bytes]

..............................................................
..............................................................
INIT: version 2.85 booting
002: Scanning for filesystems
003: Using system disk
004: Checking file system integrity
005: Configuring swap devices
006: Configuring software packages
007: Restoring system configuration
020: Configuring

AdOS/4.1 (ados)
login:
Upgrading Appliances to Proventia Network ADS Version 3.6.1

Introduction
ISS provides an automatic upgrade script with the Proventia Network ADS 3.6.1 software. Follow the prompts in the script to upgrade your Analyzer and Collector appliances.

Before you begin
You must access the 3.6.1 version software package files from the ISS Support Website (www.iss.net/support). The files include the AdOS and Proventia Network ADS 3.6.1 software packages. You can either burn the files from the support site onto a CD to install from CD, or copy the files to your computer or remote location to install from disk.

Upgrade procedure
To upgrade your appliances:

1. Log on to the appliance with the administrator password.
2. Type `services ads stop` to stop the Proventia Network ADS services.
3. Type `config write` to save the configuration before you begin the upgrade.
4. Type `system` to navigate to the system menu.
5. Choose your next step based on how you are installing the upgrade software:

<table>
<thead>
<tr>
<th>If you are installing from a ...</th>
<th>Then, do the following...</th>
</tr>
</thead>
<tbody>
<tr>
<td>CD</td>
<td>1. Type <code>cdrom unlock</code>.</td>
</tr>
<tr>
<td></td>
<td>2. Eject the old CD ROM, and then place the new CD ROM in the CD drive.</td>
</tr>
<tr>
<td></td>
<td>3. Type <code>cdrom lock</code> to lock it into place.</td>
</tr>
<tr>
<td></td>
<td>4. Type <code>files</code> to navigate to the <code>/system</code> files menu.</td>
</tr>
<tr>
<td></td>
<td>5. Type <code>directory cd</code> to see the directory listing.</td>
</tr>
<tr>
<td></td>
<td>The directory listing includes the build number you need to uninstall the old software packages.</td>
</tr>
<tr>
<td></td>
<td>6. Type <code>install cd:ados-4.1-build number</code> to install the AdOS package from CD.</td>
</tr>
</tbody>
</table>

| Download file                   | 1. Type `files` to navigate to the `/system` files menu.  |
|                                 | 2. Type `copy`, and then one of the following commands to copy the file from the Internet Security Systems Support site:  |
|                                 |   - `ftp://[user:passwd@]A.B.C.D[:port]/filename`  |
|                                 |   - `http://A.B.C.D[:port]/filename`  |
|                                 |   - `scp://[user@]A.B.C.D[:port]/filename`  |
|                                 | 3. Type `disk:` to specify the destination for the package files.  |
|                                 | 4. Type `directory disk:` to see the directory listing.  |
|                                 | The directory listing includes the build number you need to uninstall the old software packages.  |
|                                 | 5. Type `install disk:ados-4.1-build number` to install the AdOS package from downloaded file.  |

6. Type `reload`, and then press ENTER.
7. The appliance restarts with the new version of AdOS.
8. Type `uninstall Proventia-ADS_3.5` to remove the version 3.5 software packages.
9. Type `install Proventia-ADS_3.6.1 build number` to install the new software package.
   The build number is included as part of your upgrade software package.

10. Navigate to the `/services/ads` menu.
11. For Collectors only, type `secret set` and the `shared secret` that you set on the appliance.
    You must set a shared secret to allow communication with the Analyzer appliance.
12. Type `start` to start Proventia Network ADS services.
13. Type `config write` to save all configuration changes.

   **Important:** Close and reopen your Web browser if it was open when you upgraded your appliances. Performing this step avoids issues with browsers that cache session information such as CSS information.

### Example upgrade configuration

The following shows example configuration for an Analyzer upgrade:

```
login: admin
Password:

Proventia Network ADS v3.5
Welcome to Proventia ADS.
admin@mariner.sea:/# services ads stop
admin@mariner.sea:/services# config write
admin@mariner.sea:/# / system
admin@mariner.sea:/system# cdrom unlock
admin@mariner.sea:/system# cdrom lock
admin@mariner.sea:/# system files
admin@mariner.sea:/system/files# directory cd
Directory listing of device:
Filename       Kbytes    Date/Time    Type
Proventia-ADS-####    21154     Aug7 07:38 Signed package
ados-4.1-####    2393       Aug7 07:37 Signed package
admin@mariner.sea:/system/files# install cd:ados-4.1-####
Do you wish to proceed? [n] y
095: Halting disk operations... done
***: Rebooting...
boot>

AdOS/4.1

login: admin
Password:
Last login: CLI on Thu Aug 7 12:40:43 2005 from console

Proventia Network ADS v3.5

Welcome to AdOS
admin@mariner.sea:/# system files
admin@mariner.sea:/system/files# show
  Installed packages:
   AdOS-4.1        (build ####)
Proventia-ADS-3.5 (build ####)
admin@mariner.sea:/system/files# uninstall Proventia-ADS_3.5
```
Uninstalling package Proventia-ADS-3.5................done.
admin@mariner.sea:/system/files# install cd:Proventia-ADS_3.6.1-####
Extracting package................done.
Upgrading Proventia Network ADS installation........done.
admin@mariner.sea:/# /ser ads start
Starting Proventia Network ADS services....................done.
admin@mariner.sea:/# conf write
Chapter 4

Configuring External Flow Storage

Overview

Introduction

You can configure extensible flow storage, which allows you to store virtually limitless amounts of Proventia Network ADS data offline in your existing storage area networks (SANs) using Fibre Channel-connected logical disks.

In this chapter

This chapter contains the following topics:

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>About Proventia Network ADS External Flow Storage</td>
<td>38</td>
</tr>
<tr>
<td>Configuring the External Disk</td>
<td>39</td>
</tr>
<tr>
<td>Removing a Fibre Channel Disk</td>
<td>41</td>
</tr>
</tbody>
</table>
About Proventia Network ADS External Flow Storage

Introduction

Proventia Network ADS allows you to connect a Fibre Channel-connected logical disk to store flow data, provided Proventia Network ADS formats and controls the Fibre Channel disk. Connect and configure your external flow storage disk on the Analyzer appliance.

How external flow storage works

You can configure multiple external Fibre Channel disks. After you connect these disks, Proventia Network ADS fills the first disk with traffic flow data. When that disk is full, the system automatically begins storing additional flow data on the next disk that you added. It will continue to do this until there are no more disks, at which time it will evict the oldest flows.

Flow eviction

When either the flow log size (used) or inodes (used) reaches 95%, and you do not have additional external disks configured, the system automatically evicts old flows to make room for the new ones. When it evicts flows, it removes the oldest flows in 10 time-period segments. When flows are evicted, the system generates a syslog message that states that the flowlog was evicted and includes the time period that was removed.

Before you begin

You must connect the external disk to the Analyzer before you can begin. If you do not have a disk connected, when you try to initialize the disk, the system displays an error message. You must connect the fibre channel disk and then restart the Analyzer if this happens.

Configuration task overview

The following table shows the tasks you should complete to configure the Fibre Channel extensible flow storage:

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Initialize the Fibre Channel disk.</td>
</tr>
<tr>
<td>2</td>
<td>Add the new Fibre channel external disk.</td>
</tr>
<tr>
<td>3</td>
<td>Connect to the Fibre channel external disk.</td>
</tr>
<tr>
<td>4</td>
<td>Add the disk to the Proventia Network ADS flow log.</td>
</tr>
</tbody>
</table>

Table 14: Fibre Channel configuration tasks

About disk partitioning

ISS recommends that you start with a blank partition table. If you initialize a disk that does not have a partition table, the system assumes there is only one partition and initializes the whole disk, but if the disk already contains a partition table, you must initialize each partition separately.
Configuring the External Disk

Introduction
You must follow the configuration steps in the order they are presented to configure a Fibre Channel disk for external flow storage.

Initializing the Fibre Channel disk
To initialize the Fibre Channel disk:

1. Navigate to the / system disk menu.
2. Type `external initialize fc` to initialize the Fibre Channel disk.
3. Type a `name` that you want to assign to the external disk.
4. Type `?` to see the list of unused fibre channel partitions.
   
   Note: If you do not see anything displayed, it means there are no disks found.

5. Type the `name` of the unused fibre channel partition that you want to initialize.
6. Press ENTER.
7. Type `y` when you see the confirmation prompt to continue.

Initializing configuration example
The following example shows configuration for initializing an external flow storage disk:

```
admin@mariner.sea:/system/disk/external# initialize ?
fc               External type "fc"
admin@mariner.sea:/system/disk/external# initialize fc ?
<WORD>           Assign a name to the external disk
admin@mariner.sea:/system/disk/external# initialize fc disk1 ?
sdb1             Specify unused Fibre Channel partition
admin@mariner.sea:/system/disk/external# initialize fc disk1 sdb1
Partition: "sdb1" Size:29332M:
Formatting "sdb1" will erase ALL data that may be on it.
Continue with initialization? [n] y
Initializing filesystem "disk1" (fc partition "sdb1").............done.
```

Adding and connecting to the Fibre Channel disk
Before you can connect to the Fibre Channel to store flow data, you must add the disk.

To add and then connect the Fibre Channel disk:

1. Navigate to the /system disk external menu.
2. Type `add fc`.
3. Type the `name` of the Fibre Channel partition you want to add and connect to.
4. Press ENTER.
5. Type `connect`, followed by the `name` of the Fibre Channel partition, and then press ENTER.
6. The system displays a message indicating it is connecting.
7. To verify that that the disk is connected, type `show`, and then press ENTER.

Configuration example
The following shows an example of adding and connecting to Fibre Channel disk “disk1” and then verifying the connection:

```
admin@mariner.sea:/system/disk/external# add fc disk1
```
admin@mariner.sea:/system/disk/external# connect disk1
Connecting external disk "fc1" @ sdb1 (type fc) ...OK.
admin@mariner.sea:/system/disk/external# show
External disks:
  Filesystem      Size/Used       Inodes/Used
  "disk1"         2.0T/185G (10%)   33280000/6048 (1%
type: fc

Adding a disk to the Proventia Network ADS flow log

After you add and connect the Fibre Channel disk, you must add that disk to the Proventia Network ADS flowlog so that the flows will be directed to it.

To add a disk to the flow log:

1. Navigate to the /services/ads menu.
2. Type storage add flowlog.
3. Type the name of the disk you added, and then press ENTER.
4. Type start to start ads services.
5. Type config write to save the configuration, and then press ENTER.

Example flowlog configuration

The following shows an example of adding a disk to the flowlog:

admin@mariner.sea:/# services ads
admin@mariner.sea:/services/ads# storage add flowlog fc1
Adding fc1 to database flowlog for the first time.ok.
admin@mariner.sea:/services/ads# start
admin@mariner.sea:/services/ads# config write
Removing a Fibre Channel Disk

Introduction

In some cases, you might want to remove an external disk that you have been using for backup purposes. You can do this to attach a new disk to the Analyzer or to attach the current disk to another device to copy the flows.

Task overview for removing a disk

The tasks you perform for removing a disk are the reverse of those you perform for adding an external disk. The following table lists the steps you must perform for removing an external disk:

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Remove the disk from the Proventia Network ADS flow log.</td>
</tr>
<tr>
<td>2</td>
<td>Disconnect the Fibre channel external disk from Proventia Network ADS.</td>
</tr>
<tr>
<td>3</td>
<td>Remove the Fibre channel external disk from Proventia Network ADS.</td>
</tr>
<tr>
<td>4</td>
<td>Disconnect the Fibre channel disk from the Analyzer.</td>
</tr>
</tbody>
</table>

Table 15: Task overview for removing an external disk

Disconnecting and removing an external disk

To disconnect an external Fiber Channel disk:

1. Navigate to the /services/ads menu.
2. Type `storage remove flowlog`.
3. Type the name of the external disk you want to remove.
4. Press ENTER.

Removing an external disk

To remove an external disk:

1. Navigate to the /system/disk/external menu.
2. Type `disconnect`, followed by the name of the external disk you want to remove.
3. Press ENTER.

Configuration example

The following shows example configuration for disconnecting and removing an external disk:

```
admin@mariner.sea:# services ads
admin@mariner.sea:/services/ads# storage remove flowlog disk1
admin@mariner.sea:/services/ads# / system disk external
admin@mariner.sea:/system/disk/external# disconnect disk1
admin@mariner.sea:/system/disk/external# remove disk1
```
Chapter 5

Configuring DHCP for Identity Tracking

Overview

Introduction
This chapter provides the instructions for configuring DHCP on your Collectors, and enabling Proventia Network ADS Identity Tracking.

Identity Tracking allows Proventia Network ADS to associate user information from your DHCP servers with the traffic it detects. This allows you to quickly identify the users that are involved in alert traffic.

In this chapter
This chapter contains the following topics:

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>About Identity Tracking with DHCP</td>
<td>44</td>
</tr>
<tr>
<td>Configuring DHCP for Identity Tracking</td>
<td>45</td>
</tr>
</tbody>
</table>
# About Identity Tracking with DHCP

## Introduction
Before deploying Proventia Network ADS using DHCP, you need to determine the best physical location for your Analyzer or Collector that will be collecting DHCP Identity Tracking data.

## Determining which appliance to set up for DHCP
You must enable DHCP monitoring for your Analyzer or Collector with interfaces sitting just outside your corporate DHCP server. Additionally, because Proventia Network ADS watches the actual DHCP requests and responses, you must position the appliance within the broadcast domain of the client network.

**Note:** You can also set up Proventia Network ADS to create flows from the same tap/span port that they receive the DHCP user information from.

## How DHCP works with Identity Tracking
Proventia Network ADS Identity Tracking supports DHCP hostnames by monitoring DHCP lease request and lease grant messages. When a DHCP lease is granted, Proventia Network ADS maps the Client ID from the DHCP lease request to the newly-granted IP address.

**Note:** Identity Tracking also works with information Proventia Network ADS collects from your Microsoft Active Directory or Novell eDirectory servers.

**Reference:** For instructions for configuring your Microsoft Active Directory or Novell eDirectory Servers, see “Configuring Identity Tracking Settings” in the *Proventia Network ADS 3.6.1 User Guide*. 
Configuring DHCP for Identity Tracking

Introduction
To configure DHCP for Identity Tracking, you must specify DHCP as the Identity Tracking source for the Analyzer or the Collector that will be collecting DHCP user data, and then you must enable Identity Tracking on the Analyzer.

Configuring DHCP
To configure DHCP as the Identity Tracking source:

1. Log on to the Analyzer or Collector that you want to collect DHCP user data.
2. Navigate to the /services/ads/interface menu.
3. Type add ? to see the configured interfaces.
4. Enter the interface name for the interface that you want to collect DHCP.
5. Type dhcp to specify it as a DHCP interface.
6. Press ENTER.

DHCP source configuration example
The following example adds interface e3/7/1 on the Collector and specifies it as a DHCP interface:

```
admin@mariner.sea1:/services/ads/interface # add ?
e3/7/1
e3/7/0
admin@mariner.sea1:/services/ads# interface add e3/7/1 ?
netflow
promisc
netscout
sflow
dhcp
admin@mariner.sea1:/services/ads# interface add e3/7/1 dhcp
```

Enabling Identity Tracking
After you configure DHCP as the flow source for Proventia Network ADS to use for Identity Tracking, you must enable Identity Tracking on the Analyzer. You can do this in the CLI or in the Web user interface.

To enable Identity Tracking in the CLI:

1. Log on to the Analyzer appliance.
2. Navigate to the /services/ads menu.
3. Type show_auth enable.
4. Press ENTER.
5. Type show_auth, and then press ENTER to confirm it is enabled.

Identity Tracking configuration example
The following shows example configuration for enabling Identity Tracking:

```
admin@ariner.sea:/services/ads# show_auth enable
admin@ariner.sea:/services/ads# show_auth
Display Identity Tracking Information: enable
```

Reference: For the instructions for enabling Identity Tracking in the Web user interface, see “Enabling Identity Tracking” in the Proventia Network ADS 3.6.1 User Guide.
Chapter 6

Configuring TACACS+ and RADIUS

Overview

Introduction

You can use TACACS+ and RADIUS for authentication with your Proventia Network ADS deployment.

In this chapter

This chapter contains the following topics:

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring TACACS+ Integration</td>
<td>48</td>
</tr>
<tr>
<td>Configuring RADIUS Integration</td>
<td>50</td>
</tr>
<tr>
<td>Setting the Method for TACACS+ and RADIUS</td>
<td>52</td>
</tr>
</tbody>
</table>
Chapter 6: Configuring TACACS+ and RADIUS

Configuring TACACS+ Integration

Introduction
Proventia Network ADS can perform static password authentication with any TACACS+ deployment. This is an optional feature that you can integrate with your already existing TACACS+ implementation. TACACS+ authentication is available for CLI connections through SSH and Telnet, and Web interface access via HTTPS.

About adding servers
You can add both a primary and backup server. When the system is connecting, it first tries to connect to the primary server, then to the backup server listed. If the system cannot reach either of the servers, it then attempts to authenticate locally.

Adding a TACACS+ server
To configure a TACACS+ server:

1. Navigate to the services/aaa menu.
2. Type one of the following:
   ■ server set primary to set the primary server
   ■ server set backup to set the backup server
3. Type the IP address for the server.
4. Type the port on which the Analyzer should communicate with the TACACS+ server.
5. Type one of the following:
   ■ encrypted to enter an encrypted secret
   ■ unencrypted to enter an unencrypted secret
6. Type the secret the ADS appliances should use to communicate with the TACACS+ server.
   Note: You should use a secret that contains a variety of characters for security purposes.
7. Press ENTER.

TACACS+ server configuration example
The following example sets the primary server on port 49 with an encrypted shared secret of f8Pw3c:

```
admin@mariner.sea:/services/aaa# tacacs server set ?
primary Server type
backup Server type
admin@mariner.sea:/services/aaa# tacacs server set primary ?
<A.B.C.D> Server IP Address
admin@mariner.sea:/services/aaa# tacacs server set primary 10.0.1.11 49 ?
encrypted Unencrypted secret follows
unencrypted Encrypted secret follows
admin@mariner.sea:/services/aaa/tacacs# server set primary 10.0.1.11 49
encrypted f8Pw3c
```

The timeout setting
Set the timeout period to designate the amount of time the system attempts to connect to the servers before it tries to connect to the designated backup server. You must set the timeout value only if you want to change the default setting, which is two seconds.
**Setting the timeout period**

To set the timeout period:

1. Navigate to the `services/aaa` menu.
2. Type `tacacs timeout set`.
3. Type the number of seconds you want the system to try to connect.
   The default setting is two seconds.
4. Press ENTER.

**Viewing current configuration**

To view the current configuration:

1. In the `/services/aaa` menu, type `tacacs show`.
2. Press ENTER.

**TACACS configuration example**

The following shows example configuration:

```
admin@mariner.sea:/services/aaa# tacacs show
TACACS+ configuration:
   Authentication configuration:
      Primary server:
         Address: 10.0.1.11
         Secret: ******
         Port: 49
   Accounting configuration:
      Level: none (default)
      Timeout: 3
```

**TACACS+ authentication**

If you are logging in and authenticating via TACACS+, you must specify it as the authentication method you are using. For these instructions, see “Setting the Method for TACACS+ and RADIUS” on page 52.
Chapter 6: Configuring TACACS+ and RADIUS

Configuring RADIUS Integration

Introduction

You can use Proventia Network ADS with your existing remote authentication dial-in user service (RADIUS).

Adding a RADIUS server

To configure a RADIUS server:

1. Navigate to the services/aaa menu.
2. Type one of the following:
   ■ server set primary to set the primary server
   ■ server set backup to set the backup server
3. Type the IP address for the server.
4. Type one of the following:
   ■ encrypted to enter an encrypted secret
   ■ unencrypted to enter an unencrypted secret
5. Type the secret the Proventia Network ADS appliances should use to communicate with the RADIUS server.
   Note: You should use a secret that contains a variety of characters for security purposes.
6. Type the port number on which the Analyzer will communicate with the RADIUS server.
   Note: You only must specify a port number if you do not want to use the default RADIUS port.
7. Press ENTER.

