PureSight Content Filtering Server Installation Manual

for use with

Squid Proxy Server

Last printed: 3/8/2004 2:12 PM
Last saved: 3/8/2004 2:12 PM

Copyright Notice

Trademark

Technical Support

If you require technical support services, contact us at support@puresight.com.

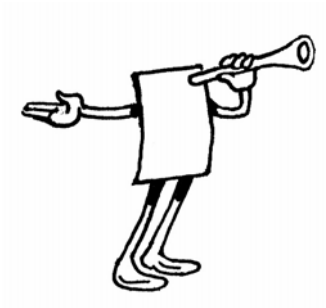
Last printed: 3/8/2004 2:12 PM
Last saved: 3/8/2004 2:12 PM

About This Manual

This manual provides instructions for installing PureSight Content Filtering Server on a Squid server platform. It contains the following chapters:

- **Chapter 1, Introduction**, introduces PureSight and describes its main features.
- **Chapter 2, Integrating PureSight with Squid**, describes how PureSight is integrated with Squid, and how it functions on the network.
- **Chapter 3, Installing the PureSight Content Filtering Server**, provides step-by-step instructions for the PureSight installation procedure and describes basic configuration features.
- **Chapter 4, Configuring PureSight**, describes various aspects of the PureSight configuration, including the PureSight daemon.
- **Chapter 5, Uninstalling PureSight**, provides instructions for removing PureSight.
- **Chapter 6, Troubleshooting**, provides instructions for checking that the PureSight filter is installed properly, and presents some possible problems and solutions. It also describes how to manually edit the OpenLDAP and Squid Proxy configuration files.

Table of Contents



Chapter 1

Introduction

PureSight was created especially for the complex requirements of the modern online corporation or institution. PureSight combines precision Internet filtering capabilities with powerful management tools to offer a highly accurate and reliable Internet content-filtering solution. PureSight is suitable for small, medium, and large organizations, as well as service providers.

PureSight is based on proprietary Artificial Content Recognition™ (ACR) technology. Using Artificial Intelligence (AI) algorithms, ACR enables PureSight to analyze the HTML page of each requested Web site and categorize the page based on its content. PureSight allows Internet usage policies to be defined, implemented and modified according to the changing needs of the organization.

DisCo System Architecture

PureSight employs an advanced Distributed Collaborative (DisCo) System architecture. This modular system architecture is designed to maximize management investments by providing flexible integration, improved performance and scalability.

Designed to simplify management of a high availability network, PureSight's distributed architecture utilizes three basic modules: PureSight Management Server, PureSight Content Filtering Server and PureSight Log Server.

This next generation architecture provides for:

- Centralized management and configuration of all PureSight Content Filtering Servers by a single PureSight Management Server. This also enables large organizations to manage remote branch office sites using the same Management Server, and thereby implementing a centralized policy throughout the organization regardless of physical location.
- Automatic, unified distribution of configuration changes to all Content Filtering Servers, eliminating the need to configure each server individually.
- Scalability. One or more additional Content Filtering Servers can be installed as new gateways are added or increased performance is required. PureSight is easily deployed in systems where load-balancing is used to distribute traffic between multiple Content Filtering Servers.
- Reduced risk for single point of failure. The distributed modular structure enables the PureSight Content Filtering servers to continue filtering, even if the PureSight Management Server or the PureSight Log Server fails or other PureSight Content Filtering Servers are down for maintenance. Cross platform support. Each module can be installed on a different operating system (Windows or Linux) and each PureSight Content Filtering Server can be installed on a different platform (Squid or ISA). The selected platform is transparent to the other modules installed.

The role of each of the system modules is described in the next section.

System Modules

The basic system architecture is comprised of three modules that interact to provide a complete content-filtering solution. The functionality of each of the modules is clearly defined as follows:

- **PureSight Management Server** - responsible for configuring and managing all PureSight modules and functions, including the PureSight Log Server and the PureSight Content Filtering Server(s). The PureSight Management Server features an intuitive user-interface that allows the administrator to define and manage the users and filtering policies that support the organization's Internet Acceptable Use Policy.
- **PureSight Content Filtering Server(s)** - responsible for analyzing all Internet traffic on the network. PureSight Content Filtering Servers can be installed on platforms located in the organization's Server Farm or on remote machines. The PureSight Content Filtering Server analyzes all HTTP traffic on the gateway where it is installed, and categorizes the content in real-time. According to the Internet Acceptable Use Policy defined on the PureSight Management Server, the PureSight Content Filtering Server then executes an Allow, Block, Monitor or Warn response, as required.
- The PureSight Management Server configures all PureSight Content Filtering Servers on the network, regardless of their location. This system-wide configuration includes the users and filtering policies that support the organization's Internet Acceptable Use Policy. The PureSight Content Filtering Servers also interact with a single PureSight Log Server, which is responsible for logging all of the filtering activity that takes place in the network.

