

Filtering remote users with Websense remote filtering software v7.6

WebSense Support Webinar April 2012

TRITON™

Web security

Email security

Data security

Mobile security



Greg Didier

- **Title:**
 - Support Specialist
- **Accomplishments:**
 - 9 years supporting Websense products
- **Qualifications:**
 - Technical Support Mentor
 - Product Trainer

- **Introduce remote filtering software**
 - Requirements and how it works.
- **Installing remote filtering software**
 - Preparation and installation.
- **Setting up remote filtering software**
 - Component configuration options.
- **Troubleshooting**
- **Demonstration**
 - Client software installation.

- **Websense remote filtering software filters HTTP, HTTPS, and FTP Internet requests from machines *outside-the-network*.**
 - All communication from external machines to your network is authenticated and encrypted.
- **Available with:**
 - Websense Web Filter
 - Websense Web Security
 - Websense Web Security Gateway
 - Websense Web Security Gateway Anywhere

- **Remote Filtering Client**
 - Allows filtering machines when they are outside the network.
 - Communicates with Remote Filtering Server installed inside your organization's firewall.
- **Remote Filtering Server**
 - Provides Web filtering for machines located outside your network firewall.
 - Acts as a proxy.
 - Accepts Remote Filtering Client requests and then forwards them to Filtering Service.
 - Remote Filtering Server only filters computers running the Remote Filtering Client software.

- Version 7.6.x installs on the following supported Microsoft Windows operating systems.

Hardware Recommendations	Operating System Requirements
<ul style="list-style-type: none">• Pentium 4 1.8 GHz• Free disk space: 25 MB for installation; 15 MB to run the application• 512 MB RAM	<ul style="list-style-type: none">• Windows 7 (x86 and x64)• Windows XP SP2 and above (x86 and x64)• Windows Vista SP1 and above (x86 and x64)• Windows Server 2003 SP2 and R2 SP2 and above (x86 and x64)• Windows Server 2008 SP1 and above (x86 and x64)• Windows Server 2008 R2 (x64)

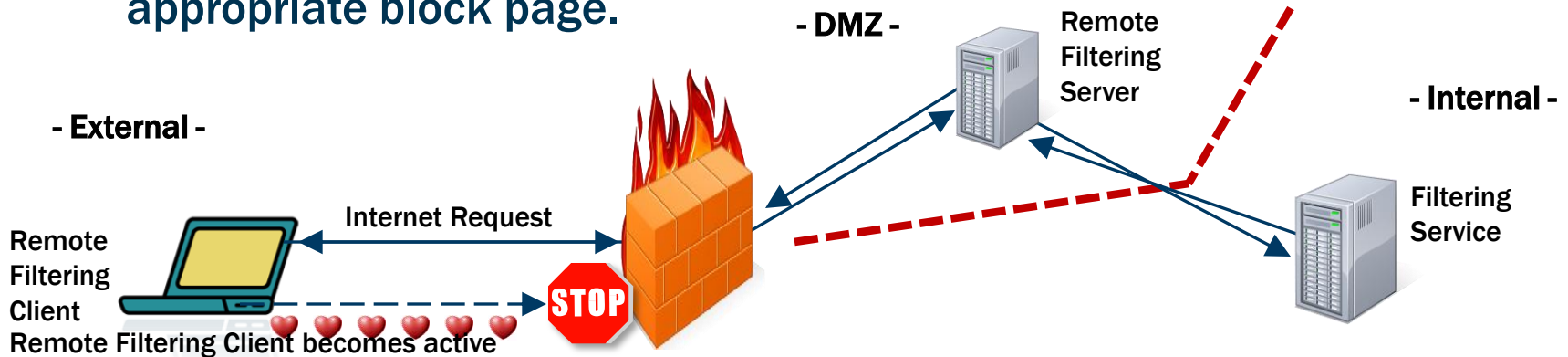
System Requirements – Remote Filtering Server **websense**

- **Version 7.6.x is supported on the following operating systems:**
 - Red Hat Enterprise Linux 4 and 5.
 - Windows Server 2003 and 2003 R2.
 - Windows Server 2008 and 2008 R2.

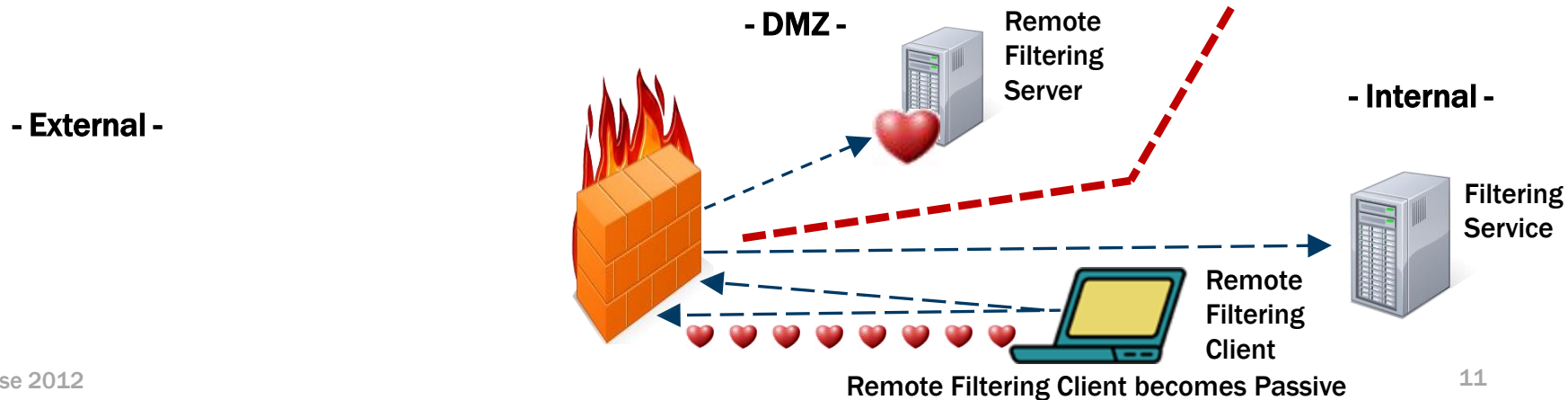
- **Guidelines for installing Remote Filtering Server:**
 - Inside your organization's outermost network firewall.
 - In the DMZ.
 - On its own, dedicated machine.
 - Do not install with Filtering Service or Network Agent.
 - Does not need to be joined to the domain.
 - Must be able to communicate with:
 - External Remote Filtering Clients.
 - Internal Filtering Service, Policy Server, and Policy Broker.
 - Install only one primary Remote Filtering Server per Filtering Service.

- **Remote Filtering Client resides on client machines that are sometimes or always used outside your organization's network.**
 - When a user makes a browser-based Internet request, Remote Filtering Client uses a heartbeat to determine whether it is within or outside the network.
 - If the machine is *outside* the network, the Internet request is forwarded to Remote Filtering Server.
 - If the machine is *inside* the network, Remote Filtering Client becomes passive.

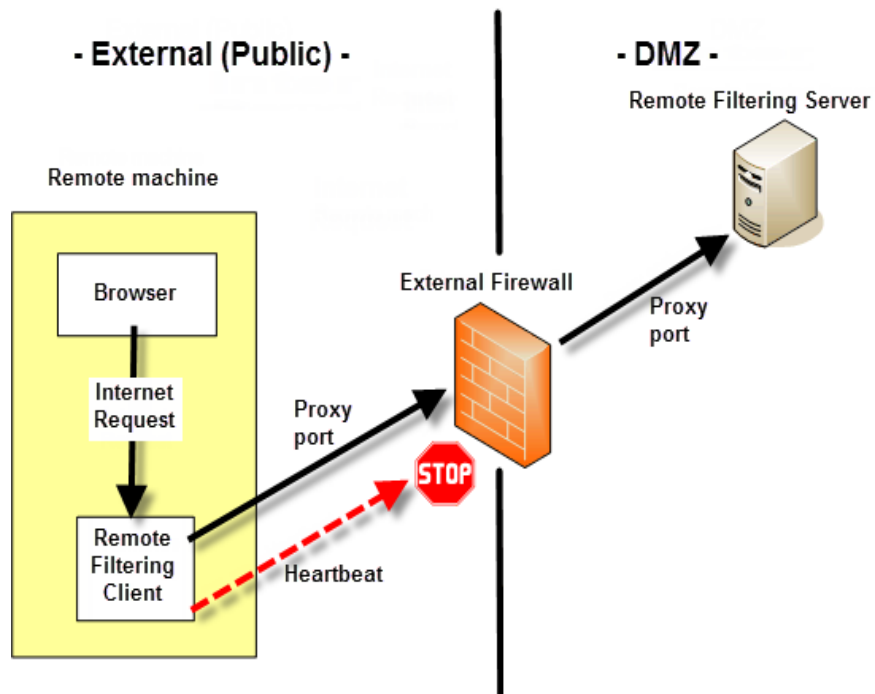
1. A heartbeat failure prompts Remote Filtering Client to send queries for each HTTP, HTTPS, or FTP request to the Remote Filtering Server.
2. Remote Filtering Server then forwards the request to Filtering Service.
3. Filtering Service evaluates the request and sends back a response.
4. Remote Filtering Server sends the response to the client.
5. If the site is blocked, Remote Filtering Client requests and receives the appropriate block page.



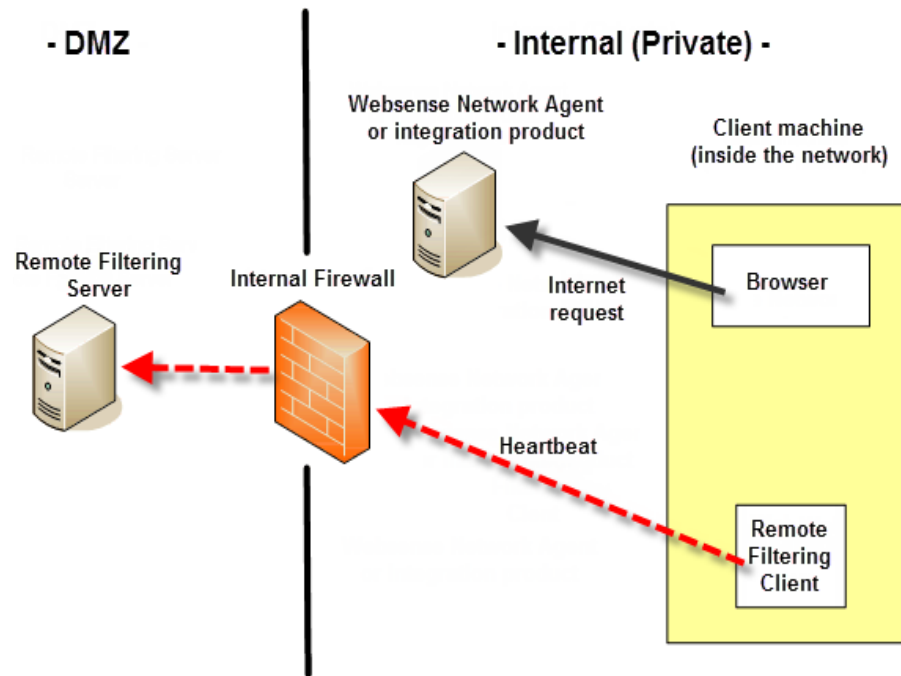
1. When a heartbeat connection **succeeds**, Remote Filtering Client becomes passive.
 - It does not query Remote Filtering Server about Internet requests.
2. Browser requests are passed directly the Websense integration.
 - Internet request are filtered like any other internal request.



