

Webinar Information

- **Title: Websense Remote Filtering**
- Audio information:
 - **This presentation incorporates STREAMING AUDIO.**
 - Use of speakers or headsets is required. *If unable to hear streaming audio or it is choppy, a limited number of dial-in numbers are available.*
- Dial-in numbers:
 - **U.S. dial-in numbers:**
 - Toll free: **1-866-288-9872**, pass-code: **312558**
 - Toll: **1-913-312-2900**, pass-code: **312558**
 - **Find international dial-in numbers at:**
 - http://kb.websense.com/pf/12/webfiles/Webinars/international/May09_webinar_international_numbers.pdf
 - Pass-code: **312558**



Websense Remote Filtering

Websense Support Webinar

Goals and objectives

To understand:

- Requirements for Remote Filtering Server and Client
- How to deploy Remote Filtering Server
- How to install and configure:
 - Remote Filtering Server
 - Remote Filtering Client
- Firewall configuration requirements
- Basic troubleshooting steps

Agenda

- Remote Filtering Server requirements and recommendations
- Remote Filtering Client requirements
- Deploying Remote Filtering Server
- Installing and configuring Remote Filtering Server.
- Installing and configuring Remote Filtering Client
- Configuring the firewall
- Troubleshooting Remote Filtering Server and Client
- Common issues

Webinar Presenter



Imran Rai

- Title: Tech Support Specialist
- Accomplishments:
 - Over 4 years supporting Websense products
- Education / Certifications:
 - BSc Hons in Computer Science
 - CWSE – Certified Web Security Engineer
- Qualifications:
 - New Hire Training
 - v7 Tech Support Training
- For additional information:
www.websense.com/support/

Requirements: Remote Filtering Server

- Supported operating systems:
 - Red Hat Enterprise Linux 3 or 4: AS, ES, and WS
 - Red Hat Enterprise Linux 5 (Standard, Advanced Platform, Desktop with Workstation option)
 - Windows Server 2003, SP1 (Standard or Enterprise)
 - Windows Server 2003, R2 (Standard or Enterprise)
- Hardware recommendations by network size:
 - 1 - 5000 clients:
 - *Quad-Core Intel Xeon, 2.5 GHz or greater*
 - *2 GB RAM*
 - *20 GB of free disk space*

