Installation Guide Supplement

for use with

Squid Web Proxy Cache

Websense® Web Security
Websense Web Filter

v7.5

Published 2010
Printed in the United States of America and Ireland

Trademarks

WinPcap

Contents

1 Squid Web Proxy Cache Integration

This supplement provides additional information for installing and configuring Websense® Web Security or Websense Web Filter with Squid Web Proxy Cache. See the Websense Web Security and Websense Web Filter *Installation Guide* for complete Websense software installation instructions.

When Websense software is integrated with Squid Web Proxy Cache, the following components are configured differently than in a stand-alone installation:

- **Websense Squid plug-in** must be installed on each Squid Web Proxy Cache machine (Squid machine) to allow Squid Web Proxy Cache to communicate with Filtering Service.
- **Websense Network Agent** is configured to manage only the Internet protocols not managed by Squid Web Proxy Cache (e.g., instant messaging, streaming media, peer-to-peer). Typically, Network Agent runs on a machine connected to a bi-directional span port (or mirror port) on a network switch processing the traffic to be monitored. Network Agent monitors the non-HTTP(S)/FTP traffic directed through the switch. You can install Network Agent on the same machine as Squid Web Proxy Cache. If you do so, a span port on a switch is not necessary for Network Agent to operate—it will be able to monitor the same traffic visible to the Squid machine.

Supported Squid versions

- Websense Web Security and Websense Web Filter are compatible with STABLE releases of Squid Web Proxy Cache v2.5 and 2.6.
- The Websense Squid plug-in for the Squid Web Proxy Cache is supported only on 32-bit Red Hat Enterprise Linux 4.7 and 5.3.

Client computers

- To be filtered by Websense software, a client computer must access the Internet through the Squid Web Proxy Cache.
- Browsers must be set for proxy-based connections.

How Websense filtering works

When Squid Web Proxy Cache receives an Internet request from a client, it queries Websense Filtering Service to find out if the requested site should be blocked or permitted.

- If the site is blocked, the user receives a block page.
- If the site is permitted, Filtering Service notifies Squid Web Proxy Cache and the client is given access to the site.

See *Filtering Order* in the TRITON - Web Security Help for information about how Filtering Service determines whether a site should be blocked.

HTTPS blocking

To block HTTPS traffic, you must configure the Squid integration with one of these options:

- Install Network Agent, the Websense component that performs protocol filtering, and configure it to block HTTPS traffic.

  For instructions on installing Network Agent, see the *Installation Guide*. See the *Deployment Guide* for Websense Web Security Solutions (*Deployment Guide*) for location information and the TRITON - Web Security Help for configuration instructions.
- If Squid acts as a proxy server, you can configure it to filter all HTTPS traffic.
  1. Go to the **/etc/wsLib/** directory and open the **wsSquid.ini** file in a text editor.
  2. Under **initSection**, change the value of **UseHTTPSBlockPage** to **yes**.

     The default setting is **no**, which causes Squid to permit all HTTPS traffic.
  3. Save your changes.
  4. Restart Squid Web Proxy Cache.

  All requests for HTTPS pages are filtered, but if a request is blocked, Squid Web Proxy Cache sends a Squid-generated error page to the user. Users do not see the Websense block page, because Squid Web Proxy Cache is unable to deliver it.

  

  Note

  In some cases, when HTTPS is blocked, the Websense block page may be delivered to the user's browser, or a blank page is displayed, instead of the Squid-generated error page. Regardless, HTTPS is filtered properly. If a request should be blocked, it is blocked.

Installation

The Squid plug-in must be installed on the Squid Web Proxy Cache machine (Squid machine) to allow Websense Filtering Service and the Squid software to communicate.

> **Note**
> Prior to installing Websense software verify you have a correctly installed and operating version of Squid Web Proxy Cache. See Squid documentation and support resources for installation and configuration instructions.

You can install the Websense components on the Squid machine or on a different machine. If you install Filtering Service on the Squid machine, you must still install the Squid plug-in as well.

If you install Filtering Service on a separate machine from Squid Web Proxy Cache, you must subsequently install the Squid plug-in on every Squid machine that communicates with Filtering Service.

> **Important**
> If you are installing Websense software on a machine running an SELinux-enabled Red Hat Enterprise Linux operating system* with the version of Squid that is prepackaged with the Red Hat installation, Squid cannot launch the Websense Squid plug-in (**WsRedtor**).
>
> If the plug-in does not launch, Websense filtering cannot occur. Configure SELinux permissions so that **WsRedtor** can launch. See your Red Hat Enterprise Linux documentation for details.
>
> *Websense software supports Red Hat Enterprise Linux 4.7 or 5.3.

Websense software and Squid Web Proxy Cache on separate machines

In this case, installation is a two-part process:

1. Install Websense software.

   On the designated machine or machines, install Websense components. See the *Installation Guide* for instructions.

