



## Best practices for Websense Network Agent, Microsoft ISA Server, and Cisco PIX firewall integrations

**Websense Support Webinar July 2009**

# Goals and objectives

- Deployment recommendations for Network Agent
- Websense Standalone deployment using Network Agent
- Integrating Websense Filtering Service with Microsoft ISA Server
- Integrating Websense Filtering Service with Cisco PIX Firewall
- Troubleshooting deployments with Network Agent
- Troubleshooting ISAPI plug-in
- Troubleshooting tips for Cisco PIX integration

# Webinar Presenter



**Ravi Desai**

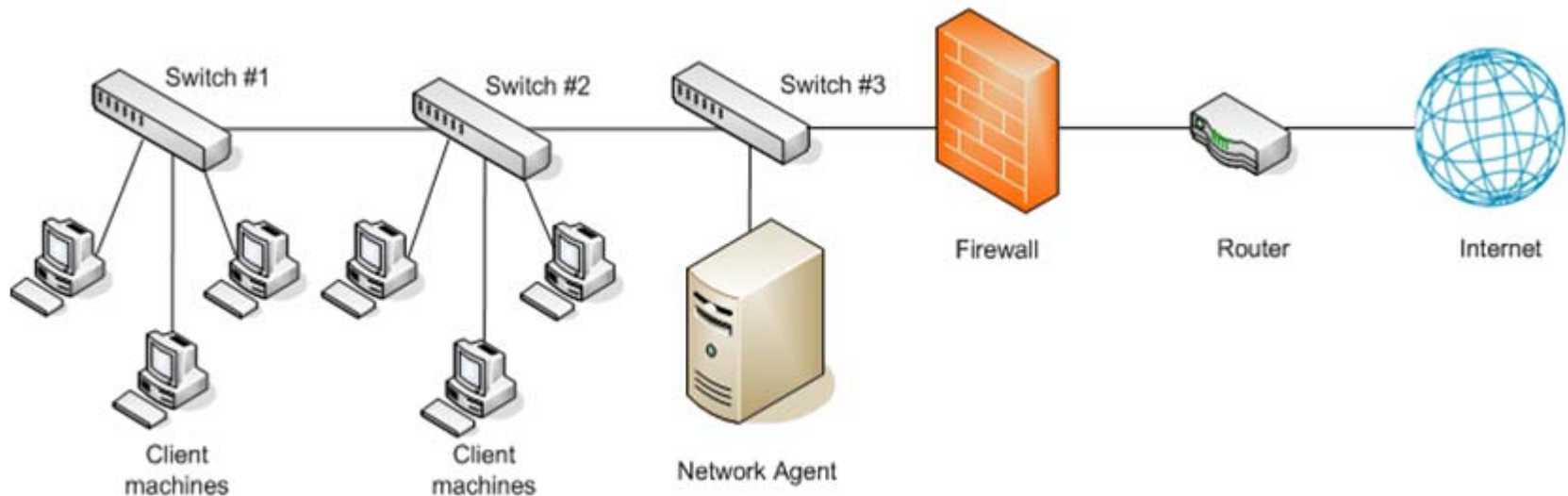
- Title: Tech Support Specialist
- Accomplishments:
  - Over 2 years supporting Websense products
- Education / Certifications:
  - B.Eng (Hons) Computer Systems and Networks
  - MCP
  - CCNA
  - WCWSA – Websense Certified Web Security Associate
- Qualifications:
  - New Hire Training
  - v7 Tech Support Training
- For additional information:  
[www.websense.com/support/](http://www.websense.com/support/)

# Network Agent Deployment

- Websense Network Agent deployment.
  - Also known as standalone deployment.
  - Filtering Service needs to be installed as standalone.
  - Enables filtering of all protocols in a standalone installation.
  - Can be installed along with an integration product to monitor and filter non-HTTP/HTTPS traffic and for bandwidth calculation.
  - Deploy Network Agent according to the network topology.
  - Switched Environment – Network Agent should be placed closely to the external firewall/router. For example, if the firewall connects to the core switch then Network Agent should connect to this switch.