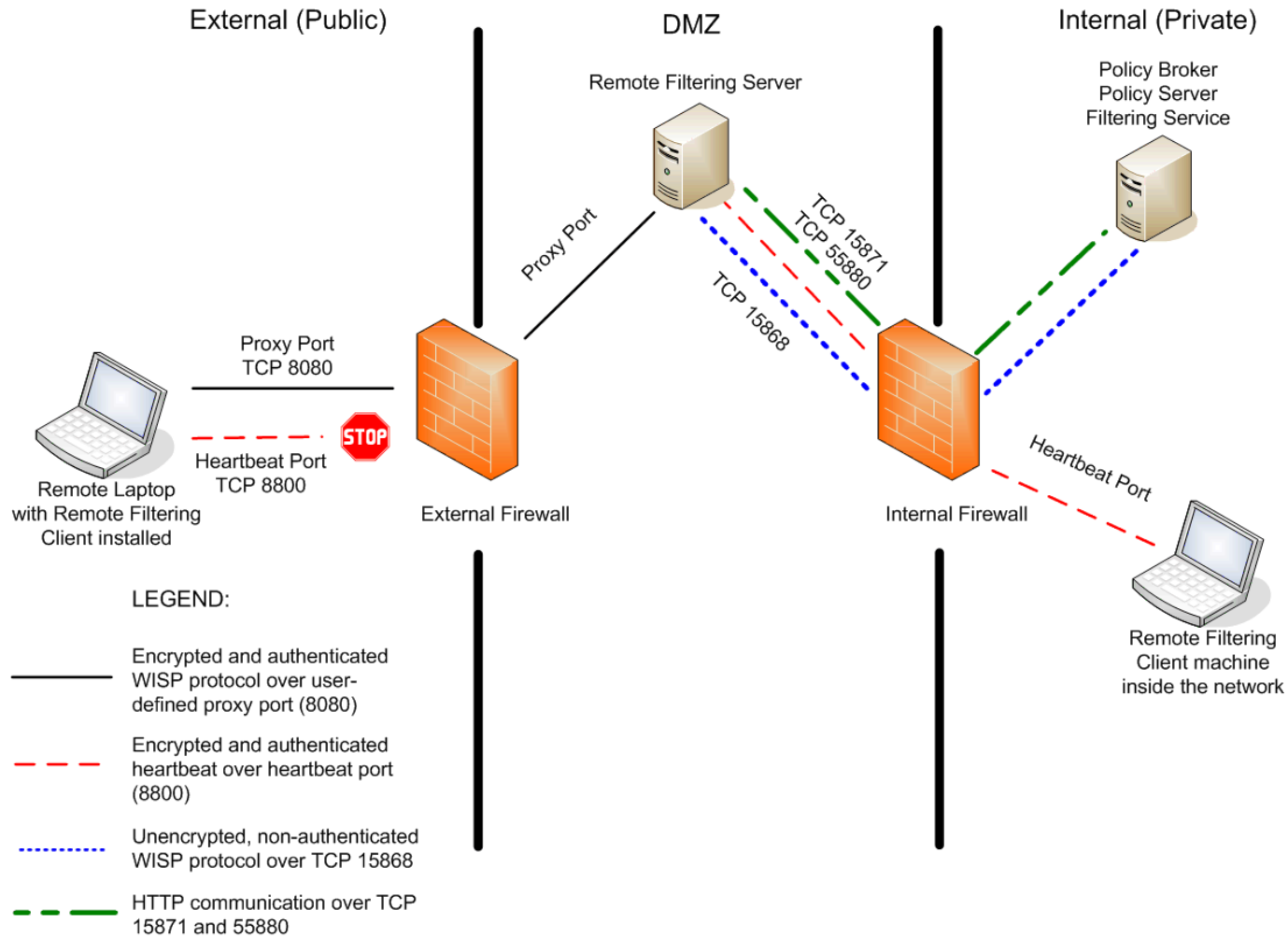
Requirements: Remote Filtering Server

- Hardware recommendations by network size (continued):
 - 5000 - 10000 clients:
 - *Quad Xeon, 3.2 GHz or greater, or static load balancing with Dual Xeon, 3.2 GHz or greater*
 - *2 GB RAM*
 - *20 GB of free disk space*
 - 10000+ clients:
 - *Static load balancing with Dual Xeon, 3.2 GHz or greater*
 - *2 GB RAM*
 - *20 GB of free disk space*

Requirements: Remote Filtering Client

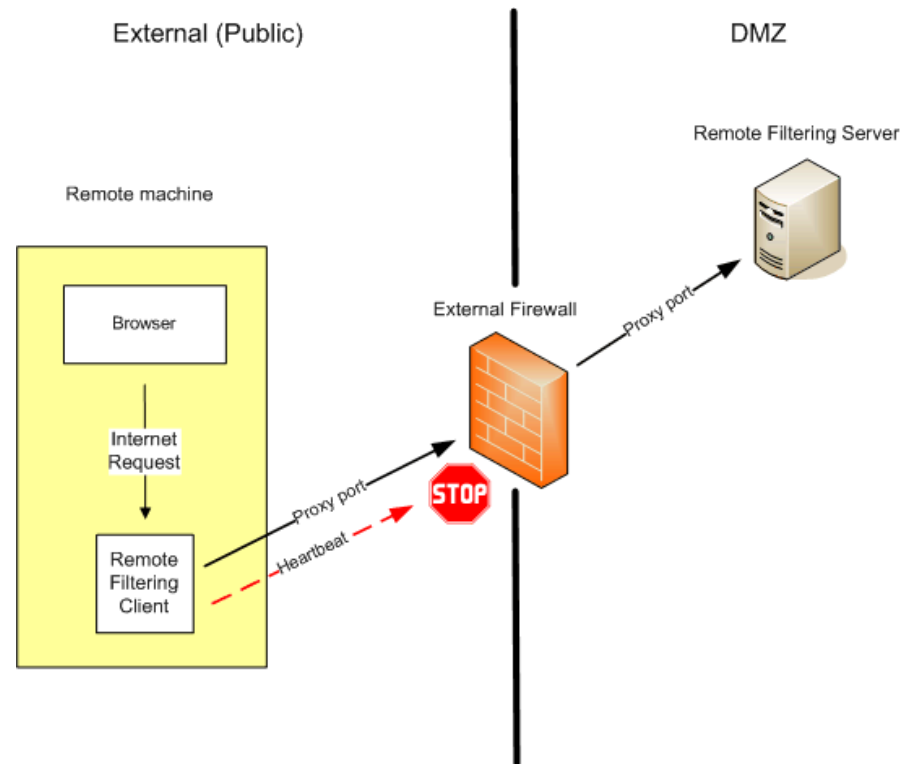
- Remote Filtering Client is supported only on Microsoft Windows operating systems:
 - Windows XP Professional with SP1, SP2, or SP3
 - Windows Vista (Ultimate, Enterprise, or Business)
 - Windows Server 2003 (Standard or Enterprise)
 - Windows Server 2003, SP1 (Standard or Enterprise)
 - Windows Server 2003, R2 (Standard or Enterprise)
- Hardware recommendations:
 - Pentium 4 or greater
 - Free disk space: 25 MB for installation; 15 MB to run
 - 512 MB RAM

