Installation Guide Supplement

for use with

Squid Web Proxy Cache

Websense® Web Security
Websense Web Filter

v7

Published 2008
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 setting up an of Websense® Web Security or Websense Web Filter with the Squid Web Proxy Cache.

See the Websense *Installation Guide* for complete instructions.

When Websense software is integrated with Squid, some differences exist in the installation and configuration, as compared to the Stand-Alone Edition:

- **Websense Filtering plug-in**: The Websense Squid plug-in must be installed on each Squid Web Proxy Cache machine to allow the Squid Web Proxy Cache to communicate with Filtering Service.
- **Network Agent**: Manages the Internet protocols that are not managed by the Squid Web Proxy Cache.

  If Network Agent will be used to filter non-HTTP protocols or perform logging, installing Network Agent on the same machine as Squid Web Proxy Cache ensures traffic visibility, as all traffic passes through the Squid machine. Having Network Agent on the same machine as Squid eliminates the need for port-forwarding or port-mirroring configurations on a switch to allow traffic visibility for Network Agent. This visibility is needed if it is installed on a separate machine.

Supported Squid versions

- Websense Web Security and Websense Web Filter v7 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 Linux.

Client computers

- To be filtered by the 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. Filtering Service consults the policy assigned to the client. Each policy designates specific time periods and lists the category filters that are applied during those periods.

After Filtering Service determines which categories are blocked for that client, it checks the Websense Master Database.

- If the site is assigned to a blocked category, the user receives a block page instead of the requested site.
- If the site is assigned to a permitted category, Filtering Service notifies the Cisco product that the site is not blocked, and the client is allowed to see the site.

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 Websense *Installation Guide*. See the *Deployment Guide* for location information and Websense Manager Help for configuration instructions.
- If Squid acts as a proxy server, you can configure it to filter all HTTPS traffic.
  1. Open the `wsSquid.ini` file in a text editor. This file is located in the `/etc/wsLib/` directory.
  2. Under the **initSection** heading, change the value of the `UseHTTPSBlockPage` parameter to **`yes`**.

     The default setting for this parameter is **no**, causing Squid to permit all HTTPS traffic.
  3. Save your changes.
  4. Restart the Squid Web Proxy Cache.

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

Installation

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

You can install the Websense components on the Squid Web Proxy Cache machine or on a different machine. If you install Filtering Service on the machine running Squid Web Proxy Cache, install the Squid plug-in on that machine, too.

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

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 `WsRedtor` does not launch, Websense filtering cannot occur. Configure SELinux permissions so that `WsRedtor` can launch. See your Red Hat Enterprise Linux documentation for details.

The following options are available from the installer's Integration Plug-in screen:

- **Install selected Websense components with plug-in**: Installs Websense components and the Squid plug-in together. Choose this option to install Websense filtering components (Policy Broker, Policy Server, Filtering Service, User Service, etc.) and the Squid plug-in on the same machine as Squid Web Proxy Cache.
- **Install plug-in:** installs only the Squid plug-in on the machine running Squid Web Proxy Cache. Squid must be running on the installation machine to complete this installation.
- **Install selected Websense components without plug-in**: installs only the Websense components that have been selected and not the Squid plug-in. Choose this option when installing Websense components on machines not running Squid Web Proxy Cache.

Installing the Squid plug-in on the Squid machine

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

The Squid plug-in is supported only on Linux.

Filtering Service and the plug-in can be installed at the same time on the Squid machine.

If Filtering Service is installed on a separate machine than the Squid Web Proxy Cache, it must be installed before you install the Squid plug-in.

Filtering Service also must be installed in the integration mode, with Squid Web Proxy Cache selected as the integration. You cannot install the plug-in if the installer cannot find Filtering Service during plug-in installation.

When installing the 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, an error message advises you that the Squid plug-in can only be installed if Squid Web Proxy Cache is present. Click **OK** to return to the integration option, or click **Next** to exit the installer.