About the retries and timeout settings

The retries setting designates the number of times Proventia Network ADS tries to authenticate if the first attempt fails. The timeout setting designates the amount of time the system attempts to connect to the servers before it tries to connect to the designated backup server. The default settings are two retry attempts and a two second timeout. You only must set these values if you want to change the default settings.

Setting the retries and timeout period

To set the reset and timeout period:

1. Navigate to the services/aaa/radius menu.
2. Type retries set.
3. Type the number of times you want the system to try to connect.
   The values are 1-60.
4. Press ENTER.
5. Type timeout set.
6. Type the number of seconds you want the system to try to connect.
   The values are 1-60.
7. Press ENTER.
| The RADIUS authentication method | If you are logging in and authenticating using RADIUS, you must specify RADIUS as the authentication method. For these instructions, see “Setting the Method for TACACS+ and RADIUS” on page 52. |
Chapter 6: Configuring TACACS+ and RADIUS

Setting the Method for TACACS+ and RADIUS

Introduction

If you are logging in and authenticating using TACACS+ or RADIUS, you must also specify which authentication method you are using and, for multiple methods, the order you want the system to try each method (tacacs, radius, or local). When you set multiple methods, the system tries each method in the order you list them until either one succeeds or they all fail.

Note: If you do not specify any method, the system uses local authentication.

Setting the method

To set the method:

1. Navigate to the /services/aaa menu.
2. Type method set.
3. Do one of the following:
   ■ Type tacacs to set only tacacs
   ■ Type radius to set only radius
   ■ Type any combination of tacacs, radius, or local, in the order you want the system to try authenticating.

   Important: If you want the system to perform both RADIUS and local authentication, then you must explicitly set both methods.

4. Press ENTER.

Exclusive method

You can also set the method to exclusive, which allows you to specify that you want each method tried, and that if the method is working (for example, the RADIUS server responds), but if the user cannot log in to it, then the user is unable to log in at all.

Important: This means that if the exclusive method is enabled and the TACACS+ server is operational, but the user does not have a TACACS+ account, then that user cannot log on at all. Proventia Network ADS only tries to authenticate with the next listed method if the TACACS+ server is not operational or is unreachable on the network.

Setting exclusive method

To set the method as exclusive:

1. Type method exclusive
2. Type one of the following:
   ■ enable
   ■ disable

Note: If you set the method exclusively to “tacacs local” and you do not have an admin-level user that also has an account on the TACACS+ server, then you cannot log on as an admin-level user anymore.

Example: If mariner has an admin-level user called “admin” and that is the only privileged user, but TACACS+ doesn’t have an admin user, then admin won’t be able to log on to mariner unless he can make the TACACS+ server unavailable (i.e., by unplugging the network, etc.)

3. Press enter.
### About accounting levels

You can configure accounting settings for each authentication method (local, RADIUS, and TACACS+). Use local and TACACS+ accounting to track and log software log ons, configuration changes, and interactive commands. Use RADIUS accounting to track log ons.

### Configuring accounting settings

To configure accounting settings:

1. Navigate to one of the following menus:
   - `/services/aaa/radius`
   - `/services/aaa/tacacs`
   - `/services/aaa/local`
2. Type `accounting set level`.
3. Type one of the following levels:
   - `login`
   - `change`
   - `commands`
4. Press ENTER.
5. Repeat Steps 1 through 3 to set additional accounting levels.

### Accounting configuration examples

The following configuration shows examples of RADIUS and local accounting levels:

```
admin@mariner.sea:/services# aaa radius
admin@mariner.sea:/services/aaa/radius# accounting set level ?
   none
   login
admin@mariner.sea:/services/aaa/radius accounting set level login
admin@mariner.sea:/services/aaa/radius# ..
admin@mariner.sea:/services/aaa/ local
admin@mariner.sea:/services/aaa/local# accounting set level ?
   none
   login
   change
   commands
admin@mariner.sea:/services/aaa/local# accounting set level change
admin@mariner.sea:/services/aaa/local# accounting
Accounting level: change
```

### Authorization attributes for TACACS+ and RADIUS

If you are using TACACS+ or RADIUS authentication or logging with your Proventia Network ADS deployment, you might be required to configure some attributes on your servers to allow them to operate with your Proventia Network ADS Collectors.

### Defining TACACS+ service attributes

For TACACS+ servers, you must define the service attribute for Proventia Network ADS. The entry in your configuration should be similar to the following example:

```python
    service = system {
        system_group = system_admin(or system_analyst or system_user)
    }
```
Defining RADIUS service attributes

For RADIUS servers, you must define the vendor specific attribute, System-Privilege-Level:

```
VENDOR Arbor 9694
ATTRIBUTE Arbor-Privilege-Level string Arbor
```

You also must define the user accounts for the Proventia Network ADS user on the RADIUS server:

```
radadmin        Auth-Type = Local, Password = “xxxx”
Arbor-Privilege-Level = “system_admin (or system_analyst or system_user)”
```
Chapter 7

Configuring Flow

Overview

Introduction

Proventia Network ADS supports three types of flow: NetFlow, cFlowd, and sflow. This chapter contains the instructions for configuring flow on your routers and switches and the instructions for configuring your routers and switches to forward flow to your Proventia Network ADS Collectors.

In this chapter

This chapter contains the following topics:

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring Flow on Collectors</td>
<td>56</td>
</tr>
<tr>
<td>Configuring NetFlow for Cisco IOS</td>
<td>57</td>
</tr>
<tr>
<td>Configuring Cflowd for JunOS</td>
<td>59</td>
</tr>
<tr>
<td>Configuring sFlow</td>
<td>63</td>
</tr>
<tr>
<td>Configuring SNMP Polling on Collectors</td>
<td>65</td>
</tr>
</tbody>
</table>
Chapter 7: Configuring Flow

Configuring Flow on Collectors

Introduction
Configure flow settings on your Collectors, or on the Analyzer, if the Analyzer is collecting flows.

Configuring flow
To configure your Collector to receive flow data from your routers and switches:

1. Navigate to the /services/ads menu.
2. Type `interface add` to add the interface.
3. Type the interface `name`.
4. Type one of the following to specify the type of flow you want the appliance to receive:
   - `netflow` to receive NetFlow or Juniper cFlowd packets
   - `sflow` to receive sFlow packets
   - `netscout` to receive
5. Press ENTER.

sflow configuration example
The following example sets interface e3/7/1 to receive sflow:

```bash
admin@mariner1.sea:# services/ads
admin@mariner1.sea:/services/ads# interface add e3/7/1 ?
   netflow
   promisc
   netscout
   sflow
admin@mariner1.sea:/services/ads# interface add e3/7/1 sflow
```
**Configuring NetFlow for Cisco IOS**

**Introduction**

The correct NetFlow configuration is important so that your Proventia Network ADS system performs correctly. This topic includes instructions for configuring the ISS recommended settings.

**Supported versions**

Proventia Network ADS currently supports NetFlow versions 1, 5, and 7, and it supports NetFlow version 9 when the exported flow includes the same data fields as versions 5 and 7.

**Configuration examples**

The examples in this topic, unless otherwise noted, are from Cisco IOS Version 12.0(16)S running on a Cisco 12000 Series GSR (Gigabit Switch Router).

**Configuring NetFlow settings**

To configure NetFlow settings:

1. Log on to the router (via telnet, console, etc.)
2. Type `configure`, and then press ENTER to enter configuration mode.
3. Type `ip flow-export version number` to set the version number.
   - **Note:** If you are configuring devices that export version 7, you must configure the device to include the source and destination IP address and ports in the flow mask.
4. Type `interface` followed by the interface `name` to enable the interface, and then press ENTER.
   - **Note:** You must enable NetFlow on each interface on the router that sees inbound traffic.
5. Repeat Step 4 to add additional interfaces.

**Examples**

The following show examples of logging on to the router, setting the version, and enabling NetFlow on Packet over Sonnet (POS) interface 0/0:

```
$ telnet gsr1
Trying 10.0.1.1...
Connected to gsr1.
Escape character is '^]'.

GSR-1>enable
Password:
GSR-1#configure
Configuring from terminal, memory, or network [terminal]? enter configuration commands, one per line. End with CNTL/Z.
GSR-1(config)#
GSR-1(config)#ip flow-export version 5
GSR-1(config)#interface POS 0/0
GSR-1(config-if)#ip route-cache flow
GSR-1(config-if)#exit
GSR-1(config)#
```

**Export IP address**

NetFlow is sent out of an interface on the router. The IP address assigned to that interface is the source IP for all NetFlow packets. This is the export IP address you should configure in the Proventia Network ADS interface.
Export IP configuration example

In this example, NetFlow is exported on FastEthernet interface 1/1, with an IP address of 192.168.10.1:

GSR-1#show interfaces FastEthernet 1/1 | include Internet address
Internet address is 192.168.10.1/24
GSR-1#configure
Configuring from terminal, memory, or network [terminal]?
enter configuration commands, one per line. End with CNTL/Z.
GSR-1(config)#ip flow-export source FastEthernet 1/1

Destination IP address

You must specify the appliance’s IP address as the NetFlow destination. You can use any port; however, if you are teeing NetFlow from the appliance to another destination, you must type an appropriate UDP port for that destination.

Active flow timeout

Active flows are ejected from the NetFlow cache after a default period of 30 minutes. If you do not update this value, it is possible that an attacker can hide attack traffic within a very small number of extremely long-lived flows. To prevent this, ISS recommends that you set the active flow timeout to one minute. This setting should not affect router performance. In surveys done on Internet traffic, less than 1% of all flows last for more than 1 minute.

Destination IP and flow timeout configuration examples

The following examples set the destination IP to 192.168.10.11, port 5000 and the active flow timeout setting to one minute:

GSR-1(config)# ip flow-export destination 192.168.10.11 5000
GSR-1(config)# ip flow-cache timeout active 1

Enabling NetFlow on your Proventia Network ADS Collectors

After you configure your routers to forward NetFlow to your Collector, you must enable NetFlow on your Collector so that it can receive the flow data.

Reference: See “Configuring Flow on Collectors” on page 56 for these instructions.

Cisco switch example

The following example shows unsampled Cisco Catalyst configuration on a switch running version 12.1(13)E or later:

mls aging long 64
mls flow ip interface-full
mls nde sender version 5 (or 9)
ip flow-export source <Interface>
ip flow-export version 5
ip flow-export destination <IP address> <port number>
interface <Interface>
ip route-cache flow

Cisco router example

The following example shows unsampled Cisco router configuration:

ip flow-export source <Interface>
ip flow-export version 5
ip flow-export destination <IP address> <port number>
ip flow-cache timeout active 1
interface <Interface>
ip route-cache flow
Configuring Cflowd for JunOS

Introduction
This topic provides information about and procedures for configuring your Juniper routers to forward cflowd to your Proventia Network ADS Collectors.

About Proventia Network ADS and JunOS integration
Proventia Network ADS works seamlessly with Juniper M-series routers, interoperating with Juniper cflowd when the JUNOS version is 5.2R2 and higher and the correct sampling rate is set.

The Juniper architecture exports cflowd flow records that summarize the traffic that matches the cflowd-configured filter. The matching traffic is sampled at the configured sampling rate. Because the appropriate cflowd configuration is important to the performance of your Proventia Network ADS system, the following background information is included to help you familiarize yourself with cflowd export and Proventia Network ADS integration.

About Juniper traffic sampling
Juniper traffic sampling allows you to sample a fixed percentage of packet headers from all or some traffic passing through a Juniper M-series router, it is not meant to capture all packets received.

**Note:** This feature is only available on Juniper M-series routers that are equipped with an Internet Processor II ASIC.

Supported versions
Proventia Network ADS interoperates well with versions 5.2R2 and later. In these versions, flows are exported every 5 seconds, even when the router is under stress. Further, the traffic rates reported by cflowd closely resemble the actual traffic rates at reasonable sampling rates such as 1/100 and 1/500.

Recommended sampling rates
Reported traffic rates, at very low sampling rates, are not accurate. As the sampling rate increases, the reported traffic rates become less accurate. For example, 1/1,000 sampling is more accurate than 1/1,000,000.

Though Juniper does not recommend sampling at a rate more frequently than 1/1,000, ISS has successfully used sampling rates less than 1,000.

**Note:** It is not necessary to set active and inactive flow timeouts in JunOS. The sampled packets are aggregated in one-minute “bins” and, unlike other vendor implementations, flows are always expired at this one-minute interval. They do not timeout or expire based on information in the packet (such as TCP flags). Because of this, settings like “active timeout” and “inactive timeout” do not apply; both are always effectively one minute.

Cflowd configuration commands in JunOS
The following table provides a description of many of the cflowd configuration commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>set forwarding-options family inet filter input filter name</td>
<td>Applies the filter to all packets that are evaluated against the default forwarding table (inet.0). In most cases, this is the easiest way to apply a filter to all packets received by the system.</td>
</tr>
</tbody>
</table>

**Table 16: cflowd configuration commands**
### Versions of examples

The examples shown in this topic are from JunOS 5.5B1.3 on a Juniper M5 Router.

### Logging on and configuring a filter

To log on and configure a filter:

1. Log on to the router (via telnet, console, SSH, etc.).
2. Type `configure` to enter the configuration mode.
3. Type `set firewall filter` then enter a filter `name`.
4. Type `term sampled_packets from source address 0.0.0.0/0` to configure a filter that selects all traffic, so you can see all of the traffic flowing through the router.
5. Press `ENTER`.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
</table>
| set forwarding-options sampling input family inet max-packets-per-second `number` | Sets a limit on the number of packet headers that are sampled per second.  
   **Note:** Though the maximum allowed value is 65535, the system might have a defined hard limit that is lower than this value. The system-defined hard limit depends on the type of hardware and software you are using. |
| set forwarding-options sampling input family inet rate `number` | Defines the sampling rate as `1/number (1-in-number)` of packets. The lower the number, the larger the percentage of packets sampled.  
   **Important:** You must not set this number lower than the recommended value. If this rate exceeds the max-packets-per-second or the system’s defined hard limit, cflowd output statistics will be significantly under-reported. |
| set forwarding-options sampling input family inet run-length `number` | Samples `(1+number)/rate` packets instead of `1/rate` packets.  
   **Important:** You must set this value to zero to operate properly with Proventia Network ADS. |
| set forwarding-options sampling output cflowd `IP address` | Sets the IP address of the Proventia Network ADS appliance that receives the cflowd output packets. |
| set forwarding-options sampling output cflowd `IP address port portnumber` | Sets the UDP destination port to the port number for the Proventia Network ADS appliance that receives the cflowd output packets. Recommended values are between 2000 and 65535. |
| set forwarding-options sampling output cflowd `Destination IP address source-address` `Source IP address` | Sets the source as the address of the interface where the flows leave the router.  
   **Example:** If flows are exported out of a Fast Ethernet port on IP address 1.1.1.1, that is the source address.  
   **Note:** You can only set this for JunOS 5.7 and later versions. |
| set forwarding-options sampling output cflowd `IP address version number` | Sets the cflowd output protocol version to the `number` you enter.  
   **Important:** Proventia Network ADS currently only supports version 5, so you must set this to version 5. |

---

Table 16: `cflowd` configuration commands (Continued)
6. Type `set firewall filter cflowd term sampled_packets then sample accept`, and then press ENTER to set a filter that samples matching traffic and then accepts it.

7. If you set a filter that doesn’t match all traffic, you can then type `set firewall filter cflowd term other then accept`, and then press ENTER to set a filter that samples traffic that does not match the filter, and then accepts it.

**Log on and filter configuration example**

The following example shows configuration for a filter named cflowd:

```
$ ssh admin@m5
admin@m5's password:
Last login: Tue Feb 25 17:54:39 2006 from 10.0.2.220
--- JUNOS 5.5B1.3 built 2002-07-31 00:38:59 UTC

admin@m5> configure
entering configuration mode
[edit]
admin@m5# set firewall filter cflowd term sampled_packets from source-address 0.0.0.0/0
admin@m5# set firewall filter cflowd term sampled_packets then sample accept
admin@m5# set firewall filter cflowd term other then accept
```

**Setting the sampling rate**

Select a sampling rate that is appropriate for your traffic load. In addition to the sampling rate, set the run-length and maximum packets per second to sample. The run length of zero indicates that all packets should have an equal probability of being sampled. The maximum packet per second rate is set to the largest value allowed to prevent clipping of the sample.

**Setting the destination address**

You must specify the appliance’s IP address as the cflowd destination. You can use any port as the destination. However, if the cflowd stream is to be “teed” from the appliance to another destination, you must select the appropriate UDP port for that destination.

**Sampling rate and destination configuration example**

In the following example, the sampling is set to one in five hundred packets and the destination as 192.168.10.11, port 5000:

```
admin@m5# set forwarding-options sampling input family inet rate 500
admin@m5# set forwarding-options sampling input family inet run-length 0
admin@m5# set forwarding-options sampling input family inet max-packets per-second 65535
admin@m5# set forwarding-options sampling output cflowd 192.168.10.11 port 5000
```

**Setting the export IP address**

The Juniper router sets the source IP address of the cflowd packets according to its internal routing table. You are not required to set this; however, if you are running versions 5.7 or later, you can set this manually.

**Enabling interfaces**

You should apply the cflowd filter to each interface on the router that sees inbound traffic for your customers.

The following example enables sampled cflowd on interface e3/4/1:
Enabling cflowd on your Proventia Network ADS Collectors

Admin@m5# set forwarding-options sampling output cflowd 192.168.10.11
            version 5
admin@m5# set interfaces e3/4/1 unit 0 family inet filter input cflowd

After you configure your Juniper routers to forward cflowd packets to your Collector, you must enable flow on your Collector so that it can receive the flow data. See “Configuring Flow on Collectors” on page 56 for these instructions.
Configuring sFlow

Introduction
This topic includes the instructions for enabling sFlow, forwarding sFlow data to Proventia Network ADS, and changing sampling rates.

Overview
Proventia Network ADS accepts sFlow versions 2, 4, and 5 from all devices that support sFlow. To monitor traffic in data networks, the sFlow agent uses sampling technology to capture traffic information from the device it monitors. Then it uses sFlow datagrams to forward the sampled traffic information to Proventia Network ADS for analysis. This results in a thorough, network-wide view of traffic flows in real time.

Reference: For more information about sFlow devices and collectors, see the sFlow organization Website at http://sflow.org.

Configuring sFlow devices
To configure your sFlow devices to send flow records to Proventia Network ADS, you must configure the agent to forward the flows to a Proventia Network ADS Collector and then configure the Collector to receive them. Configuration instructions vary depending upon the type of sFlow agent you are configuring.

This topic covers standard configuration on Foundry switches and uses examples based on a Foundry FastIron 4802 switch. For configuration information about routers and other types of switches, see the product documentation for your particular router or switch.

Note: sFlow is a sampled protocol, which means it performs a sampling of flow data and does not forward every flow across a switch or router to your Collector appliance. Because of this, Proventia Network ADS might not be able to detect or identify security events that require every flow to be identified.

Configuring sFlow settings
To configure sFlow settings:

1. Log on to the switch via telnet or SSH.
2. Type `conf t` to configure terminal mode so that you can make changes.
3. Type `sflow enable`, and then press ENTER to enable sFlow services on the switch.
4. Type `sflow version`, followed by the sFlow version number your router or switch uses, and then press ENTER to set the version.

   Note: Currently ISS supports sFlow versions 2, 4, and 5.

5. Type `sflow destination`, followed by the destination IP address, which is the Proventia Network ADS Collector IP address.
6. Type `interface`, followed by the interface that you want the switch to use to forward data to the Collector appliance, and press ENTER.
7. In the interface menu, type `sflow forwarding`, and then press ENTER to set forwarding for that interface.

