

Configuring and Troubleshooting Websense Solutions for Filtering Off-Site Users

Websense Support Webinar August 2010

Support Webinars

Goals And Objective

- Understanding Websense filtering options for off-site users
- Remote Filtering Server and Client Deployment considerations
- Installing and configuring Remote Filtering Server and Client
- Firewall Configuration for Remote Filtering
- Remote filtering software upgrade information and compatibility guidance
- Troubleshooting remote filtering software
- Configuring hybrid filtering of off-site users
- Configuring client browsers to use a PAC file
- Identification methods for off-site users
- Tips for applying hybrid filtering to off-site users

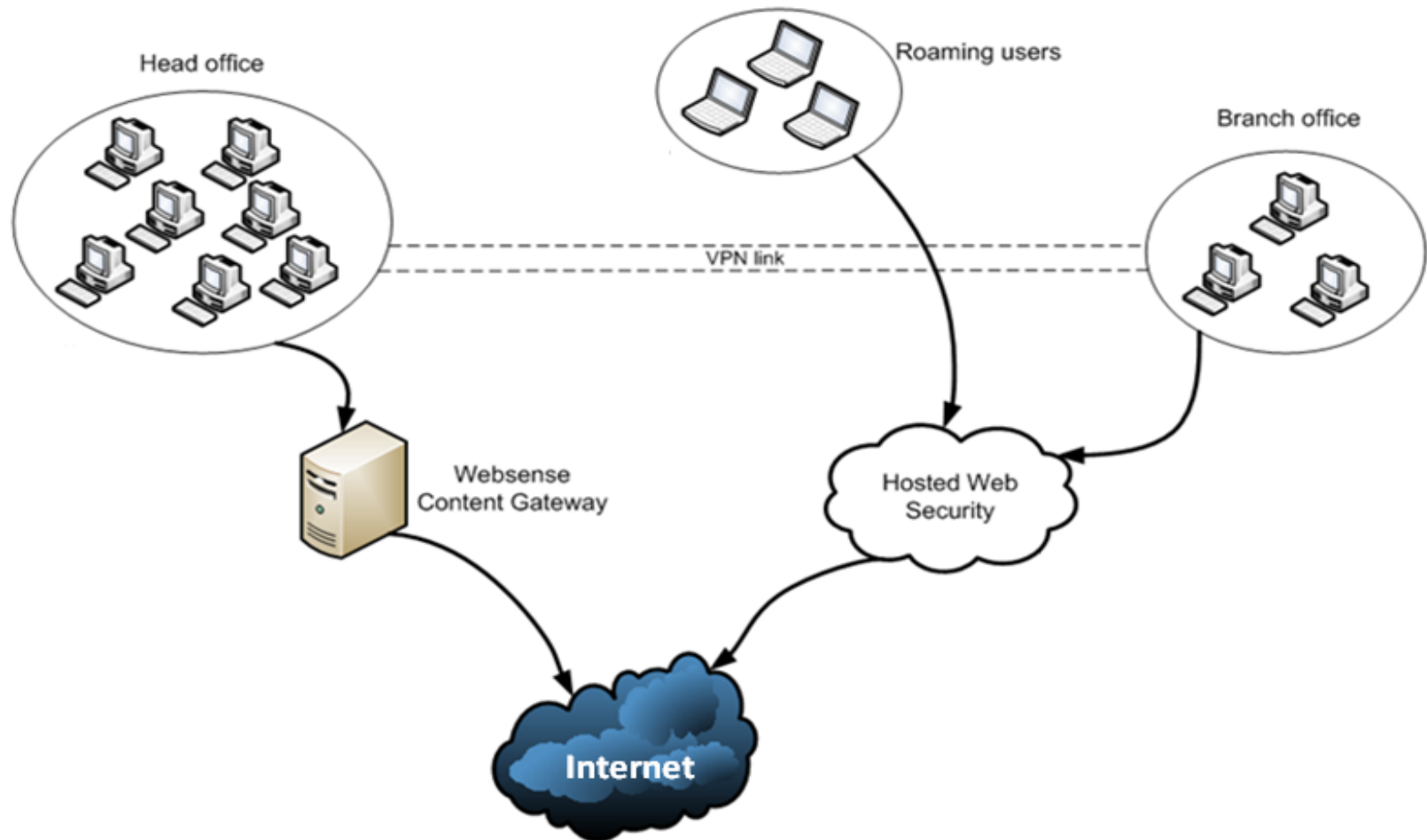


Ravi Desai

- Title: Technical Support Specialist
- Accomplishments:
 - Over 3 years supporting Websense products
- Education / Certifications:
 - B.Eng (Hons) Computer Systems and Networks
 - CCNA
 - WCWSA – Websense Certified Web Security Associate

- Websense Remote Filtering
 - Requires **Remote Filtering Server** that resides inside **your firewall**, and acts as a proxy to Websense Filtering Service
 - Also requires **Remote Filtering Client** that is installed **on each machine that will be filtered when** used outside the network.
 - Client communicates with Remote Filtering Server
 - Communication between RF client and RF server is encrypted.