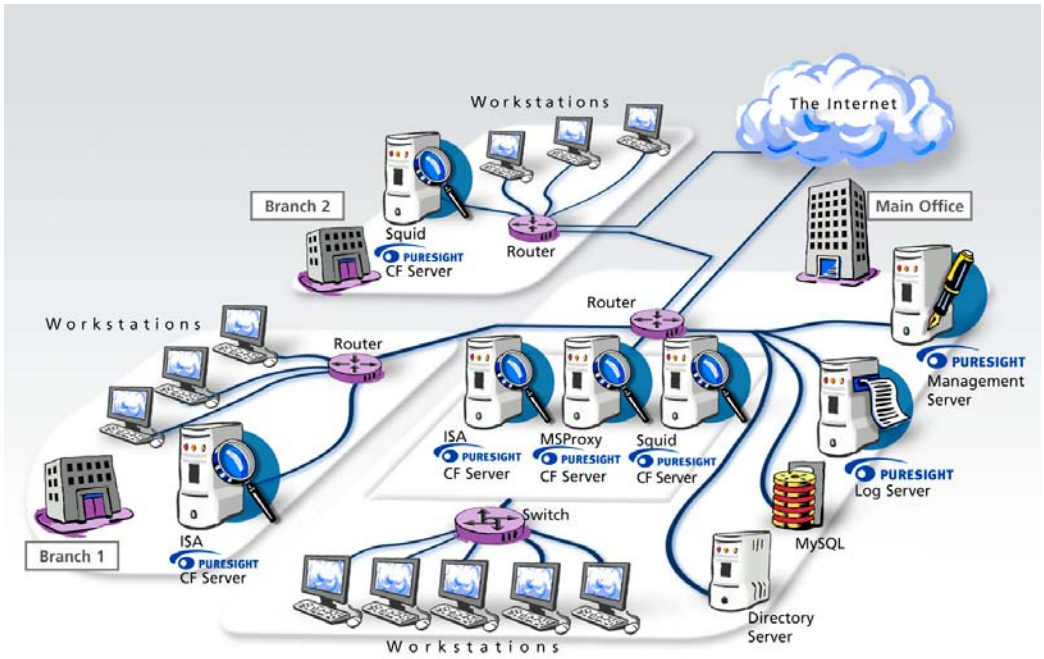
- **PureSight Log Server** - provides real-time tracking, monitoring and accounting information for all Internet activity - the details of all HTTP requests and replies, including time, users and the resulting filtering actions (allow/block/warn).

  The PureSight Management Server accesses the data on the PureSight Log Server to generate reports on the sites that were visited, the users that access those sites and other information that helps managers to evaluate employee productivity, bandwidth consumption and Internet usage. A single PureSight Log Server logs the activity for all PureSight Content Filtering Servers in the network, regardless of location or platform to enable generating unified reports for all activity. The PureSight Log Server supports logging to the file system or to an SQL database (MySQL).

These independent modules can be installed together on one machine or on separate machines, on varying combinations of platforms and operating systems. This architecture is highly flexible and customizable, allowing the systems administrator to easily adapt the deployment to the organization's network environment.

Network Architecture Diagram

One possible implementation of the PureSight network architecture is shown in the following diagram:

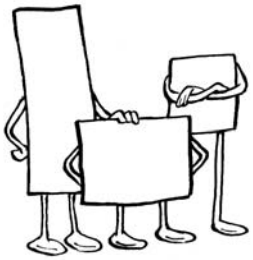


This example shows PureSight deployed in a network with a headquarters and two remote branch offices.

This network includes one PureSight Management Server for the system-wide configuration of five PureSight Content Filtering Servers and one PureSight Log Server. This system-wide configuration includes the users and filtering policies that support the organization's Internet Acceptable Use Policy.

Internet traffic originating in the Headquarters' workstations is monitored by one of three PureSight Content Filtering Servers located in the PureSight Server Farm. The PureSight Content Filtering Server located on the branch gateway routers monitors Internet traffic originating in the remote branch workstations.

The PureSight Log Server generates logs and the log contents are stored in a file system or in an SQL database (MySQL) on a separate server.



Chapter 2

Integrating PureSight with Squid

The PureSight Content Filtering Server for Squid is installed on the same machine as the Squid Proxy server, either on the network, or as part of the DMZ (Demilitarized Zone) connecting directly to the router. PureSight communicates with the Squid Proxy server via the Squid redirector program, to provide Internet Access Management according to the specific policy defined for the requesting user.

How PureSight Works with Squid

The following components are installed during the PureSight installation:

- **PureSight ACR**: The "brain" behind PureSight. Its function is to analyze and categorize the request, and determine how the Squid Proxy server handles user URL requests.
- **PureSight Request Handler (PSRH)**: This component handles all outgoing requests, and enables communication between PureSight's ACR and the Squid Proxy server. Squid is configured to use this program as a Squid Redirector.
- **PureSight Content Filtering Server**: This component handles all incoming data (including HTML text), and enables communication between PureSight's ACR and the Squid Proxy Server.

- **puresight_auth**: This component is responsible for authenticating user requests directed to the Squid Proxy Server against the user Directory Server defined in the PureSight Management Server.
- **URL Cache**: This component stores previously classified URLs. This allows PureSight to block or allow requested URLs without having to process and classify them more than once via ACR, and thus enhances performance.

