Installation Guide Supplement

for use with

Microsoft® ISA Server
and
Forefront™ TMG

Websense® Web Security
Websense Web Filter

v7.5

©1996–2010, Websense Inc.
All rights reserved.
10240 Sorrento Valley Rd., San Diego, CA 92121, USA

Published 2010
Printed in the United States of America and Ireland.

The products and/or methods of use described in this document are covered by U.S. Patent Numbers 5,983,270; 6,606,659; 6,947,985; 7,185,015; 7,194,464 and RE40,187 and other patents pending.

This document may not, in whole or in part, be copied, photocopied, reproduced, translated, or reduced to any electronic medium or machine-readable form without prior consent in writing from Websense Inc.

Every effort has been made to ensure the accuracy of this manual. However, Websense Inc., makes no warranties with respect to this documentation and disclaims any implied warranties of merchantability and fitness for a particular purpose. Websense Inc. shall not be liable for any error or for incidental or consequential damages in connection with the furnishing, performance, or use of this manual or the examples herein. The information in this documentation is subject to change without notice.

Trademarks

Websense is a registered trademark of Websense, Inc., in the United States and certain international markets. Websense has numerous other unregistered trademarks in the United States and internationally. All other trademarks are the property of their respective owners.

Microsoft, Windows, Windows NT, Windows Server, Windows Vista and Active Directory are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Novell Directory Services is a registered trademark of, and eDirectory is a trademark of, Novell, Inc., in the United States and other countries.

Adobe, Acrobat, and Acrobat Reader are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries.

Pentium is a registered trademark of Intel Corporation.

Red Hat is a registered trademark of Red Hat, Inc., in the United States and other countries. Linux is a trademark of Linus Torvalds, in the United States and other countries.

This product includes software distributed by the Apache Software Foundation (http://www.apache.org).
Copyright (c) 2000 The Apache Software Foundation. All rights reserved.

Other product names mentioned in this manual may be trademarks or registered trademarks of their respective companies and are the sole property of their respective manufacturers.

WinPcap

Copyright (c) 1999 - 2005 NetGroup, Politecnico di Torino (Italy).
Copyright (c) 2005 - 20095/14/10 CACE Technologies, Davis (California).
All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- Neither the name of the Politecnico di Torino, CACE Technologies nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Contents

Chapter 1 **Microsoft ISA Server or Forefront TMG Integration 5**

How Websense filtering works with ISA/TMG 6
Supported integration versions 7
Installation 7
Websense software and ISA/TMG on separate machines 8
Installing the ISAPI Filter plug-in for ISA Server 9
Installing the ISAPI Filter plug-in for Forefront TMG 11
Websense software and ISA Server on the same machine 14
Testing visibility of Internet traffic to Network Agent 16
Upgrade 16
Removing the ISAPI Filter Plug-In 17
Converting to an integrated system 19
Tasks 19
Converting to an integrated system on a separate machine 20
Upgrade Websense software and remove Filtering Service 20
Reinstall Filtering Service 20
Install the Websense ISAPI Filter Plug-In 22
Converting to an integration on the same machine 22
Initial Setup 25
Enabling communication with the Log Database 25
WinSOCK and SOCKS proxy servers 26
Configuring for ISA/TMG using non-Web-Proxy clients 26
Firewall/Forefront TMG Client 26
SecureNAT clients 27
Configuring the ISAPI Filter plug-in 27
Configuring Websense software to ignore specific traffic 28
Client computer configuration 29
Firewall configuration 29
Migrating between Microsoft integration products 30

Chapter 2 **Authentication. 31**

ISA/TMG clients 32

Firewall/Forefront TMG and SecureNAT clients 33

Web Proxy clients 33

Authentication Methods 34

Basic authentication 34

Digest authentication 34

Integrated Windows authentication 35

Client Certificate authentication 35

Transparent identification. 36

Appendix A **Troubleshooting 37**

SecureNAT clients are not being filtered 37

No filtering occurs after the ISAPI Filter plug-in is installed. 37

Index **39**

1 Microsoft ISA Server or Forefront TMG Integration

This supplement to the *Websense Web Security and Websense Web Filter Installation Guide* (*Installation Guide*) provides information specific to integrating Websense software with Microsoft® Internet Security and Acceleration (ISA) Server and Forefront™ Threat Management Gateway (TMG). Refer to the *Installation Guide* as your primary source of installation instructions. Only additional or alternate steps required to integrate Websense software with ISA/TMG are provided here.

Notes

In this guide, "ISA/TMG" refers to ISA Server and Forefront TMG collectively. When instructions or information differ for the two products, they are referred to specifically as "ISA Server" or "Forefront TMG".

Note

In this guide, "Websense software" refers to a deployment of Websense Web Security or Websense Web Filter. A deployment consists of various Websense components that may be distributed across different machines in a network. When information pertains to a particular Websense component, the component name is used.

An integration with ISA/TMG affects the following Websense components:

- **Websense ISAPI Filter plug-in**: This additional Websense component is installed on the machine running ISA/TMG. The ISAPI Filter plug-in configures ISA/TMG to communicate with Websense Filtering Service.
- **Websense Filtering Service**: Interacts with ISA/TMG and Websense Network Agent to filter Internet requests. Filtering Service either permits the Internet request or sends an appropriate block message to the user.

  After the Filtering Service is installed, the ISAPI Filter plug-in must be installed on every ISA/TMG machine in your network.

- **Websense Network Agent**: Internet protocols that are not managed by ISA/TMG are managed by Network Agent. It can detect HTTP network activity and instruct the Filtering Service to log this information.

> **Note**
>
> Do **not** install Network Agent on the ISA Server machine if ISA Server firewall is enabled. If ISA Server is used only as a proxy server and not firewall, Network Agent may be installed on the ISA Server machine.
>
> Network Agent cannot be installed on a Forefront TMG machine because Forefront TMG runs on 64-bit Windows Server 2008 (x64) only. Websense components—except the ISAPI Filter plug-in and Control Service—do not currently support 64-bit Windows Server 2008. (Note: Control Service is automatically installed when installing the plug-in.)

- **Transparent identification agents**: Generally, ISA/TMG provides user authentication information for Websense software. If ISA/TMG is not configured to provide user information to Websense software, install the appropriate Websense transparent identification agent. See the *Deployment Guide for Websense Web Security Solutions* (*Deployment Guide*) or *Transparent Identification of Users* technical paper for more information about these agents.

If your environment includes an array of ISA/TMG machines, it is a best practice to install Websense software on a machine outside the array. For Forefront TMG this is the only configuration possible. Forefront TMG runs on 64-bit Windows Server 2008. Websense software, other than the ISAPI Filter plug-in and Control Service, does not support 64-bit Windows Server 2008.

How Websense filtering works with ISA/TMG

To be filtered by Websense software, a computer must access the Internet through ISA/TMG.