   Note: After you configure a Foundry device to send sFlow packets to the Collector, it continues forwarding until you disable the function.

8. Type `sflow sampling`, followed by the rate that is appropriate for the traffic load of your interface.

   Example: Type `100` if you want the sampling rate to be 1 out of every 100 packets.

9. Type `exit` to return to the configuration menu.
### SFlow configuration examples

The following shows example configuration for the sFlow settings described above:

```
FI4802# conf t
FI4802(config)# sflow enable
FI4802(config)# sflow version 2
FI4802(config)# sflow destination 192.168.1.1
FI4802(config)# interface ethernet 13
FI4802(config-if-e100-13)# sflow forwarding
FI4802(config)# interface ethernet 13
FI4802(config-if-e100-13)# sflow sampling 100
FI4802(config-if-e100-13)# exit
FI4802(config)#
```

### Configuring optional settings

Your sFlow device is configured with default settings for the packet size, sampling rate, and polling rate. You can override these default settings by entering settings manually. The default settings vary depending upon your switch or router. See the product documentation for specific default settings.

#### Setting the packet size

You can set the maximum packet size for the sFlow that the switch generates by specifying the preferred packet size. Smaller packets use more processing power, so you can increase the packet size to use less resources. Specify any whole number (for the FastIron, the range is from 128 to 1300) to set the maximum packet size.

#### Setting the switch sampling rate

The switch sampling rate identifies the ratio of packets observed at the data source to the samples generated. For example, a sampling rate of 100 indicates that, on average, 1 sample will be generated for every 100 packets observed on a switch. Select an sFlow switch sampling rate that is appropriate to your traffic load.

#### Setting the switch polling rate

The switch polling rate is the interval between sFlow polls, in seconds.

#### Optional settings example

In this example, we set the maximum sFlow packet size to 1300, the switch sampling rate to 200, and the interval to two minutes:

```
FI4802(config)# sflow max-packet-size 1300
FI4802(config)# sflow sample 200
FI4802(config)# sflow polling-interval 120
```

### Enabling sFlow on your Proventia Network ADS Collectors

After you configure sFlow to forward packets to your Collector, you must enable sFlow on your Collector so that it can receive them.

**Reference:** See “Configuring Flow on Collectors” on page 56 for these instructions.
# Configuring SNMP Polling on Collectors

## Introduction
You can configure router (flow sources) during the initial setup using the Proventia Network ADS Setup Wizard. If you do not configure all routers during the initial setup, you must configure additional routers in the CLI. After you configure routers in the CLI, they appear in the Web user interface in network traffic and events displayed.

## About router data
Configuring routers (and optionally, a router’s associated interfaces), allows you to see how the traffic is being routed on your network and provides greater granularity than Collector-level data. You can see where various connections happen on your network, and the traffic that travels over various switches or routers on your network. You can search by a specific router or interface and also see the utilization for each router and interface, which can help with capacity planning. You can also create reports on the Reports pages that include this data, which allows you to see how those routers and interfaces are being used.

## Router and interface maximum limits
The number of routers (or flow sources) you can configure is limited by the Collector model you have purchased. Proventia Network ADS supports up to 500 interfaces per router, and the number of routers you can have is between zero and 20.

## SNMP queries
Proventia Network ADS queries the configured routers for SNMP information, so it can then display names for the interfaces. Proventia Network ADS polls the routers for information every hour. Version 3.6.1 also supports SNMP version 3.

## Adding a router
To add a router:

1. Navigate to the `/services/ads` menu.
2. Type `router add`.
3. Type the router’s `IP address`.
   - **Example**: 10.0.1.1
4. Press ENTER.
5. Repeat Steps 2 through 4 for each additional router you want to add.

## Adding router SNMP settings
If you want the Collectors to poll the routers for SNMP and interface information, you must set the SNMP community for the router. You can also configure additional settings that are specific to SNMP version 3.

To configure SNMP settings for a router:

1. Navigate to the `/services/ads` menu.
2. Type `router snmp`.
3. Type one of the following:
   - the router’s `IP address` to configure a specific router
   - `default` to configure default SNMP settings
4. Type `community set`.
5. Type the community `phrase` or `word`, and then press ENTER.
Chapter 7: Configuring Flow

Router configuration examples

The following examples show some of the settings you can configure for routers, including the additional optional settings for SNMP version 3:

```
admin@mariner.sea:/services/ads# router ?
Subcommands:
add              Add router to list of routers that ADS will monitor
remove           Remove router from list of routers
show             Show monitored routers and SNMP settings
snmp             Show or set router SNMP parameters
admin@mariner.sea:/services/ads# router add 10.0.1.1
admin@mariner.sea:/services/ads# router snmp ?
default          Choose a router or 'default'
10.0.1.1          Choose a router or 'default'
<cr>
admin@mariner.sea:/services/ads# router snmp default community
```

Removing a router

To remove a router:

1. Navigate to the /services/ads menu.
2. Type `router remove`.
3. Type the `router IP address`.
4. Press ENTER.

The router is removed from the configuration and will not be named in reported network traffic.

Removing a router configuration example

The following shows example configuration for removing a router:

```
admin@mariner.sea:/services/ads# router remove ?
10.0.1.1 Router IP Address
admin@mariner.sea:/services/ads# router remove 10.0.1.1
```

admin@mariner.sea:/services/ads#
Chapter 8

Configuring NetScout Integration

Overview

Introduction
You can configure Proventia Network ADS to integrate with and accept flow information from NetScout probes.

Device used for examples
The examples shown in this chapter are based on a NetScout nGenius® device, Model 9221ET V6.0.0 (Build 134 NSExport-01).

In this chapter
This chapter contains the following topics:

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring NetScout Probes</td>
<td>68</td>
</tr>
<tr>
<td>Configuring Proventia Network ADS</td>
<td>69</td>
</tr>
<tr>
<td>Testing and Viewing the NetScout Probe Flow Collection</td>
<td>70</td>
</tr>
</tbody>
</table>
Chapter 8: Configuring NetScout Integration

Configuring NetScout Probes

Introduction

To configure NetScout probes to integrate with Proventia Network ADS, you must set the flow export attributes to send flow data to the Proventia Network ADS Collector. You can configure multiple probes to send flows to a single Collector appliance.

Procedure

To configure NetScout probes:

1. Log on to the NetScout probe.
2. Record the source interface number, which is the one it uses to capture data.
   Tip: The interface number is displayed at the top of the command menu.
   Example: Interface number: 3
3. From the NetScout menu, choose option 11 to open the shell environment.
4. Type `set flow_export` to set the flow export attributes, followed by the source capture interface number.
5. Type the IP address for the destination host.
6. Type the port number.
7. Type the export time.
   The export time is the interval between data capture and export. The shorter the export time, the more accurate the Proventia Network ADS data is.
   Note: The fastest export time is 30 seconds.
8. Press ENTER.

Configuration example

The following example sets the source capture interface as 3 and sends the flows to destination host 10.0.2.103, on port 4000, with exports every 30 seconds.

```bash
% set flow_export on 3 10.0.2.103 4000 30
```
Configuring Proventia Network ADS

Introduction

Configure NetScout data collection your Collector management interface. You can either configure the Collector to gather any NetScout flows it sees, or to restrict it to gather data from specific probe addresses. You can add multiple NetScout probe IP addresses so your Proventia Network ADS Collector only listens to data from select sources.

Configuring NetScout collection

To configure your Proventia Network ADS Collector to receive NetScout data:

1. Log on to the Collector via SSH.
2. Navigate to the /services/ads menu.
3. Type `interface add`.
4. Type the name of the `interface` that collect the NetScout data.
   Note: This should be the Collector management interface.
5. Type `netscout`.
6. To restrict the NetScout collection to specific sources, type the NetScout probe IP address.
7. Press ENTER.
8. Repeat Steps 3 through 7 to add additional probes.

Configuring interfaces up

You must configure any interfaces you add as “up” in the ip/interface menu.

To configure an interface up:

1. Navigate to the /ip menu.
2. Type `interface`, followed by the interface `name`.
3. Type `up`, and then press ENTER.

NetScout configuration example

The following example restricts the source of the probe data being sent to the Collector to IP address 10.0.2.145:

```
admin@mariner.sea:/services/ads# interface add e3/4/1 netscout 10.0.2.145
admin@mariner.sea:/services/ads# /
admin@mariner.sea:/ip# interface e3/4/1 up
```
Testing and Viewing the NetScout Probe Flow Collection

Introduction

After you configure NetScout on the probe and on the Collector, you should verify that it is receiving flows from the probe. You can view all of the flows or enter an expression filter to only see specific types of traffic.

Verifying receipt of flows

To verify that Proventia Network ADS is receiving flows from the configured NetScout probe:

1. Navigate to the /ip/interfaces menu.
2. Type snoop to see all flows.
3. Append the command with a PCAP filter expression to see only specific traffic.
   
   **Note:** The system continues listing the flows until you stop it.
4. Press CTRL+C to stop the snoop report listing.

Snoop configuration example

This example shows the commands that allow you to view UDP flows that your Collector receives from 10.0.2.145 on port 4000. You can confirm that traffic is being directed to the interface if Proventia Network ADS lists the flows like the following example:

```
admin@mariner2.sea:/# ip interfaces snoop gx0 udp port 4000
10.0.2.145.2054 > 10.0.2.103.4000: udp 1188
10.0.2.145.2054 > 10.0.2.103.4000: udp 1164
10.0.2.145.2054 > 10.0.2.103.4000: udp 1268
10.0.2.145.2054 > 10.0.2.103.4000: udp 1164
10.0.2.145.2054 > 10.0.2.103.4000: udp 564
```

**Note:** Proventia Network ADS accepts industry standard PFCAP expression filters when used with the ip/snoop commands. The PCAP filter is optional.

**Reference:** For more information on PCAP syntax refer to [http://tcpdump.org](http://tcpdump.org).
Chapter 9

Creating User Groups

Overview

Introduction

You can create user groups and then assign the members of those groups with specific authorization keys. This allows you to customize the access the members of each group have.

In this chapter

This chapter contains the following topics:

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>About User Groups</td>
<td>72</td>
</tr>
<tr>
<td>Creating User Groups</td>
<td>73</td>
</tr>
<tr>
<td>Editing User Groups</td>
<td>74</td>
</tr>
<tr>
<td>Deleting User Groups</td>
<td>78</td>
</tr>
<tr>
<td>Adding Users to User Groups</td>
<td>79</td>
</tr>
</tbody>
</table>
About User Groups

Introduction

User groups are groups of users whose members all have the same assigned privileges, called authorization keys. You can create custom user groups in addition to those that are preconfigured on Proventia Network ADS. After you create a user group in the CLI, that group name appears as a choice for local users in the Group list on the User Accounts page in the Web user interface (UI).

Why create user groups?

User groups allow you to add users and then assign them to the appropriate group. This provides you with a greater level of granularity for your users' permissions.

Preconfigured user groups

In addition to the user groups you create, Proventia Network ADS comes preconfigured with four default user groups. These default groups are as follows:

<table>
<thead>
<tr>
<th>User group</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>system_admin</td>
<td>User with complete read and write access to the UI and the command line interface (CLI).</td>
</tr>
<tr>
<td>system_analyst</td>
<td>User with all of the permissions that an administrator has except for those related to network-wide configuration and other users.</td>
</tr>
<tr>
<td>system_user</td>
<td>User with UI read access to view events, and permission to create reports, change their own user account name and password, and view export flow information.</td>
</tr>
<tr>
<td>system_none</td>
<td>TACACS+ or RADIUS user that is not allowed to access Proventia Network ADS.</td>
</tr>
</tbody>
</table>

Note: Because the system_none user group is not allowed to access Proventia Network ADS, this group does not appear as a choice in the User Group list on the User Accounts page.

Table 17: Preconfigured user groups

Reference: See Table 18, “Authorization keys” on page 74 for a complete listing of all permissions for each user group.

About TACACS+ and RADIUS user groups

You must set user groups for RADIUS and TACACS+ on their respective servers. You cannot set them on the User Accounts page on the Proventia Network ADS Analyzer. If a user group is not specified on that server for a TACACS+ or RADIUS user, the users are assigned to the system_user group by default. You must change the user group on the server if this allows them more privileges than intended.

Reference: See “Changing the default user group setting” on page 80 for these instructions.
Creating User Groups

Introduction
You can create a new group and assign authorization keys for the privileges you want to
assign, or you can copy an existing group if you have a group with similar privileges.

Creating a new user group
To create a new user group:

1. Navigate to the /services/aaa/groups menu.
2. Type add followed by the new group name.
3. Press ENTER.
4. Type show followed by the group name to confirm the group was added.
5. Press ENTER.

New group configuration example
The following example adds the group sailors and then confirms it was added
successfully:

```
admin@mariner.sea:/services/aaa/groups# add sailors
admin@mariner.sea:/services/aaa/groups# show sailors
Group sailors:
   Default group: system_user (default)
```

Copying an existing user group
You can also create a new group by making a copy of an existing user group and then
changing the authorization keys assigned to it. You might want to do this when you create
a group with privileges that are similar to an existing user group.

To copy an existing group:

1. Navigate to the /services/aaa/group menu.
2. Type copy.
3. Type the existing group name.
4. Type the new group name.
5. Press ENTER.

Copied group configuration example
The following example shows a new group called mates added as a copy of the
system_user group:

```
admin@mariner.sea:/services/aaa/groups# copy system_user mates
admin@mariner.sea:/services/aaa/groups# show mates
Group mates:
   conf_show    Show running or saved configuration
   login_cli    Access to the CLI environment
   Default group: system_user (default)
```
Chapter 9: Creating User Groups

Editing User Groups

Introduction
This topic provides the instructions for editing an existing user group by changing the members or the members’authorization keys.

About authorization keys
You can change the permissions assigned to a group’s members by changing that group’s authorization keys. Each key represents a user permission.

Example: The clock key allows users in a specified group to set the system clock.

Adding and deleting keys for a user group
To add or remove a key for a given user group:
1. Navigate to the /services/aaa/groups menu.
2. Do one of the following:
   ■ Type key add to add an authorization key.
   ■ Type key delete to delete an authorization key.
3. Type the name of the user group.
4. Type the name of the key you are adding or deleting for that group.
5. Press ENTER.
6. Type show followed by the group name to confirm the key was added or deleted.

Key change configuration example
The following example gives members of the mates group the ability to change the system clock settings, but removes the ability to log into the Web user interface:

```
admin@mariner.sea:/services/aaa/groups# key add mates clock
admin@mariner.sea:/services/aaa/groups# key delete mates login_ui
admin@mariner.sea:/services/aaa/groups# show mates
Group mates:
   clock          Set the system clock
   conf_show      Show running or saved configuration
Default group: system_user (default)
```

Reference: See “Copying an existing user group” on page 73 for these instructions.

Authorization keys table
When typing keys, you must type the key exactly as it is shown. The following table displays the authorization keys that represent the privileges you can assign to user groups and the default groups to which they apply:

<table>
<thead>
<tr>
<th>This authorization key...</th>
<th>Allows the user to...</th>
<th>And applies to default group(s)...</th>
</tr>
</thead>
<tbody>
<tr>
<td>clock</td>
<td>Set the system clock.</td>
<td>admin</td>
</tr>
<tr>
<td>conf_imp</td>
<td>Import configuration from a disk.</td>
<td>admin</td>
</tr>
</tbody>
</table>

Table 18: Authorization keys
<table>
<thead>
<tr>
<th>This authorization key...</th>
<th>Allows the user to...</th>
<th>And applies to default group(s)...</th>
</tr>
</thead>
<tbody>
<tr>
<td>conf_show</td>
<td>Show running or saved configuration.</td>
<td>admin, analyst, and user</td>
</tr>
<tr>
<td>conf_write</td>
<td>Save the running configuration or export it to a disk.</td>
<td>admin and analyst</td>
</tr>
<tr>
<td>ip_access</td>
<td>Edit and apply IP access rules.</td>
<td>admin</td>
</tr>
<tr>
<td>ip_arp</td>
<td>Edit ARP information.</td>
<td>admin</td>
</tr>
<tr>
<td>ip_int</td>
<td>Edit IP interface configuration.</td>
<td>admin</td>
</tr>
<tr>
<td>ip_route</td>
<td>Edit route configuration.</td>
<td>admin</td>
</tr>
<tr>
<td>ip_snoop</td>
<td>Snoop network interface traffic.</td>
<td>admin</td>
</tr>
<tr>
<td>ip_tee</td>
<td>Edit IP tee configuration.</td>
<td>admin</td>
</tr>
<tr>
<td>login-cli</td>
<td>Access the command line interface.</td>
<td>admin, analyst, and user</td>
</tr>
<tr>
<td>login_ui</td>
<td>Access the Web user interface and the pages in the UI that aren’t specified by another authorization key.</td>
<td>admin, analyst, and user</td>
</tr>
<tr>
<td>reload</td>
<td>Reload Proventia Network ADS.</td>
<td>admin</td>
</tr>
<tr>
<td>shutdown</td>
<td>Shutdown Proventia Network ADS.</td>
<td>admin</td>
</tr>
<tr>
<td>srv_aaa</td>
<td>Edit local user and AAA configuration.</td>
<td>admin</td>
</tr>
<tr>
<td>srv_dns</td>
<td>Edit DNS cache configuration.</td>
<td>admin</td>
</tr>
<tr>
<td>srv_log</td>
<td>Edit logging configuration and view logs.</td>
<td>admin</td>
</tr>
<tr>
<td>srv_ntp</td>
<td>Edit NTP configuration.</td>
<td>admin</td>
</tr>
<tr>
<td>srv_ssh</td>
<td>Edit SSH configuration.</td>
<td>admin</td>
</tr>
<tr>
<td>srv_ssh_key</td>
<td>Manage SSH keys.</td>
<td>admin</td>
</tr>
<tr>
<td>srv_telnet</td>
<td>Edit telnet configuration.</td>
<td>admin</td>
</tr>
<tr>
<td>sys</td>
<td>Edit system information.</td>
<td>admin</td>
</tr>
<tr>
<td>sys_att</td>
<td>Edit system attributes.</td>
<td>admin</td>
</tr>
<tr>
<td>sys_cdrom</td>
<td>Lock and unlock the CD-ROM drive.</td>
<td>admin</td>
</tr>
<tr>
<td>sys_disk</td>
<td>Manage system disks.</td>
<td>admin</td>
</tr>
<tr>
<td>sys_file</td>
<td>Manage files.</td>
<td>admin and analyst</td>
</tr>
<tr>
<td>sys_file_admin</td>
<td>Install and uninstall software packages.</td>
<td>admin</td>
</tr>
</tbody>
</table>