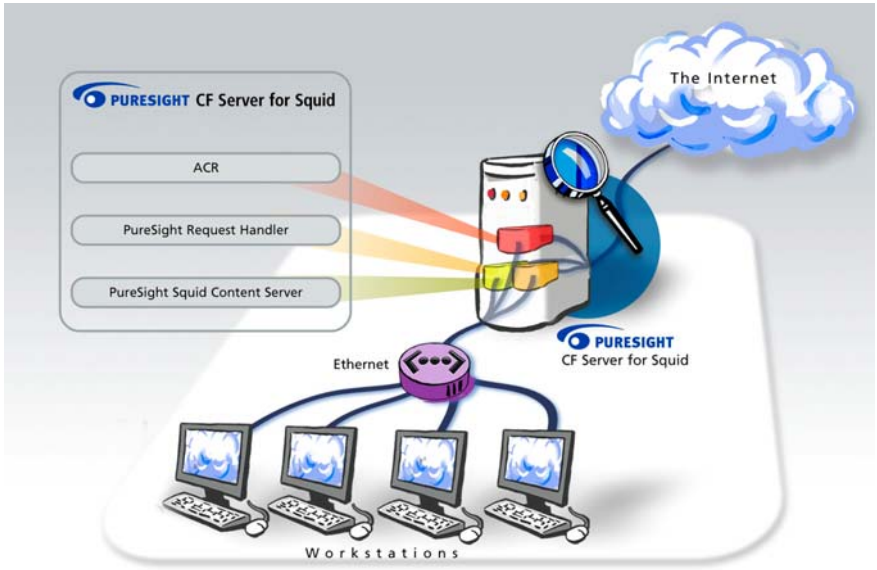


Figure 2-1: PureSight Operation on the Squid Platform

An HTTP request sent from a workstation to the Squid Proxy server prompts Squid to authenticate the requesting user by activating the puresight_auth program (if authentication is enabled). Once the user has been authenticated and allowed access, Squid activates the PureSight Request Handler. The Request handler may already have a classification for the URL, if it was previously processed. In this case, the URL will be either blocked or delivered directly by Squid, according to the user's policy. If this is not the case, and this is an unknown URL, it will be redirected to the PureSight Content Server. The content server will submit the original request to Squid and process the data received from the Internet, using the ACR component.

According to the specific predefined policy for the user, PureSight's ACR will then carry out one of the following actions:

- Allow the user access to the site.
- Deny the user access to the site, and return a message saying that the site is blocked.
- Return a warning message informing the user that although access is permitted, the site contains inappropriate material.

This filtering process is transparent to the user when requesting approved URLs.

Network Configuration

To ensure successful PureSight operation, the gateway and workstations on the network should be configured appropriately.

Gateway Configuration

To prevent users from bypassing the PureSight filtering mechanism, it is advisable to configure the network gateway (firewall or Internet router) to allow outgoing HTTP and HTTPS requests only from the Squid Proxy server.

Workstation Configuration

Squid Proxy server can be configured to work in transparent mode. If this is the case then there is no need to configure the workstations. For more information regarding configuring Squid to run in transparent mode, refer to: http://en.tldp.org/HOWTO/mini/TransparentProxy.html. If not in transparent mode, the Web browser on each workstation must be configured to gain Internet access only via the Squid Proxy server. If a browser is not configured to always pass via the Squid Proxy, the user's request bypasses PureSight, thus allowing the user direct access to the Internet.

NOTE:

It is not possible to both configure Squid to work in transparent mode and activate Squid authentication, i.e. PureSight user identification at the same time. In order to support PureSight user identification, Squid must be configured to work in non-transparent mode

PureSight Content Filtering Server Configuration

The Squid Proxy server machine must have access to both the PureSight Management Server and the PureSight Log Server on the ports specified in their respective installations. Both the LDAP and blocking ports on the PureSight Management Server must be open; as well as the port of the PureSight Log server.

Directory Services

PureSight supports the assigning of filtering policies to individual members of the organization. Assignment of policies to users can be based on IP addresses, or subnets of IP addresses. If the network in your organization includes an LDAP directory service, i.e., Windows Active Directory, Netscape iPlanet, Novell, or OpenLDAP, then policies can be assigned to individual users or groups with accounts in the directory service.

User Identification

To enforce directory users policies, for each request, the requesting user must be identified. The way to identify users on the Squid platform is via a Squid authentication program. PureSight includes a Squid authentication program, **puresight_auth**, which must be activated in order to support user identification in PureSight.

PureSight Authentication Program for Squid

PureSight authentication program for Squid proxy server offers Basic user authentication. All common browsers support Basic authentication. The following sections provide information on the impact of setting the Squid authentication method on the user identification capabilities of PureSight.

No Authentication

When Squid is set to work with no authentication program, PureSight does not receive any user information from Squid, apart from the requesting IP address. Thus, it is not possible for PureSight to support policies and reports based on directory users.

PureSight Authentication

When Squid is set to work with PureSight authentication program, Squid prompts for user information, each time the user opens a new browser (behavior varies between browsers). After receiving the username and password credentials of the user, the Squid verifies the user information on the selected LDAP user directory, according to settings specified via the PureSight Administration Tool. After authentication, PureSight receives the user information from the Squid server, and can filter based on directory object policies.

NOTE:

Squid caches username information in order to accelerate the authentication process, according to authenticate_ttl entries in squid.conf. Therefore, changing the LDAP user directory in the PureSight Administration Tool requires restarting Squid, in order to clear cached user information and for changes to take effect.

It is possible to use a different authentication program, other than puresight_auth. If working with Microsoft Windows Active Directory, it is advised to use an up to date version of ntlm_auth, which is part of Squid distribution package. Refer to *Squid Related Problems*, page 6-3. However, in order to define directory users it is still required to configure the Directory Server in the PureSight Administration Tool. Setting the Directory Server in the PureSight Administration Tool will not affect the external authentication program.