1. Stop the Squid Web Proxy Cache before installing the Squid plug-in.
2. Start the Websense installation program, and follow the prompts.
3. When you reach the Product Selection screen of the Websense installation, select **Custom**.
4. From the components list, select **Filtering Plug-in** and any other Websense components to be installed on the Squid Web Proxy Cache machine.
5. Select **Integrated** as the integration option, and then select **Squid Web Proxy Cache** as the integration type.
6. Select whether to install the plug-in with other components or to install the plug-in alone.
7. If you are installing other Websense components on the Squid Web Proxy Cache machine:
   a. Provide the path to the Squid configuration file (`squid.conf`). A default path is provided. The installer verifies this path and cannot continue unless the path is correct.
   b. Provide the file path to the Squid executable (`squid`). The installer shuts down Squid automatically before the installation continues.
8. After the installation is complete, restart the Squid Web Proxy Cache.

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 the Squid Web Proxy Cache, upgrade Websense Filtering Service **before** upgrading the filtering 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 can communicate.
- Network Agent deployment:
  - Network Agent can be installed with other Websense components on the Squid Proxy 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 9, 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 9, 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 9, 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 Websense Manager.
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. Enter **3128** for **Ports used for HTTP traffic**.
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 Websense Manager 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

After upgrading your existing Websense Stand-Alone Edition to version 7, you are ready to convert to a system that integrates with Squid Web Proxy Cache. Websense and Squid software can be installed on the same machine or a separate machines.

You can convert an existing Stand-Alone Edition to an integrated system without losing any configuration settings. The conversion process preserves such settings as policies, port numbers, and IP addresses.

Tasks

Task 1: Upgrade to the current version of Stand-Alone Edition. 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.

Task 4: Convert the Stand-Alone Edition 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*.
- If Websense software is running onthe same machine as Squid Web Proxy Cache, follow the procedures in *Converting to an integration on the same machine*, page 13.

Task 5: Complete the Initial Setup tasks (see *Initial setup*, page 8).

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 the Websense software, you must remove the existing Filtering Service, reinstall it to integrate with the Squid software, 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 installation machine:
   - **Linux**: Log in as the **root** user.
   - **Windows**: Log in with administrative privileges.
2. If you have not done so, upgrade your Websense software.
3. Use the Websense Backup Utility to back up the Websense configuration and initialization files. See Websense Manager Help for instructions.
4. Ensure that Websense software is running. The installer looks for Policy Server during the installation process.
5. Close all applications and stop any anti-virus software.
6. Run the uninstall program.
   - **Linux**: From the Websense installation directory (by default, `/opt/Websense`), run:

     ```
     ./uninstall.sh
     ```

     A GUI version is available on English versions of Linux:

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

   - **Windows**: Launch the Windows Add or Remove Programs utility from the Control Panel, and select **Websense** to start the Websense uninstall program.

   The uninstaller detects the installed Websense components and lists them. By default, all components are selected for removal.

7. Deselect all components except Filtering Service and Network Agent, and 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 uninstall program, start the Policy Server service, and then run the uninstall program again.

Warning

If Policy Server is not running, the files for the selected components are removed, but configuration information is not updated for these components. Problems could occur later if you attempt to reinstall these components.

Reinstall Filtering Service

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

1. Stop any anti-virus program and firewall on the installation machine.
2. Start the Websense installer.
3. Click **Next** in the Welcome screen to access the Add/Remove screen.
4. Select **Add Websense components**, and click **Next**.
5. Select **Filtering Service** and **Network Agent**, and click **Next**.
6. Select **Integrated** as the integration option, and click **Next**.
7. Select **Squid Web Proxy Cache** as the integration type, and click **Next**.
8. Select **Install selected Websense components without plug-in**.
9. Follow the instructions to complete the installation.

   See the Websense *Installation Guide* for more information.
10. If you stopped your anti-virus software, start it again.
11. If you stopped a firewall, start it again.
12. Make sure that all Websense components are running.
    - **Linux**: Open a command prompt, and enter `./WebsenseAdmin status` from the `opt/Websense` directory. 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**: Check the status of the Websense components in the Windows Services dialog box.
13. Provide Network Agent with the IP address and port (default 3128) for all Squid Proxy Cache machines. See *Identifying the Proxy Cache and the HTTP port for Network Agent*, page 9.

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.

1. Log on to the Squid Web Proxy Cache machine.
2. Run the Websense installer.
3. Follow the prompts to the Product Selection screen.
4. Select **Custom**, and click **Next**.
5. Select **Filtering Plug-in**, and click **Next**.
6. Select **Squid Web Proxy Cache**, and click **Next**.
7. Enter the **IP Address** for the machine running Filtering Service.