Active Remote Filtering Client



Passive Remote Filtering Client



- **Logging in with cached domain credentials.**
 - Filtering Service resolves user name and applies user and group-based policies.
- **Logging in with a local computer account.**
 - Filtering Service cannot resolve the user name.
 - If manual authentication is enabled:
 - User receives a logon prompt.
 - Internet requests are filtered by the appropriate user or group policy.
- **Logging in with a local account and manual authentication is not enabled.**
 - Internet requests are filtered by the Default policy.
 - Internet activity is logged under the local user name.
 - Filtering on policies assigned to IP addresses or IP address ranges does NOT apply.

- **Internal client filtering**

1. User
 2. Computer IP
 3. Network IP Range
 4. Group
 5. OU
 6. Default Policy
- If 1 thru 5 do not match, then the Default Policy always applies.

- **Policies assigned to computer IP or IP range do not apply for externally filtered clients.**

- **External client filtering**

1. User
 2. Group
 3. OU
 4. Default Policy
- If 1 thru 3 do not match, then the Default Policy always applies.

- For HTTP sites with a category set to the Quota or Confirm.
 - Remote filtering offers the appropriate block message, including the Quota or Continue button.

Content blocked by your organization

Reason: This Websense category is filtered: Shopping.
URL: http://testdatabasewebsense.com/shopping

Options: Click [more information](#) to learn more about your access policy.

To view sites in this category you must use quota time. You have 60 minute(s) of quota time remaining. Click the **Use Quota Time** button to start a 10 minute session for viewing this site and other sites in quota-limited categories.

Click **Go Back** or use the browser's Back button to return to the previous page.

Content blocked by your organization

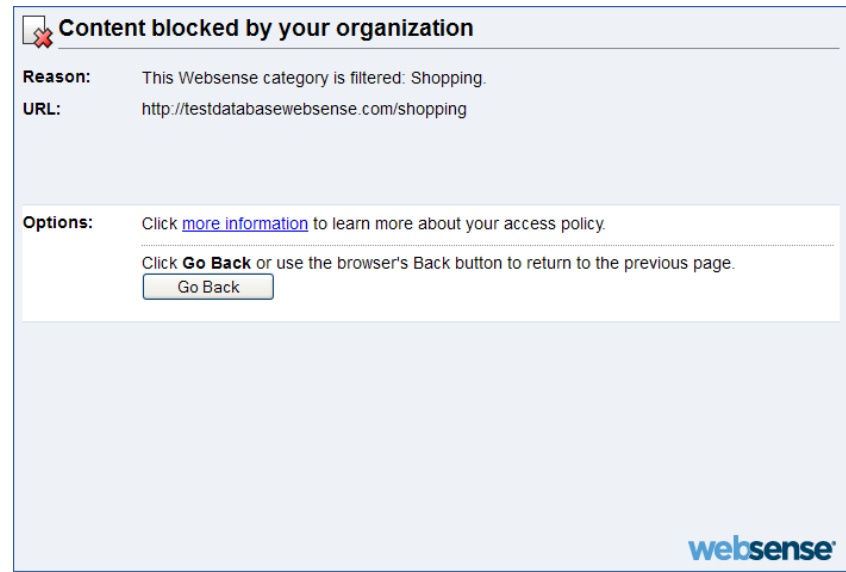
Reason: This Websense category is filtered: Shopping.
URL: http://testdatabasewebsense.com/shopping

Options: Click [more information](#) to learn more about your access policy.

Click **Continue** to view the site now for work-related purposes.

Click **Go Back** or use the browser's Back button to return to the previous page.

- For HTTP sites with a category set to the Quota or Confirm.
 - Remote filtering offers the appropriate block message, including the Quota or Continue button.
- For FTP or HTTPS sites set to Quota or Confirm.
 - The block page is presented; however, the Quota or Continue buttons are excluded.



- **Remote Filtering Client cannot contact Remote Filtering Server.**
 - By default, all HTTP, HTTPS, and FTP requests are **permitted** (fail open).
 - Remote Filtering Client continues attempting to reconnect.
 - When communication is reestablished, the appropriate filtering policy is enforced.
 - When configured to **block** all requests (fail closed).
 - No Internet access is allowed until a connection is reestablished.

- **When a user must pay for Internet access.**
 - **Remote Filtering Client detects and permits connections to payment portals.**
 - **When Internet access has been paid, Remote Filtering Client starts filtering Internet requests.**

- **A VPN connection, including split-tunneled VPN, is supported.**
 - **Split-tunnel:** All Internet requests go through the network adapter not connected to the internal network.
 - The heartbeat identifies the adapter not connected to the internal network.
- **Websense tested split-tunneling for the following VPN clients:**
 - Cisco AnyConnect 2.5 and 3.0
 - Juniper/NetScreen
 - Microsoft PPTP

- **System requirements**
- **Deployment information**
- **How remote filtering works**
- **Identifying remote users**
- **Differences between remote and local filtering**
- **When server communication fails**
- **Virtual Private Network (VPN)**


- **Next topics:**
 - **Preparing for installation**
 - **Ensuring ports are open**
 - **Installing Remote Filtering Server**
 - **Installing Remote Filtering Client**
 - **Customizing the client install package**
 - **Installing manually**
 - **Uninstalling Remote Filtering Client**
 - **Demonstration**

- A functioning Websense Web Security deployment must exist.
- **Permit communications from Remote Filtering Server in the DMZ to Policy Broker, Policy Server, and Filtering Service located inside your network.**

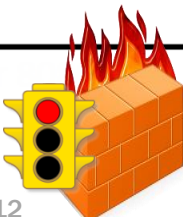
Port	Description
55825	Remote Filtering Server port. From Policy Server to Remote Filtering Server.
55806	Policy Server port. From Remote Filtering Server to Policy Server.
40000	Can be closed after installation.
55880	Broker Service port. From Remote Filtering Server to Policy Broker.
15868	Filtering Service Port. From Remote Filtering Server to Filtering Service.
15871	Block Page Port. Enables Filtering Service to send block messages. If not open, users are still blocked but do not receive a block message.

- **For remote filtering to function properly, leave these ports open.**

- **Permit external communication from Remote Filtering Clients to Remote Filtering Server on port 8080.**

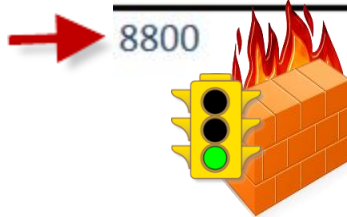
Port	Description
8080 (or 80) 	Open this external communication port on the external firewall. This enables Remote Filtering Server to accept connections from Remote Filtering Clients on computers located outside the network firewall. The default is 80, but many installations set it to port 8080 during installation.

- **Close external communication from Remote Filtering Clients on port 8800.**

Port	Description
8800 	Close access to the heartbeat port on the external firewall from computers located outside the network firewall.

- **Permit internal communication on the heartbeat port.**
 - Open access to Remote Filtering Server in the DMZ from Remote Filtering Clients residing inside your network.

Port	Description
8800	Open communication access to the Remote Filtering Server heartbeat port from internal Remote Filtering Clients.



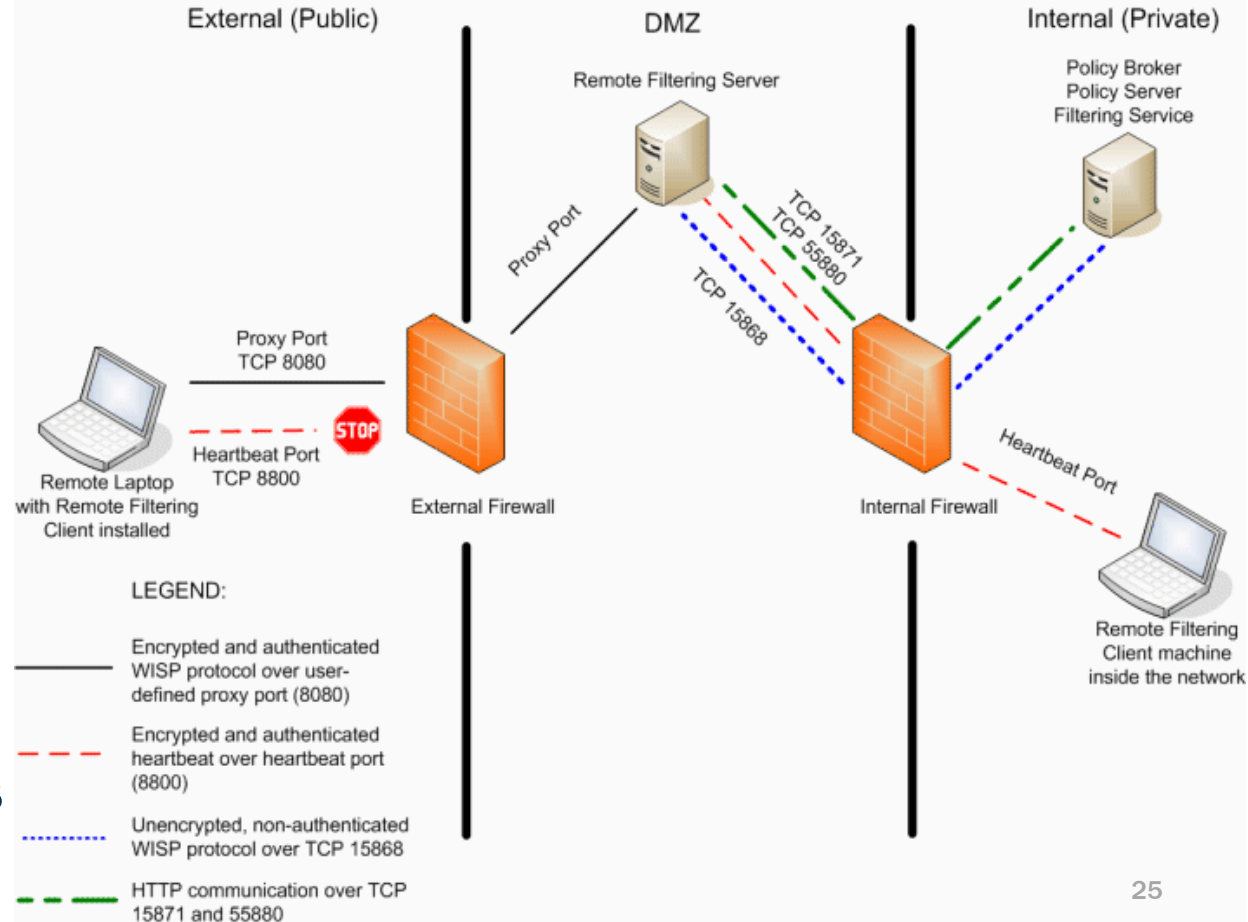
Recap: Port Communications

- **DMZ**
 - 55825*
 - 55806*
 - 40000*
 - 55880
 - 15868
 - 15871

- **External**
 - 8080 (or 80)
 - 8800 (block)

- **Internal**
 - 8800

* May close these ports after installation.