When ISA/TMG receives an Internet request from a user, it queries Websense Filtering Service to find out if the requested site should be blocked or permitted. Filtering Service checks 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 client receives a block page instead of the requested site.
- If the site is assigned to a permitted category, Filtering Service notifies ISA/TMG that the site is not blocked, and the client is given access to the site.

Supported integration versions

Websense software can be integrated with the following Microsoft products.

- Microsoft ISA Server 2004, Standard Edition and Enterprise Edition
- Microsoft ISA Server 2006, Standard Edition and Enterprise Edition
- Microsoft Forefront TMG 2010

Supported ISA/TMG clients are:

- Firewall Client/Forefront TMG Client
- SecureNAT clients
- Web Proxy clients

Installation

Typically, Websense software is not installed on the same machine as ISA Server. The only Websense component installed on the ISA Server machine is the ISAPI Filter plug-in. In the case of a Forefront TMG machine, no Websense software, except the ISAPI Filter plug-in, can be installed. See *Websense software and ISA/TMG on separate machines*, page 8.

Notes

- It is a best practice to not install Websense components, except the ISAPI Filter plug-in, on the same machine as ISA Server.
- When the ISAPI Filter plug-in is installed, Websense Control Service is installed automatically as well.

However, if the machine has sufficient resources, Websense software may be installed on an ISA Server machine. The machine must have sufficient resources or the performance of both Websense software and ISA Server may be affected.

Note

Websense software (except the ISAPI Filter plug-in and Control Service) cannot be installed on the same machine as Forefront TMG. Forefront TMG runs on 64-bit Windows Server 2008 (x64) only. Websense components, other than ISAPI Filter plug-in and Control Service, do not currently support Windows Server 2008 (x64).

Websense software and ISA/TMG on separate machines

Typically, Websense software is installed on machines separate from ISA/TMG. 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.

   Note
   Websense Filtering Service must be installed on its machine before installing the ISAPI Filter plug-in on the ISA/TMG machine. When installing Filtering Service, it must be installed as integrated with ISA/TMG.

2. Install the ISAPI Filter plug-in on the ISA/TMG machine.

   Note
   Port 55933 (Websense Control Service communication port) must be open locally, for the ISAPI Filter plug-in to be installed successfully. If installing other Websense components on the ISA Server machine, see the Websense Knowledge Base for default Websense ports (http://www.websense.com/v75_ports).

   - ISA Server:

     Run the Websense installer on the ISA Server machine and choose to install the plug-in only. See *Installing the ISAPI Filter plug-in for ISA Server*, below.

     Note
     Do not attempt to install the ISAPI Filter plug-in for ISA Server on Windows Server 2008. This plug-in supports ISA Server 2004 and 2006 only, which are not supported on Windows Server 2008.

   - Forefront TMG:

     A separate installer from Websense, referred to as the *Forefront TMG plug-in installer*, is used to install the ISAPI plug-in for Forefront TMG. See *Installing the ISAPI Filter plug-in for Forefront TMG*, page 11.

     Important
     The ISAPI Filter plug-in for Forefront TMG is supported on **only** 64-bit Windows Server 2008 (x64). Do not attempt to run the Forefront TMG plug-in installer on any operating system but Windows Server 2008 (x64).

Installing the ISAPI Filter plug-in for ISA Server

The Websense installer is used to install the Websense ISAPI Filter plug-in on the ISA Server machine. The following procedure is performed on the ISA Server machine.

Note

As part of the installation process, you must stop the Microsoft Firewall service. Depending on your network configuration, doing so may stop network traffic. It is a best practice to perform this installation during a time when such stoppage would least affect your organization. Do not stop the Firewall service until instructed to do so by the installer.

Note

Websense Filtering Service must be installed on its machine before installing the ISAPI Filter plug-in on this machine. When installing Filtering Service, be sure to specify it as integrated with ISA Server.

Note

Port 55933 (Websense Control Service communication port) must be open locally, for the ISAPI Filter plug-in to be installed successfully.

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.
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**.

> **Note**
> 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 finds the default port to be in use, it is 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 **Microsoft Internet Security and Acceleration Server** and then click Next.
10. On the **Pre-Installation Summary** screen, verify the information shown.

    Filtering Plug-in should be listed as the only component to be installed.
11. Click **Next** to start the installation. An **Installing** progress screen is displayed. Wait for the installation to complete.
12. When the **Stop Microsoft Firewall Service** screen appears, stop the Microsoft Firewall service and then click **Next**.

> **Note**
> Leave the Websense installer running as you stop the Microsoft Firewall service, and then return to the installer to continue installation.

In order to correctly install the Websense ISAPI Filter plug-in, the Microsoft Firewall Service must be stopped. Installation of the plug-in files and registration of the plug-in in the system registry cannot occur while the Microsoft Firewall Service has certain files locked. Stopping the Microsoft Firewall Service unlocks these files.

To stop the Firewall service, go to the Windows Services management console (**Administrative Tools** > **Services)**. Right-click Microsoft Firewall, and then select **Stop**. When the service has stopped, return to the Websense installer and continue the installation process. The Firewall Service may also be stopped from the ISA Server Management console or Command Prompt (using the command `net stop fwsrv`). See Microsoft's documentation for more information.

13. When the following message appears, start the Microsoft Firewall service and then click **OK**:

    The Websense ISAPI Filter has been configured, you can now start the Microsoft Firewall Service.

    > **Important**
    > When the Microsoft Firewall service is stopped, ISA Server goes into lockdown mode. Depending on your network configuration, network traffic may be stopped.

    To start the Firewall service, go to the Windows Services management console (**Administrative Tools** > **Services)**. Right-click Microsoft Firewall, and then select **Start**.The Firewall Service may also be started from the ISA Server Management console or Command Prompt (using the command `net start fwsrv`). See Microsoft's documentation for more information.

14. On the **Installation Complete** screen, click **Done**.
15. If you stopped antivirus software on this machine, restart it now.
16. You can verify successful installation of the ISAPI Filter plug-in by logging into the ISA Server Management console.

    In the console, go to **Configuration** > **Add-ins** > **Web Filters**. WsISAFilter should be present in the list of Web Filters.

Installing the ISAPI Filter plug-in for Forefront TMG

The Forefront TMG plug-in installer is used to install the Websense ISAPI Filter plug-in for Forefront TMG. The following procedure is performed on the Forefront TMG machine.

> **Important**
> The ISAPI Filter plug-in for Forefront TMG is supported on **only** 64-bit Windows Server 2008. Do not attempt to run the Forefront TMG plug-in installer on any operating system other than 64-bit Windows Server 2008.

> **Note**
> As part of the installation process, you must stop the Microsoft Forefront TMG Firewall service (Firewall service). Depending on your network configuration, doing so may stop network traffic. It is a best practice to perform this installation during a time when such stoppage would least affect your organization. Do not stop the Firewall service until instructed to do so by the installer.

Note

Websense Filtering Service must be installed on its machine before installing the ISAPI Filter plug-in on this machine. When installing Filtering Service, be sure to specify it as integrated with Forefront TMG.

