IP Binder for ISA Server Documentation

(The following graphics are screen shots from Microsoft® ISA Server 2006 which is the property of Microsoft Corp. and are included here for instructive use. Some images illustrate IP Binder for ISA Server, which is the property of Collective Software.)

Table of Contents

ISA server and outbound IP source selection

ISA server lacks the ability to choose among several external IP addresses for outbound traffic.

Solution

IP Binder from Collective Software gives you easy source IP address control in ISA 2006/2004.

Features

- Configure access rules to specify what IP should be used as the local source address.
- Works for outbound HTTP web proxy traffic
- Bind to any TCP protocol in ISA, such as outbound SMTP
- Compatible with arrays where each server has different external IP addresses
- Default behavior of access rules is preserved automatically unless you change them

Limitations

- Only operable for TCP protocols, UDP/ICMP not supported
- This does not "spoof" IP addresses; only works with the real external IPs of the server
- This is not a load-balancing or ISP failover product. It does not manage routing rules, only selects the source IP address to use for each access rule

Requirements

- ISA Server 2006 or 2004
- Microsoft .NET Framework version 2 should be installed on each ISA server.

Help is Available!

We are always happy to help you get our software set up and working. If you have questions or need assistance understanding/configuring/testing a Collective product, you can get in touch with our support staff quickly and easily. For the most up-to-date information, please see our Support page at http://www.collectivesoftware.com/Support/

Installation of IP Binder for ISA Server

Install Procedure

1. Close the ISA management console if it's open.
2. Execute the IPbinder.msi file. This will stop your firewall service, install the filter and interface software, register the filter, and then re-start the firewall service.
3. If you are installing over a remote desktop session, keep in mind that when the firewall service stops and restarts your RDP connection may be frozen, dropped or timed out. If an error occurs during the installation and the firewall service cannot be restarted, you will need to access the console to troubleshoot further (see below).
4. You must run the installer on each ISA server in an array separately, so they will all have the filter files installed and registered.
5. If the installation completes with no errors, then you can proceed to the configuration section.

Troubleshooting

The installation normally completes without errors. However there are a few possible failure modes that can occur for this complex install process.

Install rolls back (with red error message at the end)

If you are presented with an error message on the final screen, then check out the application event log, which often will contain details on why the installation failed. The problem may be immediately solvable from this information, or you may need to work with Collective support for additional troubleshooting assistance.

Frozen or hung install

The installer tries to start the firewall service after it is done registering the filter components. In rare cases, everything may register properly but there could still be a problem preventing the firewall service from starting. In this situation, the installation may appear to hang on the “Starting services...” item. This is because it is trying repeatedly to start the service, and failing. In fact if you look at the application event log, you will see several errors from the firewall service as it tries to start. These messages may help identify the cause of the problem.

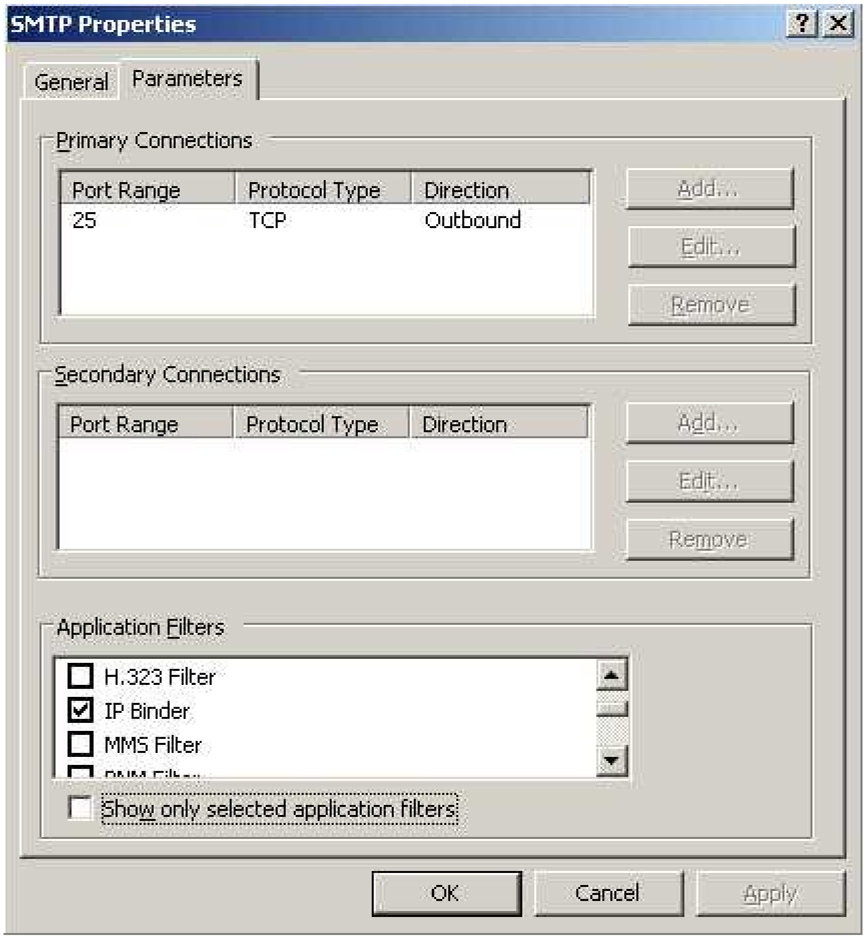
The install should eventually give up on starting the service, but it may take a long time. If necessary, you can expedite the rollback by going into the services control panel and setting the Microsoft Firewall service to Disabled temporarily (and applying that change). This will cause the installer to quickly give up, and it should then correctly roll back the installation while leaving the firewall service down. After this happens you can then re-enable and restart the firewall service.