1. Preparing to install

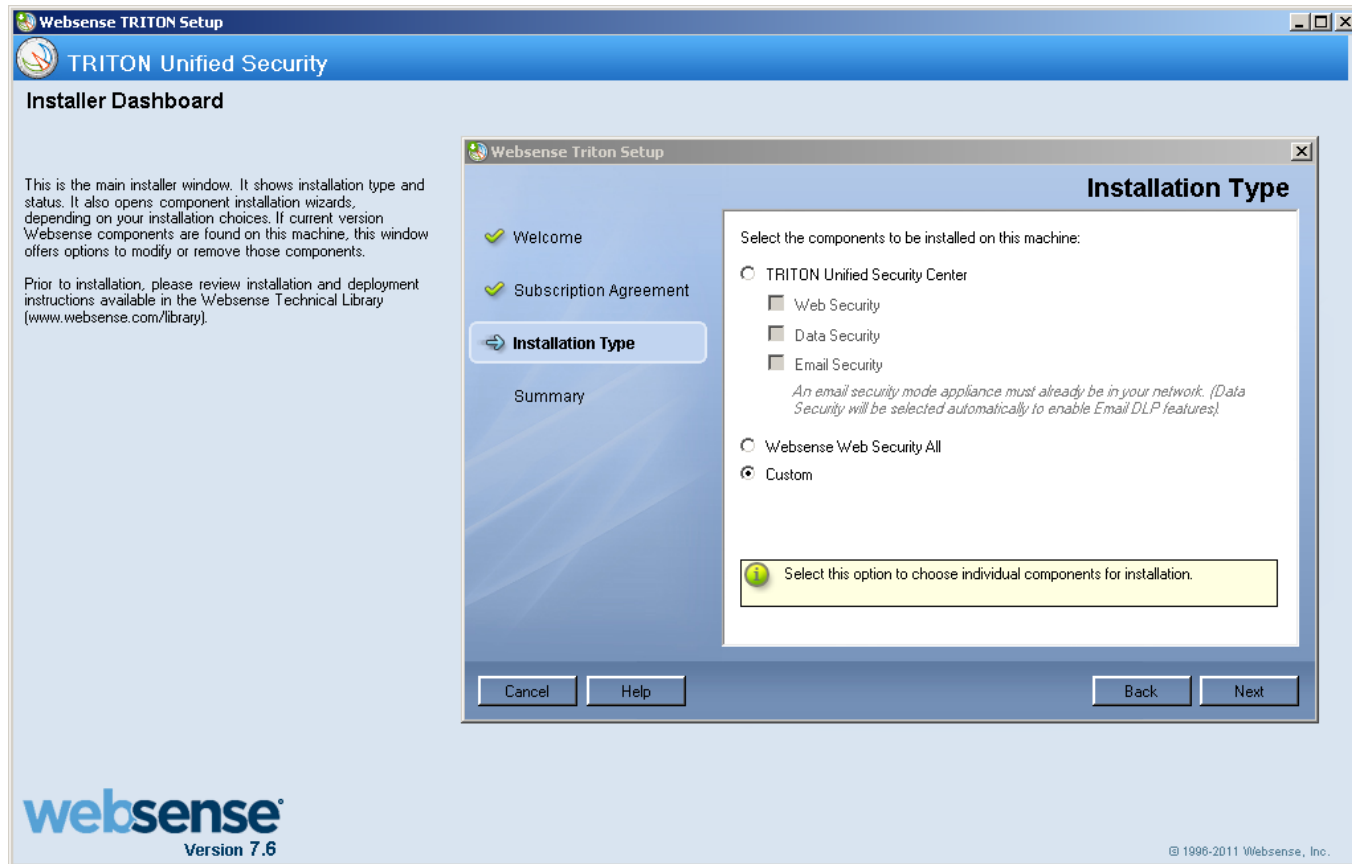
- Installer available from www.MyWebsense.com.

2. Selecting components

- In the Websense installer, select Custom mode.

3. Defining the Remote Filtering Server initial configuration

- ✓ Identify Policy Server
- ✓ External IP (of FQDN) and port
- ✓ Internal heartbeat port
- ✓ Pass phrase
 - 32-character limit on the pass phrase (in v7.6).
- ✓ Identify Filtering Service



Installing Remote Filtering Server

The screenshot shows the 'Websense TRITON Setup' window with the 'TRITON Unified Security' title bar. The main window is in the 'Custom Installation' phase, displaying a list of components to install: TRITON Infrastructure, Web Security (v7.6.2.1449), Data Security, and Email Security. The 'Web Security' component is selected. Below this list, there is a note about Microsoft SQL Server 2008 R2 Express and a 'SQL Server Express' install button. The 'Websense Web Security / Web Filter v7.6.2 Installer' dialog box is open, showing a progress list on the left with 'Introduction', 'Subscription Agreement', 'Installation Type', and 'Configuration' (selected). The 'Remote Filtering' section is expanded, showing two checked options: 'Remote Filtering Client Pack' and 'Remote Filtering Server'. The 'Interoperability' section has three unchecked options: 'Linking Service', 'Sync Service', and 'Directory Agent'. The dialog box has 'Cancel', 'Help', 'Previous', and 'Next' buttons.

Custom Installation

Click the Install link for the component type you want to install. A component installation wizard will start. In the wizard, select the components you want to install on this machine.

- TRITON Infrastructure [Install](#)
- Web Security** v7.6.2.1449 [Install](#)
- Data Security [Install](#)
- Email Security [Install](#)

Microsoft SQL Server 2008 R2 Express for small customers

SQL Server Express [Install](#)

Web Security / Web Filter v7.6.2 Installer

Select Components

- Introduction
- Subscription Agreement
- Installation Type
- Configuration**
 - Installation Directory
 - Pre-Installation Summary
 - Installation
 - Installation Complete

Remote Filtering:

- Remote Filtering Client Pack - Enables deployment of Remote Filtering Client to client machines.
- Remote Filtering Server - Allows filtering of clients outside a network firewall.

Interoperability:

- Linking Service - Gives Websense Data Security access to User Service and Master Database categorization.
- Sync Service - In Websense Web Security Gateway Anywhere deployments, communicates policy and reporting data between hybrid and on-premises components.
- Directory Agent - In Websense Web Security Gateway Anywhere deployments, collates user and group information for use by hybrid filtering.

©1996-2011 Websense, Inc.

InstallAnywhere

Cancel Help Previous Next

Help Close

©1996-2011 Websense, Inc.

Installing Remote Filtering Server

The screenshot displays the 'Websense TRITON Setup' window. The main window is titled 'TRITON Unified Security' and shows a 'Custom Installation' screen. On the left, there is a list of components to install: 'TRITON Infrastructure', 'Web Security v7.6.2.1449', 'Data Security', and 'Email Security'. The 'Web Security' component is selected and highlighted with a blue arrow. Below this list, there is a note about 'Microsoft SQL Server 2008 R2 Express for small customers' and a 'SQL Server Express' component to be installed.

Overlaid on top of the main window is the 'Websense Web Security / Web Filter v7.6.2 Installer' dialog box. This dialog has a 'Policy Server Connection' section. It contains a progress list on the left with the following items: Introduction, Subscription Agreement, Installation Type, Configuration, Installation Directory, Pre-Installation Summary, Installation, and Installation Complete. The 'Configuration' step is currently active. The main area of the dialog provides instructions on how to connect to a Policy Server, including a warning that all components must be the same version. It includes input fields for 'IP address' (containing '10.212.9.214') and 'Port' (containing '55806'). At the bottom of the dialog are 'Cancel', 'Help', 'Previous', and 'Next' buttons.

WebSense TRITON Setup
TRITON Unified Security

Custom Installation

Click the Install link for the component type you want to install. A component installation wizard will start. In the wizard, select the components you want to install on this machine.

- TRITON Infrastructure [Install](#)
- Web Security** v7.6.2.1449 [Install](#)
- Data Security [Install](#)
- Email Security [Install](#)
- SQL Server Express [Install](#)

Microsoft SQL Server 2008 R2 Express for small customers

WebSense Web Security / Web Filter v7.6.2 Installer

Remote Filtering Server Communication

- Introduction
- Subscription Agreement
- Installation Type
- Configuration**
- Installation Directory
- Pre-Installation Summary
- Installation
- Installation Complete

Enter the IP address or fully qualified domain name of the gateway or firewall machine, and then enter an unused port on this machine to receive Internet requests from Remote Filtering Clients (external port). Also enter an unused port visible only from within the network (internal port).

IP address or fully qualified domain name:

External port (10 to 65535):

Internal port (1024 to 65535):

©1996-2011 Websense, Inc.

InstallAnywhere

[Cancel](#) [Help](#) [Previous](#) [Next](#)

websense
Version 7.6

©1996-2011 Websense, Inc.

The screenshot shows two overlapping windows from the Websense installation process.

Background Window: Websense TRITON Setup

- Title: TRITON Unified Security
- Section: Custom Installation
- Text: Click the Install link for the component type you want to install. A component installation wizard will start. In the wizard, select the components you want to install on this machine.
- Components list:
 - TRITON Infrastructure [Install](#)
 - Web Security** v7.6.2.1449 [Install](#) (highlighted with a blue arrow)
 - Data Security [Install](#)
 - Email Security [Install](#)
- Bottom: Microsoft SQL Server 2008 R2 Express for small customers, SQL Server Express [Install](#)
- Logo: websense Version 7.6

Foreground Window: Websense Web Security / Web Filter v7.6.2 Installer

- Title: Remote Filtering Pass Phrase
- Progress list:
 - Introduction
 - Subscription Agreement
 - Installation Type
 - Configuration** (active)
- Configuration steps:
 - Installation Directory
 - Pre-Installation Summary
 - Installation
 - Installation Complete
- Text: Enter a pass phrase for Websense software to use to encrypt communication between Remote Filtering Client and Remote Filtering Server.
- IMPORTANT:** Keep a record of the pass phrase. You will need it to configure Remote Filtering Client.
- Form fields:
 - Pass phrase: [masked]
 - Moderate Confirm pass phrase: [masked]
- Feedback: Passwords match
- Buttons: Cancel, Help, Previous, Next
- Footer: ©1996-2011 Websense, Inc.

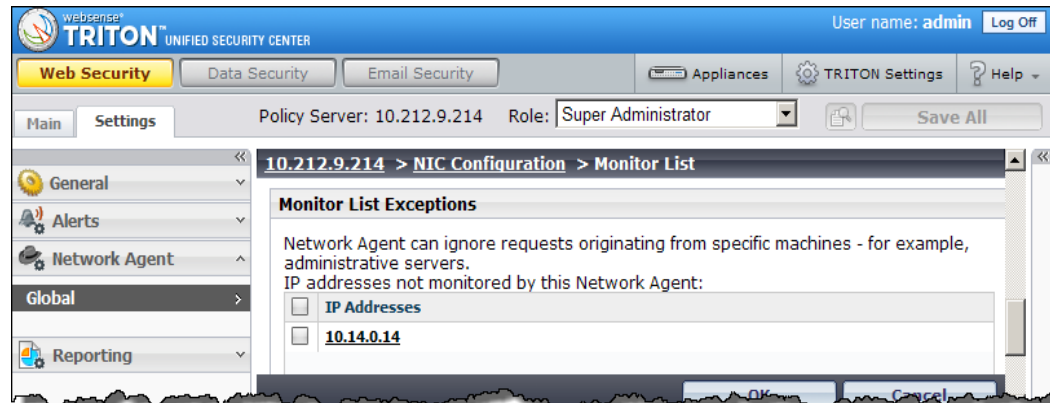
The screenshot shows two overlapping windows from the Websense installation suite. The background window is titled "Websense TRITON Setup" and "TRITON Unified Security". It features a "Custom Installation" section with a list of components: TRITON Infrastructure, Web Security (v7.6.2.1449), Data Security, and Email Security. The "Web Security" component is selected and highlighted with a blue arrow. Below this list, there is a section for "Microsoft SQL Server 2008 R2 Express for small customers" with a sub-option for "SQL Server Express".