   Websense Filtering Service must be installed on its machine before installing the Websense Squid plug-in on the Squid machine. Filtering Service must be installed as integrated with Squid Web Proxy Cache.

Install Websense Network Agent to filter non-HTTP(S)/FTP traffic (e.g., instant messaging, streaming media, peer-to-peer, and so forth) which is not handled by Squid Web Proxy Cache. If Network Agent is installed on a separate machine, it must be connected to a bi-directional span port on a network switch (see the *Deployment Guide* for Websense Web Security Solutions for information about where to place Network Agent in your network). If Network Agent is installed on the Squid machine, connecting to a span port is not necessary.

2. Install the Websense Squid plug-in on the Squid machine.

   Run the Websense installer on the Squid machine and choose to install the plug-in only. See *Installing the Squid plug-in*, below.

Installing the Squid plug-in

The Squid plug-in is installed on the Squid machine to allow Websense Filtering Service and Squid software to communicate.

> **Note**
> The Squid plug-in is supported only on Linux.

If Filtering Service is installed on a separate machine from the Squid machine, it must be installed before you install the Squid plug-in. When it is installed, Filtering Service must be installed as integrated with Squid Web Proxy Cache. You must specify the location of Filtering Service when installing the Squid plug-in, otherwise the installer will not proceed.

When installing the Squid plug-in, the installer checks for Squid Web Proxy Cache on the installation machine. If Squid Web Proxy Cache is detected, the installer continues.

If Squid Web Proxy Cache is not detected, installation of the Squid plug-in cannot proceed.

> **Note**
> The following instructions are a supplement to the full instructions in the *Installation Guide*. These instructions cover only those installer screens involved in installing the Websense Squid plug-in. Refer to the *Installation Guide* for full instructions on using the installer. The *IInstallation Guide* refers you to this guide for instructions specific to integration with Squid Web Proxy Cache.

The Websense installer is used to install the Websense Squid plug-in on the Squid machine. The following procedure is performed on the Squid machine.

> **Note**
> Websense Filtering Service must be installed on its machine before installing the Squid plug-in on this machine.

> **Important**
> Make sure `visible_hostname` is set in the squid.conf file **before** installing the Squid plug-in. See your Squid documentation for instructions.

1. Download or copy the Websense installer to this machine.

   See the *Installation Guide* for instructions on downloading the installer.
2. Close all applications and stop any antivirus software.
3. Start the Websense installer.

   See the *Installation Guide* for instructions on starting the installer.

> **Notes**
> These instructions refer to GUI installer screens. There are GUI and command-line versions of the Websense installer for Linux. In the command-line version, prompts are displayed that correspond to each GUI screen. Instructions for a screen also apply to the corresponding command-line prompt. The main difference is how options are selected. Rather than clicking items in a screen, you will enter menu-item numbers or characters.
>
> To cancel the command-line installer, press Ctrl-C. However, do **not** cancel the installer, after the **Pre-Installation Summary** screen, as it is installing components. In this case allow the installation to complete and then uninstall the components you did not want to install.

4. On the **Introduction** screen, click Next.
5. On the **Subscription Agreement** screen, choose to accept the terms of the agreement and then click Next.
6. On the **Installation Type** screen, select **Custom** and then click Next.
7. On the **Custom Installation** screen, select **Filtering Plug-in** and then click Next.

8. On the **Filtering Service Communication** screen, enter the IP address of the machine on which Filtering Service is installed and the port Filtering Service uses to communicate with integration products and Network Agent (default is 15868). Then click **Next**.

   The port used by Filtering Service to communicate with integration products and Network Agent must be in the range 1024-65535. Filtering Service may have been automatically configured to use a port other than the default 15868. When Filtering Service was installed, if the installation program found the default port to be in use, it was automatically incremented until a free port is found. To determine what port is used by Filtering Service, check the `eimserver.ini` file—located in `C:\Program Files\Websense\bin` (Windows) or `/opt/Websense/bin` (Linux)—on the Filtering Service machine. In this file, look for the **WebsenseServerPort** value.

   

   Important

   Do not modify the `eimserver.ini` file.

9. On the **Select Integration** screen, select **Squid Web Proxy Cache**.
10. On the **Squid Configuration** screen, enter paths to the squid.conf and squid executable files, and then click **Next**.

    The installation program will verify the path to squid.conf. A default path is automatically entered. Enter a different path if necessary or click **Browse** to navigate to the location. This path must be verified for the installation to continue. (Note: the path must include the file name.)

    Additionally, you must provide the path to the Squid executable so the installation program can shut it down to continue the installation.

    

    Note

    The installer will automatically start Squid Web Proxy Cache once installation is complete. Verify it is running after installation is complete (Step 15 below).