# Network Agent Deployment

- Network Agent must be able to detect traffic coming from all machines in the network. Traffic from both switch#1 and switch#2 goes through switch#3 into the firewall
- Port on Switch#3 to which Network Agent is connected must be configured to span or mirror the port to which the firewall is connected.



# Network Agent Deployment

- In order for Network Agent to see the traffic going to the gateway, port spanning needs to be configured on the switch.
- Port spanning configuration depends on the switch vendor.
- Higher-end switches support **bidirectional** port spanning, which allows the same network interface card (NIC) to both listen (monitor traffic) and send on the same port.

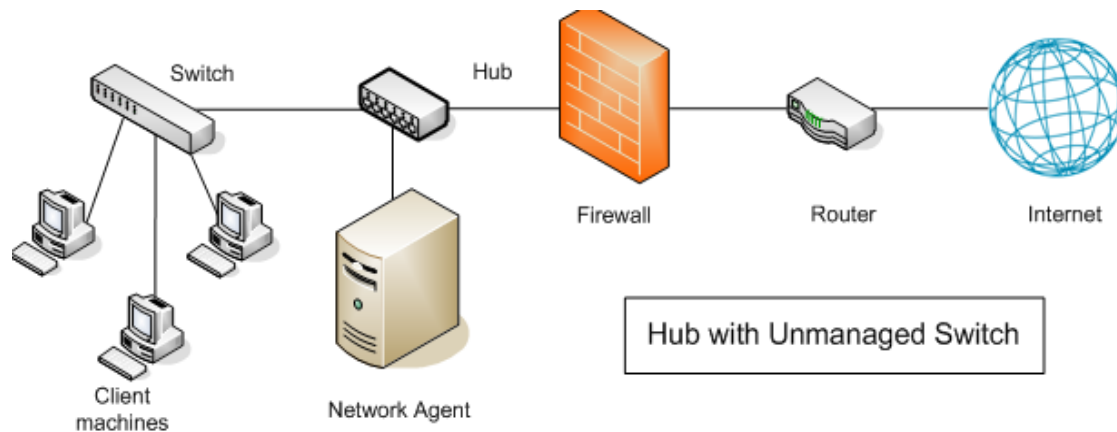
# Network Agent Deployment

- Low-end to mid-range switches may support a more limited form of port spanning: the NIC can monitor, but not send. In this type of environment, the Network Agent machine needs to have 2 NICs: one for normal network communication and one dedicated to monitoring traffic.
  - Both NICs connect to the same switch as the internal interface of the gateway device.
  - The NIC used to monitor traffic must connect to the switch span port.
  - Teamed NICs are not supported.
- If your switch does not support port spanning then a hub can be used.

# Network Agent Deployment – Hub

## Hub Environment

- Must be a true hub, traffic for all ports must be visible on every port
- Network Agent requires a “dumb” hub with no management or built-in intelligence