Table 18: Authorization keys (Continued)
<table>
<thead>
<tr>
<th>Authorization key</th>
<th>Allows the user to...</th>
<th>And applies to default group(s)...</th>
</tr>
</thead>
<tbody>
<tr>
<td>web_approve_alerts</td>
<td>Approve alerts for a rule on the Alert Detail and Host Relation pages.</td>
<td>admin and analyst</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Users with web_edit_policy can approve alerts on the Rule Editor page.</td>
<td></td>
</tr>
<tr>
<td>web_clear_alerts</td>
<td>Clear alerts on the Event and Alert Details pages.</td>
<td>admin and analyst</td>
</tr>
<tr>
<td>web_create_rule</td>
<td>Create rules and access the Rule Editor page.</td>
<td>admin and analyst</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Users must have this key to recreate deleted ATF rules.</td>
<td></td>
</tr>
<tr>
<td>web_delete_rule</td>
<td>Delete rules throughout the Web UI, including ATF rules.</td>
<td>admin and analyst</td>
</tr>
<tr>
<td>web_edit_accounts</td>
<td>Edit user accounts in the Web UI, including adding users and changing passwords.</td>
<td>admin</td>
</tr>
<tr>
<td>web_edit_general</td>
<td>Edit settings on the General Settings page.</td>
<td>admin and analyst</td>
</tr>
<tr>
<td>web_edit_groups</td>
<td>Add, edit, and delete group objects.</td>
<td>admin and analyst</td>
</tr>
<tr>
<td>web_edit_itracking</td>
<td>Edit identity tracking settings.</td>
<td>admin and analyst</td>
</tr>
<tr>
<td>web_edit_notifications</td>
<td>Add, edit, and delete notification objects.</td>
<td>admin and analyst</td>
</tr>
<tr>
<td>web_edit_policy_settings</td>
<td>Manage policy settings.</td>
<td>admin and analyst</td>
</tr>
<tr>
<td>web_edit_port_groups</td>
<td>Add, edit, and delete port objects.</td>
<td>admin and analyst</td>
</tr>
<tr>
<td>web_edit_services</td>
<td>Edit service values on the Services page.</td>
<td>admin and analyst</td>
</tr>
<tr>
<td>web_edit_times</td>
<td>Add, edit, and delete time objects.</td>
<td>admin and analyst</td>
</tr>
<tr>
<td>web_edit_worm_protection</td>
<td>View and change worm protection settings.</td>
<td>admin and analyst</td>
</tr>
<tr>
<td>web_enforce_rule</td>
<td>Enforce rules on the Event Detail page.</td>
<td>admin and analyst</td>
</tr>
<tr>
<td>web_events</td>
<td>Read access to system events including the Activity page and all Detail pages.</td>
<td>admin, analyst, and user</td>
</tr>
<tr>
<td>web_explore</td>
<td>Read access to traffic data on the Explore page and Detail pages.</td>
<td>admin, analyst, and user</td>
</tr>
<tr>
<td>web_reports</td>
<td>Create and view reports and delete the reports the user created.</td>
<td>admin, analyst, and user</td>
</tr>
<tr>
<td>web_reports_delete_all</td>
<td>Delete any reports (not only those the user created).</td>
<td>admin and analyst</td>
</tr>
</tbody>
</table>

*Table 18: Authorization keys (Continued)*
**Table 18: Authorization keys (Continued)**

<table>
<thead>
<tr>
<th>This authorization key...</th>
<th>Allows the user to...</th>
<th>And applies to default group(s)...</th>
</tr>
</thead>
<tbody>
<tr>
<td>web_reports_templates</td>
<td>Create and schedule report templates.</td>
<td>admin and analyst</td>
</tr>
<tr>
<td>x_admin</td>
<td>Admin access to the CLI.</td>
<td>admin</td>
</tr>
<tr>
<td>x_flow_export</td>
<td>Export flow data.</td>
<td>admin, analyst, and user</td>
</tr>
<tr>
<td>x_flow_summary</td>
<td>View flow summaries in the CLI.</td>
<td>admin, analyst, and user</td>
</tr>
<tr>
<td>x_flow_watch</td>
<td>View flow capture data.</td>
<td>admin, analyst, and user</td>
</tr>
<tr>
<td>x_policy</td>
<td>Manage policies in the CLI.</td>
<td>admin and analyst</td>
</tr>
<tr>
<td>x_report_edit</td>
<td>Manage reports in the CLI.</td>
<td>admin and analyst</td>
</tr>
<tr>
<td>x_report_show</td>
<td>View reports in the CLI.</td>
<td>admin, analyst, and user</td>
</tr>
<tr>
<td>x_worm</td>
<td>Manage worms and quarantines in the CLI.</td>
<td>admin and analyst</td>
</tr>
</tbody>
</table>
Deleting User Groups

Introduction

When you delete a user group, the members of that group become members of the default group.

Reference: See “About the default user group setting” on page 80 for information about setting the default group.

Procedure

To delete a user group:

1. Navigate to the /services/aaa/groups menu.
2. Type `delete`.
3. Type the `user group name`.
4. Press ENTER.
   
   The delete confirmation message appears.
5. Do one of the following:
   
   ■ Type `y` (yes) to delete the group.
   
   ■ Type `n` (no) to cancel.
6. Press ENTER.

Example delete group configuration

The following example deletes the group sailors:

```
admin@mariner.sea:/services/aaa/groups# delete sailors
   Delete the configured group? [n] y
admin@mariner.sea:/services/aaa/groups#
```
Adding Users to User Groups

Introduction
You can begin adding local users to user groups after you have created the group.

Note: You can also add local users to existing user groups from the User Account Settings page in the Web user interface.


Viewing the list of configured users
Before you add a new user, you might want to see the list of current users.

To see a list of users:

1. Navigate to the /services/aaa/local menu.
2. Type show.
3. Press ENTER.

Viewing users configuration example
The following example shows the list of users, which includes the user name, the group to which they belong, and if their password is set:

```
admin@mariner.sea:/services/aaa/local# show
Local users:
    admin    system_admin      Password set
Accounting level commands
```

Adding a user to a user group
To add a local user to a user group:

1. Navigate to the /services/aaa/local menu.
2. Type add.
3. Type the user name.
4. Type the user group to which you want to assign the user.
5. Press ENTER.

Changing an existing user's group
To change the user group to which a local user belongs:

1. Navigate to the /services/aaa/local menu.
2. Type privilege.
3. Type the user name.
4. Type the new group name to which you want to add the user.
5. Press ENTER.

User example configuration
The following example adds user jdoe to the system_analyst group, and then changes her user group to system_admin:

```
admin@mariner1sea:/services/aaa/local# add jdoe system_analyst
admin@mariner.sea:/services/aaa/local# privilege jdoe system_admin
```
### About the default user group setting

If you add RADIUS or TACACS+ users but do not specify a user group for them, they will be assigned to the system_user default user group. This might provide more privileges for these users than are intended. You can change the default user group setting that applies to TACACS+ and RADIUS users that were not assigned to a group on the TACACS+ or RADIUS server, and also to any local users when the group they belong to is deleted.

### Changing the default user group setting

To change the default user group setting:

1. Navigate to the `/services/aaa/groups` menu.
2. Type `default set`.
3. Type the name of the user group that you want to be the default setting.
4. Press ENTER.

### Default user group configuration example

The following example sets the system_none group (with no privileges) as the default for any user that does not have a specified group:

```
admin@mariner.sea:/services/aaa/groups# default set system_none
```
Chapter 10

Configuring ATF Settings

Overview

Introduction

ISS’s Active Threat Feed (ATF) provides you with data about Internet-wide attacker activity as it relates to your network. The ISS security team gathers information for current and emerging threats from a wide range of sources and incorporates it into a database of threat profiles they maintain on the ATF server.

In this chapter

This chapter contains the following topics:

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>About ATF Behaviors</td>
<td>82</td>
</tr>
<tr>
<td>Setting a Proxy Server</td>
<td>83</td>
</tr>
<tr>
<td>Enabling and Updating the Poll Interval</td>
<td>84</td>
</tr>
<tr>
<td>Manually Updating the ATF Data</td>
<td>85</td>
</tr>
</tbody>
</table>
About ATF Behaviors

Introduction

The ATF database is maintained by the ISS security team and can only be accessed by current Proventia Network ADS customers. The ATF server uses your client certificate to authenticate for an SSL session to allow you to download the updated feed.

You can enable your Proventia Network ADS Analyzer to automatically poll the ATF server for updates at specific intervals. The server then correlates the data in relation to your network and automatically creates alerts and corresponding rules. Proventia Network ADS ATF generates worm, scan, and connection alerts.

ATF default settings

Automatic Threat Feed updates are enabled by default, so your Analyzer will connect back to the ISS ATF server for updates. If you do not want this feature enabled, you must disable it.

ATF rules

When the system creates rules from the ATF server, it displays them on the Rules page on the Policy tab in the Web user interface. You can then review the rules and see the involved clients, servers, and services, and make any changes (such as adding whitelist hosts you know are safe), before applying the ACL rules to your configured firewalls or switches.

Reference: For more information about viewing ATF rules, see Chapter 9, “Configuring Policy Settings,” in the Proventia Network ADS User Guide.

Prerequisite

In order to access the ATF server your Proventia Network ADS Analyzer must have DNS configured for valid name resolution.

Configuring ATF in the CLI

There is one setting you must configure in the command line interface (CLI), which is configuring a proxy server. You can set the time interval, which designates how often the Analyzer appliance polls the ATF server for updates, and manually update the ATF data from both the CLI and the Web user interface.
Setting a Proxy Server

Introduction
If you configure a proxer server to contact the ATF server, you must also set the server.

Procedure
To set a proxy server:

1. Navigate to the /services/ads/atf menu.
2. Type set proxy.
3. Type the HTTPS proxy hostname and port as a colon-separated string.
   Example: <hostname>:<port>
4. Press ENTER.

Proxy configuration example
The following example shows the commands for entering a proxy server:

admin@mariner.sea:/# services ads atf
admin@mariner.sea:/services/ads/atf# set proxy <hostname>:<port>
Enabling and Updating the Poll Interval

Introduction
To allow your Proventia Network ADS Analyzer to access the active threat feed, the ATF service must be enabled.

Enabling ATF updates
To enable automatic ATF updates:

1. Navigate to the /services/ads menu.
2. Type `atf set`.
3. Type `set server` followed by the host name of the ATF server.
   
   Note: You only need to set the host name if you want to use something other than the default ATF HTTPS server (atf.ISS.net) that is preconfigured on your Proventia Network ADS Analyzer.
4. Press ENTER.
5. Type `atf set status enable`.
6. Press ENTER.

Updating the poll interval
To update the interval that your Analyzer automatically polls the ATF server for updates:

1. In the /services/ads menu, type `atf set update`.
2. Type the number of hours from 1 to 168 (7 days).
3. Press ENTER.

Configuration errors
The system displays an error message when any of the following occur:

- You enable ATF without setting a server value.
- You enter an invalid server host name.
- You set a proxy server without setting a server.
- The system cannot contact either the proxy or the server.

ATF configuration example
The following configuration shows an example of setting the server and updating the poll interval time to every 24 hours:

```
admin@mariner.sea:/services/ads# atf ?
set              Set ATF configuration
clear            Clear ATF configuration
raw              Show ATF raw configuration
<cr>
admin@mariner.sea:# services ads atf
admin@mariner.sea:/services/ads/ads/atf# set ?
server           Configure ATF server
update           Configure ATF update interval (in hours)
proxy            Configure ATF proxy server
status           Enable or disable automatic ATF updates
admin@mariner.sea:/services/ads/ads/atf# set server atf.mariner.sea
admin@mariner.sea:/services/ads/ads/atf# set status enable
admin@mariner.sea:/services/ads/ads/atf# set update 24
```
Manually Updating the ATF Data

**Introduction**

If you do not have automatic updates configured, or are not able to configure automatic ATF updates, you can you can take advantage of the automatic threat feed by importing the most recent ATF data.

**How to access ATF**

You can access the most recent ATF file from the Customer Support Site. You might want to do this if you do not have outside network access, but still want the option of using the AFT policy data to help identify Internet threats and secure your network.

The ATF files on the Customer Support Site are package (.pkg) files and are named for the time time they were posted.

**Example:** atf-update-2006-07-07_12:05:00_GMT.pkg

**Procedure**

To import the most recent posted ATF package:

1. Log on to the Customer Support Site.
2. Copy the name of the most recent package file.
3. Log on to the Analyzer appliance.
4. Navigate to the /services/ads menu.
5. Type `atf import`.
6. Type `disk:<name of the package file>`.
7. Press ENTER.

The ATF data is updated and you can see any resulting changes to your ATF behavior rules in the Web user interface.

**ATF import configuration example**

The following shows a configuration example of an ATF imported package dated July 7, 2006:

```
admin@mariner.sea:/services/ads# atf ?
raw              Show ATF raw configuration
set              Set ATF configuration
clear            Clear ATF configuration
import           Import ATF policies
<cr>
admin@mariner.sea:/services/ads# atf import ?
  disk:<filename>
admin@mariner.sea:/services/ads# atf import disk:atf-update-2006-07-07_12:05:00_GMT.pkg
```

**Note:** You can also import the most recent ATF package in the Web user interface if you do not have automatic ATF updates configured. See the *Proventia Network ADS 3.6.1 User Guide* for these instructions.
Chapter 11

Configuring Check Point for Safe Quarantine

Overview

Introduction

Proventia Network ADS supports integration with Check Point’s Firewall-1. This chapter provides the instructions for configuring your Check Point console to communicate with and your firewall servers to accept access rules from your Proventia Network ADS appliances.

In this chapter

This chapter contains the following topics:

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>About Check Point Integration</td>
<td>88</td>
</tr>
<tr>
<td>Configuring the Check Point Console</td>
<td>89</td>
</tr>
<tr>
<td>Preparing to Configure Check Point on the Proventia Network ADS Analyzer</td>
<td>96</td>
</tr>
</tbody>
</table>
Chapter 11: Configuring Check Point for Safe Quarantine

About Check Point Integration

Overview
Integrating with Check Point’s Firewall-1 enables Proventia Network ADS to automatically apply filters on your existing firewalls to quarantine worm traffic. When you create a Safe Quarantine within Proventia Network ADS, it applies filters (or rules) on the firewall to keep out unwanted traffic, while still allowing legitimate traffic to pass.

Configuration task overview
You must configure both your Check Point SMARTmanagement console (Check Point console) and your Proventia Network ADS Analyzer to ensure they can communicate with each other.

The following table shows the tasks you must complete to configure Check Point integration:

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Add a host node for the Proventia Network ADS Analyzer on the Check Point console.</td>
</tr>
<tr>
<td>2</td>
<td>Add a Check Point management interface (CPMI) for the Proventia Network ADS Analyzer.</td>
</tr>
<tr>
<td>3</td>
<td>Create the activation key.</td>
</tr>
<tr>
<td>4</td>
<td>Retrieve and record the Proventia Network ADS SIC DN.</td>
</tr>
<tr>
<td>5</td>
<td>Save configuration.</td>
</tr>
<tr>
<td>6</td>
<td>Retrieve and record the Check Point console configuration.</td>
</tr>
<tr>
<td>7</td>
<td>Configure your Proventia Network ADS Analyzer.</td>
</tr>
</tbody>
</table>

Table 19: Check Point configuration tasks
Configuring the Check Point Console

**Introduction**

There are a series of steps you must perform to configure your Check Point SMART management console to allow communication with Proventia Network ADS. You must perform these configuration steps in the order presented.

**Adding a host node**

To add the Proventia Network ADS Analyzer host node to the Check Point console using Smart Dashboard:

1. Start the Check Point Smart Dashboard client application.

![Smart Dashboard window](image)

2. Select Manage → Network Objects.
3. Click New.
4. Select Node → Host.
   
   The Host Node window appears.

![Host Node window](image)

5. Type the Name and IP address of the Proventia Network ADS Analyzer.
6. Type any comments that describe this node to help you identify it in the Comments box.

7. Click OK.

8. Click Close in the Network Objects window to return to the SmartDashboard.

About the OPSEC CPMI application

The OPSEC Check Point management interface (CPMI) application for the Proventia Network ADS Analyzer defines the functions that the appliance is allowed to perform. First, you must add the CPMI application, and then you can specify on which host this application runs, and the permissions and client entities it uses.

Adding the OPSEC CPMI application

To add the CPMI applications and specify permissions:

1. Select Manage → Servers and OPSEC Applications.

The Servers and OPSEC application window appears.
2. Click New → OPSEC Application.

   The General tab in the OPSEC Application Properties window appears.

3. Type the Analyzer name in the Name box.

4. Select the Proventia Network ADS node you added from the Host list.

5. Select the CPMI check box in the Client Entities box.

   This activates the CPMI Permissions tab.

6. Select the CPMI Permissions tab to assign permissions to the new CPMI application (the Proventia Network ADS Analyzer).

   **Note:** You cannot use the default permissions.

7. Select the Permissions Profile option.

8. Click New.
9. The Permissions window appears.

10. Select the Read/Write All option.

11. Click OK to return to the CPMI tab.

The profile you added appears in the Permissions Profile box.

Creating the activation key

You must set up the one-time activation key (password) that the Analyzer uses to retrieve the SSL certificate. This is required to initialize the trust state between the Check Point console and your Proventia Network ADS Analyzer.
To create the activation key:

1. Click the General tab, and then click Communication.
   
   The Communication window opens.

   ![Activation Key Window]

2. Type the key in the Activation Key box.
   
   **Note:** The activation key is a password you type here and then use when you configure Check Point access on your Proventia Network ADS Analyzer.

3. Retype the key in the Confirm Activation Key box.

4. Click Initialize.
   
   This initializes the trust state.
   
   **Note:** The trust state is not established until you configure Check Point settings on your Proventia Network ADS Analyzer for Safe Quarantine.

5. Click Close to return to the General Properties tab.

**About the SIC DN**

After you create the activation key and initiate the trust state, the Check Point console generates an SSL certificate and the secure internal communication (SIC) distinguished name (DN) that it will use to identify and authenticate the Proventia Network ADS Analyzer.
Retrieving and recording the SIC DN

The Check Point console generates an SSL certificate and displays the SIC DN for your Proventia Network ADS Analyzer in the DN box.

To retrieve this information:

1. On the General Properties tab, locate the DN box.

2. Record this information in a location that you can easily access.
   
   **Tip:** ISS recommends copying and pasting this information in an accessible file.

3. Click OK to close the window and return to the Smart Dashboard.

Saving configuration

To save the configuration:

1. Click OK to close the OPSEC Applications window and return to the Smart Dashboard main screen.

2. On the Smart Dashboard main screen, click File ➔ Save.

Retrieving and recording the Check Point console configuration

You must have the Check Point console SIC DN and DN to configure your Proventia Network ADS Analyzer to communicate with Check Point.

To retrieve this information:

1. In the menu tree, click the plus sign (+) next to the Check Point icon to expand the menu.

2. Right-click the Management Server icon from the expanded Check Point menu, and then select Edit.
   
The Check Point Gateway General Properties window opens and displays the Check Point console SIC DN in the DN field at the bottom of the window.

3. Record this information in a location that you can easily access.
   
   **Tip:** ISS recommends copying and pasting this information in an accessible file.

You must enter this DN in the Check Point SMART console SIC DN field on the Worm Protection Settings page when you configure Check Point on your Proventia Network ADS Analyzer. In the meantime, we suggest copying and pasting it to a location that you can easily access later. The two systems use the DNs and the SSL certificate to communicate.
4. Click OK to close the window and return to the Smart Dashboard.
Preparing to Configure Check Point on the Proventia Network ADS Analyzer

Introduction

After you configure your Check Point console to communicate with Proventia Network ADS, you must configure Check Point worm protection settings on the Analyzer appliance.

Required information for configuring settings

Confirm you have copied or recorded the settings below. You will need these settings to configure worm protection settings in the Proventia Network ADS Web user interface.

<table>
<thead>
<tr>
<th>✓</th>
<th>Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>☐</td>
<td>Check Point OPSEC SMART Management console IP address</td>
</tr>
<tr>
<td>☐</td>
<td>Proventia Network ADS SIC DN</td>
</tr>
<tr>
<td>☐</td>
<td>Check Point SIC DN</td>
</tr>
<tr>
<td>☐</td>
<td>Activation key (password)</td>
</tr>
</tbody>
</table>

Table 20: Settings needed for Check Point configuration

Chapter 12

Using the CLI to Capture Flow Data

Overview

Introduction

You can view specific Proventia Network ADS flow data from the CLI in a variety of ways. Proventia Network ADS collects traffic information and consolidates it into proprietary flows then displays the output. You can watch incoming flows in real time, filter the flows you see, search the flow logs, and export flow data.