Caching

To improve network performance, PureSight contains a caching mechanism. When a URL request is categorized, the information is saved in the PureSight URL cache. If the URL is requested again, PureSight retrieves the classification data from the URL cache, avoiding the need to check the site classification again.

Logging

The PureSight Log Server is used for storing data describing all Internet activity as it is monitored by PureSight Content Filtering Servers. The PureSight Content Filtering Servers send the log data to the PureSight Log Server, which first saves this data to the local file system and then imports this data to the MySQL database, if PureSight Log Server is running in database mode.

Chapter 3

Installing the PureSight Content Filtering Server

This chapter describes how to install PureSight Content Filtering Server for Squid and how to check if the installation was successful. It also details the system requirements and introduces the basic configuration policies.

System Requirements

The following minimum system requirements must be met in order to run PureSight Content Filtering Server for Squid platform:

- **Hardware**:
  - The equivalent of Pentium II 400 mHz processor or higher; Pentium III recommended
  - 128 MB RAM (minimum)
  - 50 MB of free disk space

- **Software**:
  - RedHat Linux version 7.2, 7.3, 8.0 or 9.0
  - OpenLDAP Server 2.0.11 or higher
  - Fully operational and configured Squid Proxy server, version 2.3 Stable or higher, 2.4 recommended.
  - PureSight Management Server installed and running on any machine on the network

Installing the PureSight Content Filtering Server

The PureSight application is installed via an installation script, **install_psfiltersrv.sh**. The installation script can be run in script mode or in graphic mode. The procedure described herein details the installation process as it takes place in script mode.

The installation process installs the following components:

- PureSight Request Handler – the Squid redirector program. This program interacts with Squid using the standard redirector mechanism.
- PureSight Content Server – provides policy based content filtering.
- PureSight local storage of configuration settings – utilizing a local OpenLDAP server, PureSight Management Server configuration settings are distributed and stored on the local machine.
- PureSight authentication program – allows Squid to authenticate users against an LDAP directory server.
- PureSight Content Filtering Server daemon – used to control and monitor Squid and all PureSight Content Filtering Server components at run time.
- PureSight Content Filtering Server data files.
- PureSight utilities.

During the installation you will be prompted to confirm or enter various settings. The default value for each setting is indicated within brackets. You can accept the default settings or enter alternate values, as required.

Before You Begin

The PureSight Management Server must be installed before you attempt to install a PureSight Content Filtering Server. In addition, the PureSight Content Filtering Server must have access to the blocking mechanism port and the OpenLDAP port of the PureSight Management Server storage. Verify that these ports are open and accessible in order to retrieve the server configuration and enable the blocking mechanism.

The PureSight Request Handler and the PureSight Content Server must run under the same user as the Squid Proxy server. The PureSight Content Filtering Server installation will read the existing **cache_effective_user** and **cache_effective_group** from your squid.conf file. This will affect the user assigned to PureSight's files. Please make sure you have set the squid user correctly before running installation. Changing cache_effective_user after installing PureSight may require reinstallation of the PureSight Content Filtering Server.

The network settings should be properly set. Make sure the host name and host IP are set correctly. Typically your /etc/hosts file should contain an entry for your machine with an IP address other than 127.0.0.1.

NOTE:

To complete the PureSight installation process, the Squid Proxy Server must be restarted.

➢ **To install PureSight Content Filtering Server:**

1 Log in as root.

2. Go to the directory where the **install_psfiltersrv.sh** file is located.
3. Run the **install_psfiltersrv.sh** file.

NOTE:

The installation script must be run from the directory in which it is located.

The installation script can be run in graphic mode (non X like linuxconf) using **run.setup.sh ./ install_psfiltersrv.sh**. In some cases, depending on your terminal settings, the graphic mode may not display properly.

4. The License Agreement is displayed. Select [Y]es to accept the terms of the license agreement.

   The installation process begins and you are prompted to accept default values or enter new settings on a line-by-line basis.

5. Click **Enter** to accept the default setting for each of the parameters described in the sections below, or enter the required setting and then click **Enter**.

   - **Installation Path**: The path to where the application is to be installed. If the PureSight Management Server or PureSight Log Server are already installed on the machine, the installation path will be the same as the other modules and you will not be asked for the installation path.
   - **Local Storage Settings**: The PureSight Content Filtering Server receives configuration settings from the PureSight Management Server and stores them locally using a local OpenLDAP server as storage. The local storage increases performance and high availability.
     - **OpenLDAP server port**: The port of the local OpenLDAP server on the PureSight Content Filtering Server machine.
     - **OpenLDAP configuration file path**: The full path to the OpenLDAP configuration file, slapd.conf.

- **OpenLDAP daemon**: The full path to the daemon responsible for starting and stopping the OpenLDAP server.
- **OpenLDAP user**: The user under which OpenLDAP runs. This is required in order to set proper permissions on the PureSight directories and files for the user running OpenLDAP.

NOTE:

The OpenLDAP server will be stopped and restarted during the installation process.

The installation process edits the slapd.conf file and a backup copy of the original file is created (slapd.conf.icg.bak).

The slapd.conf file can also be configured manually, refer to *Manually Configuring the OpenLDAP Serve*r, page 6-9.