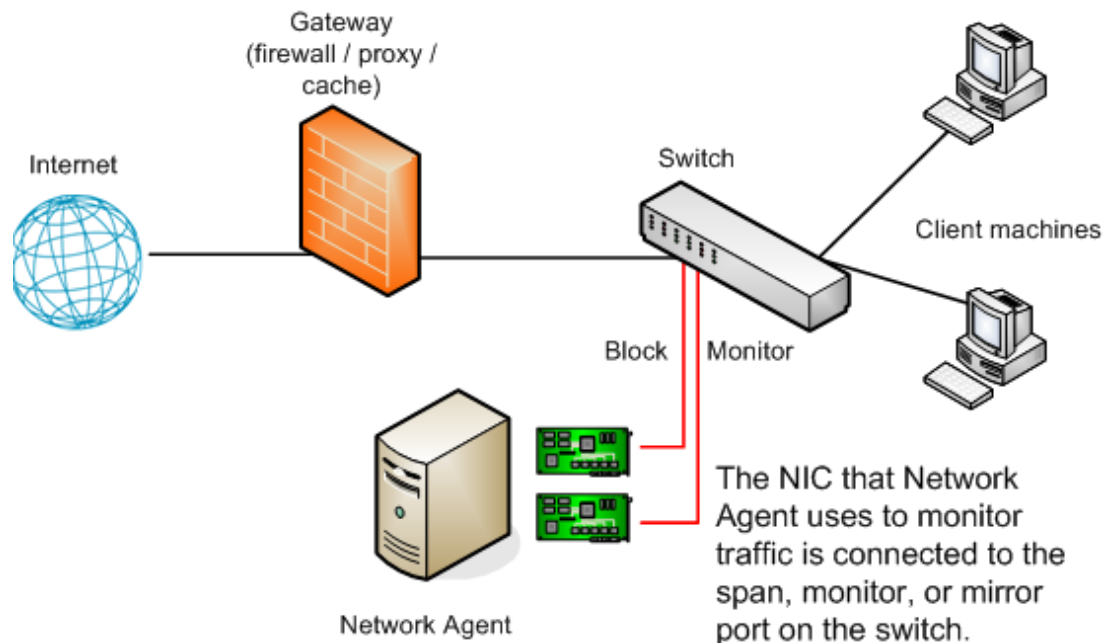
# Network Agent Deployment – Hub

- Hub should be the last device on the network before the gateway

# Network Agent Deployment – NIC configuration

## ■ NIC Configuration

- Websense recommends using 2 NICs in larger environments for load balancing



# Network Agent Deployment – NIC configuration

- *Both NICs must be connected to the same switch as the internal interface of the gateway device.*
- *Monitoring NIC should be connected to a span port.*
- *Primary (non-monitoring) NIC associated with an IP address is used for network communication and for sending block messages.*
- *Monitoring NIC can be installed in “stealth” mode, i.e. without an IP address.*

# Network Agent Deployment – NIC configuration

- *In a smaller environment, the choice of one or two NICs is determined by the type of switch you are using:*
  - *If bidirectional port spanning is supported, then one NIC is sufficient. The single NIC can both monitor traffic and send block pages.*
  - *If bidirectional port spanning is **not** supported, 2 NICs are needed.*
  - *If a hub is used, one NIC can perform both network communication and monitoring functions.*

# Installing Network Agent

- Filtering Service needs to be installed as Standalone:
  1. Run the installer and select **Add Components**.
  2. Select Network Agent and click **Next**.
  3. Installer shows a warning about not installing Network Agent on a machine running a firewall.
  4. Select the appropriate NIC for monitoring traffic. This should be the NIC connected to the span port.

# Configuring Network Agent using Manager

Network Agent settings are divided into Global and Local settings

- Global Settings – Specify behavior of all Network Agent instances. Is used to:
  - Identify the machines in your network.
  - List machines in your network that Network Agent should monitor for incoming requests (for example, internal Web servers).
  - Specify bandwidth calculation and protocol logging behavior

# Network Agent settings using Manager

- Local Settings – Apply to the selected Network Agent instance. Is used to:
  - Identify which Filtering Service instance is associated with each Network Agent.
  - Note proxies and caches used by the machines that this Network Agent monitors.
  - Configure how each NIC in the Network Agent machine is used (to monitor requests, send block pages, or both). If you have multiple Network Agent instances, you can also use the NIC settings to determine which segment of the network each Network Agent instance monitors.
  - Fail Open/Closed can be configured from Websense Manager Local settings.

# Network Agent settings using Manager

- Configure NIC settings
  - Select the appropriate NIC for Monitoring.
  - After setting the NIC to monitoring, further configuration can be done for the monitoring NIC.
  - Choose to monitor All, None, or only specific machines under the monitor list.
  - Under **Monitor List Exceptions**, identify machines that Network Agent should **not** monitor.
  - Select the appropriate NIC for blocking.