The foreground window is titled "Websense Web Security / Web Filter v7.6.2 Installer". It displays a progress list on the left: Introduction, Subscription Agreement, Installation Type, Configuration (selected), Installation Directory, Pre-Installation Summary, Installation, and Installation Complete. The main area of this window is titled "Filtering Service Information for Remote Filtering". It contains the following text and fields:

- Text: "In order to filter requests from remote clients, Remote Filtering Server must be able to communicate with Filtering Service. Enter Filtering Service IP address and port information."
- Text: "Internal IP address:" followed by a text box containing "10.212.9.214".
- Text: "Translated IP address:" followed by an empty text box.
- Text: "Filtering port:" followed by a text box containing "15868".
- Text: "Block page port:" followed by a text box containing "15871".
- Text: "A firewall or other network device performs address translation between Filtering Service and Remote Filtering Server." with an unchecked checkbox.

At the bottom of the foreground window, there are "Cancel", "Help", "Previous", and "Next" buttons. The background window also has "Help" and "Close" buttons at the bottom right.

- Is Network Agent or an integration product configured to filter HTTP requests?
 - If so, then make sure that it does NOT filter requests going to or from the Remote Filtering Server machine.
 - **For Network Agent:** In TRITON - Web Security, go to *Settings > Network Agent > Global > IP_address > Network Interface Cards > NIC-x > Monitoring > Configure button > Monitor List Exceptions > Add*, then enter the Remote Filtering Server IP address.



- Review the remote filtering options within the manager.

The screenshot displays the Websense TRITON Unified Security Center interface. The top navigation bar includes 'Web Security', 'Data Security', and 'Email Security'. The user is logged in as 'admin'. The main content area is titled 'Remote Filtering' and contains an information box about remote filtering settings, followed by a section for configuring these settings, including a checkbox to block requests and a dropdown for the timeout interval.

Remote Filtering

About Remote Filtering Settings

Remote Filtering is used to filter HTTP, HTTPS, and FTP requests from clients outside the network firewall. The settings established here apply to all Remote Filtering clients.

Remote Filtering Settings

If the client cannot communicate with the Remote Filtering Server, all Internet requests can be permitted (default) or blocked (fail closed). For older clients (pre-v7.6), the timeout interval determines how long the client has to contact the server before the fail closed condition is enforced.

Block all requests when client is unable to connect to Remote Filtering Server

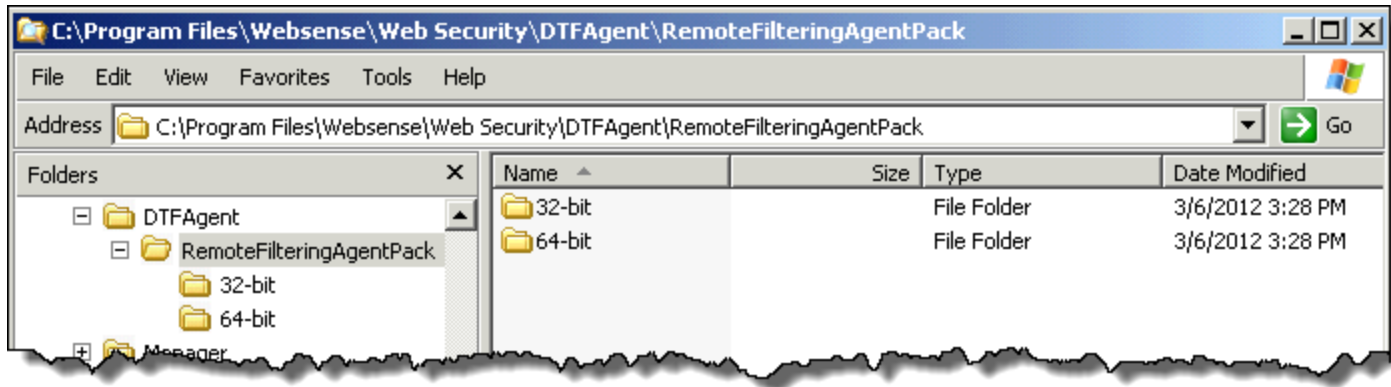
Timeout interval (client versions 7.5.x and earlier): 15 minutes

To enable logging for debugging purposes, specify a maximum size for the log file.

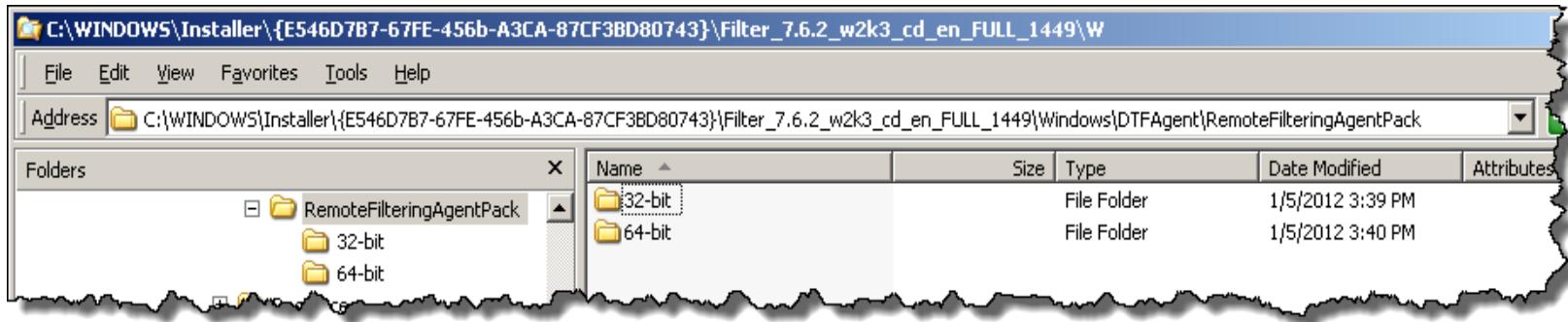
Maximum size for log file: 1 MB

- **To start using your remote filtering software, you must also:**
 1. **Obtain the Remote Filtering Client Pack.**
 2. **Create one or more client profiles.**
 - **Demonstration**
 3. **Install the Remote Filtering Client profile on computers.**
 - **Demonstration**

- Run the Websense Installer, select *Custom > Web Security*.
 - The client pack files are in the “32-bit” and “64-bit” subfolders under:
 - ... \Websense\Web Security\DTFAgent\RemoteFilteringAgentPack\

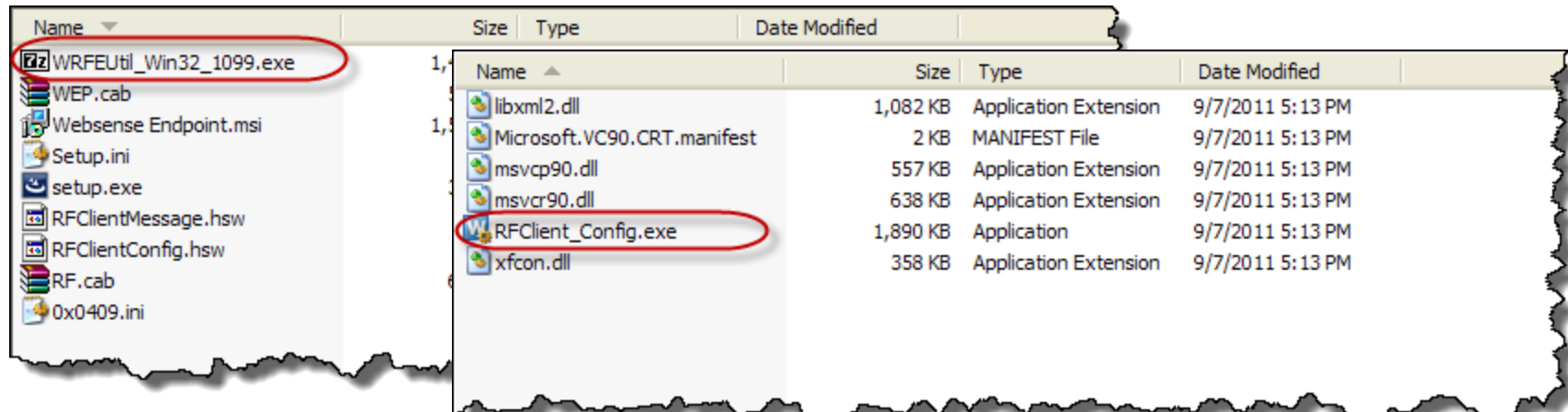


- Also available from within the decompressed installer directory.
 - *C:\WINDOWS\Installer\{E546D7B7-67FE-456b-A3CA-87CF3BD80743}\Filter_7.6.2_w2k3_cd_en_FULL_1449\Windows\DTFAgent\RemoteFilteringAgentPack*

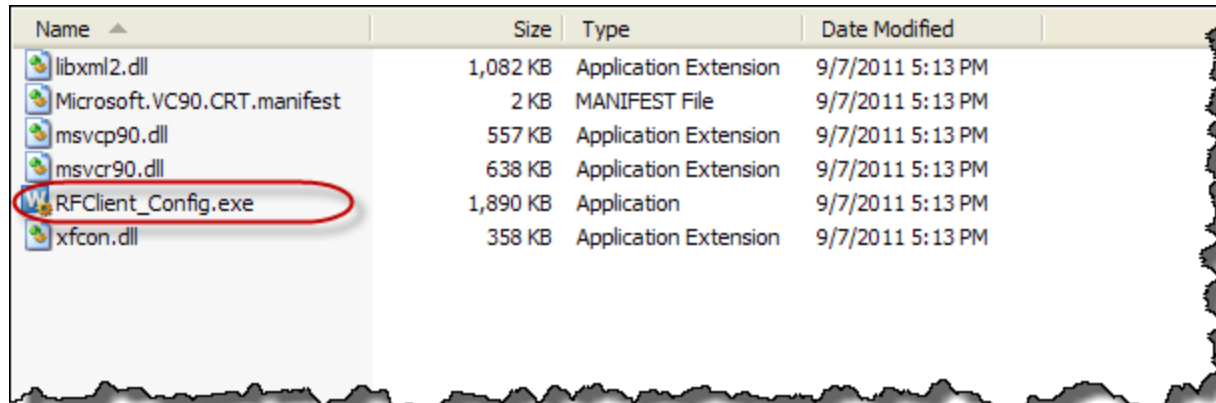


- The “Windows\Installer” directory is hidden by default. To display, select “Show hidden files and folders” in the Folder Options settings.
- This path is specific for v7.6.2 build 1449. Your path may differ slightly.

- You must create at least one profile (a customized installation package) to successfully deploy Remote Filtering Client.
 - The Remote Filtering Client Pack contains the Remote Filtering Client Configuration tool (**WRFEUtil_*platform_version*.exe**).
 - Double-click to extract the Client Configuration tool file.