■ Websense Hybrid Filtering



Remote Filtering Server 7.5 Requirements

- Supported operating systems
- Red Hat Enterprise Linux 5, update 3 (32-bit)
- Red Hat Enterprise Linux 4, update 7 (32-bit)
- Windows Server 2008 SP2 (32-bit x86 only)
- Windows Server 2003 SP2 or R2 SP2

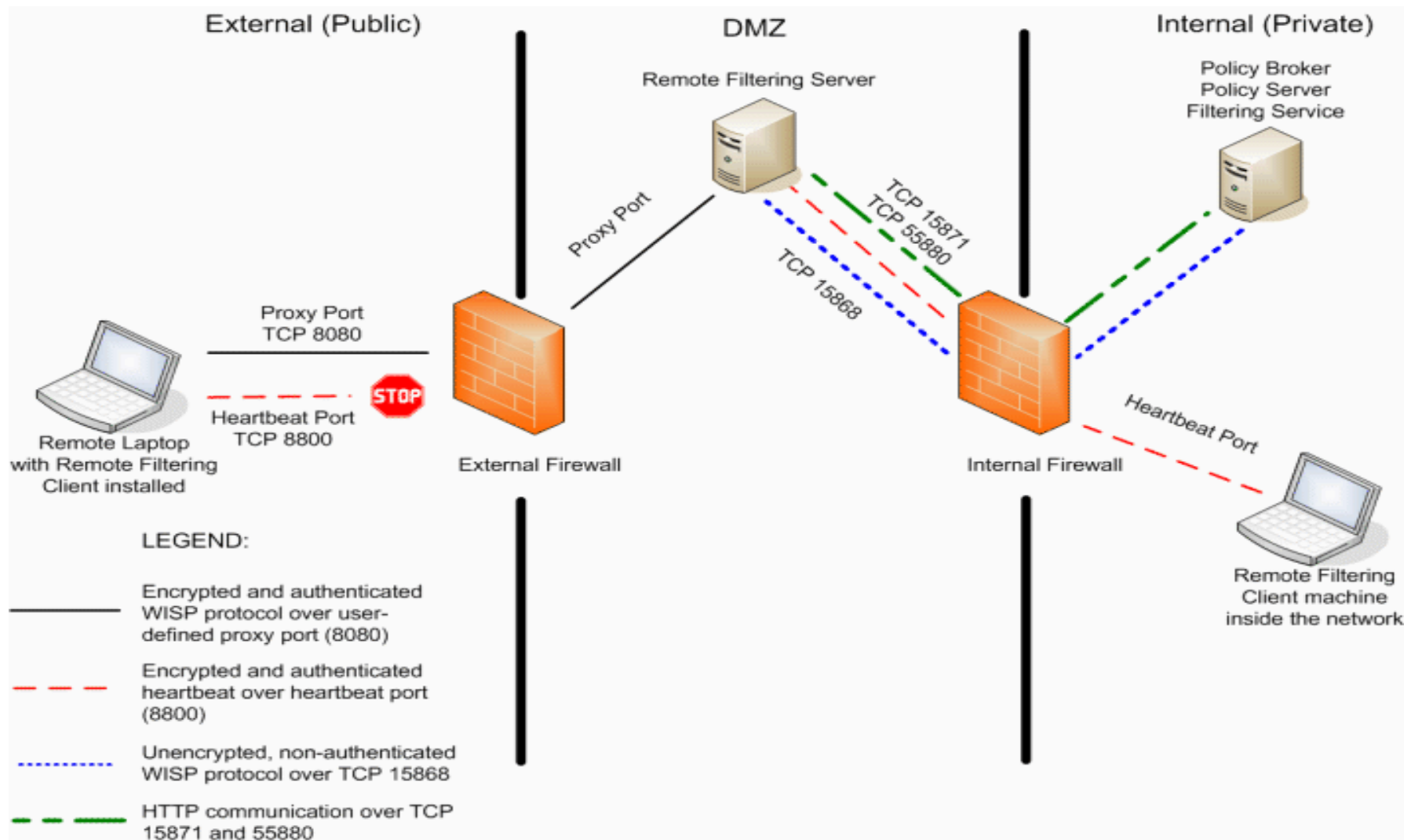
Remote Filtering Client 7.5 is supported only on Microsoft Windows operating systems:

- Windows 7 (32-bit only)
- Windows XP SP3
- Windows Vista SP2

Install the RFS server

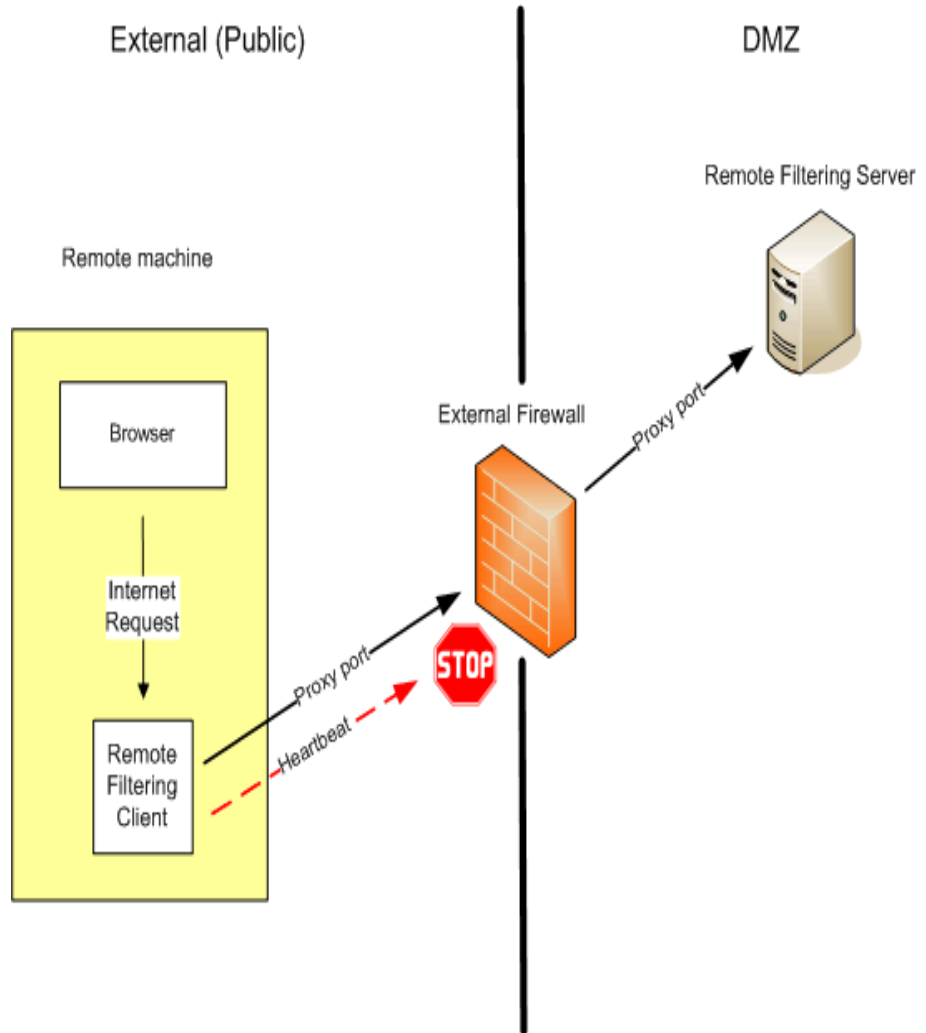
- Inside your organization's outermost network firewall
- In the DMZ outside the firewall that protects the rest of the network
- On its own, dedicated machine
- Do not install Remote Filtering Server on the same machine as Filtering Service or Network Agent.
- Install only one primary Remote Filtering Server for each Filtering Service in your network.
- Secondary and Tertiary RF Servers can be installed to provide failover.
- Remote Filtering clients should be configured to connect to backup servers in case of server failure.

