Filtering remote users with Websense remote filtering software v7.6

Websense Support Webinar April 2012
Title:
- Support Specialist

Accomplishments:
- 9 years supporting Websense products

Qualifications:
- Technical Support Mentor
- Product Trainer
Goals And Objectives

• 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
Introduce – Remote Filtering Software

• 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.
System Requirements – Remote Filtering Client

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

<table>
<thead>
<tr>
<th>Hardware Recommendations</th>
<th>Operating System Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Pentium 4 1.8 GHz</td>
<td>• Windows 7 (x86 and x64)</td>
</tr>
<tr>
<td>• Free disk space: 25 MB for installation; 15 MB to run the application</td>
<td>• Windows XP SP2 and above (x86 and x64)</td>
</tr>
<tr>
<td>• 512 MB RAM</td>
<td>• Windows Vista SP1 and above (x86 and x64)</td>
</tr>
<tr>
<td></td>
<td>• Windows Server 2003 SP2 and R2 SP2 and above (x86 and x64)</td>
</tr>
<tr>
<td></td>
<td>• Windows Server 2008 SP1 and above (x86 and x64)</td>
</tr>
<tr>
<td></td>
<td>• Windows Server 2008 R2 (x64)</td>
</tr>
</tbody>
</table>
System Requirements – Remote Filtering Server

- Version 7.6.x is supported on the following operating systems:
  - Red Hat Enterprise Linux 4 and 5.
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.
- Install only one primary Remote Filtering Server per Filtering Service.
How Remote Filtering Works

• 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.
When The Client Is Outside Your Network

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.
Recap – Examining The Heartbeat Attempt

Active Remote Filtering Client

- External (Public) -

Remote machine

Browser

Internet Request

Remote Filtering Client

External Firewall

Proxy port

External Firewall

Proxy port

Remote Filtering Server

Heartbeat

Passive Remote Filtering Client

- DMZ -

Remote Filtering Client

- Internal (Private) -

Client machine (inside the network)

Browser

Remote Filtering Client

Websense Network Agent or integration product

Internet request

Internal Firewall

Heartbeat

©Websense 2012
Identify Remote Users – Determining The Policy

• 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.
Identify Remote Users – Determining The Policy

• 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.

• 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.

• Policies assigned to computer IP or IP range do not apply for externally filtered clients.
Remote And Local Filtering Differences

- 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 And Local Filtering Differences

• 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.
Payment Portals

• 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
Recap: Introducing Remote Filtering Software

- 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)
Installing Remote Filtering Software

• 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
Preparing for installation

- 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.

<table>
<thead>
<tr>
<th>Port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>40000</td>
<td>Can be closed after installation.</td>
</tr>
<tr>
<td>55880</td>
<td>Broker Service port. From Remote Filtering Server to Policy Broker.</td>
</tr>
<tr>
<td>15868</td>
<td>Filtering Service Port. From Remote Filtering Server to Filtering Service.</td>
</tr>
<tr>
<td>15871</td>
<td>Block Page Port. Enables Filtering Service to send block messages. If not open, users are still blocked but do not receive a block message.</td>
</tr>
</tbody>
</table>

- For remote filtering to function properly, leave these ports open.
Preparing for installation

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

<table>
<thead>
<tr>
<th>Port</th>
<th>Description</th>
</tr>
</thead>
</table>
| 8080  | **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.

<table>
<thead>
<tr>
<th>Port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8800</td>
<td><strong>Close</strong> access to the heartbeat port on the external firewall from computers located outside the network firewall.</td>
</tr>
</tbody>
</table>
Preparing for installation

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

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

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

- **Internal**
  - 8800

* May close these ports after installation.
Installing Remote Filtering Server

1. Preparing to install

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

This is the main installer window. It shows installation type and status. It also opens component installation wizards, depending on your installation choices. If current version Websense components are found on this machine, this window offers options to modify or remove those components.

Prior to installation, please review installation and deployment instructions available in the Websense Technical Library (www.websense.com/library).