In this chapter

This chapter contains the following topics:

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Watching Flows</td>
<td>98</td>
</tr>
<tr>
<td>Viewing Flow Summaries</td>
<td>99</td>
</tr>
<tr>
<td>FCAP Flow Filters</td>
<td>102</td>
</tr>
</tbody>
</table>
Chapter 12: Using the CLI to Capture Flow Data

Watching Flows

Introduction

By default, the system displays start, update, and end flows. You can choose whether you want to see only the end flows, the flows from a specific Collector, or you can enter an PFCAP rule for Proventia Network ADS to use to filter the flows.

Viewing flows

To see incoming flows in real time:

1. Navigate to the /services/ads menu.
2. Type `flow watch`.
3. Type `end` to see only the end flows.
4. Type `collector`, followed by a Collector IP address to see flows from a specific Collector.
5. Type `fcap`, followed by a PFCAP filter to see specific flows.

Reference: See Table 21 on page 102 for examples of commands and options.

Note: You can also combine the two commands (end and collector) to see only the end flows from a specific Collector.

6. Press ENTER.

The system displays the flow data as comma-separated values.

Flow watch configuration example

The following example shows only the end flows that are destined to port 80, going through Collector `chicago`:

```
admin@mariner.sea:/# services ads
admin@mariner.sea:/services/ads# flow ?
Subcommands:
   export       Export flow data
   summary      View flow summary data
   watch        View real-time flows
admin@mariner.sea:/services/ads# flow watch ?
   end          Show only end-flows
   collector    Show flows from a specified collector
   fcap         Filter using FCAP
<cr>
admin@mariner.sea:/services/ads# flow watch fcap "dst port 80" collector chicago end
```

Note: If you have multiple Collectors with the same name, you cannot use that Collector’s name as part of the command. The system generates an error message if you enter a duplicate name.
Viewing Flow Summaries

Introduction
You can also use the flow summary fcap command to search through the database for specific flows using an FCAP expression.

Using PFCAP rule expressions
When you use an PFCAP rule expression, the system filters the traffic in the database to show you a summary of the matching traffic. The rule expressions allow you to create custom filters that you can use to see specific sources, destinations, ports, etc. You must enter the fcap command followed by the rule expression in quotations.

Reference: For additional information PFCAP rules, see “Appendix A: Searching by Using PFCAP Expressions,” in the Proventia Network ADS 3.6.1 User Guide.

Viewing flows
To see flow summaries:

1. Navigate to the /services/ads menu.
2. Type flow summary.
3. Type fcap, followed by an FCAP filter to see specific flows.
   Reference: See Table 21 on page 102 for examples of commands and options.
4. Type the timeframe for which you want to see the summary:

<table>
<thead>
<tr>
<th>Timeframe Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>day</td>
<td>Data aggregated over the past 24 hours.</td>
</tr>
<tr>
<td>week</td>
<td>Data aggregated over the last 7 days.</td>
</tr>
<tr>
<td>month</td>
<td>Data aggregated over the last 30 days.</td>
</tr>
<tr>
<td>year</td>
<td>Data aggregated over the last 12 months.</td>
</tr>
</tbody>
</table>

5. Press ENTER.
The system displays the flow data as comma-separated values.

PFCAP flow summary examples
The following example shows an FCAP rule that filters traffic to show a summary of the traffic destined for port 80 over the last week.

```
admin@mariner.sea:/services/ads/flow# summary ?
fcap Filter using FCAP
admin@mariner.sea:/services/ads/flow# summary fcap ?
 <filter>
admin@mariner.sea:/services/ads/flow# summary fcap “dst port 80”
timeframe ?
 year
 month
 week
 day
admin@mariner.sea:/services/ads/flow# summary fcap “dst port 80”
timeframe week
```

Example results
For the command above, Proventia Network ADS would return the following results (as comma-separated values):
src,dst,proto,sport,dport,in,out
141.213.40.22,141.211.175.122,6,65535,80,7002,1340
141.213.54.69,141.211.14.96,6,65535,80,8625,8452
141.213.50.163,141.211.61.47,6,65535,80,927320,71906
141.213.66.237,141.211.144.237,6,65535,80,192453,58974
141.213.66.220,141.211.144.218,6,65535,80,156454,57718
141.213.74.30,141.211.144.188,6,65535,80,818442,555676

Sorting the flow data
You can also specify how you want the system to show the data, sorted by a particular field, or limited to a certain number of output lines.

To sort the flows:

1. In the /services/ads/flow menu, type sort.
2. Type the field that you want the system to use when displaying the output.
3. Values are as follows: source, destination, protocol, port, or bytes.
4. Press ENTER.

Flow sort example
The following example sorts the output by the source field.

admin@mariner.sea:/services/ads/flow# summary fcap “dst port 80”
timeframe week ?
sort       Sort by field
limit      Limit output lines
<cr>
admin@mariner.sea:/services/ads/flow# summary fcap “dst port 80”
timeframe week sort source

Limiting flows
You can specify the number of lines of output the system returns when you view the flows.

To limit the number of lines:

1. In the /services/ads/flow menu, type limit.
2. Type the number of lines you want the system to display.
3. Press ENTER.

The limit command allows you to enter an integer and the system limits the output to that specified number of lines.

Flow limit example
The following example limits the output to 20 lines:

admin@mariner.sea:/services/ads/flow# summary fcap “dst port 80”
timeframe week limit 20

About the export command
You can search the flow log, similar to searching flows on the Flows page in the Web user interface. Use the count command, with the export command to see a top count of hosts by source, destination, source port, or destination port. If you enter the recent command, Proventia Network ADS only searches through the last one million flows.
Exporting flows

To export flows:

1. In the /services/ads/flow menu, type export.
2. Type fcap, followed by a PFCAP filter to see specific flows.
   Reference: See Table 21 on page 102 for examples of commands and options.
3. Type count, followed by the type of results you want to see.
   Values are: src, dst, sport, and dport.
4. Type recent if you only want ADS to search the most recent one million flow records.
5. Press ENTER.

Flow export example

The following example searches the flow log and displays the number of time destination port 80 appears:

```
admin@mariner.sea:/services/ads/flow# summary fcap "dst port 80"
```

```
timeframe week limit 20
```

```
admin@mariner.sea:/services/ads/flow# export ?
fcap Filter using FCAP
admin@mariner.sea:/services/ads/flow# export fcap ?
<filter> FCAP filter expression
admin@mariner.sea:/services/ads/flow# export fcap "dst port 80" ?
count Count number of times that field appears
recent Display recent flows
<cr>
```

```
admin@mariner.sea:/services/ads/flow# export fcap "dst port 80" count src
```

Count configuration example

The following example shows the count command string that would show you which source is sending the most Web traffic:

```
admin@mariner.sea:/services/ads/flow# export fcap "dst port 80" count src
```

```
count__x_,source
1,10.0.1.0
1,10.0.1.1
1,10.0.1.2
1,10.0.1.3
```
# FCAP Flow Filters

The following table shows examples commands and options you can use to create FCAP filters to see flow information:

<table>
<thead>
<tr>
<th>For</th>
<th>Use Command</th>
<th>With Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Flow-related filters</td>
<td>filter input</td>
<td>src/dst ip</td>
</tr>
<tr>
<td></td>
<td>filter flowlog</td>
<td>src/dst net</td>
</tr>
<tr>
<td></td>
<td>flow watch</td>
<td>-proto</td>
</tr>
<tr>
<td></td>
<td></td>
<td>src/dst port</td>
</tr>
<tr>
<td></td>
<td></td>
<td>src/dst tcpflags</td>
</tr>
<tr>
<td></td>
<td></td>
<td>src/dst bytes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>src/dst packets</td>
</tr>
<tr>
<td></td>
<td></td>
<td>icmptype</td>
</tr>
<tr>
<td></td>
<td></td>
<td>icmpcode</td>
</tr>
<tr>
<td>Database-related FCAP filters</td>
<td>flow summary</td>
<td>src/dst ip</td>
</tr>
<tr>
<td></td>
<td></td>
<td>src/dst net</td>
</tr>
<tr>
<td></td>
<td></td>
<td>proto</td>
</tr>
<tr>
<td></td>
<td></td>
<td>src/dst port</td>
</tr>
<tr>
<td></td>
<td></td>
<td>icmptype</td>
</tr>
<tr>
<td></td>
<td></td>
<td>icmpcode</td>
</tr>
<tr>
<td>SQL flowlog-related FCAP filters</td>
<td>flow export</td>
<td>src/dst ip</td>
</tr>
<tr>
<td></td>
<td></td>
<td>srd/dst net</td>
</tr>
<tr>
<td></td>
<td></td>
<td>proto</td>
</tr>
<tr>
<td></td>
<td></td>
<td>icmptype</td>
</tr>
<tr>
<td></td>
<td></td>
<td>icmpcode</td>
</tr>
<tr>
<td></td>
<td></td>
<td>src/dst port</td>
</tr>
<tr>
<td></td>
<td></td>
<td>src/dst tcpflags</td>
</tr>
<tr>
<td></td>
<td></td>
<td>src/dst bytes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>src/dst packets</td>
</tr>
</tbody>
</table>

*Table 21: PFCAP filter commands and options*
Chapter 13

Manually Installing Proventia Network ADS on your Appliances

Overview

Introduction While most network operators choose to use the Web-based setup wizard to install Proventia Network ADS and configure the initial settings, this chapter includes the manual instructions for completing these tasks in the CLI. You might not want to configure every setting. Unless otherwise specified, you can configure these settings on both the Analyzer and Collector appliances.

In this chapter This chapter contains the following topics:

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Task Overview for Manual Installation</td>
<td>104</td>
</tr>
<tr>
<td>Determining the Mode and Setting Up Communication</td>
<td>106</td>
</tr>
<tr>
<td>Configuring Interfaces</td>
<td>108</td>
</tr>
<tr>
<td>Setting the System Name and Default Route</td>
<td>110</td>
</tr>
<tr>
<td>Setting up Services for Remote Access</td>
<td>111</td>
</tr>
<tr>
<td>Configuring Access Rules</td>
<td>112</td>
</tr>
<tr>
<td>Setting up Domain Name Services and SMTP</td>
<td>113</td>
</tr>
<tr>
<td>Changing the Administrative Password</td>
<td>114</td>
</tr>
<tr>
<td>Setting System Time</td>
<td>115</td>
</tr>
<tr>
<td>Saving the Configuration Changes and Starting Proventia Network ADS</td>
<td>117</td>
</tr>
<tr>
<td>Configuring Additional Optional Settings</td>
<td>118</td>
</tr>
</tbody>
</table>
Task Overview for Manual Installation

Introduction
You should complete the installation tasks in the order presented for the Analyzer and the Collector appliances to ensure proper installation.

Tasks for the Analyzer
The following table shows the tasks you should complete to install or reinstall an Analyzer appliance:

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Configure the Management Interface and subnet mask.</td>
</tr>
<tr>
<td>2</td>
<td>Configure NetFlow sources. <strong>Note</strong>: This only applies for Standalone mode when you do not have Collectors.</td>
</tr>
<tr>
<td>3</td>
<td>Configure the shared secret. <strong>Note</strong>: This only applies for Two-tier mode deployments.</td>
</tr>
<tr>
<td>4</td>
<td>Configure the default route.</td>
</tr>
<tr>
<td>5</td>
<td>Configure the Hostname.</td>
</tr>
<tr>
<td>6</td>
<td>Configure services for remote access.</td>
</tr>
<tr>
<td>7</td>
<td>Configure IP access rules.</td>
</tr>
<tr>
<td>8</td>
<td>Configure the DNS server.</td>
</tr>
<tr>
<td>9</td>
<td>Configure the SMTP relay.</td>
</tr>
<tr>
<td>10</td>
<td>Reset the administrator password.</td>
</tr>
<tr>
<td>11</td>
<td>Set the system time.</td>
</tr>
<tr>
<td>12</td>
<td>Initialize the database.</td>
</tr>
<tr>
<td>13</td>
<td>Start Proventia Network ADS services.</td>
</tr>
<tr>
<td>14</td>
<td>Save the configuration.</td>
</tr>
<tr>
<td>15</td>
<td>Stop Proventia Network ADS services.</td>
</tr>
<tr>
<td>16</td>
<td>Reload (reboot) the appliance.</td>
</tr>
</tbody>
</table>

Table 22: Analyzer tasks

Task list for Collectors
The following table shows the tasks you should follow to install or reinstall a Collector appliance:

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Configure the Management Interface and subnet mask.</td>
</tr>
<tr>
<td>2</td>
<td>Configure NetFlow sources. This step is for Collector models that allow you to set NetFlow interfaces. You cannot configure NetFlow sources on PCAP Collector models.</td>
</tr>
<tr>
<td>3</td>
<td>Configure the default route.</td>
</tr>
<tr>
<td>4</td>
<td>Configure the Hostname.</td>
</tr>
</tbody>
</table>

Table 23: Collector tasks
### Task Overview for Manual Installation

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>Configure services for remote access.</td>
</tr>
</tbody>
</table>
| 6    | Configure access rules.  
**Note**: Configuring Web access (https) on the Collector is optional. |
| 7    | Configure the DNS server. |
| 8    | Reset the administrator password. |
| 9    | Set the time. |
| 10   | Initialize the database. |
| 11   | Configure the sendto address.  
**Note**: The sendto address is the IP address for the Analyzer to which this Collector forwards data. |
| 12   | Set the shared secret to allow communication between the Collector and Analyzer. |
| 13   | Start Proventia Network ADS services. |
| 14   | Save the configuration. |
| 15   | Stop Proventia Network ADS services. |
| 16   | Reload (reboot) the appliance. |

**Table 23**: Collector tasks (Continued)
Determining the Mode and Setting Up Communication

Introduction

When you initially configure the appliances by using the Setup Wizard, you can select the mode. In the CLI, if you enter a sendto address for the Analyzer on the Collector, this automatically configures the appliances in Two-tier mode.

About the shared secret

For the Proventia Network ADS Analyzer to accept connections from Collectors, you must set a shared secret for communications on the Analyzer and all Collectors. The secret is word or phrase that the system uses to encrypt traffic between the Analyzer and Collectors.

Setting the secret

To set the shared secret on the Analyzer and the Collectors:

1. Navigate to the /services/ads menu.
2. Type secret set.
3. Type the secret.

   Note: The secret can be any word or phrase, but you must set the same shared secret when you configure the Analyzer and each Collector.
4. Press ENTER.

Secret configuration example

The following example sets the secret on the Analyzer as sharedsecret:

```
admin@mariner.sea:/services/ads# secret set sharedsecret
admin@mariner.sea:/services/ads# secret
Encrypted zone secret: kDQCLKF.ayg7OI
```

Setting up the sendto address

In order for the Collector to send traffic to the Analyzer, you must configure the Analyzer address as the send to destination on the Collector. The Collector sends traffic data to the configured Analyzer, using the shared secret.

To set the sendto address:

1. Connect to the Collector appliance.
2. Navigate to the /services/ads menu.
3. Type sendto add.
4. Type the Analyzer IP address to which this Collector will forward traffic data.
5. Type the shared secret that you set on the Analyzer in the procedure above.
6. Press ENTER.

Sendto configuration example

This example sets up communication with the Analyzer (IP address 10.0.1.1), using the secret added on the Analyzer, sharedsecret:

```
admin@mariner2.sea:/services/ads# sendto ?
    add              Add remote destination
    delete           Delete remote destination
    clear            Clear remote destinations
    <cr>             Show remote destinations
admin@mariner2.sea:/services/ads# sendto add ?
```
<A.B.C.D>
encrypted
admin@mariner2.sea:/services/ads# sendto add 10.0.1.1 ?
<shared secret>
admin@mariner2.sea:/services/ads# sendto add 10.0.1.1 sharedsecret
Notifying destination.................................Ok
admin@mariner2.sea:/services/ads# sendto
Sendto destinations:
10.0.1.1
Configuring Interfaces

Introduction
This topic provides the instructions for setting the Management interface and for setting additional interfaces.

About the Management interface
To set the Management interface, enter the unique IP address and netmask for your network. This usually corresponds to the Management/NetFlow Ethernet port on the back of the appliance.

Reference: See “Analyzer appliance back panel diagram” on page 16 and “Collector Ports Diagram” on page 17.

Setting the management interface
To set the management interface:

1. Navigate to the `ip/interfaces` menu.
2. Type `ifconfig ?` to see the available IP interfaces.
3. Type the command `ifconfig`.
4. Type the interface name.
   Example: `e3/4/1`
5. Type the IP address for the interface, followed by the netmask.
6. Type `up` to set the state.
7. Press ENTER.

Management interface configuration example
The following example sets the Analyzer management interface as `e3/4/1`:

```
admin@mariner.sea:/ip/interfaces# ifconfig e3/4/1 10.0.1.2 255.255.255.0 up
```

Setting NetFlow sources
When you complete the initial setup using the Setup Wizard, you can set NetFlow interfaces using the Web user interface. After you complete the initial setup, if you want to change the settings or add NetFlow interfaces, you must do so in the CLI.

Flow source maximums
The number of flow sources you can add is as follows:

<table>
<thead>
<tr>
<th>Mode</th>
<th>Appliance Configured On</th>
<th>Maximum Number of Flow Sources</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standalone</td>
<td>Analyzer</td>
<td>3</td>
</tr>
<tr>
<td>Two-tier</td>
<td>Collector Model AD3000</td>
<td>None, packet capture</td>
</tr>
<tr>
<td>Two-tier</td>
<td>Collector Model AD3007</td>
<td>7</td>
</tr>
<tr>
<td>Two-tier</td>
<td>Collector Model AD3014</td>
<td>14</td>
</tr>
<tr>
<td>Two-tier</td>
<td>Collector Model AD3020</td>
<td>20</td>
</tr>
</tbody>
</table>

Table 24: Maximum number of NetFlow sources
Adding NetFlow sources

To make changes to settings you configured during the setup process or to add new NetFlow interfaces:

1. Navigate to the `/services/ads/interface` menu.
2. Type `add`.
3. Type the name of the interface.
   
   Example: e3/7/1

4. Type `netflow`.
5. Type the IP address for the router that is sending the NetFlow.
6. Press ENTER.
7. Repeat Steps 2 through 7 for each additional NetFlow source you want to add.
Setting the System Name and Default Route

Introduction
This topic provides the instructions for setting the system name (hostname) and for setting the default route.

Default route
The default route, or gateway, is the first hop that sends outbound network traffic. This is typically the subnet switch or router.

Setting the default route
To set the default route:

1. Navigate to the ip/route menu.
2. Type add default.
3. Type the IP address for the default route (gateway).
4. Press ENTER.

Default route configuration example
The following example sets the default route as 10.0.1.1:

```
admin@mariner.sea:/# ip route
admin@mariner.sea:/ip/route# add default 10.0.1.1
```

About the system (or host) name
The default setting for the hostname is ados. You should change this to your system name, which is usually the appliance’s DNS name. After you set the name, it is displayed in the command prompts in the CLI and appears in any alert notifications. You should use the fully qualified domain name so that when it is included in alert notifications, the links work properly.

Setting the system name
To set the system name:

1. Navigate to the /system menu.
2. Type name set.
3. Type the name for the system.

You can use any combination of characters and dashes. Spaces are not allowed.

Note: ISS recommends using the FQDN.

System name configuration example
For this example, the Proventia Network ADS Analyzer is named mariner.sea.

```
ados:/system# name set mariner.sea
admin@mariner.sea:/system#
```
Setting up Services for Remote Access

Introduction

You can set up remote access services through SSH and Telnet. Both are disabled by default, so you must configure them. ISS highly recommends that you use SSH to ensure safe communications.

Setting up SSH service

To set up SSH remote access:

1. Navigate to the /services/ssh menu.
2. Type `port set`.
3. Type either the port number or to use port 22, type `default`.
4. Press ENTER.
5. Type `key host set default` to set the host key file.
   - If the system displays a message that the key file does not exist, type `y` to confirm that you want to generate it.
6. Press ENTER to set or generate the file.
7. Type `start`, and then press ENTER to start SSH services.