11. On the **Installation Directory** screen, accept the default installation path, or click **Choose** to specify another path, and then click Next.
12. On the **Pre-Installation Summary** screen, verify the information shown.

    Filtering Plug-in should be listed as the only component to be installed.
13. Click **Next** to start the installation. An **Installing** progress screen is displayed. Wait for the installation to complete.
14. On the **Installation Complete** screen, click **Done**.

15. Start Squid Web Proxy Cache if necessary.

    The installer attempts to start Squid Web Proxy Cache once installation is complete. In some cases, it must be manually started:

    a. Verify Squid Web Proxy Cache is running, for example, by using the command `ps -ef | grep squid`.

    b. If it is not running, start it.

       See Squid documentation or support resources for the start command appropriate to your installation of Squid Web Proxy Cache.

16. If you stopped antivirus software on this machine, restart it now.

Websense software and Squid on the same machine

If the machine has sufficient resources, Websense software may be installed on the same machine as Squid Web Proxy Cache. You may install all core Websense components (see below) or particular components (see *Particular Websense components on the Squid machine*, page 12)

All core Websense components on the Squid machine

> **Note**
>
> Installing all core Websense components on one machine is typically appropriate for small networks (less than 500 users, or less than 25 Internet requests per second).
>
> See the *Deployment Guide* for more information.

Follow the installation instructions under *Typical installation* in *Chapter 2* of the *Installation Guide*. The steps below provide specific options to select, or alternate instructions to be used, as you follow the instructions in the *Installation Guide*. Unless a specific option or alternative instruction is provided here, you should follow the steps as described in the *Installation Guide*.

> **Note**
>
> Following this procedure installs Websense Network Agent on this machine. Network Agent can be used to filter non-HTTP(S)/FTP traffic (e.g., instant messaging, streaming media, peer-to-peer, and so forth) which is not handled by Squid Web Proxy Cache.

1. At the **Installation Type** screen, select **Filtering and Management**.
2. At the **Integration Option** screen, select **Integrated with another application or device**.
3. On the **Select Integration** screen, select **Squid Web Proxy Cache**.

4. On the Filtering Plug-In screen, select both **Yes, install the plug-in on this machine** and **Install other selected components**.

   See the *Installation Guide* for explanations of these options.

5. On the **Squid Configuration** screen, enter paths to the squid.conf and squid executable files, and then click **Next**.

   The installation program will verify the path to squid.conf. A default path is automatically entered. Enter a different path if necessary or click **Browse** to navigate to the location. This path must be verified for the installation to continue. (Note: the path must include the file name.)

   Additionally, you must provide the path to the Squid executable so the installation program can shut it down to continue the installation.

   > **Note**
   > The installer will automatically start Squid Web Proxy Cache once installation is complete. Verify it is running after installation is complete (Step 7 below).

6. Complete the remaining steps as described in the *Installation Guide*.
7. Start Squid Web Proxy Cache if necessary.

   The installer attempts to start Squid Web Proxy Cache once installation is complete. In some cases, it must be manually started:

   a. Verify Squid Web Proxy Cache is running, for example, by using the command `ps -ef | grep squid`.
   b. If it is not running, start it.

      See Squid documentation or support resources for the start command appropriate to your installation of Squid Web Proxy Cache.

8. If you stopped antivirus software on this machine, restart it now.

Particular Websense components on the Squid machine

This section describes how to install particular components on the Squid machine (as opposed to installing all core components; see *All core Websense components on the Squid machine*, page 11).

Websense components may be distributed across multiple machines. Depending on the size of your deployment (i.e., number of users and amount of network traffic) there are best practices of grouping certain components together on the same machine and separating certain components onto their own machine (e.g. reporting components). See the *Deployment Guide* for information about distributing components across machines.

1. Install the Websense components you want on the other machines (i.e., those other than the Squid machine).

   See the *Installation Guide* for instructions.

   > **Note**
   > Websense Filtering Service must be installed on its machine before installing the Websense Squid plug-in on the Squid machine. Additionally, Filtering Service must be installed as integrated with Squid Web Proxy Cache. If Filtering Service will be on the Squid machine, it can be installed at the same time as the Squid plug-in.

2. Install Websense components (including the Squid plug-in) on the Squid machine:
   a. Download or copy the Websense installer to the Squid machine.

      See the *Installation Guide* for instructions on downloading the installer.

   b. Close all applications and stop any antivirus software.
   c. Start the Websense installer.

      See the *Installation Guide* for instructions on starting the installer.

   d. Follow the installation instructions under *Installing individual components* in *Chapter 2* of the *Installation Guide* to select and install components. Follow the instructions to completion.

      On the **Select Components** screen, be sure to select **Filtering Plug-In** along with any other Websense components to be installed on the Squid machine.