Note

Port 55933 (Websense Control Service communication port) must be open locally, for the ISAPI Filter plug-in to be installed successfully.

1. Download or copy the Forefront TMG plug-in installer to this machine.

   This installer is available at mywebsense.com.
2. Close all applications and stop any antivirus software.
3. Start the Websense installer.
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 **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**.

   Note

   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 is installed, if the installation program finds the default port to be in use, it is 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.
7. On the **Installation Directory** screen, accept the default location and click **Next**.
8. On the **Pre-Installation Summary** screen, verify the information shown.

   Filtering Plug-in should be listed as the only component to be installed.

9. Click **Install** to start the installation. An **Installing** progress screen is displayed. Wait for the installation to complete.
10. When the **Stop Microsoft Forefront TMG Firewall Service** screen appears, stop the Microsoft Forefront TMG Firewall service (Firewall service) and then click **Next**.

> **Note**
> Leave the Websense installer running as you stop the Firewall service, and then return to the installer to continue installation.

In order to correctly install the Websense ISAPI Filter plug-in, the Firewall service must be stopped. Installation of the plug-in files and registration of the plug-in in the system registry cannot occur while the Firewall service has certain files locked. Stopping the Firewall service unlocks these files.

To stop the Firewall service, go to the Windows Services management console (**Administrative Tools** > **Services)**. Right-click Microsoft Forefront TMG Firewall, and then select **Stop**. When the service has stopped, return to the Websense installer and continue the installation process. The Firewall service may also be stopped from the Forefront TMG management console. See Microsoft's documentation for more information.

> **Important**
> When the Firewall service is stopped, Forefront TMG goes into lockdown mode. Depending on your network configuration, network traffic may be stopped. Typically, the Firewall service must be stopped for only a few minutes.

11. When the following message appears, start the Firewall service and then click **OK**:

    The Websense ISAPI Filter has been configured, you can now start the Microsoft Firewall Service.

> **Note**
> Leave the Websense installer running as you start the Firewall service, and then return to the installer to continue installation.

To start the Firewall service, go to the Windows Services management console (**Administrative Tools** > **Services)**. Right-click Microsoft Forefront TMG Firewall, and then select **Start**.The Firewall Service may also be started from the Forefront TMG management console. See Microsoft's documentation for more information.

12. On the **Installation Complete** screen, click **Done**.

13. If you stopped antivirus software on this machine, restart it now.
14. You can verify successful installation of the ISAPI Filter plug-in by logging into the Forefront TMG management console.

    In the console, go to **System** > **Web Filters**. WsISAFilter should be present in the list of Web Filters.

Websense software and ISA Server on the same machine

If the machine has sufficient resources, Websense software may be installed on the same machine as ISA Server. You may install all core Websense components (see below) or particular components (see *Particular Websense components on the ISA Server machine*, page 15)

> **Note**
> Websense software cannot be installed on a Forefront TMG machine. Forefront TMG runs on 64-bit Windows Server 2008 (x64).Websense components (other than the ISAPI Filter plug-in and Control Service) do not currently support Windows Server 2008 (x64).

All core Websense components on the ISA Server machine

> **Note**
> Following this procedure installs Websense Network Agent on this machine. However, it is a best practice to not run Websense Network Agent on the same machine as ISA Server. After installation, you should disable Network Agent on this machine (see the TRITON - Web Security Help). Install and run Network Agent on another machine. For information about where to place Network Agent in your network, see the *Deployment Guide*.
>
> An exception to this is if ISA Server firewall is not enabled and ISA Server is running as a proxy server only. In this case, Network Agent may run on the ISA Server machine.

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*.

1. At the **Installation Type** screen, select **Filtering and Management**.

> **Note**
> Installing Websense reporting components on an ISA Server machine is not recommended. Do not select the **Filtering, Management, and Reporting** installation type.

2. At the **Integration Option** screen, select **Integrated with another application or device**.
3. On the **Select Integration** screen, select **Microsoft Internet Security and Acceleration Server**.
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 explanation of these options.
5. Complete the remaining steps as described in the *Installation Guide*.
6. If you stopped antivirus software on this machine, restart it now.

Particular Websense components on the ISA Server machine

If it has sufficient resources, you can install Websense components on the ISA Server machine. This section describes how to install particular components on the ISA Server machine.

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 to their own machines (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 ISA Server machine).

   See the *Installation Guide* for instructions.

> **Note**
> Websense Filtering Service must be installed on its machine before installing the ISAPI Filter plug-in on the ISA Server machine. If Filtering Service will be on the ISA Server machine, it can be installed at the same time as ISAPI Filter plug-in. When installing Filtering Service, be sure to specify it as integrated with ISA Server. See the *Installation Guide* for more information.

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

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

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

> **Note**
> Do not attempt to install the ISAPI Filter plug-in for ISA Server on Windows Server 2008. This plug-in supports ISA Server 2004 and 2006 only, which are not supported on Windows Server 2008.

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

Testing visibility of Internet traffic to Network Agent

If you installed Network Agent, you can use the Websense Network Traffic Detector to test whether Network Agent is able to monitor Internet requests from the desired network (and to see replies). See the TRITON - Web Security Help for instructions.

Upgrade

- Upgrade Websense Filtering Service before upgrading the ISAPI Filter plug-in. This ensures proper communication between Filtering Service and ISA/TMG.
- To upgrade the ISAPI Filter plug-in:
  - ISA Server: Run the Websense installer on the ISA Server machine and follow the on-screen instructions.
  - Forefront TMG: Run the Forefront TMG plug-in installer on the Forefront TMG machine and follow the on-screen instructions.

> **Note**
> As part of the upgrade process, you must stop the Microsoft Firewall service. Depending on your network configuration, doing so may stop network traffic. It is a best practice to perform this upgrade during a time when such stoppage would least affect your organization. Do not stop the Firewall service until instructed to do so by the installer.

- If you are upgrading your Websense system and migrating from Microsoft Proxy Server to ISA Server, see *Migrating between Microsoft integration products*, page 30.

> **Note**
> This version of Websense software does not support an integration with Microsoft Proxy Server.

Removing the ISAPI Filter Plug-In

Detailed instructions for removing Websense filtering components are provided in the *Installation Guide*. However, additional steps are required when you remove the ISAPI Filter plug-in from an ISA/TMG machine.

1. Log on with **local** administrator privileges.
2. Choose to uninstall a program:
   - Windows Server 2003: Go to Windows **Control Panel** > **Add or Remove Programs**.
   - Windows Server 2008 (x64): Go to Windows **Control Panel** > **Control Panel Home** > **Uninstall a program** (under **Programs**).
3. Select **Websense Web Security / Web Filter**, and then click **Change/Remove** (Windows Server 2003) or **Uninstall/Change** (Windows Server 2008).

   This launches the Websense uninstaller.
4. On the **Remove Components** screen, select **Filtering Plug-in** and any other components to be removed, and then click **Next**.
5. When the **Stop Microsoft Firewall Service** screen appears, stop the Microsoft Firewall service and then click **Next**.