This kind of problem should not normally occur, and will probably require additional troubleshooting by Collective support. However if you are able to fix the problem you can re-run the install safely after completing this procedure.

Hooking the filter to a protocol

For efficiency, ISA does not send all traffic protocols to each application filter. To use IP Binder for a specific protocol such as SMTP, it is necessary to "hook" the filter in the ISA protocol definition.

Go to the properties page of the outbound protocol you are using, and select the "IP Binder" item in the Application Filters section. Save and apply your settings before going on.



Primary Connections

Port Range	Protocol Type	Direction
25	TCP	Outbound

Secondary Connections

Port Range	Protocol Type	Direction

Application Filters

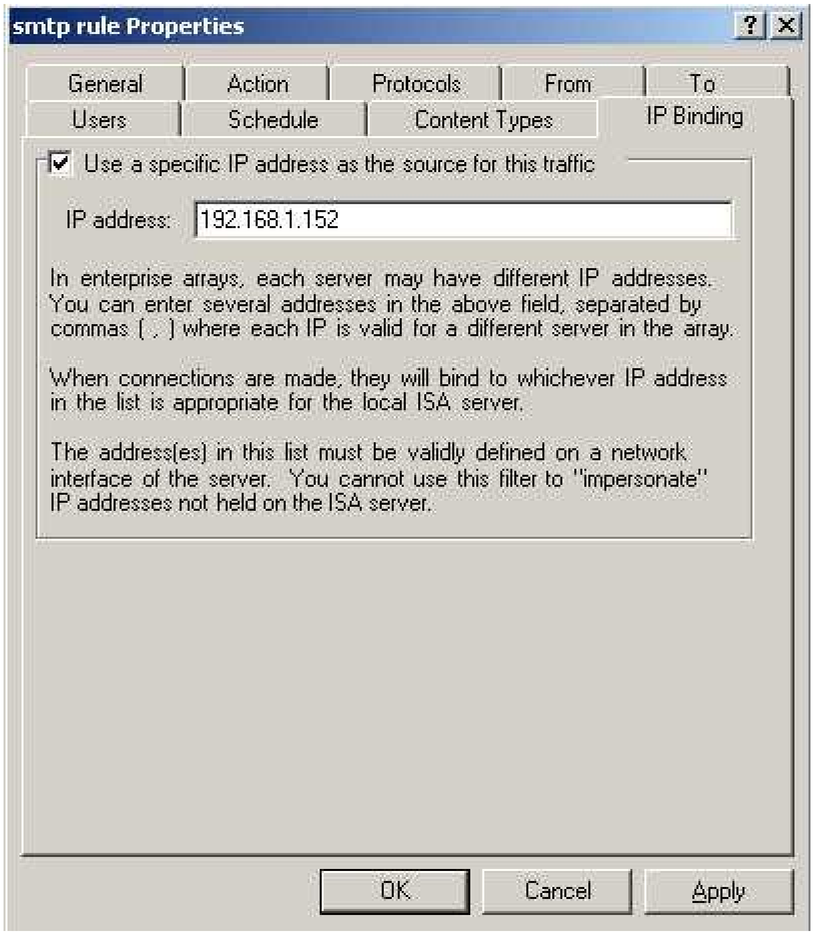
☐ H.323 Filter
☑ IP Binder
☐ MMS Filter

☐ Show only selected application filters

Note that you *do not need* to hook the "HTTP" protocol, as long as that protocol has the "Web Proxy Filter" hooked already. The web proxy makes its own separate outbound connections, and IP Binder manages these connections via a web filter. Therefore, it is necessary and sufficient to select the "Web Proxy Filter", but selecting "IP binder" will have no effect on this protocol.

Access rule settings

For IP binder to control the source IP address of an outbound connection, you must activate it for the access rule which that traffic will be using. Go into the property pages of the access rule and find the IP Binding tab. Enter one or more IP addresses in a comma separated list in the "IP address" field, as shown:



☑ Use a specific IP address as the source for this traffic

IP address: 192.168.1.152

In enterprise arrays, each server may have different IP addresses. You can enter several addresses in the above field, separated by commas (,) where each IP is valid for a different server in the array.

When connections are made, they will bind to whichever IP address in the list is appropriate for the local ISA server.

The address(es) in this list must be validly defined on a network interface of the server. You cannot use this filter to "impersonate" IP addresses not held on the ISA server.