# Network Agent – NIC settings

- Different options appear under **Stand-Alone** and **Integrations**, depending on your Websense software configuration:
  - In standalone mode, Network Agent must be used to filter HTTP and non-HTTP requests. All of the **Stand-Alone** and **Integrations** options are disabled.
  - When Websense software is used in conjunction with an integration product, you determine whether or not Network Agent is used to **Log HTTP requests** to improve reporting, and/or **Filter all requests not sent over HTTP ports** to monitor requests not sent through the integration product.
- Under Protocol Management, indicate whether or not Network Agent should **Filter non-HTTP protocol requests** and/or **Measure bandwidth usage by protocol**

# Integrating with Microsoft ISA Server

## Supported Integration versions

- Websense v7 can be integrated with the following versions of ISA Server
  - Microsoft ISA Server 2004, Standard and Enterprise Edition
  - Microsoft ISA Server 2006, Standard and Enterprise Edition
  
- Supported ISA Server clients are
  - Firewall clients
  - SecureNAT clients
  - Web Proxy clients

# Integrating with Microsoft ISA Server

- Requires ISAPI plug-in also known as Filtering plug-in to be installed on the ISA Server machine.
- Filtering Service should be installed as integrated with Microsoft ISA Server.
- ISAPI Plug-in is not supported on Server 2008.
- ISA can pass HTTP, HTTPS, and FTP traffic to Websense software.
- All other protocol filtering can be handled by Network Agent.
- ISA Server can also identify users transparently and can pass this information to Websense software for user-based filtering. Authentication needs to be enabled on ISA Server.

# Installing ISAPI Plug-in

- All Websense components apart from Network Agent can be installed along with the ISAPI plug-in on the same ISA Server.
- Firewall service may need to be stopped briefly during the installation of ISAPI plug-in. This may affect Internet access for a short time depending on the network configuration.
- Select **Custom Install** and select the components you would like to install on the ISA Server.
- If Filtering Service is being installed, select integration as Microsoft ISA Server.
- Firewall service can be turned on once the plug-in has been installed.

# Installing ISAPI plug-in

- After installing the plug-in it should appear under ISA Add-ons under Web Filters as shown below.
- This ensures the plug-in is registered and successfully installed.
- In case of an ISA array, the plug-in must be installed on each ISA Server on the physical NIC.

Application Filters		Web Filters					
Order	Name	Description	Direction	Version	Vendor	Relative Path	Priority
1	DiffServ Filter	Enables DiffServ tagging of Web traffic accor...	Both	4.0	Microsof...	DiffServ.dll	High
2	Web Publishing Load Balancing Filter	Enables publishing of load balanced farms of ...	Incoming Web Requests	4.0	Microsof...	WPLoadBalancer.dll	High
3	Compression Filter	Enables HTTP/HTTPS compression	Both	4.0	Microsof...	comphttp.dll	High
4	Authentication Delegation Filter	Enables authentication delegation to the publi...	Incoming Web Requests	4.0	Microsof...	authdfilt.dll	High
5	Forms-Based Authentication Filter	Enables forms-based (cookie) authentication a...	Incoming Web Requests	4.0	Microsof...	CookieAuthFilter.dll	High
6	RADIUS Authentication Filter	Enables RADIUS authentication	Both	4.0	Microsof...	radiusauth.dll	High
7	LDAP Authentication Filter	Provides LDAP Authentication	Incoming Web Requests	4.0	Microsof...	ldapfilter.dll	High
8	WsISAFilter	Websense Filter	Outgoing Web Requests	7.0.0	Websen...	Websense-ISA.dll	Medium
9	Link Translation Filter	Enables link translation for published Web ser...	Incoming Web Requests	4.0	Microsof...	LinkTranslation.dll	Medium
10	HTTP Filter	Filters HTTP traffic and enforces configurable ...	Both	4.0	Microsof...	HttpFilter.dll	Low