- **PureSight Management Server**: The PureSight Content Filtering Server connects to the PureSight Management Server to retrieve configuration data regarding users, policies, filters, server license and other settings.
  - **PureSight Management Server OpenLDAP server IP**: The IP address of the OpenLDAP server on the PureSight Management Server machine.
  - **PureSight Management Server OpenLDAP server port**: The port of the OpenLDAP server on the PureSight Management Server machine.
- **PureSight Content Filtering Server General Settings**: PureSight Content Filtering Server requires information regarding the IP address of the machine on which the PureSight Filtering Server is installed.

- **PureSight Content Filtering Server IP**: The actual IP address of the machine on which this Content Filtering Server is being installed. The IP address cannot be 127.0.0.1 (the alias of any local machine), it must be the real physical address.

- **Squid File Settings**: PureSight Content Filtering Server connects to Squid using the Squid Redirector program. The Squid proxy will be stopped and restarted during the installation process.
  - **Squid configuration file**: The full path of the file containing the Squid configuration settings (squid.conf).
  - **Squid binary file**: The location of the Squid binary file (squid).

NOTE:

The installation process edits the squid.conf file and a backup copy of the original file is created (squid.conf.icg.bak).

The editing includes adding settings to your squid.conf file inside a marked frame, at the end of the file. Anything added inside this frame will be removed during the uninstall of the PureSight Content Filtering Server.

The squid.conf file can also be configured manually, refer to *Manually Configuring the Squid Proxy Server*, page 6-9.

- **Squid Configuration Settings**: PureSight Content Filtering Server requires information regarding the Squid configuration settings in order to apply the appropriate permissions and settings in PureSight Content Filtering Server.
  - **Squid effective user**: The user under which Squid runs. This is required in order to set proper permissions on the PureSight directories and files for the user running Squid.
  - **Squid effective group**: The group to which Squid user belongs. This is required in order to set proper permissions on the PureSight directories and files.
  - **Squid HTTP port**: The HTTP port of the Squid proxy server.

- **PureSight Content Filtering Server Daemon**: A daemon is a process that is run without an associated terminal. The PureSight Content Filtering Server daemon is used for running PureSight Content Filtering Server.

  For details regarding the Squid daemon commands, refer to *PureSight Content Filtering Server Daemon Commands*, page 4-2.

  - **Run PureSight Content Filtering Server daemon at startup**: Select ***y*** to set the PureSight Content Filtering Server for Squid daemon to run at startup.

NOTE:

The PureSight Content Filtering Server daemon is responsible for starting both PureSight Content Filtering Server and Squid Cache. Therefore, if you choose to run the daemon at startup, make sure there are no other references to run Squid Cache at system startup. Otherwise, PureSight Content Filtering Server may fail to start properly.

After accepting or editing each of the above parameters, installation of the PureSight Content Filtering is completed automatically.

After successfully installing PureSight, you will need to initiate the PureSight Content Filtering Server and enter the license key before the filtering server can be run. For details on configuring the PureSight Content Filtering Server, please refer to *Chapter 3, Managing the Content Filtering Servers*, in the *PureSight Enterprise User's Guide*.

NOTE:

The PureSight Content Filtering Server installation does not configure the Squid authentication mechanism. To support directory user identification in PureSight you will need to manually configure the Squid to work with the PureSight authentication program: **puresight_auth**. Refer to Chapter 6, *Manually Configuring the Squid Proxy Server*, page 6-8 for more information.

NOTE:

If Squid is configured to run with cache_peer, you should instruct Squid to access directly URLs residing on PureSight servers: PureSight Management Server and PureSight Content Filtering. This will enable the PureSight blocking mechanism and the content filtering mechanism to work properly. The required always_direct entries in squid.conf have been added during installation but need to be uncommented and transferred to the appropriate location in the file.

Installation Script (Default Installation)

The example below illustrates an installation based on the default values.

NOTES:

The installation will vary slightly if the PureSight Content Filtering Server is installed on the same machine as the PureSight Management Server.

