

[Activate your FREE membership today](#) | [Log in](#)



ADVERTISEMENT



Up to 16 hours of battery life.
The HP Compaq nc6400 Business Notebook with Intel® Centrino® Duo Mobile Technology.
[Learn more »](#)



THE COMPUTER IS PERSONAL AGAIN.

- [HOME](#)
- [NEWS](#)
- [TOPICS](#)
- [ITKNOWLEDGE EXCHANGE](#)
- [TIPS](#)
- [ASK THE EXPERTS](#)
- [WEBCASTS](#)
- [WHITE PAPERS](#)
- [WINDOWS IT DOWNLOADS](#)
- [CAREERS](#)

SEARCH this site and the web [ADVANCED SEARCH](#) | [SITE MAP](#) Search Powered by 

ADVERTISEMENT [Sign up to receive the White Paper Alerts newsletter to keep up with the latest additions to our library from SearchExchange.com.](#)

[Home](#) > [Microsoft Exchange Tips](#) > [Exchange Server Administration Tips](#) > A ban on dynamic IP addresses for Exchange Server

Exchange Tips:

 [EMAIL THIS](#)

[TIPS & NEWSLETTERS TOPICS](#)

EXCHANGE SERVER ADMINISTRATION TIPS

A ban on dynamic IP addresses for Exchange Server

Brien M. Posey

08.09.2006

Rating: --- (out of 5)

RSS FEEDS: [Exchange Server tips, tutorials and expert advice](#)

Some companies, including Microsoft, have decided to block any inbound email messages originating from a dynamic IP address in an effort to prevent spam. Unfortunately, while almost every large company uses a static IP address for its Exchange servers, smaller companies are often forced to use dynamic IP addresses.

Fortunately, you can configure Exchange Server to route mail through your ISP's SMTP server, so it appears to recipients as if the message came from the ISP's static IP address instead of your organization's dynamic IP address.

How to route Exchange Server email through an ISP's SMTP server

How to configure Microsoft Exchange Server to route mail through your ISP's SMTP server varies depending on the versions of Exchange Server that you are running. In Exchange 2000 and Exchange 2003, the SMTP connector replaces the Internet Mail Service used in earlier versions of Exchange Server.

For the purposes of this tip, I will assume that your Exchange Server deployment is running in mixed mode, and that you will need to create an SMTP connector. If you already have an SMTP connector in place, you can modify your existing connector rather than creating a new one.

1. Open Exchange System Manager.
2. Navigate to Administrative Groups -> your administrative group -> Routing Groups -> First Routing Group -> Connectors.
3. Right click on the Connectors container and select New -> SMTP Connectors to view the new connector's properties sheet.
4. Go to the General tab and enter a descriptive name for the connector into the space provided.
5. Just below the Name field, you are given the choice of using DNS to route messages to each address space on the connector, or to forward mail through a smart host. Choose the smart host option and then enter the IP address of your ISP's SMTP server into the space provided.
6. At this point, you must designate an SMTP virtual server to act as a local bridgehead server. To do so, click the Add button and then select the server that you want to designate as the local bridgehead.
7. To define an SMTP address space, select the Address tab and then either the Entire Organization or the Routing Group option to set the scope of the address space that you are about to define.
8. Click the Add button, select the SMTP option, and click OK.
9. You will now see a dialog box asking for an email domain and a cost. Go with the defaults and click OK to be taken back to the Address Space tab.
10. Verify that the "Allow Messages to be Relayed to these Domains" checkbox is not selected -- otherwise, the entire world may be able to relay mail through your Exchange Server.
11. Go back to the Advanced tab and click the Outbound Security button to view the Outbound Security dialog box.
12. Most ISPs require the Outbound Security option to be set to Anonymous Access, but you should check with your own individual ISP to see what settings they want you to use.
13. Click OK repeatedly until all of the open dialog boxes are closed.
14. Now verify that the SMTP virtual server you designated to act as a local bridgehead is configured to listen on TCP port 25 by navigating to Administrative Groups -> your administrative group -> Servers -> the server that's hosting the designated SMTP virtual server -> Protocols -> SMTP -> the designated SMTP virtual server.
15. Right click on the designated SMTP virtual server and select Properties.
16. Go to the General tab and click on the Advanced button.

REFERENCE DESK

**Spam Prevention and Management**

NEWS, TIPS & MORE

- [A ban on dynamic IP addresses for Exchange Server](#) (TIP)
 - [Image-based spam scams on the rise](#) (ARTICLE)
 - [Image spam paints a troubling picture](#) (ARTICLE)
 - [Exchange Intelligent Message Filter](#) (CRASH COURSE)
- [VIEW MORE](#)

VENDOR CONTENT

- [Creating an Antispam Cocktail: Best Spam Detection and Filtering Techniques](#) (PODCAST)

Wireless WAN.

The HP Compaq nc6400 Business Notebook with Intel® Centrino® Duo Mobile Technology.