# Upgrading & Removing ISAPI plug-in

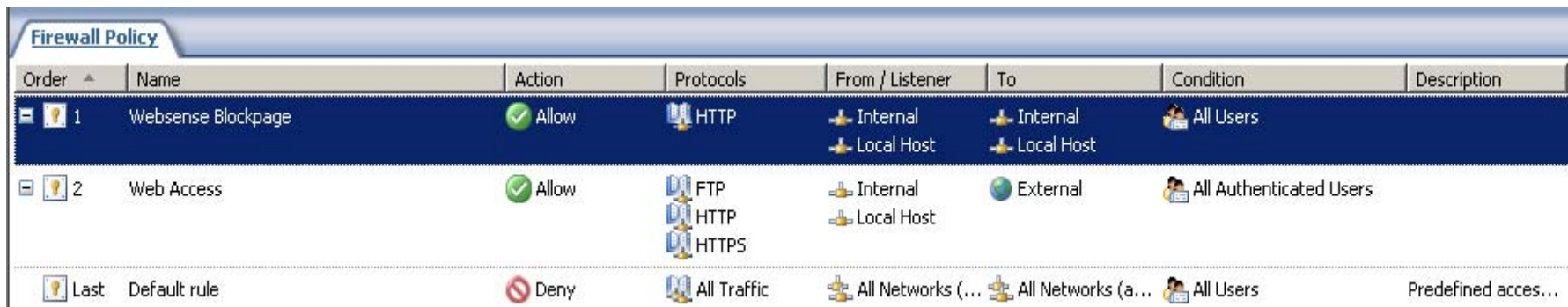
- In order to upgrade the ISAPI plug-in ensure Filtering Service has been upgraded first.
- Run the installer on ISA Server and follow on-screen instructions for upgrading the ISAPI plug-in.
- To remove the ISAPI plug-in, go to Add or Remove programs in Control Panel. Select Websense Web Filter and then the Filtering plug-in.
- Stop the Firewall service before continuing.
- System reboot will be required after removing the plug-in.

# Changing Integration

- It is possible to change integration type from one to another without uninstalling all the components.
- For example to change from Stand-Alone deployment to ISA Server Integration, the only step required is to remove the Filtering Service and reinstall it with the desired integration type.
- Policies and other settings do not change.

# User Authentication and Firewall Policy

- It is possible to configure ISA Server to pass usernames to Websense software.
- Web Access rule must be configured to allow access only to Authenticated Users.
- It is recommended you create an additional rule on the ISA Server to ensure delivery of block pages to internal clients as shown below.



Order	Name	Action	Protocols	From / Listener	To	Condition	Description
1	Websense Blockpage	Allow	HTTP	Internal Local Host	Internal Local Host	All Users	
2	Web Access	Allow	FTP HTTP HTTPS	Internal Local Host	External	All Authenticated Users	
Last	Default rule	Deny	All Traffic	All Networks (...)	All Networks (a...)	All Users	Predefined acces...

# Filtering Other Protocols

- ISA Server can be configured to pass HTTP, HTTPS, and FTP traffic to Websense software as defined in the Web Access rule.
- Any additional protocol filtering can be done using Network Agent.
- Network Agent must be installed on a separate machine and not on the ISA Server.
- Under Network Agent-Local settings in Websense Manager:
  1. Click on the IP address.
  2. Enter the proxy server IP address under Proxies and Caches so Network Agent knows about the proxy in the network.

# Configuring ISA Clients

- Clients can be configured as Web Proxy, SecureNAT, or Firewall clients.
  - Web Proxy clients – Internet browsers configured to use ISA Server as a proxy.
  - SecureNAT clients – ISA Server is configured as the default gateway for the clients.
  - Firewall clients – Client installed on the workstations with proxy settings enabled.

# Additional Configuration of ISAPI Plug-in

- If clients are configured as Firewall clients with proxy settings disabled or as SecureNAT clients, ISAPI Filter needs additional configuration to filter these requests.
- ISAPI needs to be configured to ignore requests going directly to the ISA Server and only filter requests going to the Internet.
- On the ISA Server machine, go to the **Windows\System32** folder and create a file named **ignore.txt**. Enter the hostname in upper case or IP address of the ISA Server machine and restart firewall service.
- Fail Close/Open can be configured on **Wsmisp.ini** by setting the BlockonFailure parameter.

# Integrating with Cisco PIX Firewall

- Filtering Service should be installed as integrated with Cisco PIX Firewall.
- Cisco PIX can pass HTTP, HTTPS, and FTP traffic to Websense software.
- All other protocols can be filtered using Network Agent.
- Cisco PIX cannot pass us bytes-transferred information hence bandwidth calculation is only possible if Network Agent is installed.
- User identification can be achieved by installing either DC, Logon or eDirectory Agent, as PIX cannot identify users transparently.

