Websense Web Security Gateway Anywhere v7.5: Hybrid Web Tips

Topic 45011/ Updated: 17-June-2010

Applies To:	Websense Web Security Gateway Anywhere 7.5

Setting up hybrid filtering for branch offices

Topic 45012 / Updated: 17-June-2010

Applies To:	Websense Web Security Gateway Anywhere 7.5

Problem description

I have several branch offices that I'd like to set up with hybrid filtering. How do I do this?

Resolution

Websense Web Security Gateway Anywhere offers a flexible, comprehensive Web security solution that lets you combine on-premises and hybrid (in-the-cloud) filtering as needed to manage Internet activity for your organization.

You decide which method to use for which users. For example, use our robust on-premises Web filtering for your corporate office or main campus, and filter regional

offices or satellite locations through our hybrid service. Hybrid filtering is also useful for users who are off-network, such as telecommuters and those who travel for business.

This article explains how to set up your branch or satellite offices for hybrid filtering for lower total cost of ownership.

To set up hybrid filtering:

1. *Activate your hybrid filtering account*
2. *Define the locations filtered by the hybrid service*
3. *Specify sites not filtered by the hybrid service*
4. *Configure user access to hybrid filtering*
5. *Send user and group data to the hybrid service*

Activate your hybrid filtering account

Before you can configure the hybrid service to start filtering locations, you must activate your hybrid account. This creates a connection between the on-premises and hybrid portions of Websense Web Security Gateway Anywhere.

Use the Hybrid Filtering section of the **Settings > General > Account** page to provide a contact email address and country for your Websense filtering administrators.

The email address is typically a group alias monitored by the group responsible for managing your Websense software. It is very important email sent to this account be received and acted upon promptly.

Define the locations filtered by the hybrid service

Select **Settings > Hybrid Configuration > Filtered Locations** to review, add, or edit information about the locations filtered by the hybrid portion of your Websense software.

A **filtered location** is the IP address, IP address range, or subnet from which browsers connecting to the hybrid service appear to be originating. Because the hybrid service is hosted outside your network, these must be external addresses, visible from the Internet. Filtered locations are:

- Public-facing IP addresses for offices filtered by the hybrid service
- Often the external address of your Network Address Translation (NAT) firewall
- Likely to be a branch office, remote site, or satellite campus

Filtered locations are NOT:

- IP addresses of individual client machines
- The IP address of any Content Gateway machine used by the on-premises portion of your Websense software

Each location that you define appears in a table that combines a name and description with technical configuration details, including the time zone used for policy enforcement, the type of location (single IP address, IP address range, or subnet), and the actual external IP address or addresses from which requests originate.

To edit an existing entry, click the location **Name**, and then see *Editing filtered locations* in Websense Manager Help.

To define a new location, click **Add,** and then see *Adding filtered locations* in Websense Manager Help.

To remove a location, mark the check box next to the location name, and then click **Delete**.

If you have added or edited a location entry, click **OK** to cache your changes. Changes are not implemented until you click **Save All**.

Specify sites not filtered by the hybrid service

Select **Settings > Hybrid Configuration > Unfiltered Destinations** to review, add, or edit information about target sites to which you want to grant users unfiltered access. Users can access these sites directly, without sending the request to the hybrid service. Typical unfiltered destinations include organizational Web mail sites, internal IP addresses, and Microsoft update sites.

Tip

As a best practice, add your organization's Web mail address as an unfiltered destination.

Destinations listed here are added to the Proxy Auto-Configuration (PAC) file that defines how filtered users' browsers connect to the hybrid service. By default, the PAC file excludes all non-routable and multicast IP address ranges from filtering. Therefore, if you are using private IP address ranges defined in RFC 1918 or RFC 3330, you need not enter them here.

Each unfiltered destination that you define appears in a table that combines a name and description with technical configuration details, including how the destination is defined (as an IP address, domain, or subnet), and the actual IP address, domain, or subnet that users can access directly.

To edit an existing entry, click the location **Name**, and then see *Editing unfiltered destinations* in Websense Manager Help.