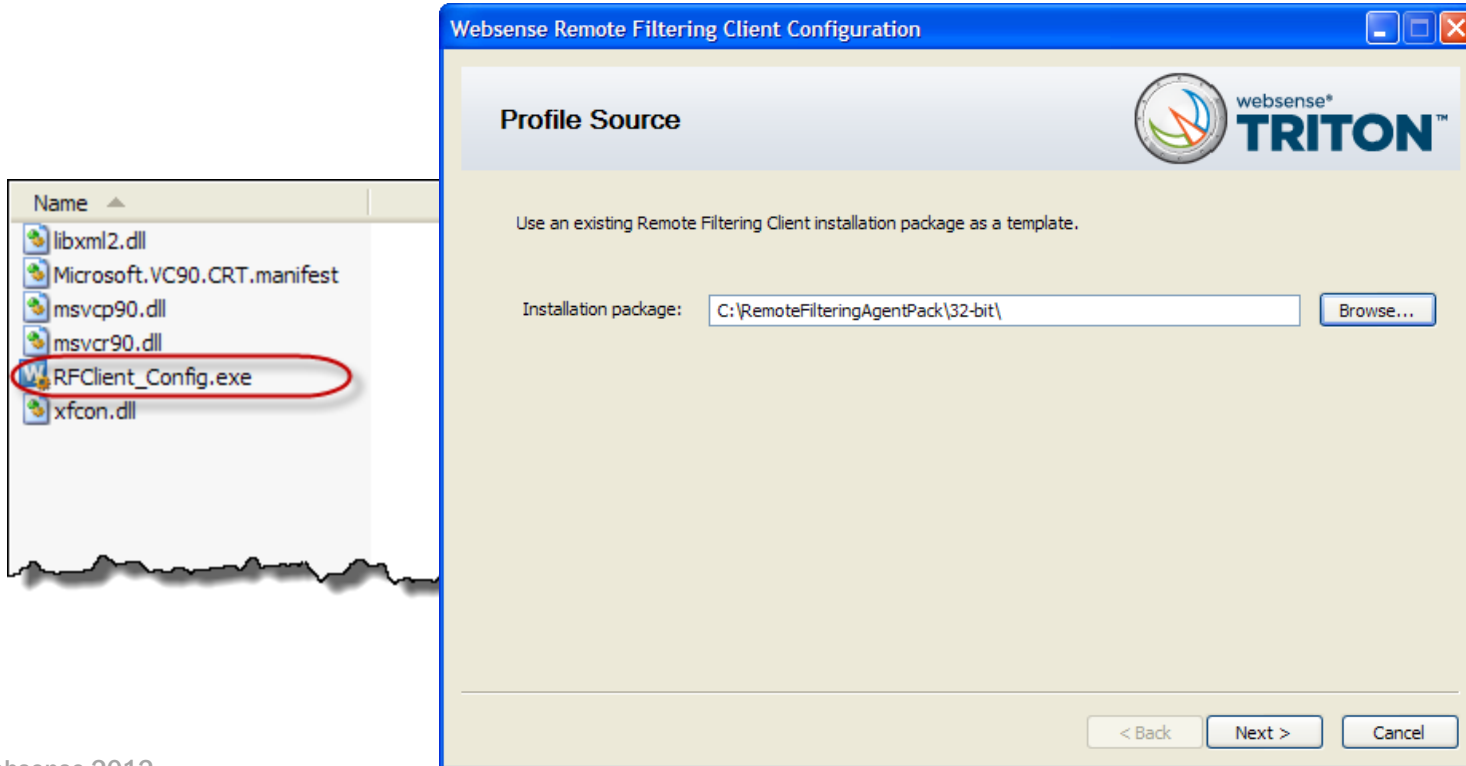


- Create your custom profile, double-click **RFClient_Config.exe**.

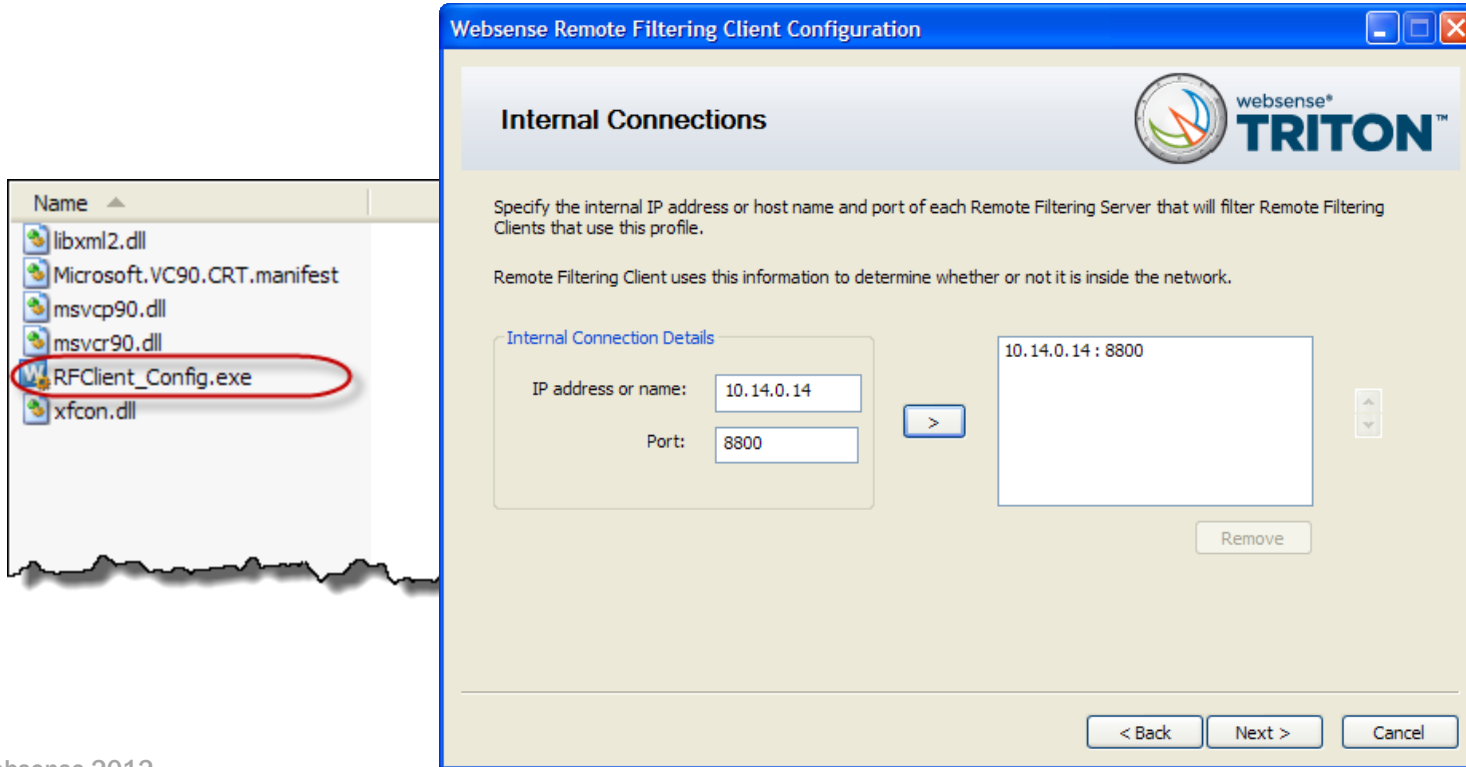


Name	Size	Type	Date Modified
libxml2.dll	1,082 KB	Application Extension	9/7/2011 5:13 PM
Microsoft.VC90.CRT.manifest	2 KB	MANIFEST File	9/7/2011 5:13 PM
msvcp90.dll	557 KB	Application Extension	9/7/2011 5:13 PM
msvcr90.dll	638 KB	Application Extension	9/7/2011 5:13 PM
RFClient_Config.exe	1,890 KB	Application	9/7/2011 5:13 PM
xfcon.dll	358 KB	Application Extension	9/7/2011 5:13 PM

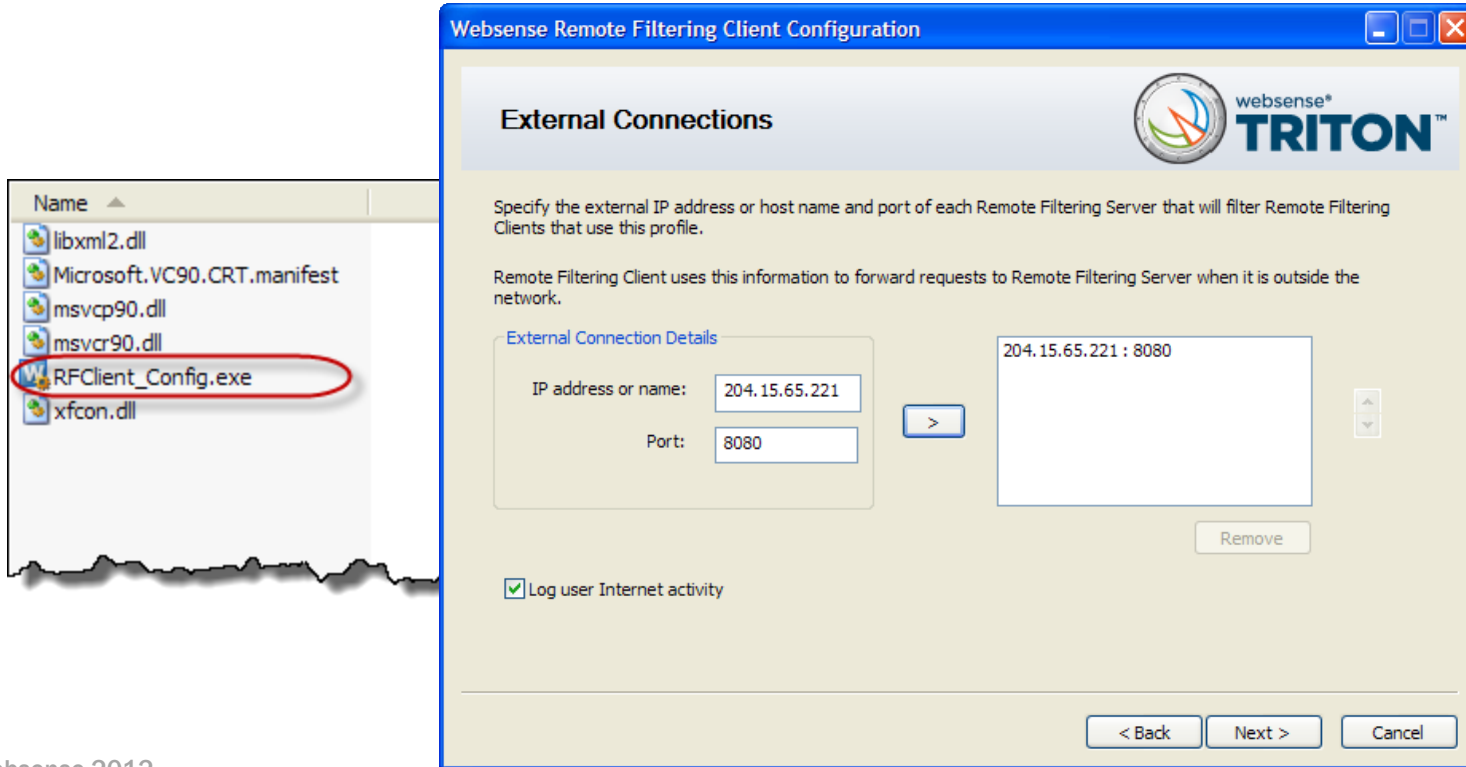
- Create your custom profile, double-click **RFClient_Config.exe**.