> **Note**
> Leave the Websense uninstaller running as you stop the Microsoft Firewall service, and then return to the uninstaller to continue.

To stop the Firewall service, go to the Windows Services management console (**Administrative Tools > Services)**. Right-click **Microsoft Firewall** (ISA Server) or **Microsoft Forefront TMG Firewall** (Forefront TMG), and then select **Stop**. When the service has stopped, return to the Websense installer and continue the uninstallation process.

> **Important**
> When the Firewall service is stopped, ISA/TMG goes into lockdown mode. Depending on your network configuration, network traffic may be stopped. Typically, the Firewall service must be stopped for only a few minutes.

6. When the following message appears, start the Firewall service and then click **OK**:

   The Websense ISAPI Filter has been unconfigured, you can now start the Microsoft Firewall Service.

   > **Note**
   > Leave the Websense uninstaller running as you start the Firewall service, and then return to the uninstaller to continue.

   To start the Firewall service, go to the Windows Services management console (**Administrative Tools > Services)**. Right-click **Microsoft Firewall** (ISA Server) or **Microsoft Forefront TMG Firewall** (Forefront TMG), and then select **Start**.

7. On the **Websense Software Removed** screen, choose whether you want to restart now or later and then click **Done**.

Converting to an integrated system

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

Tasks

The following are the main tasks to convert a stand-alone deployment to one integrated with ISA/TMG.

> **Note**
> Websense software cannot be installed on a Forefront TMG machine. Forefront TMG runs on 64-bit Windows Server 2008 (x64).Websense components (other than the ISAPI Filter plug-in and Control Service) do not currently support Windows Server 2008 (x64).

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

Task 2: Restart the installation machine.

Task 3: Uninstall and reinstall Filtering Service in integrated mode, selecting ISA Server or Forefront TMG as the integration product.

If Websense software, including Network Agent, is running on the machine on which ISA Server will be installed, then Network Agent must be moved to another machine.

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

Task 4: Convert the stand-alone deployment to a system integrated with ISA/TMG.

The procedure varies based on where Websense software is installed:

- If Websense software is running on a different machine than ISA/TMG, follow the procedures in *Converting to an integrated system on a separate machine*, page 20.
- If Websense software is running on the same machine as ISA Server, follow the procedures in *Converting to an integration on the same machine*, page 22.

Task 5: Complete the setup tasks, as described later in this supplement.

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

Converting to an integrated system on a separate machine

When ISA/TMG is running on a different machine than the Websense software, you must remove the existing Websense Filtering Service, reinstall it to be integrated with ISA/TMG, and then install the ISAPI Filter plug-in on the machine running ISA/TMG. These procedures are described below.

> **Note**
> If you are upgrading to a new version of Websense software, perform the upgrade before converting the deployment to be integrated with ISA/TMG.

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

Upgrade Websense software and remove Filtering Service

1. If you have not done so, upgrade your Websense software to the current version.
2. Use the Websense Backup Utility to back up the Websense configuration and initialization files. See the TRITON - Web Security Help for instructions.
3. Ensure that Websense software is running. The uninstaller looks for Policy Server during the removal process.

> **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 those components. Problems could occur later if you attempt to reinstall these components.

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

   The Websense uninstall program starts.
6. On the **Remove Components** screen, make sure that only **Filtering Service** is selected, and then click **Next**.
7. Follow the prompts to complete the removal process.

Reinstall Filtering Service

After Filtering Service is removed, reinstall it as integrated with ISA/TMG.

1. Stop any antivirus programs on the machine running Filtering Service.
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 then 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 **Microsoft Internet Security and Acceleration Server** or **Microsoft Forefront Threat Management Gateway** and then click **Next**.

> **Note**
> Select the particular integration product you are using (ISA Server or Forefront TMG).

7. (This applies only if ISA Server was selected) On the **Filtering Plug-In** screen, select *only* **Install other selected components** and then click **Next**.
8. On the **Filtering Feedback** screen, select whether you want Websense software to send feedback to Websense, Inc. to improve accuracy and then click **Next**.

   Choosing to allow feedback to Websense, Inc. helps improve the accuracy of Websense software for all customers. The feedback consists of any URLs that could not be categorized by Websense software. Such uncategorized URLs are evaluated by Websense, Inc. If warranted, they are investigated in more detail and put into an appropriate category. The Websense Master Database is updated with this information. When your Websense software downloads the updated database, it will be able to categorize those URLs and filter them according to the policies you have set.

> **Important**
> No information about users or your network is collected. The information is only about the visited URLs themselves. Only uncategorized URLs and the frequency of requests to them are collected. Uncategorized intranet URLs are not included in feedback.

> **Note**
> You can later choose to enable or disable feedback (the feedback mechanism is known as WebCatcher) using the Log Server Configuration utility. For more information, see the Log Server Configuration Help.

9. On the **Pre-Installation Summary** screen, verify the information shown.

   The summary shows the installation path and size, and the components to be installed.

10. Click **Install** to start the installation. An **Installing** progress screen is displayed. Wait for the installation to complete.

> **Note**
> If you are using the command-line Linux installer, do **not** cancel (Ctrl-C) 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 whose installation you wanted to cancel.

11. On the **Installation Complete** screen, click **Done**.
12. If you stopped your antivirus software, start it again.

Install the Websense ISAPI Filter Plug-In

Next, install the ISAPI Filter plug-in on the ISA/TMG machine. This plug-in allows Websense software and ISA/TMG to communicate. For instructions, see:

- *Installing the ISAPI Filter plug-in for ISA Server*, page 9 or
- *Installing the ISAPI Filter plug-in for Forefront TMG*, page 11

Converting to an integration on the same machine

After upgrading a stand-alone deployment of Websense software, you can convert it to be integrated with ISA Server installed on the same machine.

> **Note**
> Websense software (other than the ISAPI Filter plug-in and Control Service) cannot run on the same machine as Forefront TMG because it runs on 64-bit Windows Server 2008 (x64) only. Websense software does not currently support Windows Server 2008 (x64).

To convert Websense software to be integrated with ISA Server, Websense Filtering Service and Network Agent must be removed and then reinstalled after ISA Server is installed. See the *Installation Guide* for detailed instructions on running the installer, upgrading, and removing components.

> **Note**
> Internet requests are not filtered until this process is completed.

1. If you have not done so, upgrade your Websense software.

   See the *Installation Guide* for instructions.

2. Use the Websense Backup Utility to back up the Websense configuration and initialization files. See the TRITON - Web Security Help for instructions
3. Ensure that Websense software is running. The installer looks for Policy Server during the installation process.

> **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 those components. Problems could occur later if you attempt to reinstall these components.

4. Go to **Start** > **Settings** > **Control Panel** > **Add or Remove Programs**.
5. Select **Websense Web Security / Websense Web Filter**, and click **Change/ Remove**.

   The Websense uninstaller starts.
6. On the **Remove Components** screen, make sure that only **Filtering Service** and **Network Agent** are selected for removal, and then click **Next**.