Deploying Remote Filtering Server



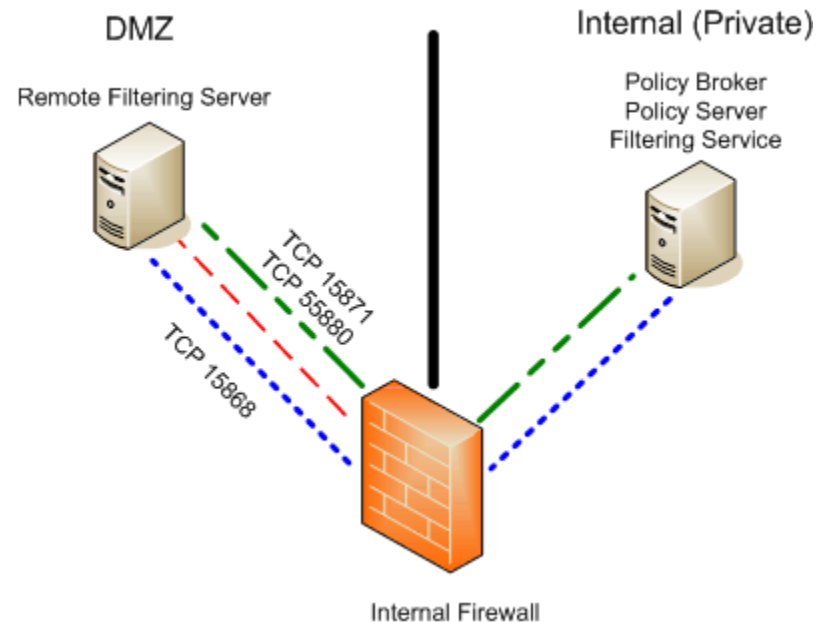
How does Remote Filtering work?

1. Machines outside the network attempt to connect to Remote Filtering Server on the heartbeat port.
2. The firewall stops the heartbeat connection.
3. Remote Filtering Client sends HTTP traffic to Remote Filtering Server in the DMZ.



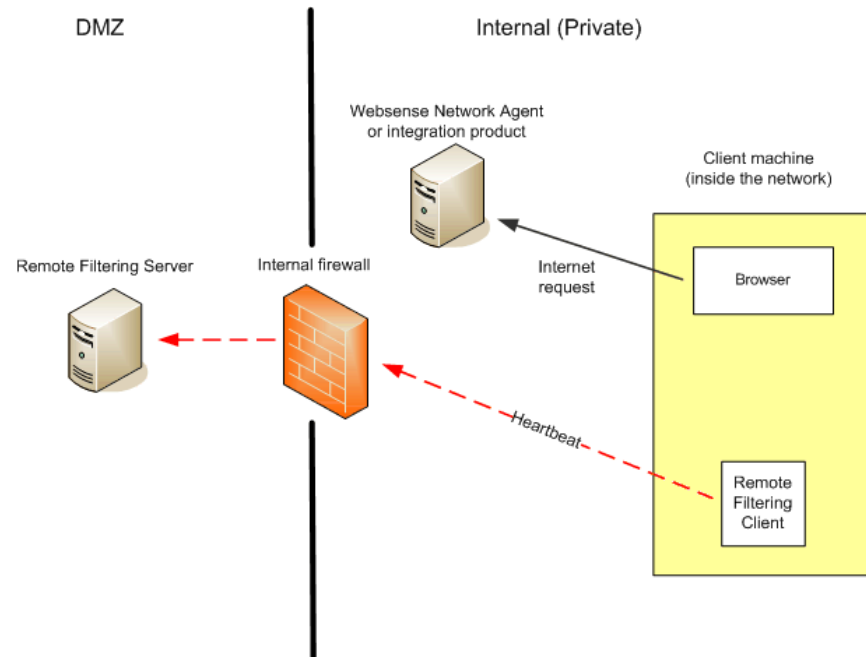
How does Remote Filtering work?