To define a new location, click **Add**, and then see *Adding unfiltered destinations* in Websense Manager Help.

To remove an unfiltered destination, mark the check box next to the destination name, and then click **Delete**.

If you have added or edited an unfiltered destination entry, click **OK** to cache your changes. Changes are not implemented until you click **Save All**.

Configure user access to hybrid filtering

To use hybrid filtering, you must configure how users connect to and are identified and filtered by the hybrid service. To do so:

1. Select **Settings > Hybrid Configuration > User Access**.
2. Select the **Common Options** tab.

Use the **Availability** section to specify whether all Internet requests should be permitted or blocked when the hybrid service is unable to access policy information for your organization.

Under **Time Zone**, use the drop-down list to select a default time zone to use when applying policies to:

Users connecting to the hybrid service from an IP address that is not part of an existing filtered location. The default time zone is used, for example, by roaming users, or for other users that self-register with the hybrid service.

Whenever time zone information is not available for a filtered location.

Use the **User Identification** section to configure how users are identified by the hybrid service, and to test and configure users' connections to the service.

1. Indicate how the hybrid service should identify users requesting Internet access (see Identifying hybrid filtering users in Manager Help for more information):
   - Mark **Use NTLM to identify users when possible** to use directory information gathered by Websense Directory Agent to identify users transparently, if possible. This is used only for users connecting from a filtered location.

     If Directory Agent is sending data to the hybrid service, using NTLM to identify users is recommended.
   - Mark **Prompt users not identified via NTLM for logon information** to have users who could not be identified via another means see a logon prompt when accessing the Internet.

     Basic authentication is used to identify users who receive a logon prompt. Advise end users not to use the same password for hybrid filtering that they use to log on to the network.

   When both options are selected, the hybrid service first attempts to use NTLM to identify the user, and then, if identification fails, provides a logon prompt.

   When NTLM is used to identify users, do not use self-registration (configured on the Off-Site Users tab under Registered Domains).
2. Specify whether or not a Welcome page is displayed when users who have not been identified via NTLM open a browser to connect to the Internet. The Welcome page:
   - Provides a simple selection of common search engines to get the user started
   - Is used mainly by those who connect to the hybrid service from outside a filtered location (while working from home or traveling, for example)

If you choose to display the Welcome page, indicate whether or not the page should be sent via HTTPS when users request a secure site.

3. When you are finished, click **OK** to cache your changes. Changes are not implemented until you click **Save All**.

Once you have set up hybrid filtering and configured user browsers to access the PAC file, you can use the links provided under **Verify End User Configuration** to make sure that end user machines have Internet access and are correctly configured to connect to the hybrid service.

If your hybrid filtering account has not been verified (which may mean that no email address has been entered on the **Settings > General > Account** page), the URLs are not displayed.

Send user and group data to the hybrid service

If your organization uses a supported, LDAP-based directory service?Windows Active Directory (Native Mode) or Novell eDirectory?you can collect user and group data and send it to the hybrid service.

When hybrid filtering is configured properly, the information from the Directory Agent can be used to apply user- and group-based filtering.

If your organization uses Windows NT Directory, Windows Active Directory (Mixed Mode), or Sun Java System directory, user and group data cannot be collected and sent to the hybrid service.

The process is similar to setting up user service for group-based policies. For more information see *Send user and group data to the hybrid service* in Websense Manager Help.

What is a PAC file?

Topic 45013/ Updated: 17-June-2010

Applies To:	Websense Web Security Gateway Anywhere 7.5

A PAC (Proxy Auto-Configuration) file is a JavaScript function definition that a browser calls to determine how to handle requests. The PAC file used to enable hybrid filtering contains a number of global settings and allows you to configure sites (for example, intranet sites or organizational Web mail) that users can access directly, without sending the request to the hybrid service.

Filtering users outside your network

Topic 45014/ Updated: 17-June-2010

Applies To:	Websense Web Security Gateway Anywhere 7.5

Problem description

I have users who frequently work outside of the network, whether travelling or telecommuting. How can I protect these users' machines from Web threats?