> **Note**
> Network Agent must be removed because it should not run on the same machine as ISA Server. After reinstalling Filtering Service (see below), you will install Network Agent on a separate machine. An exception to this case is if ISA Server firewall is not enabled. If ISA Server is running only as a proxy server, Network Agent may be installed on the same machine.

7. Follow the on-screen prompts to complete the removal process.

After Network Agent and Filtering Service are removed, you can install ISA Server. See Microsoft documentation for instructions on installing ISA Server.

After ISA Server is installed, run the Websense installer to reinstall Filtering Service and install the Websense ISAPI Filter plug-in. Then, install Network Agent on a separate machine.

1. On the **Add Components** screen, select **Install additional components on this machine** and then click **Next**
2. On the **Custom Installation** screen, select **Filtering Service** and then click **Next**.
3. On the **Integration Option** screen, select **Integrated with another application or device** and then click **Next**.
4. On the **Select Integration** screen, select **Microsoft Internet Security and Acceleration Server** and then click **Next**.

5. 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.

6. On the **Filtering Feedback** screen, select whether you want Websense software to send feedback to Websense, Inc. to improve accuracy and then click **Next**.

   Choosing to allow feedback to Websense, Inc. helps improve the accuracy of Websense software for all customers. The feedback consists of any URLs that could not be categorized by Websense software. Such uncategorized URLs are evaluated by Websense, Inc. If warranted, they are investigated in more detail and put into an appropriate category. The Websense Master Database is updated with this information. When your Websense software downloads the updated database, it will be able to categorize those URLs and filter them according to the policies you have set.

   Important

   No information about users or your network is collected. The information is only about the visited URLs themselves. Only uncategorized URLs and the frequency of requests to them are collected. Uncategorized intranet URLs are not included in feedback.

   Note

   You can later choose to enable or disable feedback (the feedback mechanism is known as WebCatcher) using the Log Server Configuration utility. For more information, see the Log Server Configuration Help.

7. On the **Pre-Installation Summary** screen, verify the information shown.

   The summary shows the installation path and size, and the components to be installed.

8. Click **Install** to start the installation. An **Installing** progress screen is displayed. Wait for the installation to complete.
9. On the **Installation Complete** screen, click **Done**.
10. If you stopped your antivirus software, start it again.
11. On a separate machine, install Network Agent. Follow the instructions for installing individual components in the *Installation Guide*.

Initial Setup

- If you installed the Websense reporting component (Log Server) on a Windows server, see *Enabling communication with the Log Database*, page 25.
- To use Websense filtering in a network that uses SOCKS or WinSOCK proxy server, see *WinSOCK and SOCKS proxy servers*, page 26, for instructions.
- Additional configuration of the Websense ISAPI Filter is required if you are using non-Web proxy clients with ISA/TMG. These ISA/TMG clients include the Firewall/Forefront TMG Client with proxy server disabled, and SecureNAT clients.

  See *Configuring for ISA/TMG using non-Web-Proxy clients*, page 26, for instructions.
- To configure Websense software to ignore certain traffic based on the user name, host name, or URL, see *Configuring Websense software to ignore specific traffic*, page 28, for instructions.
- If Network Agent was installed, configure Network Agent with the IP addresses of all proxy servers through which computers route their Internet requests. See *Network Configuration* in the TRITON - Web Security Help for instructions.
- If you installed Remote Filtering Server in your Websense deployment, configure ISA/TMG to not monitor (i.e., ignore) the machine on which Remote Filtering Server is installed. If ISA/TMG monitors this machine, it could interfere with remote filtering. See your ISA/TMG documentation for instructions.

Enabling communication with the Log Database

When you install the Websense reporting component, Log Server, ISA/TMG must be configured to permit communication with the Log Database. This **must** be completed before filtering activity can be logged.

The following procedure applies to ISA Server 2006 and Forefront TMG. See Microsoft documentation for assistance with ISA Server 2004.

1. On the ISA/TMG machine, open the ISA Server or Forefront TMG management console (management console).

   To open the management console: **Start** > **Programs** > **Microsoft ISA Server** or **Microsoft Forefront TMG** > **ISA Server Management** or **Forefront TMG Management**.
2. In the left navigation pane, select **Firewall Policy**.
3. On the **Tasks** tab (on the right side of the console), click **Edit System Policy**.

   The **System Policy Editor** dialog box appears.
4. Under **Configuration Groups**, select **Logging** > **Remote Logging (SQL)**.
5. On the **To** tab, click **Add**.
6. Select **Networks** > **Internal**, and then click **Add**.

   You are returned to the System Policy Editor dialog box.

7. On the **General** tab, select **Enable this configuration group**.
8. Click **OK** to accept your changes.

   You are returned to the management console.
9. Click the **Apply** button at the top of the window to save the changes and update the configuration.

WinSOCK and SOCKS proxy servers

Websense software filters HTTP, HTTPS, and FTP requests sent to ISA/TMG, but *cannot* filter traffic tunneled over a SOCKS or WinSOCK proxy server.

The Firewall/Forefront TMG Client replaced these proxy servers after ISA Server 2000. To use Websense filtering in a network that uses a SOCKS or WinSOCK proxy server, you can either:

- Disable the WinSOCK or SOCKS service.
- Use the WinSOCK or SOCKS proxy client to disable the specific protocols that you want Websense software to filter (HTTP, HTTPS, and FTP), then configure browsers on client computers to point to ISA/TMG for each of these protocols.

  For information about disabling a protocol, see the ISA/TMG online help.

Configuring for ISA/TMG using non-Web-Proxy clients

Note

Ensure that TCP/IP stacks are installed on all the client computers if protocols have been disabled on the SOCKS or WinSOCK proxy server, and sent through the normal proxy server for filtering by Websense software.

If you are using non-Web-Proxy clients with ISA Server 2004/2006 or Forefront TMG, additional configuration is required so that Websense software can filter Internet requests correctly. The term non-Web-Proxy clients refers to:

- Firewall/Forefront TMG Client with the proxy server disabled
- SecureNAT clients

Firewall/Forefront TMG Client

If you are using Firewall/Forefront TMG Client with ISA Server 2004/2006 or Forefront TMG, and the proxy server is enabled (default setting), Websense software filters Internet requests normally.

However, if the proxy server is disabled, Websense software cannot filter Internet requests without additional configuration.

Check the Firewall/Forefront TMG Client machine to see if the proxy server is disabled.

1. Open the Firewall/Forefront TMG Client configuration screen, and select the **Web Browser** tab.
2. View the **Enable Web browser automatic configuration** check box.
   - If it is marked, the proxy server is enabled. Websense software requires no additional configuration.
   - If it is cleared, the proxy server is disabled. See *Configuring the ISAPI Filter plug-in*, page 27, for additional configuration steps.

> **Note**
> If the proxy server is disabled, then Websense software filters HTTP only; it will not be able to filter HTTPS.