      You can install Websense Network Agent to filter non-HTTP(S)/FTP traffic (e.g., instant messaging, streaming media, peer-to-peer, and so forth) which is not handled by Squid Web Proxy Cache. If Network Agent is installed on the Squid machine it does not need to be connected to a span port on a network switch (as it would if installed on a separate machine). See the *Deployment Guide* for more information about the placement of Network Agent in a network.

3. Start Squid Web Proxy Cache if necessary.

   To install the filtering plug-in (i.e., Squid plug-in), the installer stops Squid Web Proxy Cache. At the end of the installation process, the installer automatically starts Squid Web Proxy Cache. In some cases, the installer is unable to start Squid Web Proxy Cache and it must be manually started:

   a. Verify Squid Web Proxy Cache is running, for example, by using the command `ps -ef | grep squid`.
   b. If it is not running, start it.

      See Squid documentation or support resources for the start command appropriate to your installation of Squid Web Proxy Cache.

4. If you stopped antivirus software on this machine, restart it now.

Upgrading

To upgrade the Squid plug-in, run the Websense installer on the Squid Web Proxy Cache machine and follow the onscreen instructions. For proper communication to be established with Squid Web Proxy Cache, upgrade Websense Filtering Service **before** upgrading the Squid plug-in.

Initial setup

- Be sure to install the Squid plug-in on each Squid Web Proxy Cache machine so that Filtering Service and Squid Web Proxy Cache can communicate.
- Network Agent deployment:
  - Network Agent can be installed with other Websense components on the Squid machine, or on a separate machine.
  - Network Agent must be installed to use protocol management.
  - If Network Agent is installed, the IP addresses of all proxy servers through which computers route their Internet requests must be defined. See *Identifying the Proxy Cache and the HTTP port for Network Agent*, page 14, for instructions.
  - Identify the port used for HTTP traffic by the Squid integration. See *Identifying the Proxy Cache and the HTTP port for Network Agent*, page 14, for instructions.
- Configure authentication of users. See *Chapter 2: Authentication* for more information.
- To block HTTPS traffic, you must configure Squid appropriately. See *HTTPS blocking*, page 6, for instructions.
- Configure browsers on client computers. See *Client computer configuration*, page 15, for instructions.

Identifying the Proxy Cache and the HTTP port for Network Agent

If you have installed Network Agent, you must provide the IP addresses of all Squid Web Proxy Cache machines through which filtered Internet requests are routed. You also must provide the port that Squid uses for HTTP traffic. Without this data, Network Agent cannot filter or log requests properly.

1. Open TRITON - Web Security.
2. In the **Settings** tab, expand **Network Agent**.
3. Select the appropriate IP address in the left navigation pane to open the Local Settings page.
4. **Add** the IP addresses for all proxy servers under **Proxies and Caches**.
5. Click **Advanced Network Agent Settings**.

6. For **Ports used for HTTP traffic**, enter the port used by Squid Web Proxy Cache for HTTP traffic (default: 3128).
7. Click **OK** to cache changes on the Local Settings page. Changes are not implemented until you click **Save All**.

See the *Network Configuration* topic in the TRITON - Web Security Help for more information.

Client computer configuration

Client computers must have a Web browser that supports proxy-based connections and Java technology.

Internet browsers on client computers must be configured to use the Squid Web Proxy Cache to handle HTTP, HTTPS, FTP, and Gopher requests. Browsers must point to the same port (default: 3128) that Squid Web Proxy Cache uses for each protocol.

See your browser online help for instructions on configuring the browser to send all Internet requests to the proxy server, Squid Web Proxy Cache.

Configuring firewalls or routers

To prevent users from circumventing Websense filtering, your firewall or Internet router should be configured to allow outbound HTTP, HTTPS, FTP, and Gopher requests only from Squid Web Proxy Cache. See your router or firewall documentation for information about configuring access lists on the router or firewall.

Converting to an integrated system

You can convert an existing stand-alone deployment of Websense software to an integrated system without losing any configuration settings. The conversion process preserves settings such as policies, port numbers, and IP addresses.

Websense and Squid software can be installed on the same machine or a separate machines.

Tasks

Task 1: Upgrade to the current version of stand-alone Websense software. Keep it as a stand-alone deployment. See the Websense *Installation Guide* for upgrade paths.

Task 2: Restart the installation machine.

Task 3: Uninstall and reinstall Filtering Service and Network Agent.

See the *Installation Guide* for instructions on removing components and installing them separately.

Warning

Use caution when removing Websense components. Removing Policy Server deletes all existing configuration settings. If you accidently delete Policy Server, use the backup files created in the following procedures to restore your system.

Task 4: Convert the stand-alone deployment to a system integrated with Squid Web Proxy Cache.