4. Remote Filtering Server sends the request to Filtering Service.
5. Filtering Service checks the client's policy and the site's category.
6. Filtering Service notifies Remote Filtering Server whether to permit the page or to send a block page.



How does Remote Filtering work?

- When a machine is inside the network, the Remote Filtering Client heartbeat succeeds.
- Remote Filtering Client becomes passive.
- Requests are passed directly from the browser to Network Agent or an integration product, just like any other internal client.

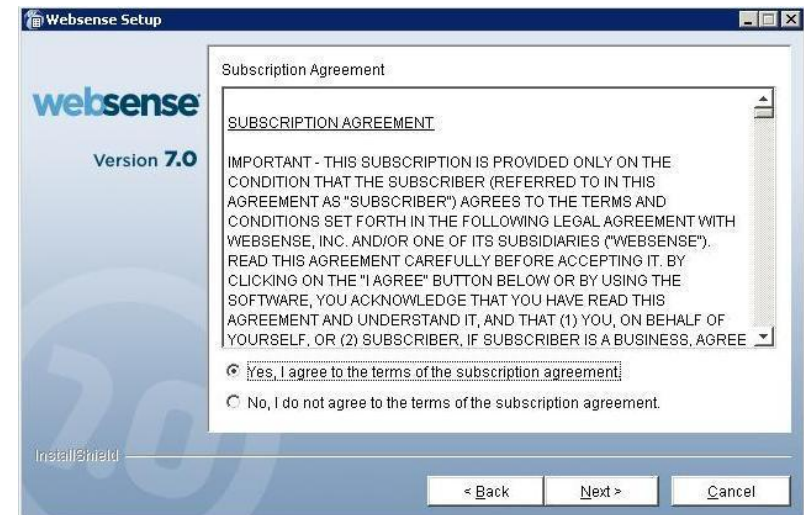


Remote Filtering and user identification

- If users log on to the remote machine using cached credentials, those credentials are used to perform user-based filtering.
- If users log on to the remote machine using local accounts, the Default policy is applied.