Remote Filtering Server Deployment



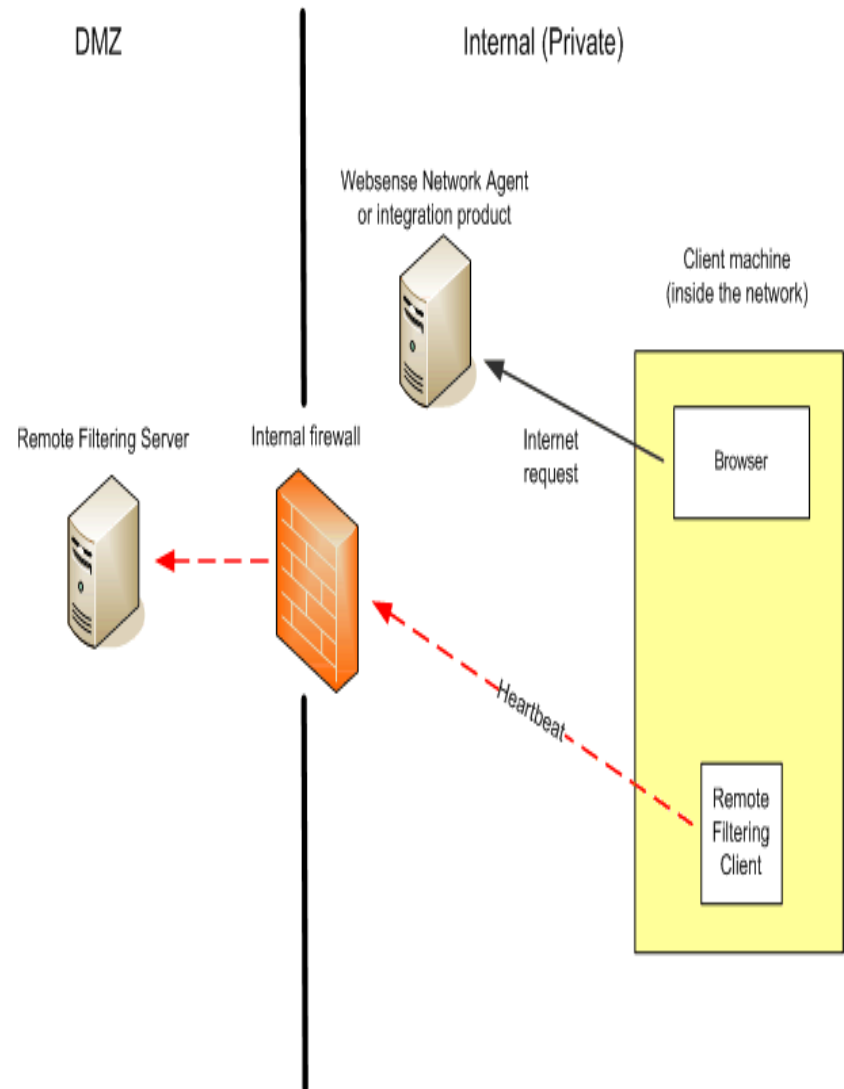
How Remote Filtering works

- Remote Filtering client determines whether client is inside or outside the network
- If client is outside the network, request is sent to Remote Filtering Server
- External Clients attempt to connect to the Remote Filtering Server on the heartbeat port
- This port should be blocked on the external firewall
- Client will then connect using the proxy port to the RF Server in the DMZ.
- RF Server then forwards the request to Filtering service



How Remote Filtering works

- Filtering Service evaluates the request and sends response to RF server.
- If site is blocked, RF client requests and receives the appropriate block page.
- When client is inside the network, the Remote filtering client attempts to connect on heartbeat port.
- This is successful hence client becomes passive and does not query Remote Filtering server.
- These requests are served by the integration partner as normal.



- If a user logs on using cached domain credentials, Filtering service is able to resolve the user name
- If users log on with a local user account then Filtering service cannot resolve the username and Default Policy will be applied
- Manual Authentication can be enabled to prompt users for entering user information. In this situation correct user based policy will be applied
- If user logs on using local account and manual authentication is not enabled Default Policy applies.
- Remote filtering cannot filter based on IP or networks.

Remote Filtering Server Installation

- Run the installer, select Custom install and select Remote Filtering Server.
- Enter Policy Server IP and port number
- Enter External IP of Remote Filtering Server and port number.
- Enter Internal Communication port (HeartBeat)
- Enter and confirm passphrase
- Enter the Filtering service IP. If there is a firewall in between the RF server and Filtering service then enter the translated IP or clear the check box.
- Enter installation path and finish install

Remote Filtering Client Installation

- Run the CPMclient.msi file to begin installation
- Enter the External IP and port number for Primary RF Server
- Enter the Internal IP and port number
- If any Secondary or Tertiary servers are installed enter the details.
- Enter the passphrase.

Remote Filtering Client - InstallShield Wizard

Remote Filtering Server Connection Information

The following information is necessary to allow the Remote Filtering Client deployed on this machine to communicate with the Remote Filtering Server:

Primary Remote Filtering Server:

External IP or Domain Name: [0] Port: [80]

Internal IP or Hostname: [0] Port: [8800]

Secondary Remote Filtering Server (optional):

External IP or Domain Name: [0] Port: [80]

Internal IP or Hostname: [0] Port: [8800]

Tertiary Remote Filtering Server (optional):

External IP or Domain Name: [0] Port: [80]

Internal IP or Hostname: [0] Port: [8800]

Encryption and Authentication

☒ Pass Phrase: [*]

☐ Encrypted Key: [0]

InstallShield

< Back Next > Cancel

- Client can also be deployed using third party tools. Refer to installation document for more information
- Before installing the client on Windows Vista machines, User Account Control (UAC) must be disabled.

- On the External firewall, Remote Filtering proxy port must be opened for clients to communicate from outside with the Remote filtering server
- Heartbeat port should be blocked
- On the Internal Firewall, ports allowing communication between Remote Filtering server and Filtering server and Policy Server must be opened
- 15868, 15871 for filtering and block page
- 55806, 55880 for Policy Server and Broker. Also port 40000 for secure communication.

- Before upgrading the Remote Filtering Server to 7.5 ensure that the Websense Filtering Service has been upgraded
- Remote Filtering Server is backwards compatible with the previous 2 versions of Remote Filtering Client
- So v7.5 Remote Filtering Server is compatible with Remote Filtering Client versions v7.1 and 7.0.x
- We recommend that clients should also be upgraded to the same version to ensure clients can use filtering enhancements available in the latest version

- To upgrade Remote Filtering Server, run the installer and select option to upgrade. Follow on screen instructions
- To upgrade Remote Filtering Client, the following methods can be used
Manual upgrade: Use the v7.5 Remote Filtering Client Pack installer on each client machine to upgrade the Remote Filtering Client. This upgrade method preserves existing Remote Filtering Client configuration settings.

Automatic upgrade with third-party tool: Use the v7.5 Remote Filtering Client Pack and a third-party deployment tool to upgrade the Remote Filtering Client on client computers.

For more information on the above methods please see Remote Filtering document on

http://www.websense.com/content/support/library/web/v75/remote_filtering/remote_filtering.pdf

For Manual procedure, see page 32.

For Automatic upgrade using Third-party deployment tool, see page 33.