The procedure depends on where Websense software is installed:

- If Websense software is running on a different machine than Squid Web Proxy Cache, follow the procedures in *Converting to an integrated system on separate machines*, page 16.
- If Websense software is running on the same machine as Squid Web Proxy Cache, follow the procedures in *Converting to an integration on the same machine*, page 18.

Task 5: Complete the Initial Setup tasks (see *Initial setup*, page 14).

Task 6: Enable authentication so that users can be properly identified and filtered. See *Chapter 2: Authentication* for instructions

Converting to an integrated system on separate machines

When Squid Web Proxy Cache is running on a different machine than Websense software, you must remove the existing Filtering Service, reinstall it as integrated with Squid Web Proxy Cache, and then install the Squid plug-in on the machine running Squid Web Proxy Cache. Network Agent also must be removed and reinstalled.

See the *Installation Guide* for complete instructions on running the installer, backing up files, and removing components.

Upgrade Websense and remove Filtering Service

1. Log on to the machine running Filtering Service:
   - **Linux**: Log in as the **root** user.
   - **Windows**: Log in with administrative privileges.
2. If you have not done so, upgrade your Websense software to the current version.
3. Use the Websense Backup Utility to back up the Websense configuration and initialization files. See the TRITON - Web Security Help for instructions.
4. Ensure that Websense software is running. The uninstaller looks for Policy Server during the removal process.
5. Close all applications and stop any antivirus software.

6. Run the uninstaller.
   - **Linux**: Go to the Websense installation directory (by default, /opt/Websense) and enter the following command:

     ```
     ./uninstall.sh
     ```

     A GUI version is available on English versions of Linux:

     ```
     ./uninstall.sh -g
     ```

   - **Windows**: Go to Windows **Control Panel** > **Add or Remove Programs**. Select **Websense Web Security / Web Filter** and then click **Change/ Remove**.

   The uninstaller detects the installed Websense components and lists them.

7. Select Filtering Service and Network Agent, and then click **Next**.

   Note

   If there are multiple Network Agents for the same Filtering Service, uninstall all those Network Agents before you uninstall the associated Filtering Service.

   Trying to uninstall Network Agent *after* its associated Filtering Service has been removed causes an error message.

8. Follow the prompts to complete the removal process.

   If Policy Server is not running, a message tells you that removing Websense components may require communication with Policy Server. You must exit the uninstaller, start the Policy Server service, and then run the uninstaller again.

   Warning

   Do not remove Websense components without the associated Policy Server running. Policy Server keeps track of Websense configuration and component locations. If Policy Server is not running, files for the selected components are still removed, but configuration information is not updated for removed components. Problems could occur later if you attempt to reinstall these components.

Reinstall Filtering Service

After Filtering Service is removed, reinstall it as integrated with Squid Web Proxy Cache. Network Agent also must be reinstalled.

1. Stop any antivirus program and firewall on the machine.
2. Start the Websense installer.
3. On the **Add Components** screen, select **Install additional components on this machine**, and then click **Next**.

4. On the **Custom Installation** screen, select **Filtering Service** and **Network Agent**, and click **Next**.
5. On the **Integration Option** screen, select **Integrated with another application or device** and then click **Next**.
6. On the **Select Integration** screen, select **Squid Web Proxy Cache**.
7. On the **Filtering Plug-In** screen, select *only* **Install other selected components** (do *not* select **Yes, install the plug-in on this machine**).
8. Follow the remaining installer prompts to complete the installation. See the *Installation Guide* for instructions.
9. If you stopped your antivirus software, start it.
10. If you stopped a firewall, start it.
11. Make sure that all Websense components are running.
    - **Linux**: Go to the Websense installation directory (/opt/Websense, by default) and enter the following command:

      ```
      ./WebsenseAdmin status
      ```

      If some services are not running, stop and then start them again by entering:

      ```
      ./WebsenseAdmin restart.
      ```

      Warning
      Do NOT use the **kill -9** command to stop Websense services. This procedure may corrupt the services.

    - **Windows**: Use the Windows **Services** dialog box.
12. Provide Network Agent with the IP address and port (default 3128) of all Squid Proxy Cache machines. See *Identifying the Proxy Cache and the HTTP port for Network Agent*, page 14.

Install the Squid plug-in

Next, the Squid plug-in must be installed on the machine running Squid Web Proxy Cache to enable communication between Websense software and Squid Web Proxy Cache.

See *Installing the Squid plug-in*, page 8.

Converting to an integration on the same machine

After upgrading Websense software, you can convert it to be integrated with Squid Web Proxy Cache that is installed on the same machine.

Important

If you are installing Websense software on a machine running an SELinux-enabled Red Hat Enterprise Linux ES 4 operating system with the version of Squid that is prepackaged with the Red Hat installation, Squid cannot launch the Websense Squid plug-in (**WsRedtor**).