Installing Remote Filtering Server

1. Launch the Websense Web Security / Web Filter installer.
2. Accept the subscription agreement.

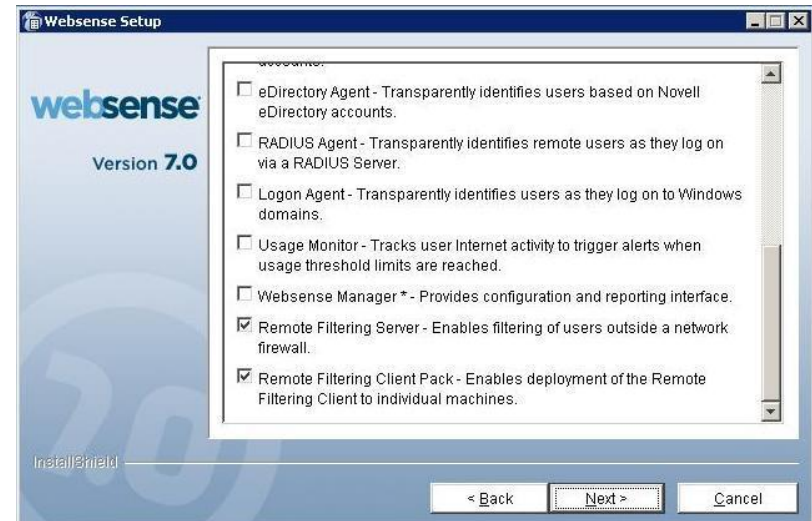


Installing Remote Filtering Server

3. Select Custom installation.

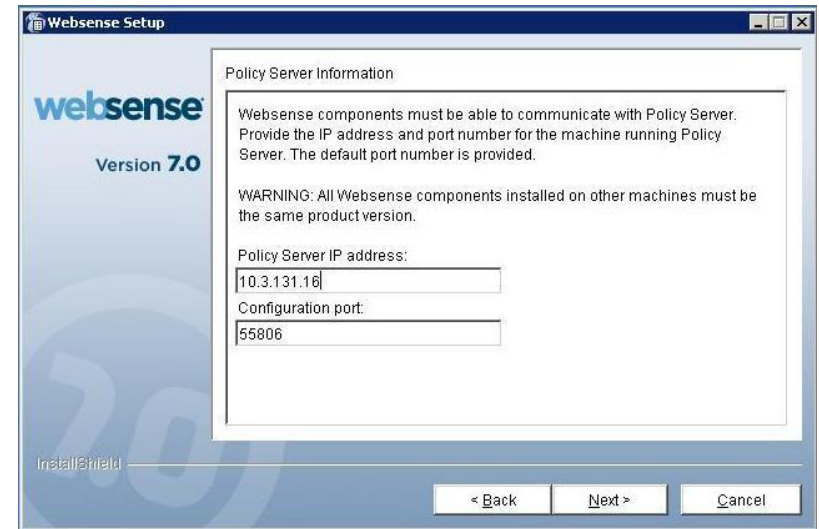


4. Select Remote Filtering Server. If installing on Windows, also select Remote Filtering Client Pack.



Installing Remote Filtering Server

5. Provide the Policy Server IP address and configuration port.
6. Enter the Remote Filtering Server machine's external (public-facing) IP address, the port used to communicate with remote clients, and the heartbeat port.



The screenshot shows the 'Websense Setup' dialog box, Version 7.0, at the 'Policy Server Information' step. The dialog contains the following text and input fields:

Policy Server Information

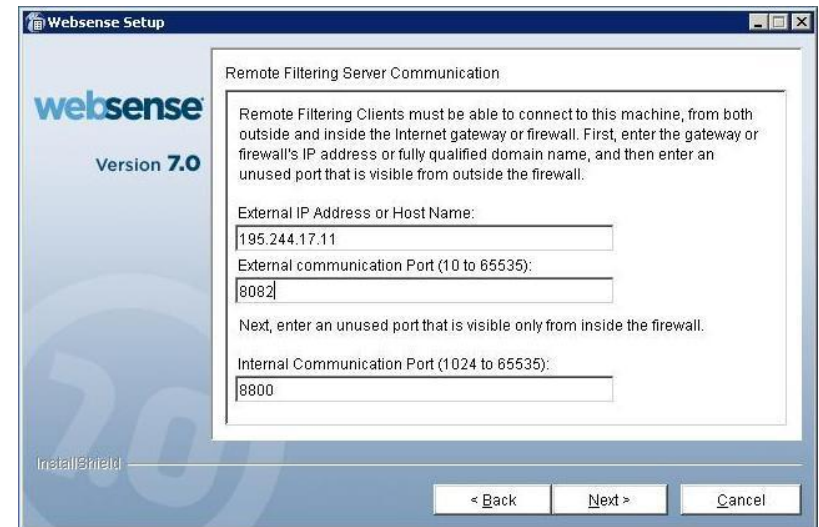
Websense components must be able to communicate with Policy Server. Provide the IP address and port number for the machine running Policy Server. The default port number is provided.

WARNING: All Websense components installed on other machines must be the same product version.

Policy Server IP address:

Configuration port:

At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.



The screenshot shows the 'Websense Setup' dialog box, Version 7.0, at the 'Remote Filtering Server Communication' step. The dialog contains the following text and input fields:

Remote Filtering Server Communication

Remote Filtering Clients must be able to connect to this machine, from both outside and inside the Internet gateway or firewall. First, enter the gateway or firewall's IP address or fully qualified domain name, and then enter an unused port that is visible from outside the firewall.

External IP Address or Host Name:

External communication Port (10 to 65535):

Next, enter an unused port that is visible only from inside the firewall.

Internal Communication Port (1024 to 65535):

At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

Installing Remote Filtering Server

7. Enter and confirm the pass phrase used when communicating with remote clients (no spaces).
8. Enter the Filtering Service IP address.
 - If there is a firewall between Filtering Service and Remote Filtering Server, enter the translated or external Filtering Service IP address.
 - If not, clear the check box.

The screenshot shows the 'Remote Filtering Encryption Pass Phrase' dialog box in the Websense Setup window. The dialog box contains the following text: 'Enter any combination of keyboard characters to create an encryption pass phrase. The phrase may be any length.' Below this, it states: 'The Pass Phrase is combined with unpublished Remote Filtering Server keys to create an authentication key. Remote Filtering Server uses the authentication key to ensure secure communications.' There are two input fields: 'Pass phrase:' and 'Confirm pass phrase:', both containing asterisks. At the bottom of the dialog box, there are three buttons: '< Back', 'Next >', and 'Cancel'.