The License Agreement is displayed before the script is run. Select [Y]es to accept the license or [N]o to exit the installation.

```
############################################################
Welcome to the PureSight Content Filtering for Squid
Installation, version 4.6

PureSight Content Filtering Server includes a number of
settings. To accept the default settings press 'Enter'.

############################################################

Installation path [ /user/local/ ]:

[N]ext \ [B]ack \ [C]ancel [N]:

Extracting files...

############################################################

Local storage settings

PureSight Content Filtering Server requires OpenLDAP to be
installed and running on the PureSight Content Filtering
machine. The OpenLDAP server is used for locally storing
configuration settings retrieved from the PureSight Management
server.

############################################################

OpenLDAP server port [389]:

OpenLDAP configuration file path [ /etc/openldap/slapd.conf]:

OpenLDAP deamon [ /etc/rc.d/init.d/ldap ]

OpenLDAP user [ldap ]:

[N]ext \ [C]ancel [N]:
```

```
################################################################

PureSight Management Server

PureSight Content Filtering Server connects to PureSight
Management Server configuration storage (OpenLDAP) to retrieve
configuration settings.
################################################################

PureSight Management Server OpenLDAP server IP [ getHostIP() ]:

PureSight Management Server OpenLDAP server port [ 389 ]:

[N]ext \ [B]ack \ [C]ancel [N]:

################################################################

PureSight Content Filtering Server general settings

PureSight Content Filtering Server requires information
regarding the IP address of the machine the filtering server
is installed on.
################################################################

PureSight Content Filtering Server IP [getHostIP()]:

[N]ext \ [B]ack \ [C]ancel [N]:

################################################################

Squid File settings

PureSight Content Filtering Server integrates with Squid to
provide content filtering.

################################################################

Squid configuration file [/etc/squid/squid.conf]:

Squid binary file [/usr/sbin/squid]:

[N]ext \ [B]ack \ [C]ancel [N]:

################################################################

Squid Configuraiton settings
```

```
PureSight Content Filtering Server requires information
regarding the Squid configuration settings in order to apply
the appropriate permissions and settings in PureSight Content
Filtering Server

#############################################################

Squid effective user [ squid ]:

Squid effective group [ squid ]:

Squid HTTP port [ 8080 ]:

[N]ext \ [B]ack \ [C]ancel [N]:

#############################################################

PureSight Content Filtering Server daemon

PureSight Content Filtering Server daemon is used for running
PureSight Content Filtering Server.

Control PureSight filter server by running
/etc/rc.d/init.d/psfiltersrvd.

Available commands [start|stop|restart|cron|snapshot|status].

See the PureSight Content Filtering Server for Squid
Installation Guide for more information regarding PureSight
Content Filtering Server daemon.

#############################################################

Would you like PureSight Filter Server to be run at startup?
Please enter [F]inish \ [B]ack \ [C]ancel \[F]:

#############################################################

Updating installation…

Stopping slapd: [ok ]

Starting slapd: [ ok ]

Updating installation…  complete

#############################################################
```

Running PureSight

NOTE:

Before the filtering server can be run, the PureSight Content Filtering Server must be initialized and a valid license key must be set. Refer to the PureSight User Guide for more information.

You are now ready to run the PureSight Content Filtering Server.

- To run the PureSight Content Filtering Server, simply run:

  <PureSight install directory>/util/psfiltersrvd (start | stop | restart | cron | snapshot | status)

Chapter 4

Configuring PureSight

This chapter describes various aspects of the PureSight configuration, including the basic commands used by the PureSight Content Filtering Server daemon.

PureSight Configuration

After successfully installing PureSight, you will need to initialize the PureSight Content Filtering Server and enter a valid license key before the filtering mechanism is activated.

The PureSight Management Server is responsible for configuring and managing all PureSight modules and functions, including the PureSight Log Server and the PureSight Content Filtering Server(s). Configuration of the PureSight Content Filtering Server(s) is performed using PureSight's intuitive user-interface – the PureSight Administration Tool.

For details on configuring the PureSight Content Filtering Server, please refer to *Chapter 3, Configuring PureSight Content Filtering Servers* in the *PureSight User's Guide*.

PureSight Content Filtering Server Daemon Commands

The PureSight Content Filtering Server daemon is used for running the PureSight Content Filtering Server.

The following are the basic commands used by the PureSight Content Filtering Server daemon:

- **Start**: Starts both the PureSight Content Filtering Server and Squid.
- **Stop**: Stops both the PureSight Content Filtering Server and Squid.
- **Restart**: Stops and then restarts both the PureSight Content Filtering Server and Squid.
- **Status**: Displays the status of the PureSight Content Filtering Server to the standard output (stdout).
- **Cron**: Checks the status of the PureSight Content Filtering Server and the status of Squid. If either server is not functioning, it outputs the status to the cron error log and tries to restart them. This command is intended to be run as a watchdog mechanism, using the crond daemon.
- **Snapshot**: Outputs detailed status information for the PureSight Content Filtering Server to the snapshot log, including:
  - The number of PSCS threads and PSRH processes;
  - The number of file descriptors consumed by the PSCS and by Squid;
  - PS lines, including memory and CPU usage for PSCS and Squid processes.

Configuring PureSight Cron

It is recommended to add psfiltersrvd cron and psfiltersrvd cleanup to be run periodically by the crond daemon. The psfiltersrvd cron script monitors PureSight and Squid at run time. If a problem is found, psfiltersrvd cron automatically restarts both Squid and PureSight. The psfiltersrvd cleanup erases all temporary local files as well as entries marked for deletion in the local OpenLDAP server.

➢ **To configure PureSight cron**

1. Add lines to the cron table telling it to run the psfiltersrvd cron every 5 minutes. The cron will restart Squid and PureSight in case of system failure, and will cleanup the ldap server. To configure the cron table on RedHat linux:
   - Open **/etc/crontab** file
   - Add the lines:

     */5 * * * * root <PureSight Install Directory>/util/psfiltersrvd cron

     4 * * * * root <PureSight Install Directory>/util/ psfiltersrvd cleanup

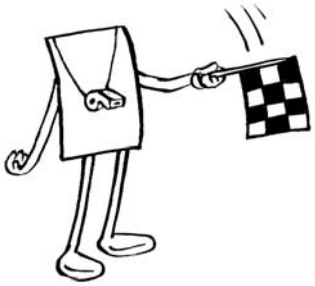
2. Make sure the crond daemon is run at startup

NOTE:

It is recommended to add >& /dev/null to the above lines to avoid mail sent to root inbox when PureSight cron script is run.

Another change should be to log files generated by cron, either to /var/log/messages or other files. Look in the /var/log directory. It may be necessary to do the following:

In /etc/syslog.conf, change line *.info;news,mail,authpriv,auth.none -/var/log/messages to *.info;cron,news,mail,authpriv,auth.none -/var/log/messages, add a line cron.* /var/log/cron, and restart cron and syslog daemons



Chapter 5

Uninstalling PureSight

This chapter describes how to remove the PureSight Content Filtering Server from the Squid machine.