- No Remote Filtering clients are being filtered
 - Verify that the correct Passphrase is being used while installing the clients
 - Verify the parameters on Securewispproxy.ini file, this can be located in C:\Program Files\Bin directory on the RF Server
 - Parameters entered on the RF client should match with what is entered in this file.
 - The client parameters can be verified from registry by checking the following registry key
HKLM\Software\WebSense\Desktop Client\Desktop Filtering

Troubleshooting Remote Filtering



```
securewispproxy.ini - Notepad
File Edit Format View Help

[SecureWISPProxy]

# The protocol used to for wrapping WISP requests
raw|http|secure
wispMode=secure

# Proxy Server parameters
ProxyIP=10.3.131.1
ProxyPort=8082
ProxyMaxConnections=10000
ProxyPublicAddress=195.244.17.11

# Time to wait for WISP requests, handshake, etc., seconds
ProxyTimeout=120

# HeartBeat Server Parameters
HeartBeatPort=8800
HeartBeatTimeout=5

# Web-Filtering connection parameters
WebFilterIP=10.3.131.16
WebFilterPort=15868
WebFilterMaxConnections=50

# Time to wait for WISP lookup responses, seconds
WebFilterTimeout=10

# Object Model connection parameters
objectModelIP=10.3.131.16
objectModelPort=55880
objectModelToken=6B9A07396664793EB7D38AC907E7999B6B8951DE6E
4690D0B3FAE1865C00DA60E55A1598DE4186874FF167E9FDAB2186127D
B4A333867CC50725DE64BFC03C698680FAC26F3555EAAC28BCD1678131B
6CE18F5B3A292BE5C0301A6C339F1EEC0C8B8C7C99955E799AE85AF4923
219E7FE09B10E5D06778E3DFB68DE46CDB107A01996E0074566E806AE7A
12D362FBE75B2763E789585B919EE4DEBE4BE19D4CD926F4E341D6157E
objectModelRetryTime=10
objectModelWaitTime=180

# Blockserver connection parameters
BlockServerIP=10.3.131.16
BlockServerPort=15871

# Time to wait for BlockPage responses, seconds
BlockServerTimeout=10

# Trace type to trace All|WISP|BlockPage|HeartBeat
TraceType=none
TraceFile=tracerfile.log
TraceFileSize=1
```

Private Remote Filtering Server IP address, used for internal communication with Filtering Service.

TCP port used by Remote Filtering Clients for the filtering of Web requests.

Public IP Address of the Remote Filtering Server. This is the IP address that Remote Filtering Clients connect to.

TCP port used for internal heartbeat communication between the client and server.

Internal IP address and port of the Filtering Service that handles Remote Filtering requests.

IP address and port of the server that sends block pages to Remote Filtering Clients.

- Remote Filtering Server logs errors in the RFSerrors.log file in the Websense installation directory (C:\Program Files\Websense or /opt/Websense, by default).
- To enable more detailed tracing:
 1. Open the Remote Filtering Server **SecureWispProxy.ini** file
 2. Set **TraceType=All**.
 3. Restart the Remote Filtering Server service or daemon.
 4. A trace file called **traceFile.log** is created in the **Websense installation directory**

- Remote Filtering client trace can also be useful in troubleshooting problems
 1. Open the Windows Registry and navigate to:
HKLM\Software\WebSense\Desktop Client
 2. Add a new string variable and called **Trace Target with a value of 2.**
 3. Restart the machine.
 4. A trace file called trace.log is created in C:\Program Files\WebSense\WDC\Debug, by default.

- Remote Clients do not receive Block page
 - Ensure that the firewall between Remote Filtering Server and the Filtering Service machine is correctly configured. Port 15871 must be allowed on the internal firewall.
 - Make sure Remote Filtering Client is not installed on the Remote Filtering Server machine. This can use up all available connections meaning remote clients cannot connect to RF Server.
- Clients with mobile data cards are not filtered on the default port (80)
 - Select another proxy port (such as 81 or 8082).
 - Modify the **ProxyPort** parameter in the Remote Filtering Server **SecureWispProxy.ini** file to reflect the new port.
 - Install Remote Filtering Client using the new port or modify the registry key related to Proxyport
 - Modify firewall rules to allow the port.

Configuring Hybrid Filtering

General

Account

Linking

Filtering

Database Download

Directory Services

Ligon Directory

Logging

Risk Classes

User Identification

Remote Filtering

Policy Servers

Scanning

Scanning Options

Scanning Exceptions

SSL Decryption Bypass

Hybrid Configuration

Filtered Locations

Unfiltered Destinations

User Access

Shared User Data

Scheduling

Alerts

Network Agent

Reporting

About Account Settings

Enter and view subscription information, change the WebsenseAdministrator password, and indicate whether to submit category and protocol usage data to Websense, Inc.

Subscription Key

Enter your Websense subscription key exactly as you received it. After the first Master Database download, this area displays information about your subscription.

Subscription key:

Key expires: 2011-04-27

Subscribed Users: 25

☐ Block users when subscription expires or is exceeded

Change Password

To change the WebsenseAdministrator password, first provide the current password. Please use a password that is at least 8 characters long, and that contains at least one special character, number, capital letter, and lower case letter.