SecureNAT clients

SecureNAT clients require that you configure the default gateway so that all traffic to the Internet is sent through ISA/TMG. If you need information about configuring and using SecureNAT clients, see your ISA/TMG documentation.

See *Configuring the ISAPI Filter plug-in*, page 27, for additional configuration steps.

Configuring the ISAPI Filter plug-in

If you are using the ISA/TMG Firewall Client with the proxy server disabled, or SecureNAT clients, the ISAPI Filter plug-in must be configured to ignore requests going directly to the ISA/TMG and to filter only those requests going out to the Internet.

> **Note**
> If you are using the ISA Server Firewall Client with the proxy server disabled, then Websense software filters HTTP only; it will not be able to filter HTTPS.

1. On the ISA/TMG machine, create a file called **ignore.txt** in the Windows **system32** directory.
2. Enter the host name or IP address of the ISA/TMG machine in the text file.

   Host names must be entered in ALL CAPS. Entries that are not in all capital letters are not used.
3. If the ISA/TMG machine hosts multiple Web sites, add the names of all the Web sites being hosted. For example: **webmail.rcd.com**.

   If only one Web site is hosted, do not add it to this file.
4. Restart the ISA/TMG machine.

Configuring Websense software to ignore specific traffic

You can configure the ISAPI Filter plug-in to bypass both filtering and logging for certain traffic, based on the user name, host name, or URL. This may be used for a small group of Web sites or users, or for machines in a complex proxy-array or proxy-chaining configuration.

To prevent filtering and logging of this traffic, add the user names, host names, and URLs that you do not want Websense software to filter to the **isa_ignore.txt** file.

1. On the ISA/TMG machine, open the **isa_ignore.txt** file in a text editor. This file is located in the Windows **system32** directory.

> **Important**
> The default **isa_ignore.txt** file installed during a Websense upgrade or installation contains the following URL:
>
> `url=http://ms_proxy_intra_array_auth_query/`
>
> Do **not** delete this URL. It is used by ISA/TMG in a CARP array for communication. This URL must be ignored by Websense software to allow filtering and logging to work properly when multiple ISA/TMG instances are deployed in an array.

2. Enter each user name, host name, or URL that you want Websense software to ignore. Enter each item on its own line in the file, using the formats below.

> **Important**
> You must enter each user name, host name, or URL in the exact same format that ISA Server passes it to Filtering Service.

- **User name**: Enter the name of a user whose Internet requests should not be filtered or logged by Websense software:

  `username=``<user_name>`

  Examples:

  `username=jsmith`
  `username=domain1/jsmith`

- **Host name**: Enter a destination host name that Websense software should not filter or log user visits to:

  `hostname=``<host_name>`

  Example:

  `hostname=yahoo.com`

- **URL**: Enter a URL that Websense software should not filter or log user visits to:

  ```
  url=<URL>
  ```

  Example:

  ```
  url=http://mail.yahoo.com/
  url=mail.yahoo.com/
  ```

> **Note**
> To assure that the correct format is available for all situations, it is recommended that you enter the same name in all available configurations. For example, make 2 entries for user name: one with and one without the domain. Make 2 entries for URL: one with and one without the protocol.

3. Restart the ISA/TMG service.

Client computer configuration

Internet browsers on client computers should be configured to use ISA/TMG to handle HTTP, HTTPS, and FTP requests.

An exception to this configuration is browsers in an ISA/TMG environment using Firewall/Forefront TMG Clients or SecureNAT. These browsers must point to the same port, 8080, that ISA/TMG uses for each protocol.

See the browser online help for configuration instructions.

Firewall configuration

To prevent users from circumventing Websense filtering, configure your firewall or Internet router to allow outbound HTTP, HTTPS, and FTP requests only from ISA Server.

Contact your router or firewall vendor for information about configuring access lists on the router or firewall.

> **Important**
> If Internet connectivity of Websense software requires authentication through a proxy server or firewall for HTTP traffic, the proxy server or firewall must be configured to accept clear text or basic authentication to enable the Websense Master Database download.

Migrating between Microsoft integration products

You can migrate from Microsoft Proxy Server to ISA Server and keep your Websense configuration settings. This must be done prior to installing or upgrading Websense software. This version of Websense software does not support an integration with Microsoft Proxy Server.

- If Websense software is not already installed:
  - Complete the installation of ISA Server before beginning the Websense installation.
  - Install Websense software following the instructions in the Websense *Installation Guide*, plus the instructions in this supplement. See *Installation*, page 7.
- If a previous version of Websense software is installed:
  - Follow the migration procedures in the *Installation Guide Supplement for use with Microsoft ISA Server* for the installed version.
  - Follow the upgrade procedures for the new version of Websense software.

2 Authentication

Authentication is the process of identifying an individual within a network who has an account in a directory service. Depending on the authentication method selected, ISA/TMG can obtain user identification and send it to Websense Filtering Service with the Internet request. Filtering Service can filter requests based on policies assigned to directory clients (users, groups, and domains [OUs] defined in a supported directory service).

> **Note**
> In any environment, Websense software can filter based on computer (individual IP address) or network (IP address range) policies.

To filter Internet access for directory clients, Websense software must be able to identify the user making the request. This requires one or more of the following:

- Enable an authentication method within ISA/TMG that sends user information to Websense software.
- Install a Websense transparent identification agent (DC Agent, Logon Agent, eDirectory Agent, or RADIUS Agent) to identify users, if user information is not supplied by ISA/TMG.

  See the Websense *Deployment Guide* and the *Transparent Identification of Users* technical paper for more information.
- Enable manual authentication within Websense software. Users who cannot be identified by other means are prompted for logon information when they open a browser.