Uninstalling the PureSight Content Filtering Server

PureSight can be uninstalled and removed from the Squid machine. The PureSight Content Filtering Server is uninstalled by running an uninstall script (**uninstall_psfiltersrv.sh**) in script mode.

The uninstall process removes all of the files that relate to the PureSight Content Filtering Server and restores the original OpenLDAP and Squid configurations. Any changes to the OpenLDAP configuration that were made after the installation was completed and which may affect the operation of other applications must be re-implemented after the uninstall process is complete. Any changes made in the Squid configuration file within the PureSight frame will be removed, other changes will be saved.

➢ **To uninstall the PureSight Content Filtering Server:**

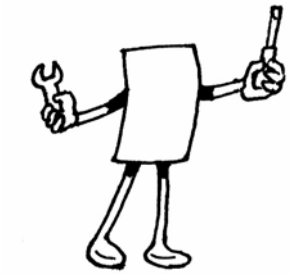
1. Log in as root.
2. Go to the directory where the **uninstall_psfiltersrv.sh** file is located.

3 Run the **uninstall_psfiltersrv.sh** file.

NOTE:

The uninstall script must be run from the directory in which it is located.

The uninstall process runs automatically and all PureSight files are removed from the Squid server.



Chapter 6

Troubleshooting

This chapter describes how to check that the PureSight Content Filtering Server for Squid is running properly, and how to handle some possible problems and solutions. This chapter also includes procedures for manually editing the OpenLDAP and Squid Proxy configuration files.

Checking if PureSight is Running

After completing the installation process, you can check that PureSight is up and running. This optional procedure can also be used to check if there are previous installations of PureSight.

➢ **To check if PureSight is running:**

1. Run <PureSight install directory>/util/psviltersrvd status. This will display the status of the PureSight Content Filter and the Squid proxy server.
2. Set your browser to use the Squid Proxy Server and try to surf. Try out regular sites and sites with sexual material to make sure that these sites are blocked.

General Troubleshooting Issues

The following are issues that are often neglected and can cause trouble:

PS_HOME_DIR

In order for all PureSight applications and tools to function correctly, the PS_HOME_DIR environment variable must be properly defined. If PS_HOME_DIR is not properly defined for the user, the application will simply not run. In order to make sure the PS_HOME_DIR is always defined for all users, the definition can be added to **/etc/profile(bash users), /etc/csh.cshrc (tcsh) etc**.

Squid User

PureSight Content Server (pscs) and Request Handler (psrh) always run under user squid. If some of the tools are run with a different user, it could cause problems. For example, running a tool that edits a configuration file as user **root**, will change the permissions of the file and squid user will not have write permissions for that file. Therefore, it is advised that all PureSight tools and applications be run under user squid.

Squid Configuration Problems

Many of the problems you may encounter are related to the Squid proxy server configuration. If you are not sure whether your problem is caused by PureSight or Squid, simply remove the redirect_program entry from the squid.conf file, this will totally disable the use of PureSight filtering. Now see if the problem persists without PureSight involvement. A solution to many of these potential problems resides in the Squid configuration manual, and user groups. See www.squid-cache.org.

Squid Related Problems

Problem	Solution
Squid Proxy refuses to start	First try to find the reason in the cache.log file. This could occur due to various reasons; the following are some common examples: 1. Squid cache directory was not initialized using the squid –z option. 2. The cache_effective_user, which should be Squid, does not have permissions to the Squid directory, cache_dir or other. Change the owner of the Squid installation directory and cache directory. 3. DNS is not configured properly.

Problem	Solution
Everything seems to work fine, but large files cannot be attached to outgoing requests, such as sending mail via webmail.	In the configuration of the Squid Proxy there is a limit to the size of outgoing requests. In order to increase the limit, set the request_body_max_size parameter in the Squid configuration file.
Message: 'could not open new connection to squid !!!' appears in the PureSight error log.	This message appears in the PureSight error log when the Squid port defined in the Squid configuration file and the Squid port defined in the PureSight Administration Tool, under the server advanced settings, are not the same.

Problem	Solution
Message: 'Error getting request client message queue ... No space left on device' appears in the PureSight error log.	By default Redhat 7.2 allows only 16 system wide message queues (RedHat 6.2 allowed 128 by default). To see the limit on a given machine run: ipcs -l . The filtering mechanism requires one message queue for each PSRH process and one message queue for PSCS. This means that using Redhat 7.2's default configuration you can only have, de facto, 15 PSRH processes working. If a larger number is defined, the other processes will send the error message to the error log file. If you wish to use more than 15 PSRH processes, you need to increase the message queues limit, as follows: 1. Edit /etc/sysctl.conf file by adding the line: kernel.msgmni = <number of required message queues> at the end of the file. 2. Run /sbin/sysctl -p. 3. Run ipcs -l, see that the value has changed.