SSH configuration example

The following example shows the configuration for adding SSH service and generating the key file.

```
admin@mariner.sea:/# services ssh
admin@mariner.sea:/services/ssh# ?
Subcommands:
  key/             SSH key management
  port             Show or set the SSH service port
  show             Show SSH configuration and status
  start            Start the SSH service
  stop             Stop the SSH service
admin@mariner.sea:/services/ssh# port ?
<cr>             Show configured port
admin@mariner.sea:/services/ssh# port set ?
<1-65535>        Port number
  default          Use port 22
admin@mariner.sea:/services/ssh# port set default
admin@mariner.sea:/services/ssh# key host set default
Key file does not exist.
  Generate? [y] y
Generating new SSH host key file.................done.
admin@mariner.sea:/services/ssh# start
```
Chapter 13: Manually Installing Proventia Network ADS on your Appliances

Configuring Access Rules

Introduction
To ensure a high level of security, Proventia Network ADS denies all incoming IP traffic by default. You must manually configure a set of IP access rules to allow traffic through to the local SSH port from designated remote IP addresses or networks. You must also add an access rule to allow the appliance to receive pings from other appliances to ensure the appliance is connected to the network, and an access rule to access the Web user interface.

Committing rules
After you add the access rules, you must commit them. The system maintains both the inactive and active rules. When you make add new rules or make changes to the existing access rules, you are editing the inactive set. Committing the access rules installs and activates them.

Note: You can see if the status of the rules by showing the IP access rule list. If the system displays the IP access rules as “Inactive”, it indicates you must commit them to activate them.

Configuring access rules
To configure access rules:

1. Navigate to the ip/access menu.
2. Type one of the following:
   
   Access Type | Command
   :------------|----------
   SSH         | add ssh  
   Pings to your appliance | add ping 
   Web user interface | add https

Note: You are only required to add Web access on the Analyzer.

3. Type the interface name.
   Example: e3/7/1
4. Type the IP address for the appropriate network.
5. Press ENTER.
6. Type commit to activate the rules, and then press ENTER.

Access list configuration example
This example allows SSH connections, pings, and http access from the 10.0.1.0/24 network:

```
admin@mariner.sea:// ip access
admin@mariner.sea://ip/access# add ssh e3/4/1 10.0.1.0/24
admin@mariner.sea://ip/access# add ping e3/4/1 10.0.1.0/24
admin@mariner.sea://ip/access# add https e3/4/1 10.0.1.0/24
admin@mariner.sea://ip/access# commit
admin@mariner.sea://ip/access# show active
```

Active IP access rules:

```
ssh e3/4/1 10.0.1.0/24
ping e3/4/1 10.0.1.0/24
https e3/4/1 10.0.1.0/24
```
Introduction

This topic provides the procedures for setting the DNS server and for configuring SMTP. The SMTP relay is the address that Proventia Network ADS uses to send email alert notifications. Configure SMTP settings on the Analyzer appliance.

The DNS server setting

You must designate the DNS server for Proventia Network ADS to use to lookup host names. This DNS server is currently only used within the Proventia Network ADS user interface, not in the CLI.

Configuring DNS

To configure the DNS server:

1. Navigate to the /services/dns menu.
2. Type `server add`.
3. Type the IP address for the DNS server.
4. Press ENTER.

DNS configuration example

```
admin@mariner.sea:/ # services dns
admin@mariner.sea:/services/dns# server add 10.0.1.11
admin@mariner.sea:/services/dns#
```

Configuring SMTP

To configure SMTP:

1. Navigate to the /services/ads menu.
2. Type `smtp set`.
3. Type the IP address for the SMTP relay.
4. Press ENTER.

SMTP configuration example

```
The following example shows setting the SMTP server as 10.0.1.25.

admin@mariner.sea:/ # services ads
admin@mariner.sea:/services/ads# smtp ?
    set              Set SMTP relay address
    clear            Clear SMTP relay address
<cr>
admin@mariner.sea:/services/ads# smtp set ?
    <A.B.C.D>
admin@mariner.sea:/services/ads# smtp set 10.0.1.25
```
Chapter 13: Manually Installing Proventia Network ADS on your Appliances

Changing the Administrative Password

Introduction

You must change the default admin password to ensure only authorized parties have the ability to administer the server.

Choosing a secure and acceptable password

You should choose a password that contains a sufficient mix of letters and numbers. The password must meet the following criteria:

- must be at least 7 characters in length
- must be no more than 35 characters in length
- cannot be all digits
- cannot be all lower-case letters
- cannot include spaces

Changing the password

To change the password:

1. Navigate to the services/aaa/local menu.
2. Type the password command.
3. Type the username for the account (admin).
4. Type interactive, and then press ENTER.
   
   The system displays the New password and Retype password prompts.
5. Type the new password, and then press ENTER.
6. Type the new password again to confirm, and then press ENTER.

Password configuration example

The following shows an example of the commands for changing the password:

```
admin@mariner.sea:/# services aaa local
admin@mariner.sea:/services/aaa/local# password admin ?
interactive Change password interactively
encrypted Encrypted password follows
unencrypted Unencrypted password follows
<cr>
admin@mariner.sea:/services/aaa/local# password admin interactive
Changing local password for admin.
New password:
Retype new password:
```
Setting System Time

Introduction

You can configure the system time either by setting an NTP server, or by using the global clock command. This topic includes instructions for both; however, ISS highly recommends that you set each Analyzer and Collector to use network time protocol (NTP) to synchronize the time across the zone. If you do not set NTP, the system might show data with skewed times.

Setting NTP

To set NTP:

1. Navigate to the services/ntp submenu.
2. Type the server set command.
3. Type the IP address for the appropriate server address.
4. Press ENTER.
5. Type start, and then press ENTER to start NTP services.

NTP configuration example

The following example sets the server 10.0.1.2 as the NTP server:

```
admin@mariner.sea:/# services ntp
admin@mariner.sea:/services/ntp# ?
Subcommands:
  server           Configure NTP servers
  show             Show NTP configuration and status
  start            Start the NTP service
  stop             Stop the NTP service
admin@mariner.sea:/services/ntp# server set 10.0.1.2
admin@mariner.sea:/services/ntp# start
admin@mariner.sea:/services/ntp# show
NTP status:
  Status: running
  NTP Configuration:
    Primary server:
      Address: 10.0.1.2
admin@mariner.sea:/services#
```

Using the clock command

To use the clock command to set the time, enter the time in the standard Unix date format.

To set the time manually:

1. Stop Proventia Network ADS services.
   Navigate to the services/ads/ menu and type stop.
2. Type clock set from any menu in the CLI.
   Note: You can use the clock set command from any menu within the CLI. In this case you will be in the /services/ads menu.
3. Type the date in Unix format, and then press ENTER.
   Example: 200608071000
4. Type start to start ads services after you set the clock, and then press ENTER.
Clock configuration example

The following command sets the current time to August 7, 2006 at 11:56 GMT:

```
admin@mariner.sea:# services ads
admin@mariner.sea:/services/ads# stop
Stopping Proventia ADS services.................................done.
admin@mariner2.sea:/services/ads# clock set 200608071156
Mon Aug 7 11:56:00 GMT 2006
admin@mariner2.sea:/services/ads# start
```

Setting the timezone

You can set the timezone directly if you know the corresponding command. Otherwise, you can use the interactive menu, which displays a list of the timezone commands from which to choose.

To set the timezone:

1. Navigate to the `services/ads` menu and type `stop` to stop Proventia Network ADS services.
2. Navigate to the `/system` menu.
3. Type `timezone set`.
4. Do one of the following:
   - Type `timezone`, followed by the `command` for your timezone.
     - **Example:** EST
   - Type `timezone set ?` to set the system timezone interactively.
5. Press ENTER to see the list of command choices, and then type the `command` for the timezone that applies to your network.
6. After you set the timezone, navigate to `/services/ads` menu.
7. Type `start` to restart Proventia Network ADS services, and then press ENTER.

Timezone configuration example

The following example sets the timezone to eastern standard daylight savings time (EST5EDT):

```
admin@mariner.sea:# services ads
admin@mariner.sea:/services/ads# stop
Stopping Proventia Network ADS services.............................done.
admin@mariner.sea:/services/ads# / system
admin@mariner.sea:/system# timezone ?
    set      Set the system timezone
<cr>
admin@mariner.sea:/system# timezone set ?
<timezone>      System timezone
<cr>
    Set the system timezone interactively
admin@mariner.sea:/system# timezone set EST5EDT
```
Saving the Configuration Changes and Starting Proventia Network ADS

Introduction
You must follow the steps in the order presented to complete the final installation tasks and restart the appliance.

Shutdown and reload commands
It is important to understand the difference between the shutdown and reload commands. The `shutdown` command halts the appliance. A network operator must reboot the appliance if it is halted, whereas the `reload` command reboots the appliance without network operator intervention.

Note: You must stop ads services before using either command.

Initializing the database
The Proventia Network ADS system uses an internal database that you must initialize before the system can run.

To initialize the database:

1. Navigate to the `services/ads` menu.
2. Type `database initialize`.
3. Press ENTER.
4. The system displays a status message showing it is building the databases, and then it displays done when it finishes.
5. Type `start`, and then press ENTER to start ads services.
6. Type `conf write`, and then press ENTER to save the configuration.
7. Type `reload` to reboot the appliance.
8. Enter `y` and press ENTER to confirm.
9. When the appliance reboots, log on again to start using Proventia Network ADS.

Configuration example
The following shows an example of the commands described above:

```
admin@mariner.sea:/# services ads
admin@mariner.sea:/services/ads# database initialize
Building Databases
................................................................................................................
..................................................................
done.
admin@mariner.sea:/services/ads# start
Starting Proventia Network ADS services............................done.
admin@mariner.sea:/services/ads# conf write
admin@mariner.sea:/services/ads# stop
Stopping Proventia Network ADS.................................done.
admin@mariner.sea:/services/ads# reload
Do you wish to proceed? [n] y
094: Rebooting the system..
Broadcast message from root (pts/4) (Wed Mar  8 20:06:20 2006):

The system is going down for reboot NOW!
```
Configuring Additional Optional Settings

Introduction
This topic includes the instructions for additional settings you can configure on the Analyzer appliance.

Adding an entry to the address resolution protocol (ARP) table
You can manually add temporary or permanent entries to the ARP table. At a minimum, you can choose to add your gateway for security purposes. You can then specify whether the entry is temporary or permanent. If you do not specify, the system makes the entry static, but allows you to overwrite it in the future.

To add an entry:
1. Navigate to the `ip/arp` menu.
2. Type `add`, followed by the IP address and the MAC address of the gateway.
3. Do one of the following:
   - Type `temporary` to make the entry a temporary entry.
   - Type `permanent` to make the entry permanent.
4. Press ENTER.

ARP configuration example
The following example shows configuration for a temporary entry.

```
admin@mariner.sea:/# ip arp
admin@mariner.sea:/ip/arp# add 10.0.2.1 ff:ff:ff:ff:ff:ff ?
  temporary        Add a temporary ARP entry
  permanent        Add a static ARP entry
  <cr>             Add a static but overwritable ARP entry

admin@mariner.sea:/ip/arp# add 10.0.2.1 ff:ff:ff:ff:ff:ff temp
```

The SNMP agent community for SNMP polling
Proventia Network ADS allows external sources to SNMP query the appliances for system status and configuration information.

Setting the SNMP agent community
To set the SNMP agent community:
1. Navigate to the `services/ads` menu.
2. Type `snmpagent community`.
3. Type `set`, followed by the `community string`.
4. Press ENTER.
5. Navigate to the `ip/access` menu to add an access rule.
   This allows external sources to access the Analyzer for SNMP data.
6. Type `add snmp all`, followed by the `netmask` that covers the networks you want to allow to query the Analyzer.
7. Press ENTER.
8. Type `commit` to commit the new rule, and then press ENTER.
Configuring Additional Optional Settings

SNMP agent configuration example

The following example sets the community string to public and allows access from all (0.0.0.0/0). You can configure this setting to be more restrictive.

```
admin@mariner.sea:/# services ads
admin@mariner.sea:/services/ads# snmpagent community ?
    set     Set community
clear    Clear community
    <cr>    Show the snmpagent community
admin@mariner.sea:/services/ads# snmpagent community set ?
    <community>
admin@mariner.sea:/services/ads# snmpagent community set public
admin@mariner.sea:/services/ads# / ip access
admin@mariner.sea:/ip/access# add snmp all 0.0.0.0/0
admin@mariner.sea:/ip/access# commit
```

About teeing

NetFlow

The tee functionality in Proventia Network ADS allows you to duplicate the NetFlow records your Collector receives and forward those records to another IP address.

Adding a tee rule

To add a tee rule on your network:

1. Navigate to the `/ip/tee` menu.
2. Type `add`.
3. Type the IP address and the port of the source that will be forwarding data, using the format in the following example:

   **Example:** `[A.B.C.D]:[1-65535]`

4. Type the IP address and the port number of the destination of the teed data, using the format shown in the example in Step 3.
5. Type `start` to begin teeing NetFlow data.

   **Note:** Starting the tee resets the counter.

Deleting or stopping NetFlow tee

You can either stop the NetFlow teeing or delete a specific tee rule, allowing the remaining rules to continue teeing data:

1. Navigate to the `/ip/tee` menu.
2. Do one of the following:
   - Type `stop` to stop the NetFlow tee.
   - Type `delete`, followed by the rule to delete a specific tee rule.

   **Note:** The rule format is the IP address and the port of the source: the IP address and the port of the destination.

   **Example:** `[A.B.C.D]:[1-65535] [A.B.C.D]:[1-65535]`

3. Press enter.

Example tee configuration

The following example shows data teed from 192.168.1.1 port 111 to 198.168.1.2 port 222:

```
admin@mariner.sea:/# ip tee
admin@mariner.sea:/ip/tee# ?
Subcommands:
    add         Add a NetFlow tee rule
counter     Show or reset NetFlow tee counters
```
Chapter 13: Manually Installing Proventia Network ADS on your Appliances

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>delete</td>
<td>Delete a NetFlow tee rule</td>
</tr>
<tr>
<td>show</td>
<td>Show NetFlow tee configuration</td>
</tr>
<tr>
<td>start</td>
<td>Start the NetFlow tee</td>
</tr>
<tr>
<td>stop</td>
<td>Stop the NetFlow tee</td>
</tr>
</tbody>
</table>

admin@mariner.sea:/ip/tee# add ?
[A.B.C.D]:[1-65535] Source address:Destination port
admin@mariner.sea:/ip/tee# add 192.168.1.1:111 198.168.1.2:222
admin@mariner.sea:/ip/tee# start

The tee counter

You can verify the tee rules you added are functioning successfully by checking the counter. The counter shows the number of failed rule evaluations (the number of packets received that did not match the tee rules), the interface output failures, and all successful applications of the tee.

Viewing tee counts

To view the counts:

1. Navigate to the ip/tee menu.
2. Do one of the following:
   - Type `counter status` to see the status of the counter.
     Example: disabled
   - Type `counter reset` to restart the count at 1.
   - Type `counter` to see the tee counts.
3. Press ENTER.

Tee count example

The following example shows how tee count information is displayed:

admin@mariner.sea:/# ip tee
admin@mariner.sea:/ip/tee# counter ?
status
reset
[cr]
admin@mariner.sea:/ip/tee# counter
Rule evaluations failed: 9109
Interface output failures: 0
tee 192.168.1.1:111 to 168.1.2:222 - passed: 9259
admin@mariner.sea:/ip/tee# /
Appendix A

Notification Formats

Overview

Introduction This appendix provides examples of the notifications Proventia Network ADS sends to the configured notification object members when it detects alerts.

In this appendix This appendix contains the following topics:

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email Notification Examples</td>
<td>122</td>
</tr>
<tr>
<td>Syslog Notification Examples</td>
<td>125</td>
</tr>
</tbody>
</table>
Email Notification Examples

Introduction
The examples included here show the different types of email notifications ADS sends when it detects behavior violations.

Collector down alert
The following shows an example of a Collector down alert:

Collector Down: collector.iss.net
Type: Collector Down
URL: https://mariner.iss.net/summary/
Collector: collector.iss.net
Last seen: 20:07 03/03/06

Collector up alert
The following shows an example of a Collector up alert:

Collector Up: collector.iss.net
Type: Collector Up
URL: https://mariner.iss.net/summary/
Collector: collector.iss.net
Down since: 20:02 03/03/06
Downtime: 0h05m

Infrastructure alert
The following shows an example of an infrastructure alert:

Infrastructure: Your cert will expire in 1 day
Type: Infrastructure
URL: https://mariner.iss.net/summary/
Message: Your cert will expire in 1 day

Static high bandwidth alert
The following shows an example of a static high bandwidth alert:

Static High Bandwidth: <Unknown>
Type: Static High Bandwidth
Policy: <Unknown>
URL: https://mariner.iss.net/event_detail/alertdetail/?id=0&type=4
Severity: 1
Expected: 300 bps
Actual: 600 bps

Static low bandwidth alert
The following shows an example of a static low bandwidth alert:

Static Low Bandwidth: <Unknown>
Type: Static Low Bandwidth
Policy: <Unknown>
URL: https://mariner.iss.net/event_detail/alertdetail/?id=0&type=5
Severity: 1
Email Notification Examples

Expected: 600 bps
Actual: 300 bps

**Monitored bandwidth alert**

The following shows an example of a monitored bandwidth alert:

Monitored Bandwidth: <Unknown>
Type: Monitored Bandwidth
Policy: <Unknown>
URL: [https://mariner.iss.net/event_detail/alertdetail/?id=0&type=6](https://mariner.iss.net/event_detail/alertdetail/?id=0&type=6)
Severity: 1
Expected: 0 bps
Actual: 300 bps

**Unapproved client alert**

The following shows an example of an unapproved client alert:

Unapproved Client: <Unknown>
Type: Unapproved Client
Policy: <Unknown>
URL: [https://mariner.iss.net/event_detail/alertdetail/?type=3&search_text=client+1.2.3.4&id=0](https://mariner.iss.net/event_detail/alertdetail/?type=3&search_text=client+1.2.3.4&id=0)
Severity: 1
Client: 1.2.3.4
Server: 4.3.2.1 (crtntxl-ar9-4-3-002-001.crtntxl.dsl-verizon.net)
Service: TCP/22 (ssh)

**Unapproved server alert**

The following shows an example of an unapproved server alert:

Unapproved Server: <Unknown>
Type: Unapproved Server
Policy: <Unknown>
URL: [https://mariner.iss.net/event_detail/alertdetail/?type=3&search_text=server+4.3.2.1&id=0](https://mariner.iss.net/event_detail/alertdetail/?type=3&search_text=server+4.3.2.1&id=0)
Severity: 1
Client: 1.2.3.4
Server: 4.3.2.1 (crtntxl-ar9-4-3-002-001.crtntxl.dsl-verizon.net)
Service: TCP/22 (ssh)

**Unapproved service alert**

The following shows an example of an unapproved service alert:

Unapproved Service: <Unknown>
Type: Unapproved Service
Policy: <Unknown>
URL: [https://mariner.iss.net/event_detail/alertdetail/?type=3&search_text=service+6%2F22&id=0](https://mariner.iss.net/event_detail/alertdetail/?type=3&search_text=service+6%2F22&id=0)
Appendix A: Notification Formats

Unapproved host pair alert

The following shows an example of an unapproved host pair alert:

Unapproved Host Pair: <Unknown>
Type: Unapproved Host Pair
Policy: <Unknown>
URL: https://mariner.iss.net/event_detail/alertdetail/?type=3&search_text=client+1.2.3.4+and+server+4.3.2.1&id=0
Severity: 1
Client: 1.2.3.4
Server: 4.3.2.1 (crtntxl-ar9-4-3-002-001.crtntxl.dsl-verizon.net)
Service: TCP/22 (ssh)

Unapproved connection alert

The following shows an example of an unapproved connection alert:

Unapproved Connection: <Unknown>
Type: Unapproved Connection
Policy: <Unknown>
URL: https://mariner.iss.net/event_detail/alertdetail/?type=3&search_text=client+1.2.3.4+and+server+4.3.2.1+and+service+6%2F22&id=0
Severity: 1
Client: 1.2.3.4
Server: 4.3.2.1 (crtntxl-ar9-4-3-002-001.crtntxl.dsl-verizon.net)
Service: TCP/22 (ssh)
Syslog Notifications

Introduction
The examples included here show the different types of syslog notifications Proventia Network ADS sends when it detects behavior violations.