Resolution

In addition to filtering users inside your organization's network, Websense Web security solutions provide options for filtering users when they are outside the network:

- **Hybrid filtering:** If you have Websense Security Gateway Anywhere, you can use hybrid filtering to monitor Internet activity for users outside the network, regardless of how they are filtered when they are in the network. Hybrid filtering regulates activity through browser settings (a PAC file).

  Hybrid filtering is available only with Websense Web Security Gateway Anywhere.

- **Remote filtering software:** You can install remote filtering software to monitor Internet activity for users outside the network. Remote filtering software deployment requires installation of Remote Filtering Client on each client machine. Remote Filtering Client is protected so that it cannot easily be removed by the end-user.

  Remote Filtering Client is included with Websense Web Security Gateway Anywhere subscriptions, and is available as an option for Websense Web Filter, Websense Web Security, and Websense Web Security Gateway customers.

These methods can be used, for example, to filter users who work from home, users who travel using company laptops, or students who use institutional laptops on and off campus.

Synchronizing user and group data with the hybrid service

Topic 45015/ Updated: 17-June-2010

Applies To:	Websense Web Security Gateway Anywhere 7.5

Problem description

I understand that the on-premises portion of Web Security has to send user and group information to the cloud so branch office personnel and off-site users are recognized and my policies are applied.

How do I send information from my directory service to the cloud, and once I do, how do I ensure the data is always in sync?

Resolution

> **Note**
> Websense supports user and group data collection for Windows Active Directory (Native Mode) and Novell eDirectory. If your organization uses Windows NT Directory, Windows Active Directory (Mixed Mode), or Sun Java System directory, user and group data cannot be collected and sent to the hybrid service.

If your organization uses a supported, LDAP-based directory service – Windows Active Directory (Native Mode) or Novell eDirectory – you can collect user and group data and send it to the hybrid service. This is accomplished using two Websense components:

- **Websense Directory Agent** collects user and group information from the directory and collates it for hybrid filtering.
- **Websense Sync Service** (among other functions) transports user and group data provided by Directory Agent to the hybrid service.

When Directory Agent is configured to send data to the hybrid service, hybrid filtering is then able to apply user- and group-based filtering.

The four main steps are:

1. Establish User Service communication with a supported, LDAP-based directory service (such as Microsoft Active Directory in native mode or Novel eDirectory). This is done on the **Settings > General > Directory Services** page in TRITON - Web Security.

   Information you will need:

   - IP address or host name and communication port information for the Active Directory global catalog server(s) or Novell eDirectory server
   - Account name and password for an account with domain administrator privileges
   - A root context for users, groups, and domains (OUs) filtered on-premises components

2. Provide basic information about how users and groups will be filtered by the hybrid service. This is done on the **Settings > Hybrid Configuration > User Access** page.
3. Configure Directory Agent communication with the directory service. This is done on the **Settings > Hybrid Configuration > Shared User Data** page. Note that you must configure User Service to communicate with the directory before configuring Directory Agent.

   Information you will need:

   - A root context for users, groups, and domains (OUs) filtered by the hybrid service.

     This is used when gathering user and group data from the directory. Narrow the context to increase speed and efficiency of both directory search and processing user and group information by the hybrid service. It is best to provide a context that includes only users filtered by the hybrid service.
   - Name or IP address of the Sync Service machine
   - Port used for Sync Service communication (by default, 55832)
4. Schedule communication with hybrid filtering. This is done on the **Settings > Hybrid Configuration > Scheduling** page.

   You must send data at least once a week.

   If you have an urgent update, you have the option to initiate the send process immediately. Note that there may be a short delay between initiating the send process and seeing a change in behavior from hybrid filtering. This time is needed to gather changes from the directory, upload them to the hybrid service, and have them processed by hybrid filtering components.

Most deployments require only one Directory Agent instance. If your deployment requires additional Directory Agent instances, see "Working with hybrid filtering clients" in the TRITON - Web Security Help for important configuration considerations.

For more detailed instructions on synchronizing user and group data with the hybrid service, please see chapter 8 of TRITON - Web Security Help.