Current password:

4-255 characters

New password:

Confirm new password:

Category and Protocol Data Collection

Help improve future filtering by sending data about your organization's use of Websense-defined categories and protocols to Websense, Inc.

☐ Send category and protocol data to Websense, Inc.

Hybrid Filtering


Provide a contact email address and country information for your Web security administrators. This is required to connect the on-premises and hybrid portions of your Web security solution.

Contact email address:

Country:

23


Hybrid Filtered Locations


 **TRITON™** UNIFIED SECURITY CENTER


User name: WebsenseAdministrator Role: Super Admin

Web Security Data Security Email Security


Main **Settings** ? Help

 **General**
Account
Linking
Filtering
Database Download
Directory Services
Logon Directory
Logging
Risk Classes
User Identification
Remote Filtering
Policy Servers


 **Scanning**

 **Hybrid Configuration**

Filtered Locations
Unfiltered Destinations
User Access
Shared User Data
Scheduling


 **Alerts**

Filtered Locations

 **About Filtered Locations Settings**
View, add, or edit the external (gateway or firewall) IP addresses, IP address ranges, and subnets used to identify the locations (like branch offices or satellite campuses) filtered by the hybrid service.

<input type="checkbox"/>	Name ▾	Description ▾	Time Zone ▾	Type ▾	Address Details ▾
<input type="checkbox"/>	<u>Europe</u>	Europe Staff	<u>(UTC+00:00)</u>	Range	10.2.2.0-10.2.2.255

Hybrid Unfiltered Destinations

 **TRITON™** UNIFIED SECURITY CENTER

User name: WebsenseAdministrator Role: Super Admin

Web Security

Data Security

Email Security

Main

Settings

Help

General

Account

Linking

Filtering

Database Download

Directory Services

Ligon Directory

Logging

Risk Classes

User Identification

Remote Filtering

Policy Servers

Scanning

Hybrid Configuration

Filtered Locations


Unfiltered Destinations

User Access

Shared User Data

Scheduling

Unfiltered Destinations

 **About Unfiltered Destinations Settings**

Unfiltered destinations are the domains, IP addresses, and subnets of sites that users filtered by the hybrid service can access directly. This could include organizational webmail, or internal sites not accessible from the Internet.

<input type="checkbox"/>	Name ▾	Description ▾	Type ▾	Destination Details ▾
<input type="checkbox"/>	<u>Test</u>	Test	Subnet	10.30.0.2/24

Hybrid User Access Settings

The screenshot displays the Websense Triton Unified Security Center interface. The top navigation bar includes the Websense logo, the product name "TRITON™ UNIFIED SECURITY CENTER", and the user information "User name: WebsenseAdministrator Role: Super A". Below this, there are tabs for "Web Security", "Data Security", and "Email Security". The left sidebar contains a "Main" button and a "Settings" button, along with a tree view of configuration categories: General, Scanning, Hybrid Configuration, User Access, Alerts, Network Agent, and Reporting. The "User Access" category is selected, and its sub-items are "Shared User Data" and "Scheduling". The main content area is titled "User Access" and contains three sub-sections: "Common Options", "Off-Site Users", and "Proxy Auto-Configuration (PAC) File". The "Common Options" section includes a "Proxy Auto-Configuration (PAC) File" field with a URL, an "Availability" section with radio buttons for "Allow users to access the Internet without being filtered" (selected) and "Prevent users from accessing the Internet", and a "Default Policy Time Zone" section with a dropdown menu set to "(UTC+00:00) Greenwich Mean Time : Dublin, Edinburgh, Lisbon, London". The "Off-Site Users" section is currently empty. The "Proxy Auto-Configuration (PAC) File" section includes a "Verify End User Configuration" button and a link to confirm browser configuration.

TRITON™ UNIFIED SECURITY CENTER User name: WebsenseAdministrator Role: Super A

Web Security Data Security Email Security

Main Settings ? Help

General

- Account
- Linking
- Filtering
- Database Download
- Directory Services
- Logon Directory
- Logging
- Risk Classes
- User Identification
- Remote Filtering
- Policy Servers

Scanning

Hybrid Configuration

- Filtered Locations
- Unfiltered Destinations

User Access

- Shared User Data
- Scheduling

Alerts

Network Agent

Reporting

User Access

Common Options Off-Site Users

Proxy Auto-Configuration (PAC) File

Configure browsers on users' machines to use this URL to retrieve hybrid proxy configuration details:
<http://hybrid-web.global.blackspider.com:8082/proxy.pac?p=32skvw6>

Availability

If the hybrid service is not available:

- ☒ Allow users to access the Internet without being filtered
- ☐ Prevent users from accessing the Internet

Default Policy Time Zone

Select the default time zone to use when applying policies.

Time zone: (UTC+00:00) Greenwich Mean Time : Dublin, Edinburgh, Lisbon, London

User Identification

- ☒ Use NTLM to identify users when possible.
- ☒ Prompt users not identified via other means for logon information.

Configure Welcome Page


Specify whether users should be prompted for logon information via a Welcome page displayed in the browser, and how the page should be displayed. If the Welcome page is not used, a browser dialog box prompts users for logon information.