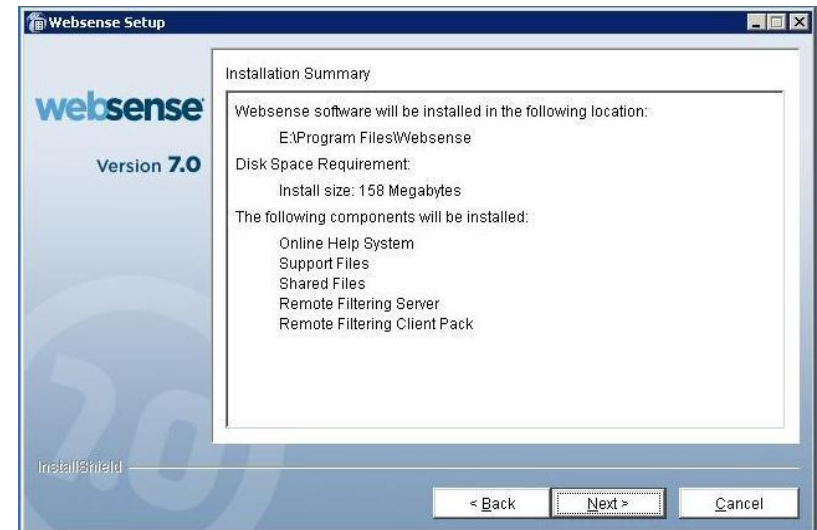
The screenshot shows the 'Filtering Service Information for Remote Filtering' dialog box in the Websense Setup window. The dialog box contains the following text: 'Provide the following information to allow Remote Filtering Server to communicate with Filtering Service to filter remote users' requests, and send block messages, if needed. The default ports are provided.' Below this, there are several input fields: 'Actual (internal) IP address of Filtering Service:' with the value '10.36.131.16', a checked checkbox 'A firewall or other network device performs address translation between Filtering Service and Remote Filtering Server.', 'Translated (external) IP address of Filtering Service:' (empty), 'Filter port:' with the value '15868', and 'Block page port:' with the value '15871'. At the bottom of the dialog box, there are three buttons: '< Back', 'Next >', and 'Cancel'.

Installing Remote Filtering Server

9. Accept the default installation path or browse to select a new path.



10. Review the summary and click **Next** if it is correct.



Installing Remote Filtering Client

1. Launch the Remote Filtering Client installer on the client machine.
2. Enter:
 - The external IP address of the Remote Filtering Server machine.
 - The internal Filtering Service IP address.
 - The pass phrase created during Remote Filtering Server installation.

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: 195.244.17.11 Port: 8082

Internal IP or Hostname: 10.3.131.1 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

Deploying Remote Filtering Client using third-party tools

- Command-line parameters:

- **PRIMARY_WISP_ADDRESS**=<external IP address or FQDN of primary Remote Filtering Server>

Externally-visible address for the primary Remote Filtering Server machine

- **PRIMARY_WISP_PORT**=<external port number of primary Remote Filtering Server>

Externally-visible port used to communicate with the primary Remote Filtering Server from outside the network firewall

- **PRIMARY_INTERNAL_WISP_ADDRESS**=<internal IP address or FQDN of primary Remote Filtering Server>

Internal address for the primary Remote Filtering Server machine

Deploying Remote Filtering Client using third-party tools

- Command-line parameters (continued):
 - **PRIMARY_INTERNAL_WISP_PORT**=<internal port number of primary Remote Filtering Server>
Heartbeat port (the port used for internal communication between the primary Remote Filtering Server and the Remote Filtering Client when located within the network)

Deploying Remote Filtering Client using third-party tools

■ Installation options

– **PATH=**<installation path>

- *Remote Filtering Client installation directory on each client machine (by default, C:\Program Files\WebSense\WDC). The WDC directory is hidden by default.*

– **PASSPHRASE=**<pass phrase for Remote Filtering Server>

- *Pass phrase entered during primary Remote Filtering Server installation. When using failover Remote Filtering Servers, the Remote Filtering Servers in the same failover group (primary, secondary, and tertiary) must have the same pass phrase.*

Deploying Remote Filtering Client using third-party tools

■ Installation options (continued):

– **REBOOT=YES | NO | PROMPT | IF_NEEDED_PROMPT**

- *Defines whether the client machine is automatically restarted after Remote Filtering Client is installed (or uninstalled). The values for this parameter are:*

YES: Machines are restarted, and users are not prompted to restart.

NO: Machines are not restarted, and users are not prompted to restart.

PROMPT: Users are prompted to restart their machines.

IF_NEEDED_PROMPT (default): Users are prompted to restart their machines only if a restart is required.