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

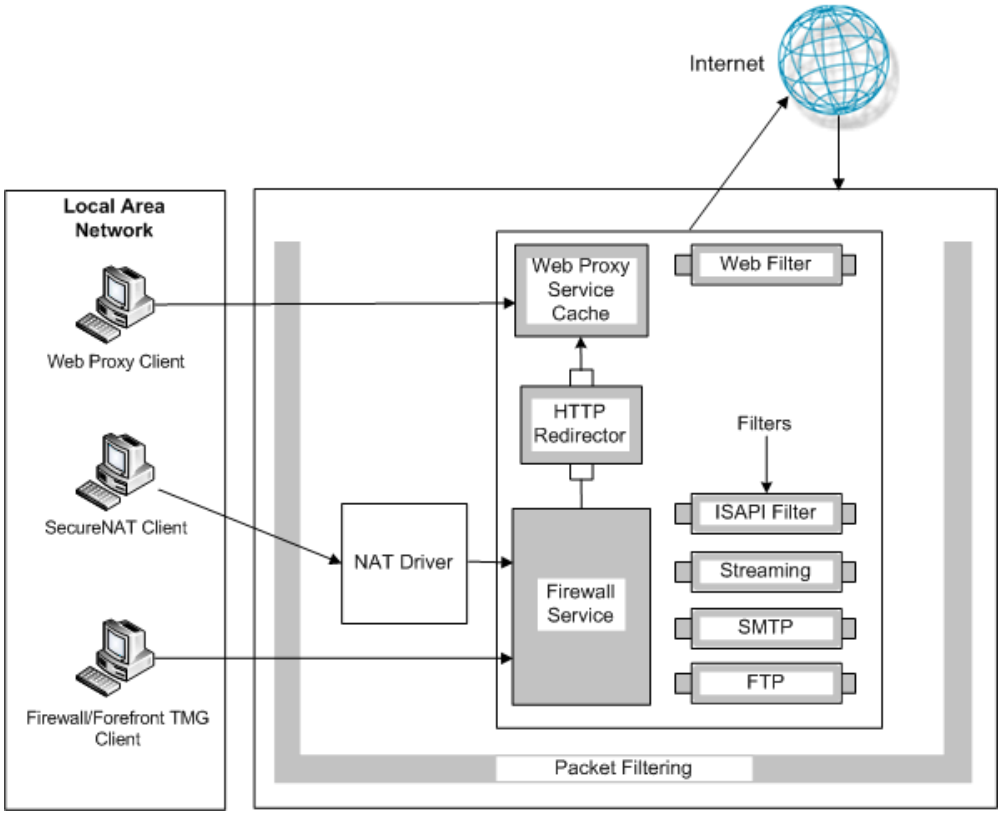
This chapter discusses authentication methods available within ISA/TMG. It also provides instructions for enabling an authentication method that identifies users transparently and sends the information to Websense software along with the Internet request.

ISA/TMG clients

These ISA/TMG clients are supported:

- Firewall/Forefront TMG
- SecureNAT
- Web Proxy

The term **clients** in this environment refers to computers or applications that run on computers and rely on a server to perform some operations. In the following diagram of ISA/TMG Firewall architecture, the relationship between ISA/TMG and the Firewall/Forefront TMG, SecureNAT, and Web Proxy clients is shown.



ISA/TMG Firewall Architecture

Each type of client can be configured so that Websense software can obtain user identification and filter Internet requests based on user and group policies.

Firewall/Forefront TMG and SecureNAT clients

Firewall/Forefront TMG and SecureNAT clients cannot identify users transparently without special settings. These clients require a Websense transparent identification agent to authenticate users. To enable user-based filtering policies with these clients, select one of these options:

- Configure computer browsers to access the Internet through ISA/TMG. This configuration allows Firewall/Forefront TMG and SecureNAT clients to also work as Web Proxy clients.

  If you choose this option, see *Web Proxy clients* for more information.
- If you are using a Windows-based directory service, disable all authentication methods within ISA/TMG and use Websense transparent identification. This method allows Websense Filtering Service to obtain user identification from the network's domain controllers or directory services.

  See *Transparent identification*, page 36, for more information.
- Enable Websense software to prompt users for authentication (manual authentication). This method allows Websense software to obtain the user information it needs if neither the ISA/TMG nor a Websense transparent identification agent provides the information.

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

Web Proxy clients

After the browser is configured to use ISA/TMG as a proxy server, Web Proxy clients send Internet requests directly to ISA/TMG. You can assign individual user or group policies with one of the following methods.

- If your network uses only Microsoft Internet Explorer® browsers, version 5.0 or later, you can enable Integrated Windows Authentication within ISA/TMG to identify users transparently.
- If you are using a Windows-based directory service with various browsers, you can identify users transparently by disabling all authentication methods within ISA/TMG and implementing Websense transparent identification.

  See *Transparent identification*, page 36, for more information.
- If the network uses a mixture of browsers, you can enable one or more of ISA/TMG's authentication methods. Some of these methods may require users to authenticate manually for certain older browsers.

  See *Authentication Methods*, page 34, for more information.
- Enable Websense software to prompt users for authentication (manual authentication). This method allows Websense software to obtain the user information it needs if neither ISA/TMG nor a Websense transparent identification agent provides the information.

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

Authentication Methods

ISA/TMG provides four methods of authentication:

- *Basic authentication*
- *Digest authentication*
- *Integrated Windows authentication*
- *Client Certificate authentication*

Microsoft Internet Explorer, version 5.0 and later, supports all of these authentication methods. Other Web browsers may support only the Basic authentication method. By default, ISA/TMG has Integrated Windows authentication enabled.

You can configure both incoming and outgoing request properties within ISA/TMG. Client Web browsers must be able to use at least one of the authentication methods that you specify in an array's incoming and outgoing Web request dialog boxes. Without this authentication, the client cannot access the requested Internet site.

When no authentication method is enabled in ISA/TMG, it cannot receive any information about who is making the Internet request. As a result, Websense software does not receive user information from ISA/TMG. When this problem occurs, you can:

- Filter with computer and network policies.
- Enable Websense manual authentication to permit user-based filtering.

  See *Manual Authentication* in the TRITON - Web Security Help for more information.
- Enable Websense transparent identification to permit user-based filtering.

  See *Transparent identification*, page 36, for more information.

Basic authentication

Basic authentication prompts users to authenticate (log on) each time they open a browser. This authentication allows ISA/TMG to obtain user identification, regardless of the browser, and send the information to Websense software, which filters Internet requests based on individual user and group policies.

If Basic authentication is enabled in combination with Integrated Windows authentication:

- Users with Microsoft Internet Explorer browsers are transparently identified.
- Users with other browsers are prompted to for a user name and password.

Digest authentication

Digest authentication is a secure authentication method used in 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 ISA/TMG. The user can authenticate to ISA/TMG without the user name and password being intercepted.

User information is sent to Websense software, which then filters Internet requests based on individual user and group policies.

If Digest authentication is enabled in combination with Integrated Windows authentication:

- Users with Microsoft Internet Explorer browsers are transparently identified.
- Users with other browsers are prompted for a user name and password.

Integrated Windows authentication

Integrated Windows authentication provides secure authentication. With this authentication enabled, ISA/TMG 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.

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 for a user name and password.

Note

To transparently identify all users in a mixed browser environment, you can disable Basic or Digest authentication and use Websense transparent identification (see *Transparent identification*, page 36) in conjunction with Integrated Windows authentication.

Client Certificate authentication

Client Certificate authentication identifies users requesting information about a Web site. If Client Certificate is used, ISA/TMG requests the certificate and verifies that it belongs to a client that is permitted access, before allowing the Internet request.

Note

To use Websense transparent identification, you must disable Client Certificate authentication.

Before changing authentication methods, consider the impact of the change on other ISA/TMG functions.

For more information about ISA/TMG authentication and how to configure these authentication methods, see Microsoft's documentation.

Transparent identification

Websense transparent identification allows Websense software to filter Internet requests from users identified in a directory service, without prompting them to authenticate manually. If the authentication method enabled within ISA/TMG does not send user information to Filtering Service, you can use a Websense transparent identification agent to identify users.

For example, if ISA/TMG is configured to obtain user identification from the browser, and you want to use Network Agent to filter protocols by user or group name, use a Websense transparent identification agent to identify users for protocol traffic.