- ☒ Use HTTPS to display the page when users request a secure site; otherwise use HTTP.
- ☐ Always use HTTP to display the page.
- ☐ Do not display a Welcome page.

Verify End User Configuration

Access the link below from an end user's machine to confirm that the browser is configured properly.

Hybrid User Access Settings

 **TRITON™** UNIFIED SECURITY CENTER

User name: WebsenseAdministrator Role: Super A

Web SecurityData SecurityEmail Security

MainSettings

General

Account

Linking

Filtering

Database Download

Directory Services

Logon Directory

Logging

Risk Classes

User Identification

Remote Filtering

Policy Servers

Scanning

Hybrid Configuration

Filtered Locations

Unfiltered Destinations

User Access

Shared User Data

Scheduling

Alerts

Network Agent

Reporting

User Access

Common OptionsOff-Site Users

Filtering Users Outside Your Network

Generate User Passwords

If the hybrid service receives an Internet request that does not originate from locations filtered by the hybrid service, the user is prompted for a password. The password can be automatically generated, or be manually created by the user.

☐ Automatically generate and email passwords for users identified by Directory Agent

Combine Filtering Methods

If some users are filtered by the hybrid service when they are at home or on the road, but otherwise use on-premises filtering, enter a host name that can only be resolved from outside your network.

Host name:

If Internet requests from within your network pass through an explicit proxy, enter the proxy location and port to ensure optimized filtering.

Host name/IP address: Port:


Registered Domains

If you want users to be able to connect to the hybrid service from outside a filtered location, enter the domains belonging to your organization. Users with email addresses in these domains can self-register with the hybrid service.

<input type="checkbox"/>	Domain *	Description *	Include Subdomains *
--------------------------	----------	---------------	----------------------

AddDelete

Hybrid Shared User Data

 **TRITON™** UNIFIED SECURITY CENTER

Web Security

Data Security

Email Security

Main

Settings

User name: WebsenseAdministrator

Role: Super Admin

?

Help

General

Account

Linking

Filtering

Database Download

Directory Services

Ligon Directory

Logging

Risk Classes

User Identification

Remote Filtering

Policy Servers

Scanning

Hybrid Configuration

Filtered Locations

Unfiltered Destinations

User Access

Shared User Data


Scheduling

Alerts

Network Agent

Reporting

Shared User Data > Directory Agent

 **About Directory Agent Settings**

Review and configure the Directory Agent settings that determine how the agent collects directory service (user and group) information for the hybrid service.
Configure directory service types and locations on the Directory Services page.
Note: Directory Agent does not support Windows NT Directory / Active Directory (Mixed Mode) or Sun Java System Directory.

Active Directory (Native Mode)

Click a name or IP address to configure how Directory Agent collects user data from the selected directory server.

Name or IP Address	Port	Context	User Search	Group Search	Filters
<u>10.5.144.100</u>	3268	None	All levels	All levels	None

Go to the [Directory Services](#) page to change a directory server name or IP address.

Synchronize User Data

Provide the name or IP address of the Websense Sync Service machine and the port used to communicate with the hybrid service.

Name or IP address: Port:

Hybrid Scheduling

The screenshot shows the Websense TRITON Unified Security Center interface. The top navigation bar includes the Websense logo, the product name 'TRITON™ UNIFIED SECURITY CENTER', and user information: 'User name: WebsenseAdministrator' and 'Role: Super Admin'. Below this is a secondary navigation bar with tabs for 'Web Security', 'Data Security', and 'Email Security'. The 'Web Security' tab is active, and within it, the 'Settings' sub-tab is selected. A left-hand sidebar contains a tree view of settings categories: General, Scanning, Hybrid Configuration, Alerts, Network Agent, and Reporting. The 'Hybrid Configuration' category is expanded, and the 'Scheduling' sub-category is selected. The main content area displays the 'Scheduling' settings page. It features an 'About Scheduling Settings' information box, a 'Send User Data' section with checkboxes for days of the week and a time range, a 'Send Update Now' button, and a 'Collect and Retrieve Reporting Data' section with a checkbox and a frequency dropdown. At the bottom right, there are 'OK' and 'Cancel' buttons.

websense TRITON™ UNIFIED SECURITY CENTER User name: WebsenseAdministrator Role: Super Admin

Web Security Data Security Email Security

Main Settings

General

- Account
- Linking
- Filtering
- Database Download
- Directory Services
- Logon Directory
- Logging
- Risk Classes
- User Identification
- Remote Filtering
- Policy Servers

Scanning

Hybrid Configuration

- Filtered Locations
- Unfiltered Destinations
- User Access
- Shared User Data
- Scheduling**

Alerts

Network Agent

Reporting

Scheduling

About Scheduling Settings
Specify how frequently directory data is sent to, and how often reporting data is retrieved from, the hybrid service. Policy data is collected when you click Save All and sent to the hybrid service every 15 minutes.