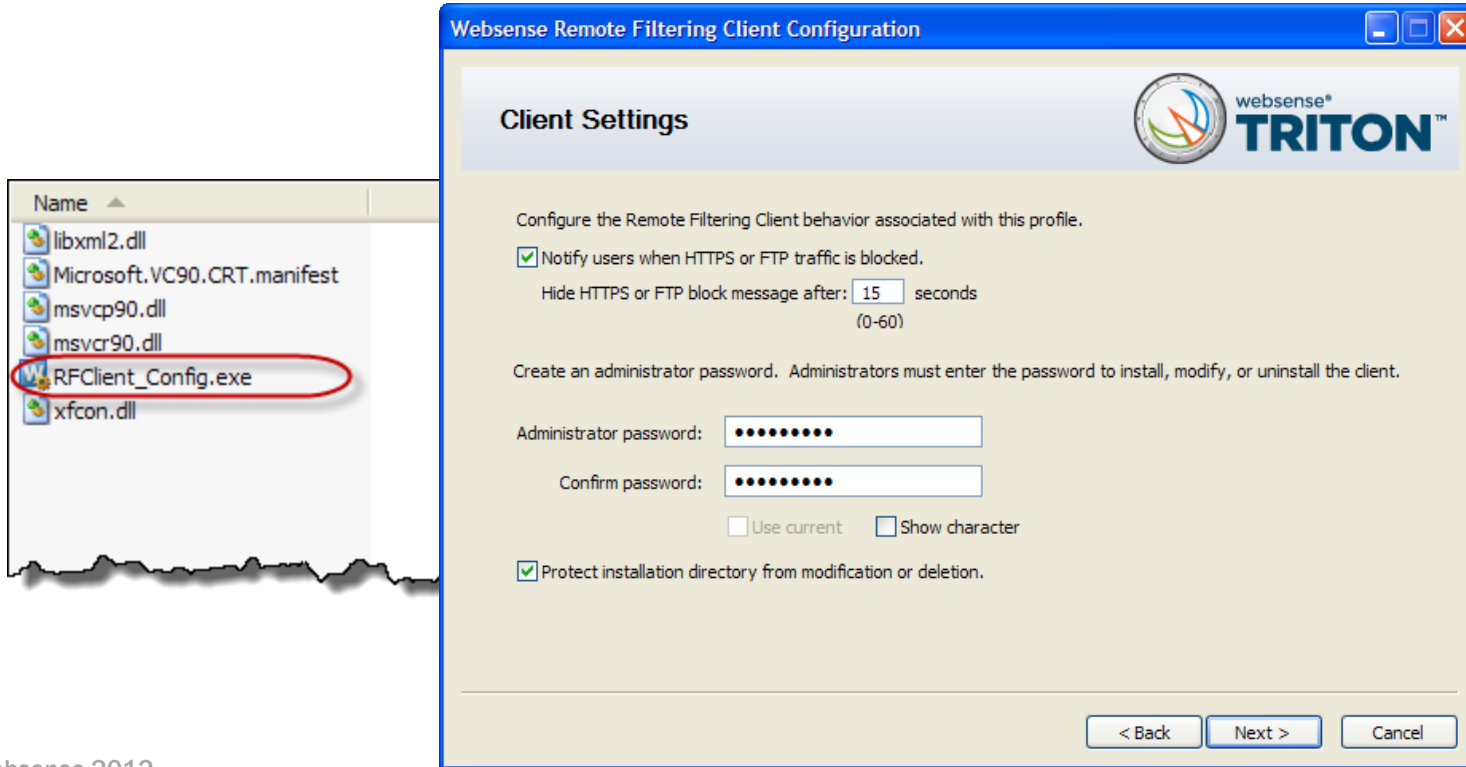
- Create your custom profile, double-click **RFClient_Config.exe**.



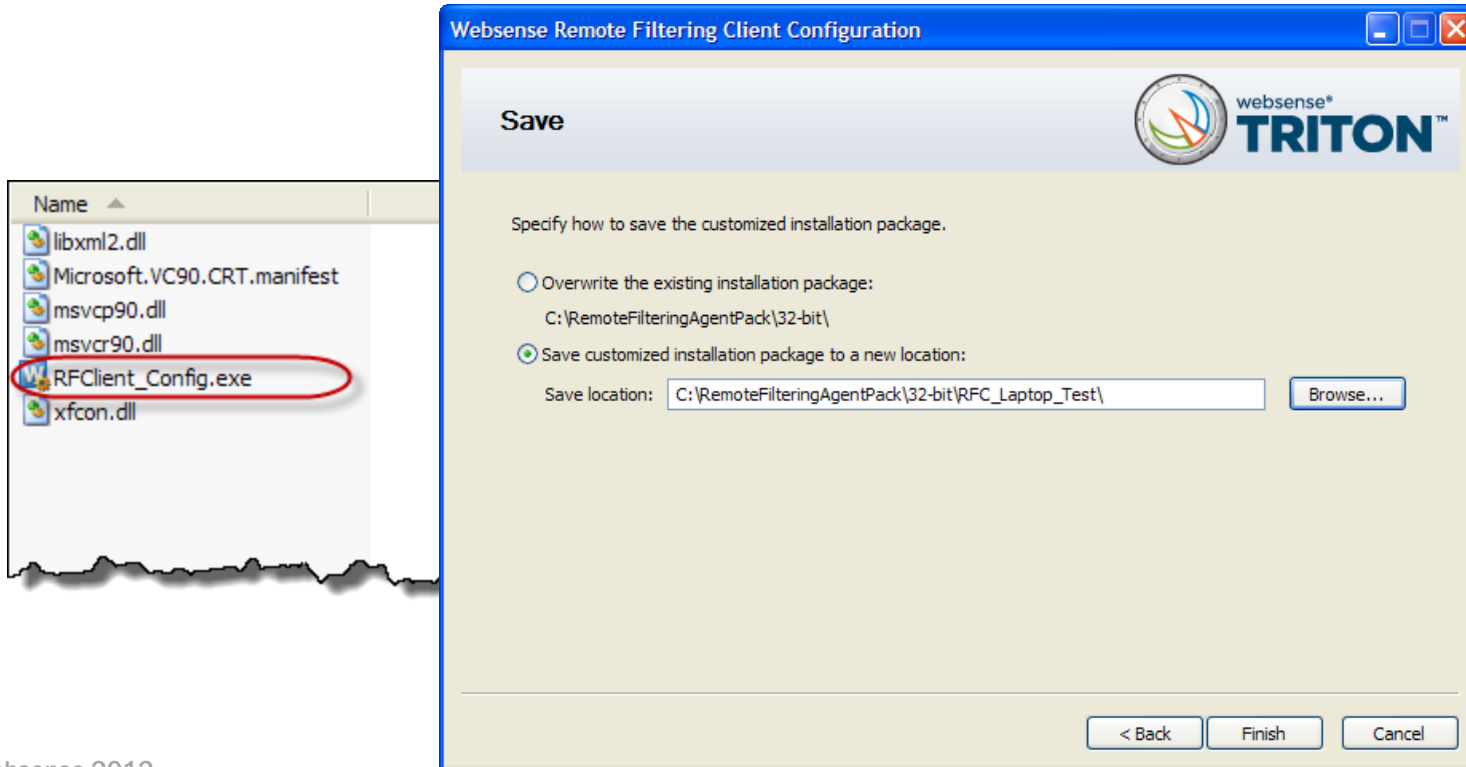
- Create your custom profile, double-click **RFClient_Config.exe**.



- Create your custom profile, double-click **RFClient_Config.exe**.

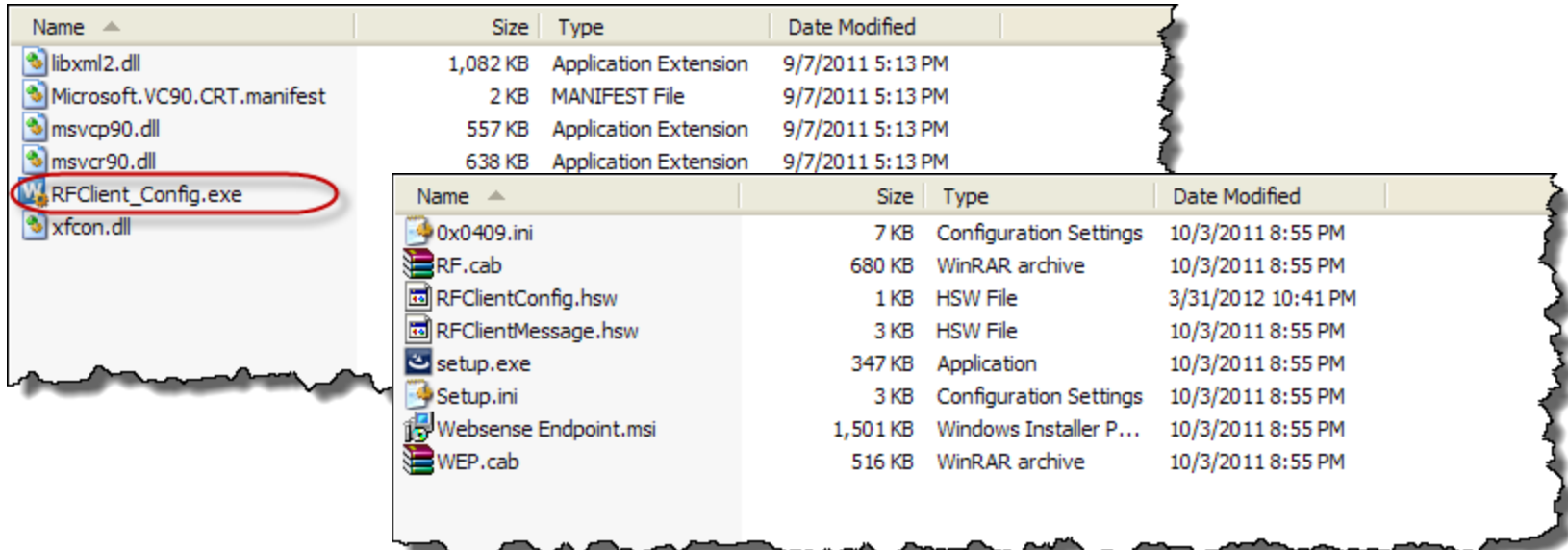


- Create your custom profile, double-click **RFClient_Config.exe**.

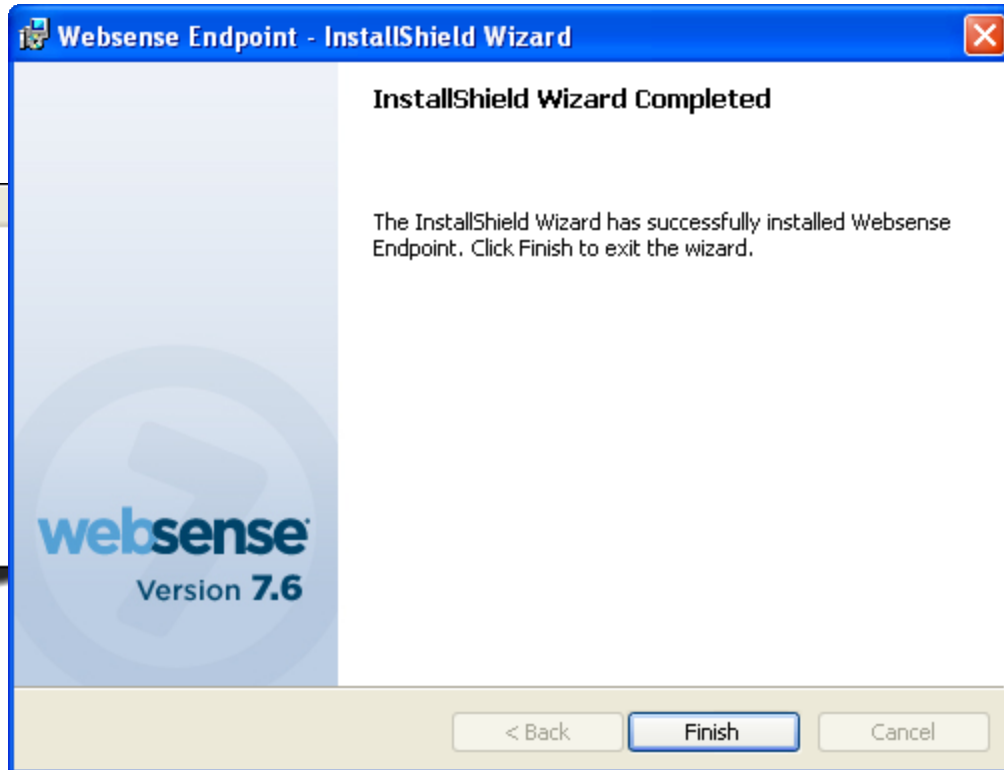
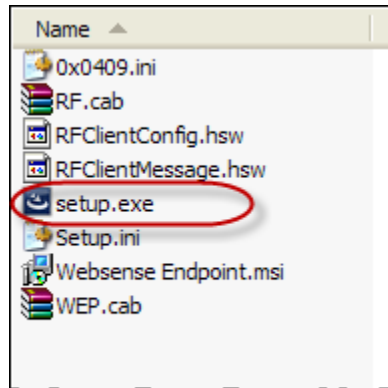


Create One Or More Client Profiles

- Create your custom profile, double-click **RFClient_Config.exe**.