The reason for allowing more than one IP is because enterprise ISA array members may have differing external IP addresses (but they share the same firewall policy configuration). You should include one IP that will match each array member's configuration, and the correct IP for each member will be chosen automatically.

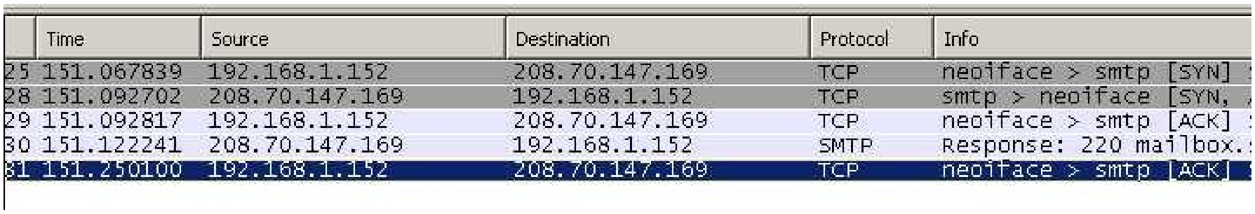
If the "IP Binding" tab is not shown, verify the following checks:

- Make sure you are looking at an access rule. For publishing rules, the IP address is controlled by the web listener, or the server publishing rule properties. You do not need a third party filter in this case!
- Make sure that at least one of the protocols in the access rule has been configured to use IP Binder, or includes the HTTP protocol.
- If you hooked the protocol but the access rule properties are already displayed, close the property sheet and go back in. The filter decides to show the tab when the property sheet is first invoked, so it is necessary for the protocols to be set up before going into the access rule property sheet.

Note: If your access rule applies to several protocols, only the ones hooked to IP Binder (and also HTTP) will have their source IP controlled. Unhooked protocols will behave as normal.

Testing the configuration

After applying these settings, it should be possible to verify that the filter is working by using Network Monitor or Wireshark on the external interface. In the image below, the ISA server has external IP addresses of 192.168.1.150-152. The SMTP traffic normally sources from the .150 address, but after configuring IP binder on its access rule, the traffic originates at .152:



	Time	Source	Destination	Protocol	Info
25	151.067839	192.168.1.152	208.70.147.169	TCP	neoiface > smtp [SYN]
28	151.092702	208.70.147.169	192.168.1.152	TCP	smtp > neoiface [SYN,
29	151.092817	192.168.1.152	208.70.147.169	TCP	neoiface > smtp [ACK]
30	151.122241	208.70.147.169	192.168.1.152	SMTP	Response: 220 mailbox.
31	151.250100	192.168.1.152	208.70.147.169	TCP	neoiface > smtp [ACK]

Note that in this example, the "external" interface of ISA is a private IP subnet behind another router. However this is just an artifact of the test lab configuration. if you use ISA as an edge firewall that has live internet IP addresses, you can still select between them using IP Binder.

Filter licensing

To view your evaluation period or enter a key, go to Add-ins, Web Filters, and select IP Binder properties, and select the License tab.

The License tab is used to check how long remains in the evaluation period, and to activate a permanent license.

To be eligible for a license key, you need to purchase license(s). You can do this on our web store or by contacting us.

Once you have available license(s) you can request a key for your array (or single server) at our licensing page. When requesting a license key, you will need to tell us the name of the ISA array, which is indicated on this dialog. The exact name is important, because it will be used to validate the key.

The license key is sensitive to the number of servers in the array. For example if you begin with only 2 servers in the array but plan to have 4, you can purchase 4 licenses and request a license key for a 4-server array. Then as you bring future servers online, they will be licensed automatically.

Warning: if you install more servers than you have licensed then the license key will be seen as invalid, and the servers will begin to operate in demo/lab mode. So if you need to add more servers to a live array then you should acquire and apply your new license key in advance, so this behavior does not take place.

Demo/Lab mode

When the evaluation period expires (after 30 days) or when an invalid license key is used, the filter runs in demo/lab mode. In this mode the filter will work normally for a period of 2 hours from the starting of the Firewall Service, and then stop working after that time. This mode is meant to be useful for test labs where you don't wish to purchase licenses but still want to be able to run meaningful test setups. After 2 hours, you can restart the firewall service and the lab timer will reset again.

Troubleshooting

The first place to look if something seems to be working incorrectly is the ISA alerts tab in the Monitoring section. Often this will directly indicate the cause of the problem. This information will also be required in almost all cases if you need support.

Support for IP Binder for ISA Server

Collective is proud to offer support for IP Binder for ISA Server, whether you need help getting a configuration working, find a bug, or just have a feature question.

Support is available from our web site at http://www.collectivesoftware.com/Support/

- *Knowledge Base*: When our staff answers questions that will apply to the whole community, they will often create a permanent KB item to disseminate this knowledge. There is a Search feature here; you can also easily browse by topic.

To get fast answers to FAQs (frequently asked questions) the knowledge base is the best place to start.

- *Support ticket*: We are always happy to help you get set up and working. If you have questions or need assistance understanding/configuring/testing a Collective product, you can get in touch with our support staff quickly and easily. For the most up-to-date information, please see our Support page.