Collector down
The following shows an example of a Collector down alert:

Collector Down: collector.iss.net, URL: https://mariner.iss.net/summary/, Last seen: 20:23 03/03/06

Collector up alert
The following shows an example of a Collector up alert:

Collector Up: collector.iss.net, URL: https://mariner.iss.net/summary/, Last seen: 20:18 03/03/06, Downtime: 0h05m

Infrastructure
The following shows an example of an infrastructure alert:

Infrastructure: Your cert will expire in 1 day, URL: https://mariner.iss.net/summary/

Static high bandwidth alert
The following shows an example of a static high bandwidth alert:

Static High Bandwidth: <Unknown>, URL: https://mariner.iss.net/event_detail/alertdetail/?id=0&type=4, Severity 1, Expected: 300 bps, Actual: 600 bps

Static low bandwidth alert
The following shows an example of a static low bandwidth alert:

Static Low Bandwidth: <Unknown>, URL: https://mariner.iss.net/event_detail/alertdetail/?id=0&type=5, Severity 1, Expected: 600 bps, Actual: 300 bps

Monitored bandwidth alert
The following shows an example of a monitored bandwidth alert:

Monitored Bandwidth: <Unknown>, URL: https://mariner.iss.net/event_detail/alertdetail/?id=0&type=6, Severity 1, Expected: 0 bps, Actual: 300 bps

Unapproved client
The following shows an example of an unapproved client alert:

Unapproved Client: <Unknown>, URL: https://mariner.iss.net/event_detail/alertdetail/?type=3&search_text=client+1.2.3.4&id=0, Severity 1, Client: 1.2.3.4, Server: 4.3.2.1
Appendix A: Notification Formats

Unapproved server alert

The following shows an example of an unapproved server alert:

Unapproved Server: <Unknown>, URL: https://mariner.iss.net/event_detail/alertdetail/?type=3&search_text=server+4.3.2.1&id=0, Severity: 1, Client: 1.2.3.4, Server: 4.3.2.1
(crtntx1-ar9-4-3-002-001.crtntx1.dsl-verizon.net), Service: TCP/22 (ssh)

Unapproved service

The following shows an example of an unapproved service alert:

Unapproved Service: <Unknown>, URL: https://mariner.iss.net/event_detail/alertdetail/?type=3&search_text=service+6%2F22&id=0, Severity: 1, Client: 1.2.3.4, Server: 4.3.2.1
(crtntx1-ar9-4-3-002-001.crtntx1.dsl-verizon.net), Service: TCP/22 (ssh)

Unapproved host pair

The following shows an example of an unapproved host pair alert:

Unapproved Host Pair: <Unknown>, URL: https://mariner.iss.net/event_detail/alertdetail/?type=3&search_text=client+1.2.3.4+and+server+4.3.2.1&id=0, Severity: 1, Client: 1.2.3.4, Server: 4.3.2.1
(crtntx1-ar9-4-3-002-001.crtntx1.dsl-verizon.net), Service: TCP/22 (ssh)

Unapproved connection alert

The following shows an example of an unapproved connection alert:

Unapproved Connection: <Unknown>, URL: https://mariner.iss.net/event_detail/alertdetail/?type=3&search_text=client+1.2.3.4+and+server+4.3.2.1+and+service+6%2F22&id=0, Severity: 1, Client: 1.2.3.4, Server: 4.3.2.1
(crtntx1-ar9-4-3-002-001.crtntx1.dsl-verizon.net), Service: TCP/22 (ssh)
Appendix B

Commands in the /services/ads Menus

Overview

Introduction

This appendix provides a list and description of the /services/ads commands and subcommands for reference.

In this appendix

This appendix contains the following topics:

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Commands in the /services/ads Menu</td>
<td>128</td>
</tr>
<tr>
<td>Subcommands in the /services/ads Menu</td>
<td>129</td>
</tr>
</tbody>
</table>
### Commands in the /services/ads Menu

**Introduction**

Use the table in this appendix as a reference for the /services/ads commands. You can use the help and `?` commands within the CLI to see all subcommands available within each menu.

**Commands table**

The following table shows the list of the commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>atf</td>
<td>Active Threat Feed server configuration.</td>
</tr>
<tr>
<td>collector/</td>
<td>Configure collector related parameters.</td>
</tr>
<tr>
<td>database</td>
<td>Show or initialize the database.</td>
</tr>
<tr>
<td>diagnostics</td>
<td>Collect diagnostics.</td>
</tr>
<tr>
<td>enforcement</td>
<td>Policy enforcement configuration.</td>
</tr>
<tr>
<td>filter</td>
<td>Manage flow exclusion filters.</td>
</tr>
<tr>
<td>flow/</td>
<td>View flow data.</td>
</tr>
<tr>
<td>ids</td>
<td>Manage IDS.</td>
</tr>
<tr>
<td>interface</td>
<td>Manage listening interfaces.</td>
</tr>
<tr>
<td>routers/</td>
<td>Manage routers that Proventia Network ADS will monitor.</td>
</tr>
<tr>
<td>secret</td>
<td>Show or set secret.</td>
</tr>
<tr>
<td>sendto</td>
<td>Manage where this computer sends flow data.</td>
</tr>
<tr>
<td>show</td>
<td>Show status.</td>
</tr>
<tr>
<td>show_auth</td>
<td>Show or set display of identity tracking.</td>
</tr>
<tr>
<td>siteprotector</td>
<td>Manage SiteProtector.</td>
</tr>
<tr>
<td>smtp</td>
<td>Manage SMTP relay address.</td>
</tr>
<tr>
<td>snmpagent</td>
<td>Show or set snmpagent settings.</td>
</tr>
<tr>
<td>start</td>
<td>Start Proventia Network ADS services.</td>
</tr>
<tr>
<td>stop</td>
<td>Stop Proventia Network ADS services.</td>
</tr>
<tr>
<td>storage/</td>
<td>Proventia Network ADS storage.</td>
</tr>
<tr>
<td>wormto</td>
<td>Manage where this computer sends worm data.</td>
</tr>
</tbody>
</table>

*Table 25: /services/ads command list*
Subcommands in the /services/ads Menu

Introduction
Use the table in this appendix as a reference for the /services/ads subcommands.

Commands table
The following table shows the list of the commands:

<table>
<thead>
<tr>
<th>/ads menu</th>
<th>Subcommands</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>atf</td>
<td>raw</td>
<td>Show ATF raw configuration.</td>
</tr>
<tr>
<td></td>
<td>set</td>
<td>Set ATF configuration.</td>
</tr>
<tr>
<td></td>
<td>clear</td>
<td>Clear ATF configuration.</td>
</tr>
<tr>
<td></td>
<td>import</td>
<td>Import ATF configuration.</td>
</tr>
<tr>
<td></td>
<td>&lt;cr&gt;</td>
<td>Show ATF configuration.</td>
</tr>
<tr>
<td>collector/</td>
<td>accept</td>
<td>Manage Collector flow acceptance setting.</td>
</tr>
<tr>
<td>database</td>
<td>initialize</td>
<td>Initialize or reinitialize the relational database.</td>
</tr>
<tr>
<td></td>
<td>&lt;cr&gt;</td>
<td>Show the current state of the database.</td>
</tr>
<tr>
<td>diagnostics</td>
<td>create</td>
<td>Create a diagnostic report.</td>
</tr>
<tr>
<td></td>
<td>show</td>
<td>Show diagnostic reports.</td>
</tr>
<tr>
<td></td>
<td>&lt;cr&gt;</td>
<td>Show diagnostic configuration.</td>
</tr>
<tr>
<td>enforcement</td>
<td>raw</td>
<td>Show enforcement raw configuration.</td>
</tr>
<tr>
<td></td>
<td>set</td>
<td>Set enforcement parameter.</td>
</tr>
<tr>
<td></td>
<td>clear</td>
<td>Clear enforcement parameter.</td>
</tr>
<tr>
<td></td>
<td>&lt;cr&gt;</td>
<td>Show enforcement configuration.</td>
</tr>
<tr>
<td>filter</td>
<td>input</td>
<td>Show or set the input exclusion filter.</td>
</tr>
<tr>
<td></td>
<td>flowlog</td>
<td>Show or set the flowlog exclusion filter.</td>
</tr>
<tr>
<td></td>
<td>&lt;cr&gt;</td>
<td>Show configured flow exclusion filters.</td>
</tr>
<tr>
<td>flow/</td>
<td>query/</td>
<td>Query flow data.</td>
</tr>
<tr>
<td></td>
<td>summary</td>
<td>View flow summary data.</td>
</tr>
<tr>
<td></td>
<td>watch</td>
<td>View real-time flows.</td>
</tr>
<tr>
<td>ids</td>
<td>add</td>
<td>Add IDS.</td>
</tr>
<tr>
<td></td>
<td>delete</td>
<td>Delete IDS.</td>
</tr>
<tr>
<td></td>
<td>clear</td>
<td>Clear IDS.</td>
</tr>
<tr>
<td></td>
<td>&lt;cr&gt;</td>
<td>Show configured IDS.</td>
</tr>
</tbody>
</table>

Table 26: /services/ads commands and subcommands
### /ads menu Subcommands Description

<table>
<thead>
<tr>
<th>/ads menu</th>
<th>Subcommands</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface</td>
<td>add</td>
<td>Add listening interface.</td>
</tr>
<tr>
<td></td>
<td>delete</td>
<td>Delete listening interface.</td>
</tr>
<tr>
<td></td>
<td>clear</td>
<td>Clear listening interfaces.</td>
</tr>
<tr>
<td></td>
<td>&lt;cr&gt;</td>
<td>Show configured listening interfaces.</td>
</tr>
<tr>
<td>routers/</td>
<td>add</td>
<td>Add router to list of routers that Proventia Network ADS will monitor.</td>
</tr>
<tr>
<td></td>
<td>remove</td>
<td>Remove router from list of routers.</td>
</tr>
<tr>
<td></td>
<td>show</td>
<td>Show monitored routers and SNMP settings.</td>
</tr>
<tr>
<td></td>
<td>snmp</td>
<td>Show or set router SNMP parameters.</td>
</tr>
<tr>
<td>secret</td>
<td>set</td>
<td>Shared secret follows.</td>
</tr>
<tr>
<td></td>
<td>encrypted</td>
<td>Encrypted secret follows.</td>
</tr>
<tr>
<td></td>
<td>clear</td>
<td>Clear the secret.</td>
</tr>
<tr>
<td></td>
<td>&lt;cr&gt;</td>
<td>Show the encrypted secret.</td>
</tr>
<tr>
<td>sendto</td>
<td>add</td>
<td>Add remote destination.</td>
</tr>
<tr>
<td></td>
<td>delete</td>
<td>Delete remote destination.</td>
</tr>
<tr>
<td></td>
<td>clear</td>
<td>Clear remote destinations.</td>
</tr>
<tr>
<td></td>
<td>&lt;cr&gt;</td>
<td>Show remote destinations.</td>
</tr>
<tr>
<td>show</td>
<td>raw</td>
<td>Show raw status.</td>
</tr>
<tr>
<td></td>
<td>&lt;cr&gt;</td>
<td>Show status.</td>
</tr>
<tr>
<td>siteprotector</td>
<td>certificate</td>
<td>Manage SiteProtector certificate. <strong>Note:</strong> The <code>certificate clear</code> command is useful if you replaced the certificate on your SiteProtector Agent Manager, for instances in which you reinstall or upgrade it without backing up and restoring its keys.</td>
</tr>
<tr>
<td></td>
<td>database</td>
<td>Manage MS SQL database connection</td>
</tr>
<tr>
<td></td>
<td>discovery</td>
<td>Configure SiteProtector Passive Host Discovery</td>
</tr>
<tr>
<td></td>
<td>server</td>
<td>Manage SiteProtector address</td>
</tr>
<tr>
<td></td>
<td>show</td>
<td>Show SiteProtector management status</td>
</tr>
<tr>
<td>smtp</td>
<td>set</td>
<td>Set SMTP relay address</td>
</tr>
<tr>
<td></td>
<td>clear</td>
<td>Clear SMTP relay address</td>
</tr>
<tr>
<td></td>
<td>&lt;cr&gt;</td>
<td>Show configured SMTP relay address</td>
</tr>
<tr>
<td>snmpagent</td>
<td>community</td>
<td>Show or set community settings</td>
</tr>
<tr>
<td></td>
<td>&lt;cr&gt;</td>
<td>Show the snmpagent settings</td>
</tr>
</tbody>
</table>

Table 26: /services/ads commands and subcommands (Continued)
### /ads menu Subcommands Description

<table>
<thead>
<tr>
<th>/ads menu</th>
<th>Subcommands</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>threshold</td>
<td>set</td>
<td>Set the scan threshold settings</td>
</tr>
<tr>
<td></td>
<td>clear</td>
<td>Clear scan threshold settings</td>
</tr>
<tr>
<td></td>
<td>&lt;cr&gt;</td>
<td>Show configured scan threshold settings</td>
</tr>
<tr>
<td>start</td>
<td></td>
<td>Stop Proventia Network ADS services.</td>
</tr>
<tr>
<td>stop</td>
<td></td>
<td>Stop Proventia Network ADS services.</td>
</tr>
</tbody>
</table>

Table 26: /services/ads commands and subcommands  (Continued)
Glossary

a

ACL (Access Control List)—A list composed of rules and filters stored in a router to allow, deny, or otherwise regulate network traffic based upon network parameters such as IP addresses, protocol types, and port numbers.

address—A coded representation that uniquely identifies a particular network identity.

Analyzer—A centralized device that accepts event messages from one or more Collectors and performs second-order traffic analysis in order to identify and visualize potential attacks.

anomaly—An event or condition in the network that is identified as an abnormality when compared to a predefined illegal traffic pattern.

API (Application Programming Interface)—A well-defined set of function calls providing high-level controls for underlying services.

ARP (Address Resolution Protocol)—A protocol for mapping an IP address to a physical machine address.

ADOS (Anomaly Detection System)—The Proventia Network ADS Operating System. ADOS manages many of the low-level system processes and communication facilities.

ASCII (American Standard Code for Information Interchange)—A coded representation for standard alphabetic, numeric, and punctuation characters.

Authentication—An identity verification process.

b

Behavior—Who hosts on your network talk to and how they talk to them. When Proventia Network ADS sees behavior that does not match existing rules, it sends event notifications to the operator for action.

Black hole routing—A technique to route traffic to null interfaces that can never forward the traffic.

c

CAR (Committed Access Rate)—A tool for managing bandwidth that provides the same control as ACL with the additional property that traffic can be regulated based on bandwidth usage rates in bits per second.

CIDR (Classless Inter-Domain Routing)—Method for classifying and grouping Internet addresses.

cflowd—Developed to collect and analyze the information available from NetFlow. It allows the user to store the information and enables several views of the data. It produces port matrices, AS matrices, network matrices, and pure flow structures.
Collector—A device that gathers network information from adjacent routers via NetFlow™ and performs first-order traffic analysis. Anomalous events are compressed into event messages that are then sent to the listening Analyzer.

customer—An ISP, ASP, or enterprise user of ISS technology.

d
Dark IP—Regions of the IP address space that are reserved or known to be unused.

DNS (Domain Name System)—A system that translates numeric IP addresses into meaningful, human-readable names and vice-versa.

DoS (Denial of Service)—An interruption of network availability typically caused by malicious sources.

e
encryption—The process by which plain text is scrambled in such a way as to hide its content.

exploit—Tools intended to take advantage of security holes or inherent flaws in the design of network applications, devices, or infrastructures.

f

firewall—A security measure that monitors and controls the types of packets allowed in and out of a network, based on a set of configured rules and filters.

i

ICMP (Internet Control Message Protocol)—An IP protocol that delivers error and control messages between TCP/IP enabled network devices, for example, ping packets.

IP (Internet Protocol)—A connectionless network layer protocol used for packet delivery between hosts and devices on a TCP/IP network.

IP Address—A unique identifier for a host or device on a TCP/IP network.

l

LAN (Local Area Network)—A typically small network that is confined to a small geographic space.

m

MAC (Media Access Control) Address—A unique hardware number associated with a networking device.

MPLS (Multiprotocol Label Switching)—A packet-switching protocol developed by the Internet Engineering Task Force (IETF) initially to improve switching speeds, but other benefits are now seen as being more important.

NetFlow—A technology developed by Cisco Systems, Inc. that allows routers and other network devices to periodically export information about current network conditions and traffic volumes.
**NTP (Network Time Protocol)**—A protocol that is used to synchronize clock times in a network of computers.

**PFCAP (Flow Capture) Filter**—A string-based, regular expression used to filter traffic on your Proventia Network ADS Analyzer appliance.

**packet**—A unit of data transmitted across the network that includes control information along with actual content.

**password**—A secret code used to gain access to a computer system.

**policy**—The set of behaviors that network operators determine to be acceptable or unacceptable for their network and are the standard that Proventia Network ADS measures host behaviors against.

**protocol**—A well-defined language used by networking entities to communicate with one another.

**RADIUS (Remote Authentication Dial In User Service)**—A client/server protocol that enables remote access servers to communicate with a central server to authenticate dial-in users and authorize their access to the requested system or service.

**refinement**—The process of continually gathering information about prior anomalous activity seen.

**report**—A periodic summary of anomalous activity on the network.

**router**—A device that connects one network to another. Packets are forwarded from one router to another until they reach their ultimate destination.

**rules**—The traffic flows that are either allowed or denied that serve as the standards Proventia Network ADS uses to determine when behavior matches the current policy.

**SNMP (Simple Network Management Protocol)**—A standard protocol that allows routers and other network devices to export information about their routing tables and other state information.

**SSH (Secure Shell)**—A command line interface and protocol for securely getting access to a remote computer. SSH is also known as Secure Socket Shell.

**TACACS+ (Terminal Access Controller Access Control System +)**—An authentication protocol common to Unix networks that allows a remote access server to forward a user’s logon password to an authentication server to determine whether that user is allowed to access a given system.

**Target**—A victim host or network of a worm or other malicious denial of service (DoS) attacks.

**TCP (Transmission Control Protocol)**—A connection-based, transport protocol that provides reliable delivery of packets across the Internet.

**TCP/IP**—A suite of protocols that controls the delivery of messages across the Internet.
UDP (User Datagram Protocol)—An unreliable, connectionless, communication protocol.

UNC (Universal Naming Convention)—A standard which originated from the UNIX for identifying servers, printers, and other resources in a network. A UNC path precedes the name of the computer with double slashes or backslashes. The path within the computer are separated with a single slash or backslash, as follows:
- in UNIX, //servername/path
- in Windows and DOS, \servername\path

XML (eXtensible Markup Language)—A metalanguage written in Standard Generalized Markup Language (SGML) that allows one to design a markup language for easy interchange of documents on the World Wide Web.
THIS SOFTWARE PRODUCT IS PROVIDED IN OBJECT CODE AND IS LICENSED, NOT SOLD, BY INSTALLING, ACTIVATING, COPYING OR OTHERWISE USING THIS SOFTWARE PRODUCT, YOU AGREE TO ALL OF THE PROVISIONS OF THIS SOFTWARE LICENSE AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THIS LICENSE AGREEMENT, YOU MUST NOT INSTALL, ACTIVATE OR COPY THE SOFTWARE PRODUCT OR ANY PART THEREOF. IF YOU DO NOT AGREE TO THIS LICENSE AGREEMENT, YOU MAY RETURN THE SOFTWARE PRODUCT AND ANY ASSOCIATED 문서, PRECEDES, OR FOLLOWS THIS LICENSE, AND AS MAY FURTHER BE DEFINED IN THE USER DOCUMENTATION ACCOMPANYING THE SOFTWARE PRODUCT, YOUR RIGHTS AND OBLIGATIONS WITH RESPECT TO THE USE OF THIS SOFTWARE PRODUCT ARE AS SET FORTH BELOW. IF YOU ARE NOT WILLING TO BE BOUND BY THIS LICENSE, RETURN ALL COPIES OF THE SOFTWARE PRODUCT AND ACCOMPANYING DOCUMENTATION OR OTHER MEDIA, TO ISS FOR A FULL REFUND OF ANY LICENSE FEE. IF THE SOFTWARE PRODUCT WAS OBTAINED BY DOWNLOAD, YOU MAY CERTIFY DESTRUCTION OF ALL COPIES AND ANY LICENSE KEYS IN LIEU OF RETURN.