– **REINSTALL=ALL**

- *Used only for repairing or upgrading an existing Remote Filtering Client installation. Indicates the components to remove and reinstall (should always be set to ALL).*

Deploying Remote Filtering Client using third-party tools

- Installation options (continued):
 - **REINSTALLMODE=veums | voums**
 - *Used only for repairing or upgrading an existing Remote Filtering Client installation. The possible values are **veums** (for repairs only) and **voums** (for upgrades only).*
 - **/qn**
 - *Perform a quiet installation. When you use this option, the Remote Filtering Client installs without displaying information to the end user. If you do not use this switch, the installer launches in interactive mode, and installation dialog boxes are displayed.*

Remote Filtering Client installation syntax

```
msiexec /i cpmclient.msi PASSPHRASE=<pass phrase>  
PRIMARY_WISP_ADDRESS=<external IP address or FQDN>  
PRIMARY_WISP_PORT=<port>  
PRIMARY_INTERNAL_WISP_ADDRESS=<internal IP address or  
host name> PRIMARY_INTERNAL_WISP_PORT=<port>  
REBOOT=<parameter> /qn
```

For example:

```
msiexec /i cpmclient.msi PASSPHRASE=2gbatfm  
PRIMARY_WISP_ADDRESS=63.16.200.232 PRIMARY_WISP_PORT=80  
PRIMARY_INTERNAL_WISP_ADDRESS=10.218.5.60  
PRIMARY_INTERNAL_WISP_PORT=9000 REBOOT=IF_NEEDED_PROMPT /qn
```

Remote Filtering Client repair and uninstall syntax

- repair syntax:

```
msiexec /i cpmclient.msi REINSTALL=ALL REINSTALLMODE=veums /qn
```

- Uninstall command

```
msiexec.exe /x - {14D74337-01C2-4F8F-B44B-67FC613E5B1F} /qn
```

- Type each command on a single line (no line breaks).

External firewall configuration

- Open the Remote Filtering Server external communication port to accept connections clients outside the network firewall.
 - Typically, this is port 8080 (defined during Remote Filtering Server installation).
 - The default is 80.
- Block connections to the Remote Filtering Server internal communication port from clients outside the network firewall.
 - By default, this is port 8800.

Internal firewall configuration

- Open the Filtering Service communications port (by default, 15868) to accept connections from Remote Filtering Server.
- Open the Filtering Service block page port (by default, 15871) to allow block pages to be sent to remote users.

Fail open / fail closed

- By default, Remote Filtering Client permits all requests if it cannot connect to Remote Filtering Server (**fail open**).
 - Use the **FailClose** parameter in the **SecureWispProxy.ini** file to change this behavior.
 - *When FailClose is set to **true**, all requests are blocked when the client cannot connect to the server.*
 - Use the **FailCloseTimeout** parameter to determine how long (in minutes) the client attempts to connect to the server before failing closed (the default is 15).

```
#Fail Open/Close Parameters
FailClose=true
FailCloseTimeout=20
```
 - Always restart Remote Filtering Server after editing this file.

Troubleshooting

- If Remote Filtering Clients are not being filtered, make sure that the same pass phrase is being used on by the client and the server.
 - Complete instructions are available in the Remote Filtering technical paper.
- Make sure that the [websense.ini](#) file on the Remote Filtering Server machine lists the correct location for Policy Server.
- Verify that DHCP is not enabled on the Remote Filtering Server machine.

Troubleshooting

- If Remote Filtering Server is installed on a machine that hosts a Web server, make sure the Web server does not use the port that Remote Filtering Server uses to communicate with clients.
- Make sure the [SecureWispProxy.ini](#) settings on the Remote Filtering Server machine match with those on the Remote Filtering Client machines.
 - Default location:
HKLM\Software\WebSense\Desktop Client\Desktop Filtering

SecureWispProxy.ini

```
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
4690D0B3F3AE1865C000A60E55A159BDE4186874FF167E9FDAB21861270
B4A333867CC5D725DE64BFC03C698680FAC26F3555EAC28ECB16781318
6CE18F5B3A292BE5CD301A6C339F1EEC0C8BBC7C99955E7999AE85AF4923
219E7FE09B50E5D06778E3DFB68DE46CDB107A01996E0074566E806AE7A
12D362F8E7582763E789585B919EE4DEBE4BE19D4C0926F4E341D6157E
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=traceFile.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.

Debugging Remote Filtering Server

- 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.