If the plug-in does not launch, Websense filtering cannot occur. Configure SELinux permissions so that **WsRedtor** can launch. See your Red Hat Enterprise Linux documentation for details.

For more information, and a discussion of other options for addressing this issue, see the troubleshooting topic *Internet requests are not being filtered*, page 27.

To convert to an integrated system, Websense Filtering Service and Network Agent must be removed and then reinstalled after Squid Web Proxy Cache is installed. See the *Installation Guide* for complete instructions on running the installer, upgrading, and removing components.

Note

Internet requests are not filtered until this process is completed.

1. Log on to the installation machine as **root**.
2. Install Squid Web Proxy Cache, following the instructions provided with that product.

Important

Be sure to install and configure Squid Web Proxy Cache so it is functional before integrating Websense software with it. See Squid documentation and support resources for instructions.

3. If you have not done so, upgrade your Websense software to the current version.
4. Use the Websense Backup Utility to back up the Websense configuration and initialization files. See the TRITON - Web Security Help for instructions.
5. Close all non-Websense applications, including any firewall and antivirus software.
6. Ensure that Websense software is running. The uninstaller looks for Policy Server during the removal process.

7. Run the Websense uninstaller:
   a. Navigate to the Websense installation directory (/opt/Websense, by default).
   b. Run the following command:
      ```
      ./uninstall.sh
      ```
      A GUI version is available on English versions of Linux:
      ```
      ./uninstall.sh -g
      ```
   The installer detects the installed Websense components and lists them.
8. Select Filtering Service and Network Agent (if installed), and then click **Next**.
9. Follow the prompts to remove the components.
10. Restart the machine, if prompted.
11. Start the Websense installer again.
12. On the **Add Components** screen, select **Install additional components on this machine**, and then click **Next**.
13. On the **Custom Installation** screen, select the following components and then click **Next**:
    - **Filtering Service**
    - **Network Agent**
    - **Filtering Plug-in**
14. On the **Integration Option** screen, select **Integrated with another application or device**.
15. On the **Select Integration** screen, select **Squid Web Proxy Cache**.
16. On the **Squid Configuration** screen, enter paths to the squid.conf and squid executable files, and then click **Next**.

    The installation program will verify the path to squid.conf. A default path is automatically entered. Enter a different path if necessary or click **Browse** to navigate to the location. This path must be verified for the installation to continue. (Note: the path must include the file name.)

    Additionally, you must provide the path to the Squid executable so the installation program can shut it down to continue the installation.

    

    Note

    The installer will automatically start Squid Web Proxy Cache once installation is complete. Verify it is running after installation is complete (Step 18 below).

17. Follow the remaining installer prompts to complete the installation. See the *Installation Guide* for instructions.
18. Start Squid Web Proxy Cache if necessary.

    To install the filtering plug-in (i.e., Squid plug-in), the installer stops Squid Web Proxy Cache. At the end of the installation process, the installer automatically starts Squid Web Proxy Cache. In some cases, the installer is unable to start Squid Web Proxy Cache and it must be manually started:

a. Verify Squid Web Proxy Cache is running, for example, by using the command `ps -ef | grep squid`.

b. If it is not running, start it.

   See Squid documentation or support resources for the start command appropriate to your installation of Squid Web Proxy Cache.

19. If you stopped a firewall, start it again.
20. To make sure that all Websense components are running, navigate to the Websense installation directory (/opt/Websense, by default) and enter the following command:

    ```
    ./WebsenseAdmin status
    ```

    

    Warning

    Do NOT use the **kill -9** command to stop Websense services. This procedure may corrupt the services.

21. If you stopped your antivirus software, start it again.
22. Provide Network Agent with the IP address for all Squid Proxy Cache machines. See *Identifying the Proxy Cache and the HTTP port for Network Agent*, page 14.

2 Authentication

Authentication is the process of identifying a user within a network based on an account in a directory service. Depending on the authentication method selected, Squid Web Proxy Cache can obtain user identification and send it to Websense Filtering Service along with an Internet request. Filtering Service can filter requests based on policies assigned to individual directory objects, defined as either a user or group of users.

> **Note**
> In any environment, Websense software can filter based on computer or network policies. Workstations are identified in Websense software by their IP addresses, and networks are identified as IP address ranges

To filter Internet access for individual directory objects, Websense software can identify the user making the request:

- Enable an authentication method within Squid Web Proxy Cache so that it sends user information to Websense software.
- Enable Websense software to identify users transparently, if it does not receive user information from Squid Web Proxy Cache. You can install one of the Websense transparent identification components: DC Agent, Logon Agent, eDirectory Agent, or RADIUS Agent.