# Integrating with Cisco PIX Firewall

- In order for Websense software to filter requests, all requests to the Internet must go through the PIX firewall.
- PIX will then query the Filtering Service to find out if requests should be permitted or blocked based on the filtering policy.
- On receiving a Permit response from the Filtering Service PIX will then allow client requests for a particular site.
- If a site is blocked the client will receive a block page.
- Supported Cisco PIX IOS version is v5.3 or higher.

# Configuring Cisco PIX Firewall

- In order to configure the PIX firewall follow the steps below:
  1. Access the firewall from console or using telnet from a remote terminal.
  2. Enter your password.
  3. Enter enable, followed by the password to enter Privilege EXEC mode.
  4. Enter the **config t** command to activate configuration mode.
  5. Use the **url-server** command to enable URL Filtering  
**url-server (<if\_name>) host <ip\_address> [timeout <seconds>] [protocol {TCP | UDP} version {1 | 4} [connections <num\_conns>]]**

# Configuring Cisco PIX Firewall

- It is possible to define more than one url-server.
- The following are the parameters for the **url-server** command:
  - **<if name>** is the network interface where the filtering service resides.
  - **<ip\_address>** is the IP Address of the machine running Websense Filtering Service.
  - **timeout** is the amount of time that the appliance will wait for a response from Filtering Service before switching to the next Filtering Service OR to fail open/close configuration if defined.

# Configuring Cisco PIX Firewall

- **protocol** { TCP or UDP } – Defines whether PIX uses TCP or UDP to communicate with Filtering Service and which version of the protocol to use.
  - **TCP** is recommended and is the default. The recommended version number to use is **4**.
  - **connections** – specifies the maximum number of connections permitted between PIX and Filtering Service. Default is 5. This is not available when using UDP.
- For example, the statement will look as follows
- ```
url-server (perimeter) host 10.4.150.40 timeout 30  
protocol TCP version 4
```

# Configuring Cisco PIX Firewall

- Configure PIX to pass HTTP traffic to Filtering Service using the **filter url** command.
  - To configure PIX to pass HTTP traffic for All destinations on port 80:  
**filter url http 0 0 0 0 allow**
  - To configure PIX to pass HTTP traffic for a specific network; for example, for the 10.50.x.x network to all destinations on port 80:  
**filter url http 10.50.0.0 255.255.0.0 0 0 allow**
  - To configure PIX to pass HTTP traffic for a specific host going to a specific destination on port 80:  
**filter url http 10.50.2.30 255.255.255.255 210.25.100.40 255.255.255.255 allow**
  - The **allow** option enables the PIX to fail open in the event the Filtering Service is temporarily unavailable.

# Configuring Cisco PIX firewall

- Multiple **filter url** commands can be entered to set up the firewall for filtering different parts of the network.
  - To configure PIX to pass HTTPS and FTP traffic for All destinations:  
**filter https 0 0 0 0 allow**  
**filter ftp 0 0 0 0 allow**
  - To configure PIX to pass HTTPS and FTP traffic for a specific network; for example, the 10.50.x.x network to all destinations:  
**filter https 10.50.0.0 255.255.0.0 0 0 allow**  
**filter ftp 10.50.0.0 255.255.0.0 0 0 allow**

# Configuring Cisco PIX firewall

- To configure PIX to pass HTTPS and FTP traffic for a specific host going to a specific destination:

```
filter https 10.50.2.30 255.255.255.255 10.25.100.40  
255.255.255.255 allow
```

```
filter ftp 10.50.2.30 255.255.255.255 210.25.100.40  
255.255.255.255 allow
```

- Configure PIX for long URL support, this involves increasing the size of the internal buffer.
  - To specify the amount of memory assigned to the buffer:  
**url-block url-mempool <memory\_pool\_size>**  
<memory\_pool\_size> is the size of the buffer in KB. It can take values from 2 to 10240, recommended is 1500.

# Configuring Cisco PIX Firewall

- Increase the maximum permitted size of a single URL by adding the following.

**url-block url-size <long\_url\_size>**

<long\_url\_size> is the maximum URL size in KB. It can take a value from 2 to 4, recommended value is 4.