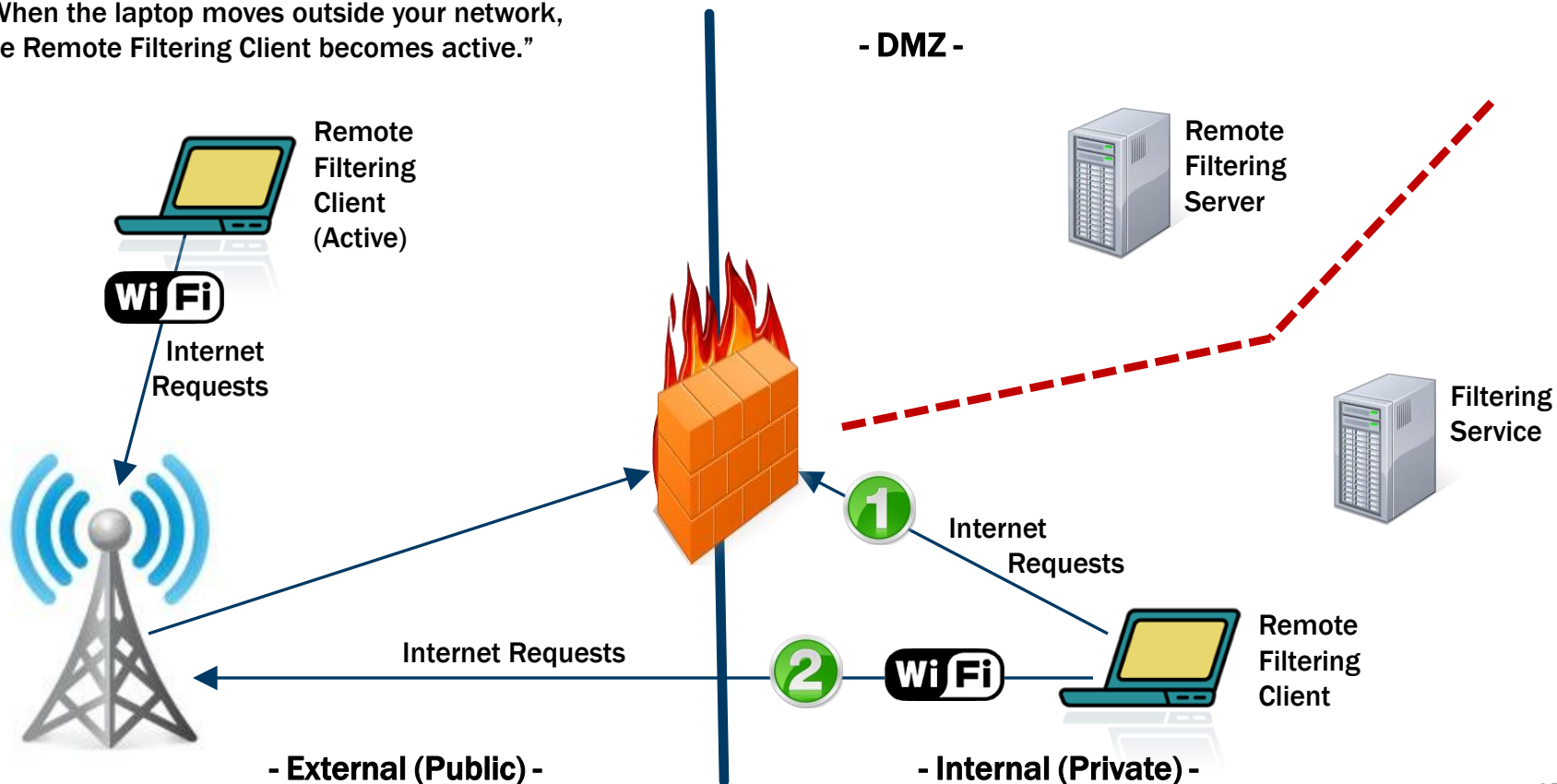


- The Remote Filtering Client install files, double-click **setup.exe**.



- **Remote Filtering Client software install.**
- **Internal block page delivered via network agent or integration.**
 - Note the internal IP address displayed in the URL.
- **External block page delivered via Remote Filtering Server.**
 - Note the external IP address displayed in the URL.

“When the laptop moves outside your network, the Remote Filtering Client becomes active.”



- Ensure the Remote Filtering Server service is running.
 - Service should restart successfully.
 - Review the Application Event log.
- Check port connectivity using **TELNET** command.
 - 55806 ~ Open to Policy Server (internal) from DMZ.
 - 15868, 15871 ~ Open to Filtering Service (internal) from DMZ.
 - 55880 ~ Open to Policy Broker (internal) from DMZ.
 - 8080 ~ Open to DMZ from external Remote Filtering Clients.
 - 8800 (Heart Beat) ~ Open to DMZ from internal network.
- Check the Server **WISP Proxy** settings.
 - **SecureWISPProxy.ini** file, located in ...\\Websense\\Web Security\\bin.

-

```
securewispproxy - Copy - Notepad
File Edit Format View Help
[SecureWISPProxy]
# The protocol used to for wrapping WISP requests raw|http|
secure
WispMode=secure
# Proxy Server parameters
ProxyIP=10.14.0.14
ProxyPort=8080
ProxyMaxConnections=10000
ProxyPublicAddress=204.15.65.221
# Time to wait for WISP requests, handshake, etc., seconds
ProxyTimeout=120
# HeartBeat Server Parameters
HeartBeatPort=8800
HeartBeatTimeout=5
```

-

-

securewispproxy - Copy - Notepad

File Edit Format View Help

Web-Filtering Connection parameters

WebFilterIP=10.212.9.214

WebFilterPort=15868

WebFilterMaxConnections=50

Time to wait for WISP lookup responses, seconds

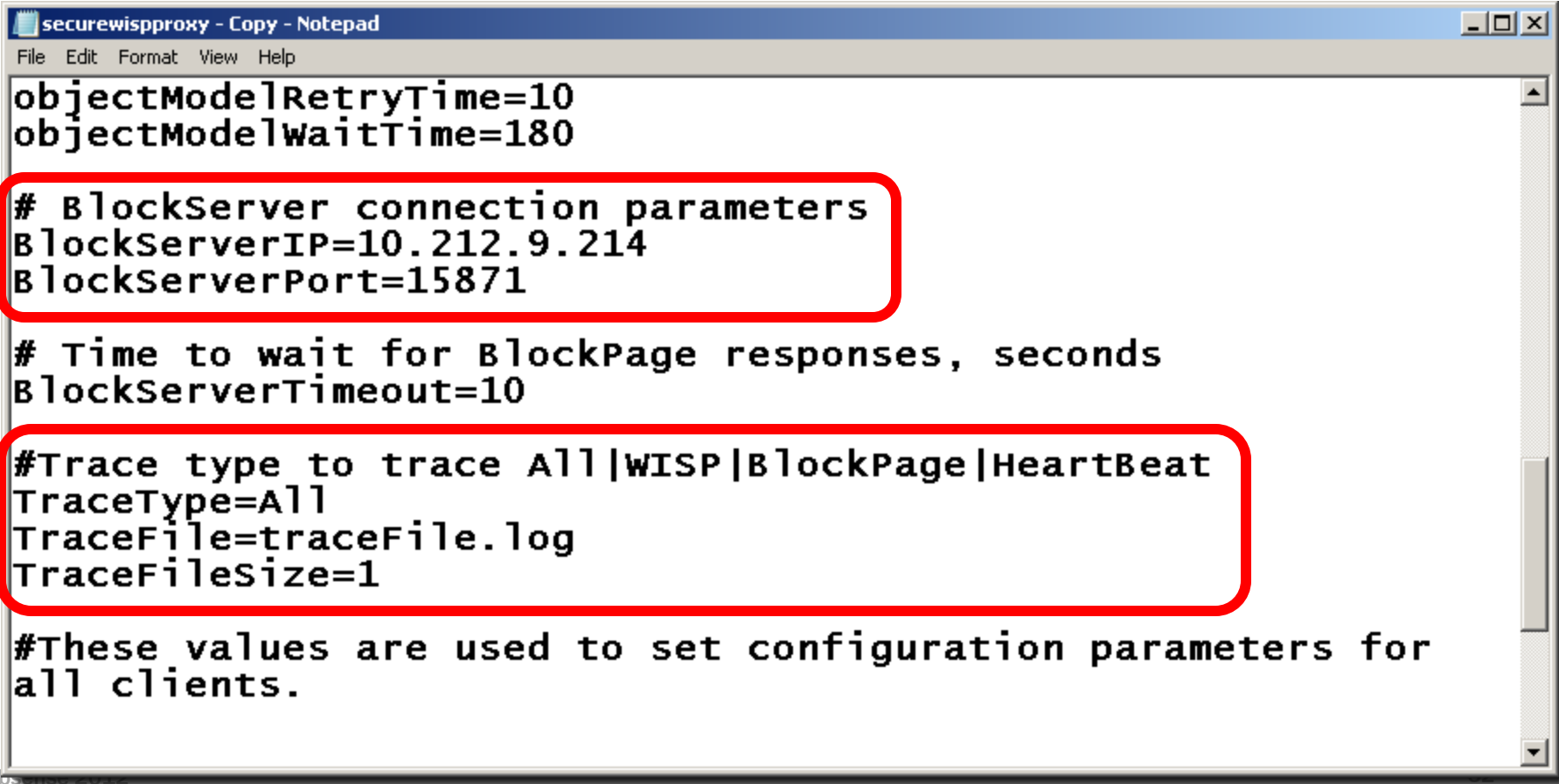
WebFilterTimeout=10

Object Model connection parameters

objectModelIP=10.212.9.214

objectModelPort=55880

objectModelToken=0542A478B62AB7773AE226F8471E4DD12E7AB78DEFF2
1A3A151621EFBF5A9855B2B5560F020CDB3AF84BE45F001619D8F20547144
7AFA83DF5CD95EAB6D9BBA0347777C8179F58DA2317511783F417639276A2
A11BC0783E3D0BB5D55BB582252461DDC09966F632601447B0A07E92A7AB3
CD4395D7B78B3CA3E9634C3B60EE0458FC22159ADDC219C4F401815FAD21B
D427175DBD1B06B28465CC20C41AD452DE2B7798A71CF17E

- 

```
securewispproxy - Copy - Notepad
File Edit Format View Help
objectModelRetryTime=10
objectModelWaitTime=180
# BlockServer connection parameters
BlockServerIP=10.212.9.214
BlockServerPort=15871
# Time to wait for BlockPage responses, seconds
BlockServerTimeout=10
#Trace type to trace All|WISP|BlockPage|HeartBeat
TraceType=All
TraceFile=traceFile.log
TraceFileSize=1
#These values are used to set configuration parameters for
all clients.
```

securewispproxy - Copy - Notepad

File Edit Format View Help

```
#Trace type to trace All|WISP|BlockPage|HeartBeat
```

```
TraceType=All
```

```
TraceFile=traceFile.log
```

```
TraceFileSize=1
```

```
#These values are used to set configuration parameters for  
all clients.
```

```
# Turns HTTPS and/or FTP filtering on or off on the RF client
```

```
[1 for on, 0 for off]
```

```
FilterHTTPS=1
```

```
FilterFTP=1
```

```
#Heartbeat Retry Interval
```

```
#Range from 0 minute to 1440 minutes (24 hours) and the  
default value is 15 minutes
```

```
HeartbeatRetryInterval=15
```