  See the *Deployment Guide* and the User Identification topic in the TRITON - Web Security Help for more information.
- Enable manual authentication within Websense software. If users cannot be identified transparently, they are prompted for authentication when they open a browser.

  See the Manual Authentication topic in the TRITON - Web Security Help for more information.

Client types

In this context, the term **clients** refers to computers or applications that run on computers and rely on a server to perform some operations. Each type of client can be configured so that Filtering Service is able to obtain user identification and filter Internet requests based on user and group policies.

Squid works with two types of clients:

- Firewall
- Web Proxy

Firewall clients

If a client is located behind a firewall, that client cannot make direct connections to the outside world without the use of a parent cache. Squid Web Proxy Cache does not use ICP queries for a request if it is behind a firewall or if there is only one parent.

Use the following lists in the **squid.conf** file to handle Internet requests.

- **never_direct**: Specifies which requests must be forwarded to the parent cache outside the firewall.
- **always_direct**: Specifies which requests must not be forwarded.

See Squid documentation and support resources for more information.

Web Proxy clients

Web Proxy clients send Internet requests directly to Squid Web Proxy Cache after the browser is configured to use Squid as the proxy server.

You can assign individual user or group policies:

- Enable one or more of the Squid authentication methods, discussed in *Authentication methods*, page 25 if the network uses multiple types of browsers. Some of these methods may require users to authenticate manually.
- Enable Websense software to prompt users for authentication. This allows Websense software to obtain the user information it needs if it does not receive that information from Squid Web Proxy Cache. See the Manual Authentication section of the *User Identification* topic in the TRITON - Web Security Help.

Authentication methods

Squid Web Proxy Cache v2.5 and 2.6 offer the following authentication methods:

- *Anonymous authentication*
- *Basic authentication*
- *Digest authentication*
- *Integrated Windows authentication*

See Squid documentation for information about enabling authentication within Squid Web Proxy Cache.

Important

Before changing authentication methods, consider the impact the change would have on other proxy server functions.

Anonymous authentication

When anonymous authentication is enabled within Squid Web Proxy Cache, user identification is not received from the browser that requests a site.

Users cannot be filtered based on individual user or group policies unless anonymous authentication is disabled and another method of authentication is enabled, or you configure Websense software to identify users.

Anonymous authentication allows Internet filtering based on computer or network policies, if applicable, or by the Default policy.

Basic authentication

When basic authentication is enabled within Squid, users are prompted to authenticate (log on) each time they open a browser. This allows Squid to obtain user identification, regardless of the browser, and send it to Websense Filtering Service, which then filters Internet requests based on individual user and group policies. Basic authentication can be enabled in combination with Integrated Windows authentication, discussed later in this section.

Digest authentication

Digest authentication is a secure authentication method used only in Windows 2000 and Windows Server 2003 domains. The features are the same as Basic authentication, but the user name and password are scrambled when they are sent from the browser to Squid Web Proxy Cache. The user can authenticate to Squid Web Proxy Cache without the user name and password being intercepted. Digest authentication can be enabled in combination with Integrated Windows authentication, discussed later in this section.

Integrated Windows authentication

Integrated Windows authentication provides secure authentication. With this authentication enabled, Squid Web Proxy Cache obtains user identification transparently from Microsoft Internet Explorer 5.0 and later. User information is sent to Websense software, which then filters Internet requests based on individual user and group policies.

> **Note**
> Squid Integrated Windows Authentication cannot obtain user identification information transparently from browsers other than Microsoft Internet Explorer.

If your network has a mixture of Microsoft Internet Explorer browsers and other browsers, you can enable both Basic and Integrated Windows authentication, or Digest and Integrated Windows authentication. In either configuration:

- Users with Microsoft Internet Explorer browsers are identified transparently.
- Users with other browsers are prompted to authenticate.

> **Note**
> To transparently identify all users in a mixed-browser environment, you can enable Anonymous authentication within Squid Web Proxy Cache and use Websense transparent identification. See *Transparent identification*, page 26.

Transparent identification

If Squid Web Proxy Cache is not configured to send user information to Websense software, you can install a Websense transparent identification agent to identify users without prompting them to log on when they open a browser. There are 4 transparent identification agents: DC Agent, Logon Agent, eDirectory Agent, and RADIUS Agent. They communicate with domain controllers or directory services to match users names with IP addresses for use in applying user- and group-based policies.

The transparent identification agents can be installed individually or in specific combinations, and can reside on the Filtering Service machine, or on a different machine. See the *Deployment Guide* and TRITON - Web Security Help for more information about deploying and configuring Websense transparent identification agents. Alternatively, refer to the *Transparent Identification of Users* technical paper for detailed information.

See the *Installation Guide* for instructions on installing individual Websense components.