Installation Type

Select the components to be installed on this machine:

- TRITON Unified Security Center
- Web Security
- Date Security
- Email Security

An email security mode appliance must already be in your network. [Data Security will be selected automatically to enable Email DLP features].

- Websense Web Security All
- Custom

Select this option to choose individual components for installation.
Installing Remote Filtering Server

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.

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 (example).

Interoperability:
- Linking Service - Extends Websense Data Security access to Users 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.

Microsoft SQL Server 2008 R2 Express for small customers
SQL Server Express

©Websense 2012
Installing Remote Filtering Server

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
Web Security v7.6.21449
Data Security
Email Security
SQL Server Express

Policy Server Connection
Policy Server facilitates communication between Websense software components. Enter the IP address and port that the components that you are installing should use to communicate with Policy Server.

Warning: To successfully deploy Websense software, all components on all machines must be the same version.

IP address: 10.212.9.214
Port: 8880
Installing Remote Filtering Server

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.

Remote Filtering Server Communication

Remote Filtering Clients must be able to communicate with this machine regardless of whether they are inside or outside the network firewall.

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:
201.15.05.221

External port (10 to 65535):
0000

Internal port (1024 to 65535):
0000
Installing Remote Filtering Server

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.
Installing Remote Filtering Server

- 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.
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\
Obtain The Remote Filtering Client Pack

- 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.

- Double-click to extract the Client Configuration tool file.
Create One Or More Client Profiles

• Create your custom profile, double-click RFClient_Config.exe.
Create One Or More Client Profiles

• Create your custom profile, double-click **RFClient_Config.exe**.
Create One Or More Client Profiles

• Create your custom profile, double-click **RFClient_Config.exe**.
Create One Or More Client Profiles

- Create your custom profile, double-click **RFClient_Config.exe**.
Create One Or More Client Profiles

- Create your custom profile, double-click RFClient_Config.exe.
Create One Or More Client Profiles

• 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 install files]

![InstallShield Wizard Completed]

**The InstallShield Wizard has successfully installed Websense Endpoint. Click Finish to exit the wizard.**
• 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.”

Remote Filtering Server

Remote Filtering Client (Active)

Internet Requests

- DMZ -

Filtering Service

Internet Requests

- External (Public) -

Internet Requests

- Internal (Private) -

Remote Filtering Client

©Websense 2012
Troubleshooting – Remote Filtering Server

• 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.
  – SecureWISPPProxy.ini file, located in ...\Websense\Web Security\bin.
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 ...

Troubleshooting – Remote Filtering Server
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 ...

```
# 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 0542A478BC2A8773AE226F8471E4DD12E7AB78DEFF21A3A151621E6BF5A9855B2B5560F020CDB3AF84BE45F001619D8F2054741447AFA83DF5CD95EAB6D9BAA0347777C8179F58DA2317511783F417639276A2A11BC0783E3D0BB5D55BB582252461DDC09966F632601447B0A07E92A7AB3CD4395D7B78B3CA3E9634C3B60EE0458FC22159ADDC219C4F401815FAD21BD427175DB1B06B28465CC20C41AD452DE2B7798A71CF17E
```
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.

Troubleshooting – Remote Filtering Server

```plaintext
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.
```
Troubleshooting – Remote Filtering Server

- 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.

---

#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
Troubleshooting – Remote Filtering Server

- 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.
  - SecureWISPPProxy -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.
  - `wedsvc.exe -stop -password <passphrase> WSRF`
  - `wedsvc.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`
Troubleshooting – Remote Filtering Client

- Check ports, IP addresses, and pass phrase settings.
  - Run the profile creator utility: RFClient_Config.exe

- Gather log files for Websense techsupport.
  - Run the file collector utility: ClientInfo.exe

- Packet capture
Additional Information

• 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.
Additional Information

- 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
Additional Information

• Use the TRITON –Web Security management help system.

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).
Recap: Remote Filtering Software

• 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

Pass phrase: webinar1

Remote Filtering Client (Active)

Internet Requests

204.15.65.221
Port: 8080

- External (Public) -

10.14.0.14
Heart beat: 8800

Remote Filtering Server

Filtering Service

- DMZ -

- Internal (Private) -
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
Questions