- Examine the Remote Filtering Server log file.
 - `traceFile.log`
- Check server for excessive connections
 - `netstat -an | find "15868" /C`
 - `netstat -an | find "15871" /C`
- Reset pass phrase from ...**\Websense\Web Security\bin** folder.
 - `SecureWISPProxy -p <new_pass_phrase>`
- **NOTE: Remote Filtering Server has no registry or file protection.**
- **Two Network Interface Cards (different networks) not supported.**
- **Obtain a packet capture.**

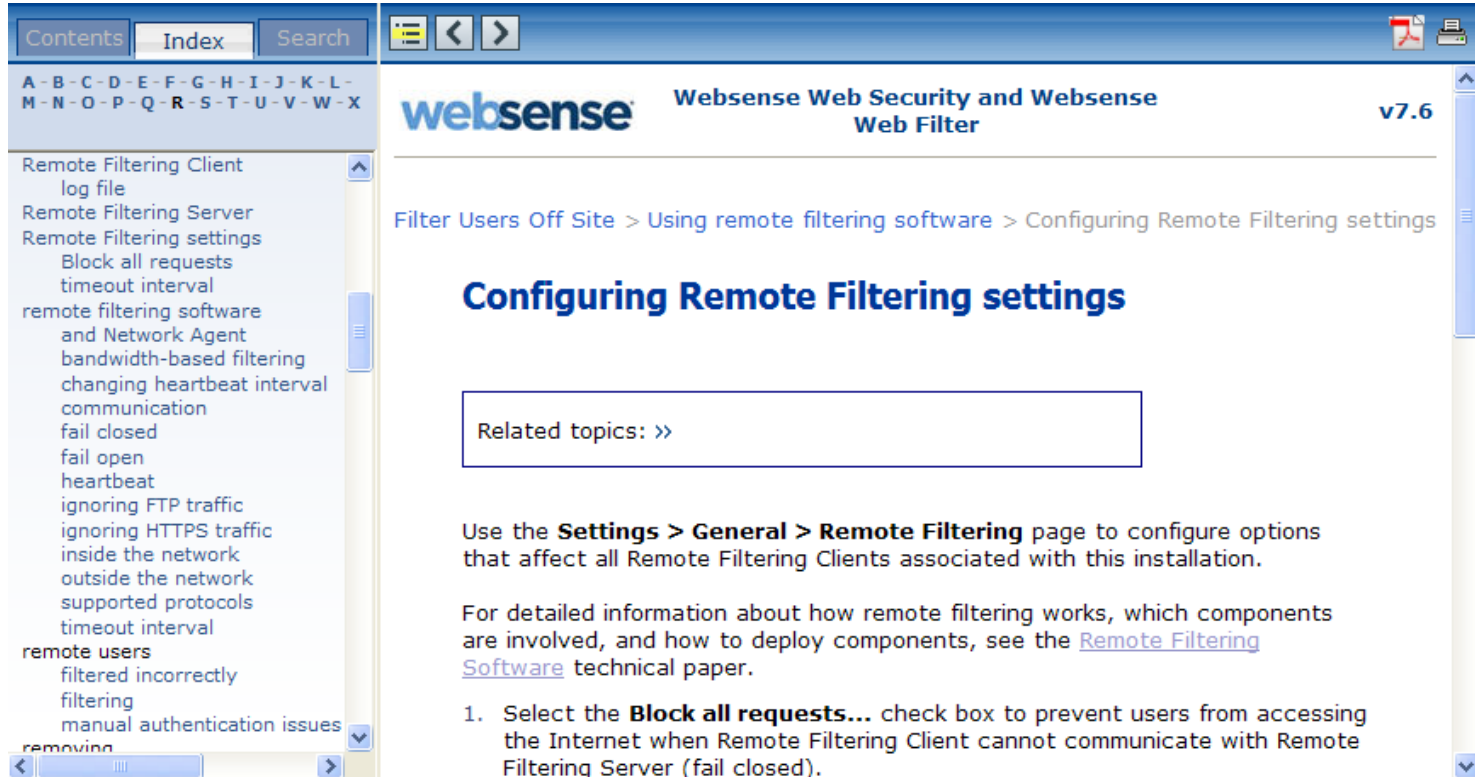
- **Ensure the Websense Desktop Client service is running.**
 - Restart client service or end client machine.
 - `wepsvc.exe -stop -password <passphrase> WSRF`
 - `wepsvc.exe -start WSRF`
 - Websense service and files are protected.
- **Check port connectivity using TELNET.**
 - 8080 ~ Open to DMZ for external Remote Filtering Clients.
 - 8800 (Heart Beat) ~ Open to DMZ from internal network.
 - 8800 (Heart Beat) ~ Blocked to DMZ from external (public) access.
- **Examine the Remote Filtering Client log file.**
 - `DebugDump.txt`

- **Check ports, IP addresses, and pass phrase settings.**
 - Run the profile creator utility: `RFCClient_Config.exe`
- **Gather log files for Websense techsupport.**
 - Run the file collector utility: `ClientInfo.exe`
- **Packet capture**

- See the Remote Filtering Software technical paper for more information about installing, configuring, and using remote filtering.
 - [PDF](#) or [HTML](#)
- [Deployment and Installation Center](#) for system requirements, integration configuration, and installation of all Websense components.

- [How do I deploy v7.6 Remote Filtering Clients?](#)
- [How to create a Remote Filtering Client profile for v7.6](#)
- [How to silently install Remote Filtering Client v7.6](#)
- [How do I modify the v7.6 Remote Filtering Client profile?](#)
- [v7.6 Remote Filtering with V-Series Appliance](#)
- [How to stop the v7.6 Remote Filtering Client service](#)
- [How to verify communication between the Remote Filtering Client and Server](#)
- [How to enable Remote Filtering debugging and Remote Filtering Client tracing](#)
- [Troubleshooting remote filtering software](#)

- Use the TRITON –Web Security management help system.



Contents Index Search

A - B - C - D - E - F - G - H - I - J - K - L - M - N - O - P - Q - R - S - T - U - V - W - X

Remote Filtering Client log file
Remote Filtering Server
Remote Filtering settings
Block all requests
timeout interval
remote filtering software and Network Agent bandwidth-based filtering
changing heartbeat interval
communication
fail closed
fail open
heartbeat
ignoring FTP traffic
ignoring HTTPS traffic
inside the network
outside the network
supported protocols
timeout interval
remote users
filtered incorrectly
filtering
manual authentication issues
removing

websense Websense Web Security and Websense Web Filter v7.6

Filter Users Off Site > Using remote filtering software > Configuring Remote Filtering settings

Configuring Remote Filtering settings

Related topics: >>

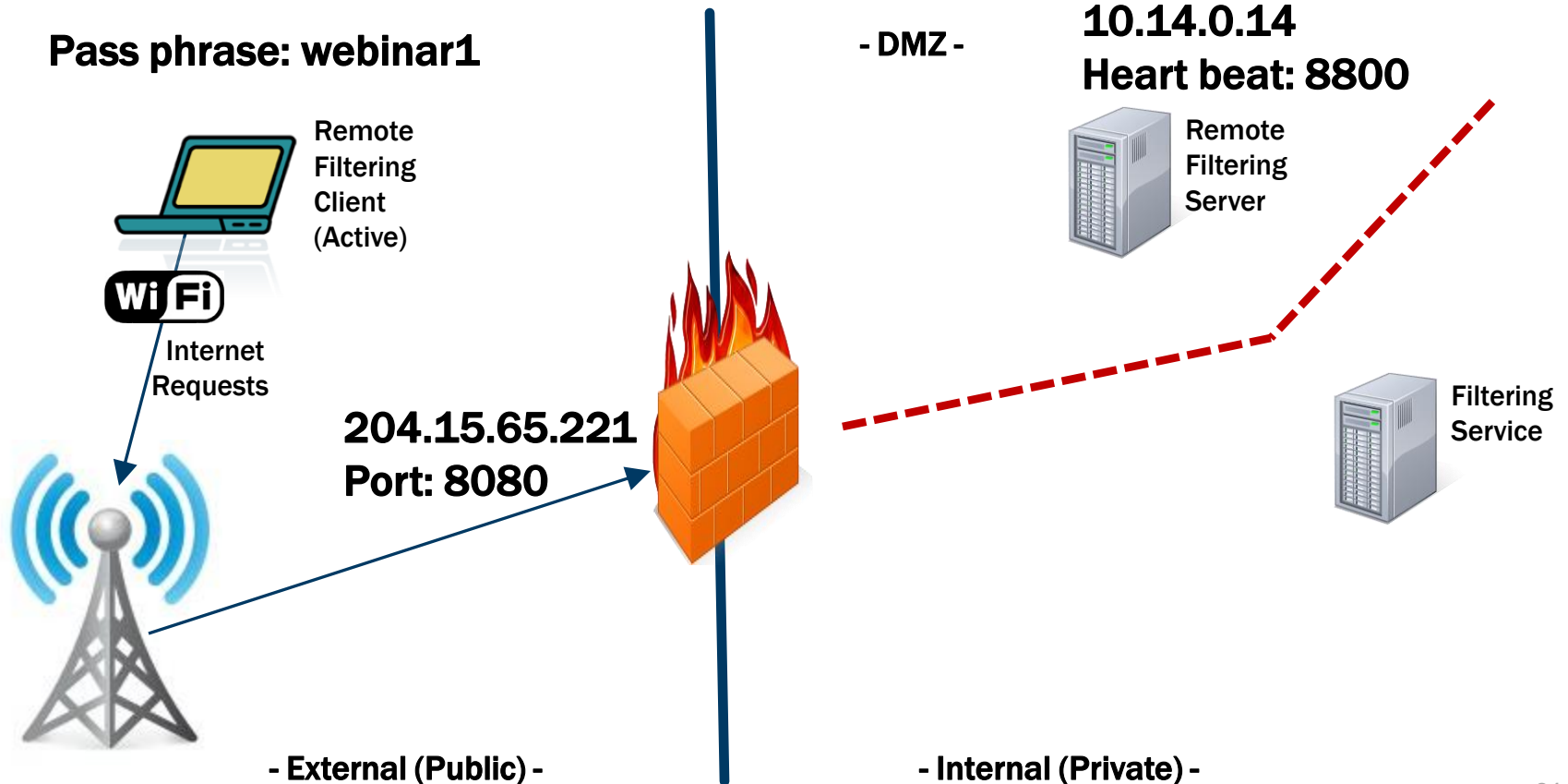
Use the **Settings > General > Remote Filtering** page to configure options that affect all Remote Filtering Clients associated with this installation.

For detailed information about how remote filtering works, which components are involved, and how to deploy components, see the [Remote Filtering Software](#) technical paper.

1. Select the **Block all requests...** check box to prevent users from accessing the Internet when Remote Filtering Client cannot communicate with Remote Filtering Server (fail closed).

- Learned how remote filtering software works.
- Installation
 - Remote Filtering Server
 - Remote Filtering Client
- Troubleshooting steps.
- Know where to find helpful information.

TEST – Install your Remote Filtering Client



Webinar Update

**Title: Identifying Users with Logon Agent:
Implementation and Troubleshooting**

Date: May 23, 2012

Time: 8:30 A.M. PDT (GMT -8)

How to register: [http://www.websense.com/content/
SupportWebinars.aspx](http://www.websense.com/content/SupportWebinars.aspx)