A Troubleshooting

Network Agent is not filtering or logging accurately

If you have configured your Squid machine to act as a proxy server for Internet traffic, you must define the IP address of the proxy server machine in TRITON - Web Security. See *Identifying the Proxy Cache and the HTTP port for Network Agent*, page 14.

Internet requests are not being filtered

If you integrated Websense software with the Squid Web Proxy Cache on a machine running the Red Hat Enterprise Linux 4.7 operating system, and Websense filtering is not working, the problem may be the Security-enhanced Linux (SELinux) configuration.

The Red Hat Enterprise Linux 4.7 operating system installs SELinux by default. The SELinux installation is a kernel modification that reduces root user and hierarchical privilege vulnerabilities. The default SELinux installation packaged with Red Hat Enterprise Linux 4.7 prevents Squid from launching the Websense Squid Plug-in (**WsRedtor**). If **WsRedtor** does not launch, filtering cannot occur.

To determine if this is the problem, verify that **WsRedtor** is not launching on the Red Hat Enterprise Linux machine:

- **WsRedtor** does not appear in the process command list, although other Websense services do.
- Error messages associated with **WsRedtor** appear in the Squid **cache.log** (see Squid documentation for the location of this log file).
- Error messages associated with **WsRedtor** appear in the Linux system log (located by default at /var/log/messages).

If you determine that **WsRedtor** is not launching, there are several options to resolve the issue:

- Do not install Websense software on a machine using an SELinux-enabled Red Hat Enterprise Linux operating system and the version of Squid prepackaged with that Red Hat installation. If SELinux is **not** enabled, you can install Websense software on a machine using a Red Hat Enterprise Linux operating system and the prepackaged version of Squid.

- Before you install Websense software on a machine using an SELinux-enabled Red Hat Enterprise Linux operating system, you can install Squid Web Proxy Cache directly from the official Squid Web site at www.squid-cache.org. This Squid installation does not stop `WsRedtor` as does the version packaged with the Red Hat Enterprise Linux ES release 4 operating system.
- If you are familiar with configuring permissions for SELinux-enabled Red Hat, you can configure permissions so that `WsRedtor` can launch. See your Red Hat Enterprise Linux ES documentation for instructions. Additional information about SELinux is available at www.nsa.gov/selinux/.

Outgoing Internet traffic seems slow

If outgoing Internet traffic is slower than expected, increase the number of redirectors spawned by Squid. In the **squid.conf** file, go to the **redirect_children** tag (v2.5) or the **url_rewrite_children** tag (v2.6), and increase the number by 10. The current default is **30**.

If the performance continues to be slow, consult Squid documentation and check your network settings.

Squid Web Proxy Cache crashes because it cannot launch Squid plug-in (WsRedtor)

If Squid Web Proxy Cache fails to start, check the **cache.log** file (by default, located in **/usr/local/squid/logs/**).

> **Note**
> This section discusses only one possible reason for Squid Web Proxy Cache to crash. Squid Web Proxy Cache may have crashed for some other reason (for example, configuration error). See your Squid documentation.

After startup messages, the log indicates startup of WSRedtor processes. For example:

```
<timestamp>| helperOpenServers: Starting 30 ‘WsRedtor’
processes
```

The log may then indicate errors while starting the processes due to a missing file. For example (message appears multiple times):

```
(WsRedtor): error while loading shared libraries:
<filename>: cannot open shared object file: No such file or
directory
```

After that, the log indicates redirectors (i.e., WsRedtor) failed. For example (message appears multiple times):

```
<timestamp>| WARNING: redirector #<x> (FD <y>) exited
```

Finally, the log indicates a fatal error. For example:

```
FATAL: The redirector helpers are crashing too rapidly, need
help!
```

If you see entries like this in cache.log, a file required by the redirectors is missing. Such files reside in two places: **../Websense/bin** and **/etc/wsLib**. A copy of each file must be in both directories. The above errors are occurring because a file is missing from the **/etc/wsLib** directory.

To correct this issue:

1. Look in **../Websense/bin** for the missing file indicated in cache.log (i.e., <*filename*> in the example log entry above).

   If you do not find the missing file in **../Websense/bin**, then the crash may be due to another issue. Contact Websense Technical Support.

   > **Note**
   > Websense Technical Support can provide support for Squid Web Proxy Cache for issues related to Websense software only. If you are experiencing problems with your installation of Squid Web Proxy Cache for reasons unrelated to Websense software, you must refer to Squid documentation and support resources.

2. Copy the missing file from **../Websense/bin** to **/etc/wsLib**.

   > **Important**
   > **Copy**, do not move, the file. A copy of the file must reside in both **../Websense/bin** and **/etc/wsLib**.

3. Start Squid Web Proxy Cache.

   Note that if more than one file is missing from **/etc/wsLib**, you must repeat these steps for each file. Squid Web Proxy Cache indicates only one missing file at a time in cache.log.

Index