```
#Trace type to trace  
All|WISP|BlockPage|HeartBeat  
TraceType=All  
TraceFile=traceFile.log  
TraceFileSize=1
```

Debugging Remote Filtering Client

- You can configure Remote Filtering Client to collect debugging information as follows:
 1. Open the Windows Registry ([regedt32](#)) 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.

Common issues

- Block pages do not display
 - Make sure the block page port (default 15871) is open on the firewall.
 - Make sure Remote Filtering Client is not installed on the Remote Filtering Server machine. This uses up all the available connections to the server, preventing remote connections.
- 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.
 - Modify firewall rules to allow the port.

Common issues

- Remote clients are not being filtered
 - Make sure that Network Agent is configured to ignore traffic from the Remote Filtering Server machine.
 - *Open Websense Manager and go to the Settings > Network Agent > Global Settings page.*
 - *Make sure the IP address of the Remote Filtering Server machine does not appear in the Internal Network Definition list as an individual entry or part of an included address range.*
 - Are there errors in the [RFSErrors.log](#) file?
 - *The file is located in the Websense [bin](#) directory (C:\Program Files\Websense\bin or /opt/Websense/bin, by default).*
 - **Error 64** may indicate that DHCP is enabled on the Remote Filtering Server machine. Acquire a static IP address and disable DHCP.
 - **Error 121** occurs on Windows Server 2003 machines, indicating that required Service Pack 1 is not installed. Install the service pack.

Summary

- We reviewed the Remote Filtering requirements.
- We looked at how Remote Filtering works.
- We went through how to install Remote Filtering Server and Remote Filtering Client.
- We talked about deployment methods for Remote Filtering Client.
- We discussed firewall configuration.
- We learned about the **fail open** and **fail closed** options.
- We talked about how to debug the Remote Filtering components.
- We discussed common Remote Filtering issues.

ENHANCED service: Tech Alerts

- Websense Global Technical Support announces enhanced Tech Alerts.

- Receive product-specific alerts.
- Find out when there are:
 - *Critical hotfixes*
 - *New releases*
 - *Other technical information that could impact your organization*

- Sign up today:

<http://support.websense.com> and click “Tech Alerts” under “Tools and Policies”

The screenshot shows the 'Websense Tech Alerts' page. At the top, there is a navigation bar with links: Resource Center, Products & Services, Downloads, Support, Security Labs, Partners, and Company. Below the navigation bar, the page title is 'Websense Tech Alerts'. There is a search bar with a 'Search' button and a link to 'Archived Alerts'. Below the search bar, there are dropdown menus for 'Search using' (set to 'All Words'), 'Search Within' (set to 'Tech Alerts'), and 'All Categories'. A 'Search' button is next to the search bar. Below the search bar, there is a 'Powered by Knowledgebase' logo. A red alert icon is visible. Below the icon, there is a text box that says: 'Click below to View your product's Tech Alerts. Click on Subscribe to be notified via email of any future Tech Alerts for your product area. Please also Subscribe to the General Tech Alerts to be notified of non product-specific alerts, such as a general security notice.' Below this text, there is a grid of six product-specific alert subscription buttons. Each button has a 'View' link and a 'Subscribe/Unsubscribe' link. The products listed are: WebSense Web Filtering, WebSense Web Security Gateway, WebSense Client Policy Manager, Surfcontrol Web Filtering, WebSense Data Security Suite, and WebSense Hosted Web Security.

Customer training and certification programs

You can receive Websense-authorized training and certification.

To see what training is available:

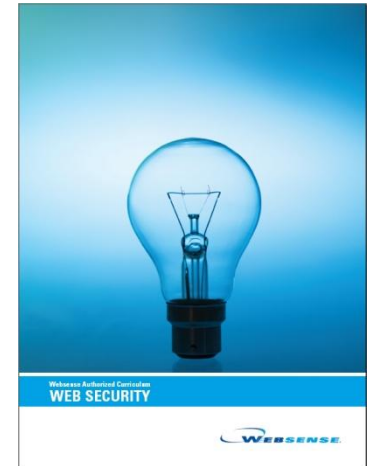
- <http://www.websense.com/training>

To find a partner:

- <http://www.websense.com/findaclass>

To find out more about our certification program:

- <http://www.pearsonvue.com/websense>



WEBSENSE®
**Authorized Training
Partner**

Questions?



- As many questions as possible will be answered in the allotted time.
- Responses to all questions submitted will be posted online on the Support Webinars home page approximately one week from today.
- To review answers to your questions, go to:
<http://www.websense.com/SupportPortal/SupportWebinars.aspx>