Install and configure Websense transparent identification agents to transparently identify users from a directory service. DC Agent, Logon Agent, eDirectory Agent, or RADIUS Agent can be installed on the same machine as Filtering Service, or on a different machine. See the *Deployment Guide* more information.

Websense also offers secure manual authentication with Secure Sockets Layer (SSL) encryption to protect user names and passwords being transmitted between client computers and Filtering Service. By default, secure manual authentication is disabled. See *Secure Manual Authentication* in the TRITON - Web Security Help for more information and instructions on activating this feature.

After Filtering Service is configured to communicate with a transparent identification agent, user information is obtained from a supported directory service and sent to Filtering Service. When Filtering Service receives the IP address of a computer making an Internet request, the address is matched with the corresponding user name provided by the transparent identification agent.

See the *Installation Guide* for instructions on installing individual Websense components. See *User Identification* in the TRITON - Web Security Help for information about configuring transparent identification agents.

A Troubleshooting

SecureNAT clients are not being filtered

If you are using non-Web proxy clients (for example, Firewall Client with proxy server disabled, or SecureNAT clients) with ISA/TMG, additional configuration of the Websense ISAPI filter is required. Follow the instructions in *Configuring for ISA/TMG using non-Web-Proxy clients*, page 26.

No filtering occurs after the ISAPI Filter plug-in is installed

Users are still not being filtered after the Websense ISAPI Filter plug-in has been installed on the machine running the ISA Server.

- If the ISAPI Filter plug-in is the only Websense component installed on the integration machine, the plug-in may not be communicating with the Websense filtering components installed on other machines. Verify that the ISAPI Filter plug-in is pointing to the correct IP address and port for the machine running Filtering Service.
  1. Go to the Windows **system32** directory and open the **wsMSP.ini** file.
  2. Under **[initSection]**, check the **EIMServerIP** and **EIMServerPort** parameters (these are the Filtering Service IP address and port, respectively). For example:

     ```
     [initSection]
     EIMServerIP=10.203.136.36
     EIMServerPort=15868
     ```

     The default port number is 15868.
- If other Websense components are installed on the same machine as ISA Server and the plug-in, try restarting the Microsoft Firewall service.

Verify an ISA firewall rule allows access to Filtering Service on the Filter port (default 15868).

Note

Filtering Service may be automatically configured to use a port other than the default 15868. When Filtering Service is installed, the installation program checks whether the default port is already in use on that machine. If it is already in use, the port number is automatically incremented until a free port is found.

To find the port used by Filtering Service for communication with integration products, check the **eimserver.ini** file—located in C:\Program Files\Websense\bin (Windows) or /opt/Websense/bin (Linux)—on the Filtering Service machine. Look for the **WebsenseServerPort** value.

Important: Do not modify the **eimserver.ini** file.

- If some Websense components are installed on the ISA Server machine, while others are installed on a separate machine, be sure the proper ports are open for communication.

  Refer to the help in the ISA Server Management console for instructions on setting a port.

  Refer to the Websense Knowledge Base, kb.websense.com, for a list of default port numbers. Search for the exact phrase **default port numbers**.

Index

Numerics

64-bit Windows Server 2008. See Windows Server 2008 (x64)

A

array configuration
  Websense software deployment, 6
authentication
  configuration tasks, 31
  definition of, 31
  Forefront TMG
    basic, 34
    client certificate, 35
    digest, 34
    Forefront TMG and SecureNAT clients, 33
    Integrated Windows Authentication, 35
    methods, 34
    types, 32
    Web proxy clients, 33
  ISA Server
    basic, 34
    client certificate, 35
    digest, 34
    firewall and SecureNAT clients, 33
    Integrated Windows Authentication, 35
    methods, 34
    types, 32
    Web proxy clients, 33

B

basic authentication, 29
block page, 6

C

CARP array
  URL for internal communications, 28
clear text, 29
clients supported, 7
computers
  configuration, 29
Control Service, 6, 7, 12
  communication port (55933), 8, 12
converting stand-alone deployment to integrated system, 22
  ISA Server/Forefront TMG not on Websense machine, 20

D

DC Agent
  and transparent identification, 36

E

eimserver.ini, 12
  Filtering Service integration communication port, 10, 12
  WebsenseServerPort, 10, 12
excluding specified traffic, 28

F

Filtering Service, 5, 8
  integration communication port (15868), 10, 12
Firewall Client, 7
Forefront TMG
  array configuration, 28
  authentication
    basic, 34
    client certificate, 35
    digest, 34
    firewall and SecureNAT clients, 33
    Integrated Windows Authentication, 35
    methods, 34
    Web proxy clients, 33
  client computer configuration, 29
  clients, 7
  Forefront TMG Client, 26
  lockdown mode, 13, 18
  supported versions, 7
  Windows Server 2008 (x64) only, 6
Forefront TMG 2010, 7
Forefront TMG Client, 7
Forefront TMG plug-in installer, 8, 12

I

ignoring specified traffic, 28
ISA Server
  array configuration, 28
  authentication
    basic, 34
    client certificate, 35
    digest, 34
    firewall and SecureNAT clients, 33
    Integrated Windows Authentication, 35
    methods, 34
    types, 32
    Web proxy clients, 33
  client computer configuration, 29
  clients, 7
  Firewall Client, 26
  installing Websense software on same machine, 14–16
  lockdown mode, 11, 18
  supported versions, 7
  Windows Server 2008, 16
ISA Server 2006, 7
isa_ignore.txt file, 28
ISAPI Filter plug-in, 5
  removing, 17

L

lockdown mode
  Forefront TMG, 13, 18
  ISA Server, 11, 18

M

Microsoft Firewall Server
  starting, 18
  stopping, 18
Microsoft Firewall Service, 10, 11
  starting, 11
  stopping, 10
Microsoft Forefront TMG Firewall service, 11, 13
  starting, 13, 18
  stopping, 13, 18
Microsoft Proxy Server
  migrating to ISA Server, 30
  not supported, 17, 30

N

Network Agent, 6
  do not install on ISA Server machine, 6, 14
Network Traffic Detector, 16

P

plug-in
  ISAPI Filter, 5
plug-in installer
  Forefront TMG, 8, 12
  ISA Server, 8
port 15868, 10, 12
port 55933, 8, 12

R

removing the ISAPI Filter plug-in, 17

S

SecureNAT Client, 26
SecureNAT client, 7
setup
  client computer configuration, 29
SOCKS proxy servers, 26
stand-alone deployment
  converting to integrated system, 19

T

transparent identification, 36

U

upgrading
  stand-alone deployment to integrated system, 19

V

versions supported, 7

W

Web Proxy client, 7
Windows Server 2008 (x64)
  not supported by Websense software, 7
  only for Forefront TMG, 6
WinSOCK proxy servers, 26
WsISAFilter, 14
  verifying installation on Forefront TMG, 14
  verifying installation on ISA Server, 11