- Configure the HTTP response buffer size to prevent replies from the Web server from being dropped in high traffic situations.

**url-block block <block\_buffer\_limit>**

<block\_buffer\_limit> is the number of 1550-byte blocks to be buffered. You can enter a value from 1 to 128.

# Troubleshooting – Network Agent

- Run **testlogserver** to check if Websense Filtering Service is able to see any traffic from the spanned port.
- Use **wireshark** to run packet capture on client machine and the Websense server.
- Network Agent debug can also be used. This can be turned on from the Websense Manager and will create a NetworkAgent.log file in the \bin directory.
- Use **netstat** to display the routing information (`netstat -r`), or to display active TCP connections (`netstat -an`). Once Network Agent has seen a packet and established communication with the Filtering Service, you should see 50 ports connecting Network Agent with Filtering Service. If any blocking has occurred, there will also be connections to port 15871 in the 'time-wait' state.

# Troubleshooting – ISA Integration

- SecureNAT clients are not filtered
  - Verify the ignore.txt file has been added to the system32 folder with the machine name of the ISA Server.
- No Filtering at all
  - Verify that the ISAPI plug-in is pointing to the correct filtering service IP address and port number.
  - Open WsMSP.ini file in system32 directory and check under the [initSection]:  
EIMServerIP=<IP of filtering service>  
EIMServerPort=15868
  - If ISA Server and Filtering Service are on the same server try restarting the Firewall service.
  - If Filtering Service resides on a different machine, check the ISA Firewall policy and verify there is an allow rule to allow access to the Filtering Service machine on port 15868.

# Troubleshooting – ISA Integration

- For advanced troubleshooting and debugging it is possible to set the ISAPI plug-in to debug mode by using the code below in the WsMsp.ini file:

```
[diagnosticSection]
```

```
ProgressTraceType=FileOnly
```

```
ProgressTraceMask=1
```

```
ProgressTraceFile=C:\Temp\wsISA.txt
```

```
DumpUserNames=any
```

Send the wsISA.txt file to Support.

# Troubleshooting – Cisco PIX Integration

- No Filtering at all
  - Run testlogserver.
  - Verify PIX rules.
  - Run packet capture.
- No Logging even though Filtering works fine.
  - If Network agent is installed check the Websense Manager settings for Network Agent. Under Integration partner logging verify that “Log HTTP requests” option is not selected.

**August  
2009  
Webinar**

## **User Identification technologies within Websense Web Security Suite v7.x**

August 19, 2009, 8:30 A.M. (GMT -7:00, Pacific Daylight Time)

How to register:

<http://connect.websense.com/f97762289>

or

Go to the Support site on

<http://www.websense.com>

And click on Support Webinars

# Support Online Resources



## Tech Alerts

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



## Knowledge Base

- Hundreds of Websense customers successfully find solutions in the knowledge base to their common product problems. Search or browse our knowledge base for documentation, downloads, top knowledge base articles, and solutions specific to your product.



## Support Forums

- Join our online community to share questions, offer solutions and suggestions with experienced Websense Customers regarding product Best Practices, Deployment, Installation, Configuration, and other product topics. Join Now.



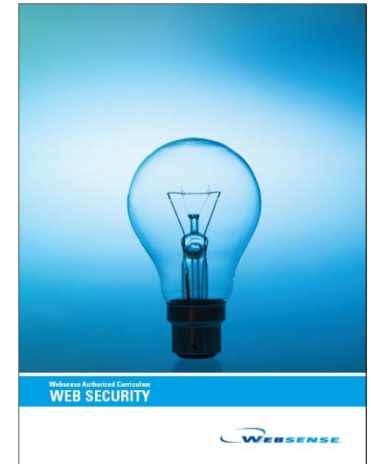
## [ask.websense.com](http://ask.websense.com)

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

# Customer Training and Certification Programs

## 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?



- We are now incorporating an extended question and answer time to answer as many questions as possible.
- Responses to all questions submitted will be posted online on the Support Webinar home page approximately one week from today.
- To review answers to your questions, go to:
  - <http://www.websense.com/content/SupportWebinars.aspx>