1. License - Upon your payment of the applicable fees and ISS delivery to you of the applicable license notification, Internet Security Systems, Inc. ("ISS") grants to you, the end user of Software ("Licensee") and the accompanying ISS software and documentation, and/or an Appliance as a part of an alpha or beta test, an exclusive, non-transferable and non-sublicensable right and license to use, copy, adapt, modify, and distribute the software, and any associated materials, for the duration of the license Term as set forth below. This License is revocable at any time by ISS upon notice to Licensee and Licensee's failure to adhere to the terms and conditions of this License Agreement. Licensee agrees to remove or disable the Software and security content from the authorized platform and return the Software, security content and documentation to ISS with which it is originally supplied and only during the usable life of such hardware. Except as provided in the immediately preceding sentence, Licensee may reproduce, install, use the Software on multiple devices, possess it in whatever form it may be in, and distribute it to others as long as it is only used for non-production, test purposes.

2. License Term - License shall commence upon delivery of the applicable Software and documentation in accordance with this License. The duration of this License is for as long as Licensee holds a valid license to the applicable Software, and shall terminate upon expiration of the license Term. Licensee may request additional copies of the Software solely for archival and disaster recovery purposes.

3. Rights and Obligations - Upon the expiration of the license Term, and as may further be defined in the related documentation, Licensee shall return all copies of the Software to ISS, including all related documentation, and certify destruction of all copies and associated materials.

4. Beta License - If ISS is providing Licensee with the Software, security content and related documentation, and/or an Appliance as a part of an alpha or beta test, the following terms of this Section 4 additionally apply and supersede any preceding provisions in this Agreement: Licensee agrees to use the Software, security content and documentation in accordance with the instructions and documentation provided by ISS, and shall implement appropriate system configuration modifications to terminate its use of the Software, security content and documentation upon the expiration of this License. Licensee agrees to certify destruction of all copies of the Software and documentation and associated materials upon the expiration of the license Term. Licensee agrees that the beta products are the property of ISS and agrees to return to ISS all software, security content and documentation, and any related association keys ("Software Association Keys") for use only on the specific network configuration, for the number and type of devices, and for the time period ("Term") that are specified in ISS quotation and Licensee purchase order, as accepted by ISS. ISS limits use of Software based on the number of nodes, users, and type of device or Appliance, and the method of delivering the Software, security content and associated materials. Use of Software not in accordance with the applicable license agreement and/or license Terms, and subject to the following limitations, may be licensed by ISS through the online software license agreements included with such software or software product. Licensee agrees that the Software, security content and documentation, and any associated Software Association Keys, for use only on the specific network configuration, for the number and type of devices, and for the time period specified in the related documentation and license agreement, is the property of ISS and may only be used in conjunction with the ISS hardware to which it is originally supplied and only during the usable life of such hardware. Except as provided in the immediately preceding sentence, Licensee may reproduce, install, use the Software on multiple devices, possess it in whatever form it may be in, and distribute it to others as long as it is only used for non-production, test purposes.

5. Evaluation License - If ISS is providing Licensee with the Software, security content and related documentation on an evaluation trial basis at no cost, such license Term is 30 days from installation, unless a longer period is agreed to in writing by ISS. ISS recommends using Software and security content for evaluation in a non-production, test environment. The following terms of this Section 5 additionally apply and supersede any conflicting provisions herein. Licensee agrees to use the Software, security content and related documentation and the associated materials in accordance with the instructions and documentation provided by ISS, and shall implement appropriate system configuration modifications to terminate its use of the Software, security content and documentation upon the expiration of the license Term. Licensee agrees that the beta products are the property of ISS and agrees to return to ISS all software, security content and documentation, and any related association keys ("Software Association Keys") for use only on the specific network configuration, for the number and type of devices, and for the time period ("Term") that are specified in ISS quotation and Licensee purchase order, as accepted by ISS. ISS limits use of Software based on the number of nodes, users, and type of device or Appliance, and the method of delivering the Software, security content and associated materials. Use of Software not in accordance with the applicable license agreement and/or license Terms, and subject to the following limitations, may be licensed by ISS through the online software license agreements included with such software or software product. Licensee agrees that the Software, security content and documentation, and any associated Software Association Keys, for use only on the specific network configuration, for the number and type of devices, and for the time period specified in the related documentation and license agreement, is the property of ISS and may only be used in conjunction with the ISS hardware to which it is originally supplied and only during the usable life of such hardware. Except as provided in the immediately preceding sentence, Licensee may reproduce, install, use the Software on multiple devices, possess it in whatever form it may be in, and distribute it to others as long as it is only used for non-production, test purposes.
NATURE, OR EXPENSES INCURRED BY LICENSEE. LICENSEE SOLE AND EXCLUSIVE REMEDY SHALL BE TO TERMINATE THE EVALUATION AND RETURN OF ANY LICENSE FEE, AS THE SOLE AND EXCLUSIVE REMEDIES FOR LICENSEE FOR SUCH NONCONFORMITY. THIS WARRANTY GIVES LICENSEE SPECIFIC LEGAL RIGHTS, AND LICENSEE MAY ALSO HAVE OTHER RIGHTS THAT VARY FROM JURISDICTION TO JURISDICTION. ISS DOES NOT WARRANT THAT THE SOFTWARE OR SECURITY CONTENT WILL MEET LICENSEE’S REQUIREMENTS, THAT THE OPERATION OF THE SOFTWARE OR SECURITY CONTENT WILL BE UNINTERRUPTED OR ERROR-FREE, OR THAT ALL SOFTWARE OR SECURITY CONTENT ERRORS WILL BE CORRECTED. LICENSEE UNDERSTANDS AND AGREES THAT THE SOFTWARE AND THE SECURITY CONTENT ARE NO GUARANTEE AGAINST UNSOLICITED E-MAILS, UNDESIRABLE OR UNPLANNED USER ACTIONS, COMPUTER VIRUSES, SPYWARE, INCOMPATIBILITY OF SOFTWARE OR SOFTWARE/SOFTWARE INTERFERENCE, OR UNDELETERIOUS PROGRAMMING ROUTINES AFFECTING LICENSEE’S NETWORK, OR THAT ALL SECURITY THREATS AND VULNERABILITIES, UNSOLICITED E-MAILS OR UNDESIRABLE INTERNET CONTENT WILL BE DETECTED OR THAT THE PERFORMANCE OF THE SOFTWARE AND SECURITY CONTENT WILL RENDER ISS SECURESYSTEMS INFRASTRUCTURES UNAFFLICTED WITH SECURITY BREACHES. THE REMEDIES SET OUT IN THIS SECTION ARE THE SOLE AND EXCLUSIVE REMEDIES FOR BREACH OF THIS LIMITED WARRANTY.

6. Covenants - ISS reserves all intellectual property rights in the Software, security content and Beta Products. Licensee agrees: (i) the Software, security content or Beta Products is owned by ISS and/or its licensors, is a valuable trade secret of ISS, and is protected by copyright laws and international treaty provisions; (ii) to take all reasonable precautions to protect the Software, security content and Beta Products from unauthorized access, disclosure, copying, modification, adapt, translate, reverse engineer, decompile, disassemble, or otherwise attempt to discover the source code of the Software, security content or Beta Product; (iv) to use ISS trademarks; (v) to reproduce all of ISS and its licensors copyright notices on any copies of the Software, security content or Beta Product; and (vi) to comply with all written instructions, lease, assign, sublicense, or distribute the Software, security content or Beta Product or make it available for time-sharing, service bureau, managed services offering, or on-line use.

7. Support and Maintenance - Depending upon what maintenance programs Licensee has purchased, ISS will provide maintenance, during the period for which Licensee has purchased applicable maintenance, of the Software, security content, and related fees, in accordance with the Support and Maintenance Policy, as amended from time to time at http://www.iss.net/maintenance_policy.pdf. Any supplemental Software code or related materials that ISS provides to Licensee as part of any support and maintenance service are to be considered part of the Software and are subject to the terms and conditions of this License, unless otherwise specified.

8. Limited Warranty - ISS reserves all intellectual property rights in the Software, security content and Beta Products for a period of thirty (30) days after the commencement date or for the Term (whichever is less). ISS warrants that the Software or security content will conform to material operational specifications described in its then current documentation. This limited warranty shall not apply unless (i) the Software or security content is materially defective at the time the Licensee accepts delivery of the Software or security content; (ii) Licensee notifies ISS of the claimed defects within ten (10) days of issuance of any documentation containing the claimed defects; (iii) Licensee promptly and properly installs all corrections, new versions, and updates made available by ISS to Licensee. Furthermore, this limited warranty shall not apply to nonconformities arising from any of the following: (i) misuse of the Software or security content, (ii) modification of the Software, failure by Licensee to utilize compatible computer and networking hardware and software, or (iv) interaction with software or firmware not provided by ISS. If Licensee timely notifies ISS in writing of any such nonconformity, then ISS shall repair or replace the Software or security content or, if ISS determines that repair or replacement is impractical, ISS may, at its option, refund the license fees, as the sole and exclusive remedies of Licensee for such nonconformity. This LIMITED WARRANTY GIVES LICENSEE SPECIFIC LEGAL RIGHTS, AND LICENSEE MAY ALSO HAVE OTHER RIGHTS THAT VARY FROM JURISDICTION TO JURISDICTION. ISS DOES NOT WARRANT THAT THE SOFTWARE OR SECURITY CONTENT WILL MEET LICENSEE’S REQUIREMENTS, THAT THE OPERATION OF THE SOFTWARE OR SECURITY CONTENT WILL BE UNINTERRUPTED OR ERROR-FREE, OR THAT ALL SOFTWARE OR SECURITY CONTENT ERRORS WILL BE CORRECTED. LICENSEE UNDERSTANDS AND AGREES THAT THE SOFTWARE AND THE SECURITY CONTENT ARE NO GUARANTEE AGAINST UNSOLICITED E-MAILS, UNDESIRABLE OR UNPLANNED USER ACTIONS, COMPUTER VIRUSES, SPYWARE, INCOMPATIBILITY OF SOFTWARE OR SOFTWARE/SOFTWARE INTERFERENCE, OR UNDELETERIOUS PROGRAMMING ROUTINES AFFECTING LICENSEE’S NETWORK, OR THAT ALL SECURITY THREATS AND VULNERABILITIES, UNSOLICITED E-MAILS OR UNDESIRABLE INTERNET CONTENT WILL BE DETECTED OR THAT THE PERFORMANCE OF THE SOFTWARE AND SECURITY CONTENT WILL RENDER ISS SECURESYSTEMS INFRASTRUCTURES UNAFFLICTED WITH SECURITY BREACHES. THE REMEDIES SET OUT IN THIS SECTION ARE THE SOLE AND EXCLUSIVE REMEDIES FOR BREACH OF THIS LIMITED WARRANTY.

9. Warranty Disclaimer - EXCEPT FOR THE LIMITED WARRANTY PROVIDED ABOVE, THE SOFTWARE AND SECURITY CONTENT ARE EACH PROVIDED AS IS, WITH ALL DEFECTS, ERRORS, VULNERABILITIES, INCOMPATIBILITIES, INCONSISTENCIES, UNDETERMINED INFLUENCES, CHANGABILITY, TITLE, NONINFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE. LICENSEE EXPRESSLY ACKNOWLEDGES THAT NO REPRESENTATIONS OTHER THAN THOSE CONTAINED IN THIS LICENSE HAVE BEEN MADE REGARDING THE GOODS OR SERVICES TO BE PROVIDED HEREUNDER, AND THAT LICENSEE HAS NOT RELIED ON ANY REPRESENTATION OR STATEMENT MADE BY ISS OR ITS AGENTS, OTHER THAN THOSE CONTAINED IN THIS LICENSE. ISS WILL NOT BE LIABLE TO LICENSEE UNDER ANY THEORY, INCLUDING CONTRACT AND TORT (INCLUDING NEGLIGENCE AND STRICT PRODUCTS LIABILITY) FOR ANY SPECIAL, PUNITIVE, INDIRECT, INCIDENTAL OR CONSEQUENTIAL DAMAGES, INCLUDING, BUT NOT LIMITED TO, DAMAGES OF LOSS OF DATA, LOSS OF USE, OR COMPUTER HARDWARE MALFUNCTION, EVEN IF ISS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

10. Termination - Licensee may terminate this License at any time by notifying ISS in writing. All rights granted under this License will terminate immediately, without notice, if Licensee breaches any of the terms and conditions of this License. Neither termination nor expiration of a License shall impair any pre-termination rights or duties of Licensee or ISS. Upon termination or expiration of a license for Software, Licensee shall cease all use of such Software, including Software pre-installed on ISS hardware, and destroy all copies of the Software and documentation and related materials. ISS will not refund to Licensee the obligation to pay all fees incurred prior to termination or shall not limit either party from pursuing any other remedies available to it.

11. Limitation of Liability - ISS ENTIRE LIABILITY FOR MONETARY DAMAGES ARISING OUT OF THIS LICENSE SHALL BE LIMITED TO THE AMOUNT OF THE LICENSE FEES ACTUALLY PAID BY LICENSEE UNDER THIS LICENSE, PRORATED OVER A THREE-YEAR TERM FROM THE DATE LICENSEE RECEIVED THE SOFTWARE. ISS SHALL NOT BE LIABLE TO LICENSEE UNDER ANY THEORY INCLUDING CONTRACT AND TORT (INCLUDING NEGLIGENCE AND STRICT PRODUCTS LIABILITY) FOR ANY SPECIAL, PUNITIVE, INDIRECT, INCIDENTAL OR CONSEQUENTIAL DAMAGES, INCLUDING, BUT NOT LIMITED TO, COSTS OF PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, DAMAGE OF GOODWILL OR REPUTATION, LOSS OF DATA, LOSS OF USE, OR COMPUTER HARDWARE MALFUNCTION, EVEN IF ISS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

12. Governing Law - This License will be governed by and construed in accordance with the substantive laws of the State of Georgia, USA, excluding the application of its conflicts of law rules. This License will be governed by the United Nations Convention on Contracts for the International Sale of Goods, the application of which is expressly excluded. If any part of this License is found void or unenforceable, it will not affect the validity of the balance of the License, which shall remain valid and enforceable according to its terms. This License may only be modified in writing signed by an authorized officer of ISS.
 injury, or severe physical or property damage. ISS disclaims any implied warranty of fitness for High Risk Use. Licensee accepts the risk associated with the foregoing disclaimers and hereby waives all rights, remedies, and causes of action against ISS and releases ISS from all liabilities arising therefrom.

18. Confidentiality - “Confidential Information” means all information proprietary to a party or its suppliers that is marked as confidential. Each party acknowledges that during the term of this Agreement, it will be exposed to Confidential Information of the other party. The obligations of the party (“Receiving Party”) which receives Confidential Information of the other party (“Disclosing Party”) with respect to any particular portion of the Disclosing Party’s Confidential Information shall not attach or shall terminate when any of the following occurs: (i) it was in the public domain or generally available to the public at the time of disclosure to the Receiving Party, (ii) it entered the public domain or became generally available to the public through no fault of the Receiving Party subsequent to the time of disclosure to the Receiving Party, (iii) it was or is furnished to the Receiving Party by a third party having the right to furnish it with no obligation of confidentiality to the Disclosing Party, or (iv) it was independently developed by the Receiving Party by individuals not having access to the Confidential Information of the Disclosing Party. Each party acknowledges that the use or disclosure of Confidential Information of the Disclosing Party in violation of this License could severely and irreparably damage the economic interests of the Disclosing Party. The Receiving Party agrees not to disclose or use any Confidential Information of the Disclosing Party in violation of this License and to use Confidential Information of the Disclosing Party solely for the purposes of this License. Upon demand by the Disclosing Party and, in any event, upon expiration or termination of this License, the Receiving Party shall return to the Disclosing Party all copies of the Disclosing Party’s Confidential Information obtained or created by the Disclosing Party. All Confidential Information of the Disclosing Party shall remain the exclusive property of the Disclosing Party.

19. Compliance - From time to time, ISS may request Licensee to provide a certification that the Software and security content is being used in accordance with the terms of this License. If so requested, Licensee shall verify its compliance and deliver its certification within forty-five (45) days of the request. The certification shall state Licensee’s compliance or non-compliance, including the extent of any non-compliance. ISS may also, at any time, upon thirty (30) days prior written notice, at its own expense appoint a nationally recognized software use auditor, to whom Licensee has no reasonable objection, to audit and examine use and records at Licensee’s offices during normal business hours, solely for the purpose of confirming that Licensee’s use of the Software and security content is in compliance with the terms of this License. ISS will use commercially reasonable efforts to have such audit conducted in a manner such that it will not unreasonably interfere with the normal business operations of Licensee. If such audit should reveal that use of the Software or security content has been expanded beyond the scope of use and/or the number of authorized devices or Licensee certifies such non-compliance, ISS shall have the right to charge Licensee the applicable current list prices required to bring Licensee in compliance with its obligations hereunder with respect to its current use of the Software and security content. In addition to the foregoing, ISS may pursue any other rights and remedies it may have at law, in equity or under this License.

20. Data Protection - The data needed to process this transaction will be stored by ISS and may be forwarded to companies affiliated with ISS and possibly to Licensee’s vendor within the framework of processing Licensee’s order. All personal data will be treated confidentially.

Revised October 7, 2005.
Index

a
Access lists
   Configuring 115
Active Threat Feed
   Configuring 83
   Enabling 83
Adding
   ARP entries 118
Analyzers
   defined 14
   appliance
   types 14
ATF
   Configuring 83
   Enabling 83

C
Cflowd for JunOS
   Configuring 59
Collector
   back panel diagram 17
   flow source limits 17
   hardware identifiers 17
   models 17
   ports 17
Collectors
   Configuring flow 56
   defined 14
Configuring
   Access lists 115
   Active Threat Feed 83
   Cflowd for JunOS 59
   Flow on Peakflow X Collectors 56
   Netflow for Cisco IOS 56
   sFlow 63
conventions, typographical
   in commands ix
   in procedures ix
   in this manual ix
diagram
   Collector back panel 17
   firewall ports 19

C
Enabling
   Active Threat Feed 83

f
firewall
   ports 19
flow source
   Collector models 17

h
hardware identifiers
   Collector 17

i
Internet Security Systems
   technical support x
   Web site x

m
mode
   standalone 14
   two-tier 14

n
Netflow
   Configuring for Cisco IOS 56
p
ports
  Collector 17
  table 19
publications
  related viii

r
related
  publications viii
Remote access
  setting-up 115

S
Setting
  System name 115
  System time 115
  timezone 116
Setting up
  Remote access 115
sFlow
  Configuring 63
standalone
  mode 14
System name
  Setting 115
System time
  Setting 115

t
table
  ports used by ADS 19
  technical support, Internet Security Systems x
two-tier
  mode 14
types of appliances 14
typographical conventions ix

W
Web site, Internet Security Systems x