   Filtering Service uses the **Filter Port** to communicate. The default port number (15868) is shown. If a different port was set for Filtering Service, enter that port.
8. Complete the installation process, as described in the *Installation Guide*.
9. If you stopped your anti-virus software, start it again.

Converting to an integration on the same machine

After you upgrade Stand-Alone Edition, you can convert Websense software to integrate with Squid Web Proxy Cache that is installed on the same machine.

Important

If you are converting the Stand-Alone Edition on a machine running Red Hat Enterprise Linux ES 4 with SELinux enabled, and using the version of Squid that is prepackaged with the Red Hat installation, Squid cannot launch the Websense Squid plug-in (`WsRedtor`).

If `WsRedtor` 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 21.

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.
3. If you have not done so, upgrade your Websense software.
4. Use the Websense Backup Utility to back up the Websense configuration and initialization files. See Websense Manager Help for instructions.
5. Close all non-Websense applications, including any firewall and anti-virus software.
6. Ensure that Websense software is running. The installer looks for Policy Server during the installation process.
7. Run the uninstall program.
   a. Open a command prompt and 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. All components are selected for removal, by default.
8. Deselect all components except Filtering Service and Network Agent (if installed), and click **Next**.
9. Follow the prompts to remove the components.
10. Restart the machine, if prompted.
11. Start the Websense installer again, and follow the prompts to the Stand-Alone Edition Detected screen.
12. Select **Add Websense components**, and click **Next**.
13. Select **Filtering Service** and **Network Agent**, and click **Next**.
14. Select **Integrated** as the integration option, and click **Next**.
15. Select **Squid Web Proxy Cache** as the integration type, and click **Next**.

16. Select **Install selected Websense components with plug-in**.
    - **Squid configuration file**: The installer asks for the path to the Squid configuration file (`squid.conf`). A default path is provided. The installer verifies this path and cannot continue unless it is accurate.
    - **Squid executable**: the installer asks for the path to the Squid executable (`squid`). The installer shuts down Squid automatically before the installation continues.
17. Follow the prompts to complete the installation.

    See the Websense *Installation Guide* for more information.
18. If you stopped a firewall, start it again.
19. Make sure that all Websense components are running.
    a. Open a command prompt and navigate to the `/Websense` directory.
    b. Enter `./WebsenseAdmin status`.

Warning

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

20. If you stopped your anti-virus software, start it again.
21. 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 9.

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. 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 Websense Manager 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 Websense Manager Help for more information.

Client types

The term *clients* in this environment 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 does not use ICP queries for a request if Squid 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.

Consult the Squid documentation for more information.

Web Proxy clients

Web Proxy clients send Internet requests directly to the 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 19 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 the Websense software to obtain the user information it needs if it does not receive that information from Squid. See the Manual Authentication section in the *User Identification* topic in Websense Manager 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.

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 the Websense Filtering Service, which then filters Internet requests based on individual user and group policies. Basic authentication can be enabled in combination or Integrated Windows authentication, discussed later in this section.

Digest authentication

Digest authentication is a secure authentication 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 the Squid Web Proxy Cache. The user can authenticate to the Squid Web Proxy Cache without the user name and password being intercepted. Digest authentication can be enabled in combination or 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 browsers using 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**
> Windows 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 and use Websense transparent identification. See *Transparent identification*, page 20.

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 Websense *Deployment Guide* and the Websense Manager 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 Chapter 3 of the Websense *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 Websense Manager. See *Identifying the Proxy Cache and the HTTP port for Network Agent*, page 9.

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 ES 4 operating system, and Websense filtering is not working, the problem may be the Security-enhanced Linux (SELinux) configuration.

The Red Hat Enterprise Linux ES 4 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 ES release 4 prevents Squid from launching the Websense Squid Plug-in (`WsRedtor`). If `WsRedtor` does not launch, Websense filtering cannot occur.

To determine if this is the problem, verify that `WsRedtor` is not launching on the Red Hat Enterprise Linux ES 4 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`, found by default at `/var/log/squid/cache.log`.
- Error messages associated with `WsRedtor` appear in the Linux system log, found 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 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 and increase the number by 10. The current default is `30`.

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

Index

W