Problem	Solution

Compiling Squid 2.5 with NTLM support	The described procedure below refers to Squid 2.5 stable version. The recommended stable version is 5.
	1. Configure Squid with the following parameters:
	`./configure --enable-ntlm-fail-open --enable-auth=ntlm,basic,digest --enable-ntlm-auth-helpers=SMB,winbind --enable-basic-auth-helpers=MSNT,LDAP,NCSA,PAM,SMB,multi-domain-NTLM,winbind --enable-digest-auth-helpers=password`
	2. Run "make" and "make install"
	3. Modify squid.conf as follows:
	`auth_param ntlm program /usr/local/squid/libexec/ntlm_auth opgal/<domain controller machine name> auth_param ntlm children 5 auth_param ntlm max_challenge_reuses 0 auth_param ntlm max_challenge_lifetime 2 minutes`
	`acl authenticated proxy_auth REQUIRED`
	`http_access allow localhost`
	`http_access allow authenticated`
	`http_access deny all`
	4. Note: Squid must know to resolve the Active Directory name and machine name. This can be achieved by editing the /etc/hosts file on the Squid machine.

Manual Configuration Procedures

Although both the Squid Proxy Server and the OpenLDAP Server are automatically configured when the installation script is run, you can manually edit their respective configuration files, if required.

Manually Configuring the Squid Proxy Server

The PureSight Content Filtering Server installation will add some essential settings to the end on your Squid configuration file (squid.conf). However, these changes can also be done manually by editing the file, normally located at /etc/squid/squid.conf or /usr/local/squid/etc/squid.conf. Some of the settings, mainly access control and authentication will still need to be done manually.

NOTE:

The installation script adds settings to your squid.conf file inside a marked frame, at the end of the file. Anything you add inside this frame will be removed if you chose to uninstall the PureSight Content Filtering Server.

➢ **To manually configure Squid:**

1. **redirector_program** - Set the Squid redirector program to point to the PureSight Request Handler (psrh). This can be done by simply altering the 'redirect_program' entry in the **squid.conf** file and setting it to **<PureSight install directory>/bin/psrh**.
2. **redirect_children** - Set the Squid redirect_children parameter. This can be done by simply altering the 'redirect_children' entry in the **squid.conf** file. The value to be entered to the 'redirect_children' parameter should be set according to the type of load that will be applied on the Squid server. The limit Squid has for the number of redirect_children is 32. For high volume servers the suggested number would be 30. If a higher number of redirect_children is necessary, the squid will notify in the **squid.log** file.

3 **Squid user** - In order to make sure that Squid runs under a certain user, change the cache_effective_user entry. It is advised to do this before installing the PureSight Content Filtering Server in order to avoid permission conflicts between PureSight and Squid.

4 **Squid debugging** - To increase performance, it is highly recommended to disable some of Squid's debug logging. This can be done by altering / adding the following lines in the squid.conf file.

```
cache_access_log /dev/null

cache_store_log none

debug_options 33,0
```

5 **Squid port** – If Squid is running with a non-default Squid port (3128) by setting the http_port entry in the squid.conf file, then PureSight must be informed. Inform the PureSight Content Filtering Server by going to the Management Server Administration tool -> Servers. Select the appropriate PureSight Content Filtering Server. Click on the **Advanced Settings** button and set the Squid Port accordingly. Refer to the *PureSight User's Guide* for more information regarding the configuration of PureSight Content Filtering Servers.

NOTE:

When setting the http_port in the squid.conf file, do not use specific IP, only port number.

6 **Squid authentication** – To support user identification in PureSight and the ability to enforce directory user policies, it is necessary to set Squid to use the PureSight user authentication program. This can be done by adding the following lines to the squid.conf file:

```
# Note: authentication settings have changed between
squid versions 2.4 and 2.5

# For squid 2.4 versions use :
```

```
# authenticate_program <PureSight Install
Directory>/auth/puresight_auth

# authenticate_children 5

# For squid 2.5 versions use :

# auth_param basic program <PureSight Install
Directory>/auth/puresight_auth

# auth_param basic children 5

# auth_param basic realm Squid proxy-caching web
server

# auth_param basic credentialsttl 2 hours

# example acls :

# acl authenticated  proxy_auth REQUIRED

# http_access allow localhost

# http_access allow authenticated

# http_access deny all
```

NOTE:

If Squid is configured to run the PureSight authentication program but the PureSight Management Server Directory Setting is set to NONE (no directory server defined), users will still be required to authenticate (enter username and password). Authentication will always be successful, and the requesting user will be filtered according to their IP address (and not directory username).

7 Restart Squid.

Manually Configuring the OpenLDAP Server

The OpenLDAP Server can be configured either via the installation script or by directly editing the **slapd.conf** file.

NOTE:

Configuring the OpenLDAP server is necessary only when the PureSight Content Filtering Server is not installed on the same machine as the PureSight Management Server.

➢ **To manually configure the OpenLDAP Server:**

1 Add the following lines to the end of the slapd.conf file:

```
#========== PureSight Database ====================
database ldbm
suffix "cn=root"
readonly off
rootdn "cn=Manager,cn=root"
rootpw secret
index objectClass eq
index cn eq,subinitial
directory /usr/local/iCognito-1/ldap
updatedn        "cn=Manager,cn=root"
include /etc/openldap/schema/PureSight.schema
#========== PureSight Database end ================
```

NOTE:

The directory entry is the <PureSight install directory>/ldap (the default is displayed in the example above).

2 After editing the slapd.conf file, restart the OpenLDAP server.

NOTE:

The PureSight Content Filtering Server must be initialized on the PureSight Management Server in order for configuration data to be locally retrieved.