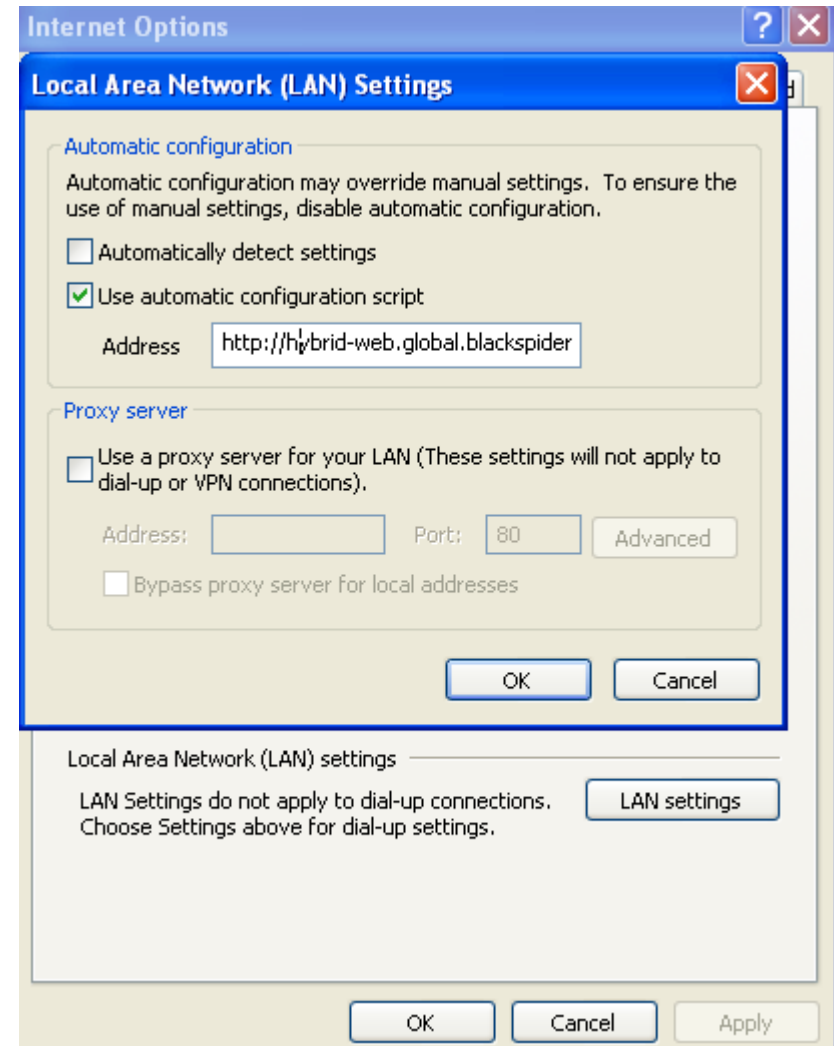
Send User Data
Specify how often new user and group data is sent to the hybrid service. Data must be sent at least once a week.
Send on: ☒ Su ☒ M ☒ Tu ☒ W ☒ Th ☒ F ☒ Sa
Between: 21:00 and 8:00

Send Update Now
If you do not want to wait for the next scheduled update, you can send user and group data to the hybrid service now. Only changes to directory data are sent.

Collect and Retrieve Reporting Data
Specify whether reporting data is collected by the hybrid service, and if so, how often the data is retrieved. A communication port must be configured on the Logging page.
☒ Have the hybrid service collect reporting data for the clients it filters
Retrieve reporting data every: 15 minutes

PAC file configuration

- Client browsers need to be configured with the PAC file URL found on the Hybrid Configuration options on the manager.
- Can be configured manually from Internet Options->Connections->LAN settings
- Configuration can also be done via GPO



- If users are coming from a filtered location they will be identified via NTLM.
- If hybrid service receives an internet request from an unfiltered location users will be prompted for a password.
- The password can be automatically generated or manually created by the user by clicking on forgot password option.
- Authentication for roaming users supports basic authentication method.

- Make **certain** that the administrator email address for your account is correct, and that messages sent to that address are read and acted on quickly.
- If you have multiple Directory Agent instances, make sure each is configured to use a unique, non-overlapping directory context.
- Make sure that you have only one Sync Service instance, and that it is configured to send user information to the hybrid service at appropriate intervals.
- Add your organization's webmail address as an unfiltered destination.

Support Online Resources



Knowledge Base

- Search or browse the knowledge base for documentation, downloads, top knowledge base articles, and solutions specific to your product.



Support Forums

- Share questions, offer solutions and suggestions with experienced Websense Customers regarding product Best Practices, Deployment, Installation, Configuration, and other product topics.



Tech Alerts

- Subscribe to receive product specific alerts that automatically notify you anytime Websense issues new releases, critical hot-fixes, or other technical information.



ask.websense.com

- Create and manage support service requests using our online portal.

Webinar Update

Title: v7.5 Websense Web Security Jump Start:
Configuration and Setup

Date: September 15, 2010

Time: 8:30 AM PDT (GMT -7)

How to register:

<http://www.websense.com/content/SupportWebinars.aspx>

Customer Training Options

- To find Websense classes offered by Authorized Training Partners in your area, visit:
<http://www.websense.com/findaclass>
- Websense Training Partners also offer classes online and onsite at your location
- For more information, please send email to:
readiness@websense.com

WEBSense®
**Authorized Training
Partner**

WEBSense®
Certified Instructor



Questions?