[Learn more »](#)

intel
Centrino
Bus
Dual-core.
Do more.

THE COMPUTER IS PERSONAL AGAIN.

hp

- [What Is UCE, and Why Should I Care?](#) (WHITE PAPER)
 - [Cut Down on Spam](#) (WHITE PAPER)
 - [Is Spyware Hurting You or Your Business?](#) (WHITE PAPER)
- [VIEW MORE](#)

SEE ALSO

- **Related Topics:**
[Spam Prevention and Management](#) , [Compliance](#), [Firewalls](#), [Message Encryption](#), [Password Management](#)
- **Site Highlights:**
[Exchange Migration Guide](#)
[Exchange Security Tip](#)

GET E-MAIL UPDATES

Submit your e-mail below to receive Exchange-related news, tech tips and more, delivered to your inbox.

Exchange Server Security

E-mail:

Not a member? We'll activate your FREE membership with your subscription.

17. Verify that the SMTP virtual server is configured to listen on TCP port 25. If the designated port is something other than 25, you can use the Add button to add port 25 to the list of ports.
18. Your Exchange Server should now be configured to route outbound SMTP email through your ISP's SMTP server. To complete the process, simply restart the Microsoft Exchange Routing Engine service and the server's SMTP service.

Make sure your ISP isn't on any spam blacklists

Routing email through an ISP's SMTP server may not be enough to prevent your organization's email from being treated as spam.

There are numerous spam blacklists, and your ISP's SMTP server could potentially be listed on any of them. In the past, it has been a very tedious process to search through all of the blacklists to see where a block was coming from.

I recently discovered a handy Web site called DNSstuff.com that makes the process of searching the spam blacklists a lot easier. The site isn't solely dedicated to searching spam blacklists, but the front page offers an option to enter your (or in this case your ISP's) mail server's IP address. It will then check all of the spam blacklists to see if the IP address appears on any of them.

In all likelihood, your ISP's mail server isn't blacklisted, but it's still good to check to be sure. Running a quick scan of the blacklists up front can save you hours of pointless troubleshooting if your ISP is blacklisted and causing email delivery issues.

If you've verified that your ISP's SMTP server is not on a spam blacklist, but your organization's email still isn't being delivered, it's possible that the domains rejecting your email are using extremely restrictive spam filters.

Some filters will not only block all dynamically assigned IP addresses, but also email from any organization whose DNS server is not configured to meet the service's specifications.

One example of an overly restrictive spam filter is the [SORBS Dynamic User and Host List \(SORBS DUHL\)](http://www.sorbs.net), which was originally intended to be a list of dynamically assigned IP address ranges. The idea was that organizations could reduce spam by blocking inbound email from any IP address within a listed range.

But as I outlined above, there is a simple technique that circumvents detection of your organization's IP dynamic IP address by routing mail through your ISP's SMTP server, which has a static IP address.

Spammers know this trick too. So if the absence of a dynamic IP address were the only criteria that SORBS used for blocking spammers, the list of dynamically assigned address ranges would quickly become useless. That being the case, SORBS came up with some additional requirements:

- The MX record of a domain needs to contain a host name that maps to the IP address involved. The "Time to Live" of the MX record needs to be at least 43,200 seconds.
- The A record for the host name needs to have a TTL of at least 43,200 seconds.
- The reverse DNS PTR record for the IP address involved needs to map back to the name given in the MX record, and to have a TTL of at least 43,200 seconds.
- If there are multiple MX entries, these rules apply to them all.

Organizations that filter email based on the SORBS-DUHL exclusion list are bound to reduce the amount of spam they receive, but they also risk making themselves inaccessible both to clients and potential clients, so I personally think this practice is a bad idea.

Even though I disagree with using the SORBS-DUHL exclusion list to filter spam, you can't ignore its requirements. Microsoft is only one of many companies now filtering inbound email using the SORBS-DUHL standards. So you might want to think about configuring your domain's DNS records to match the SORBS-DUHL requirements as a precaution.

About the author: Brien M. Posey, MCSE, is a Microsoft Most Valuable Professional for his work with Exchange Server, and has previously received Microsoft's MVP award for Windows Server and Internet Information Server (IIS). Brien has served as CIO for a nationwide chain of hospitals and was once responsible for the Department of Information Management at Fort Knox. As a freelance technical writer, Brien has written for Microsoft, TechTarget, CNET, ZDNet, MSD2D, Relevant Technologies and other technology companies. You can visit Brien's personal Web site at <http://www.brienposey.com>.

Do you have comments on this tip? [Let us know.](#)

Related information from SearchExchange.com:

- Tutorial: [How to protect Exchange Server from spam blacklists](#)
- Expert Advice: [Configuring Exchange to send/receive email through an ISP](#)
- Tip: [Should you turn off your network's outbound SMTP \(port 25\)?](#)
- Fast Guide: [Exchange Server security essentials](#)
- Reference Center: [Exchange 2003 tips and resources](#)

Please let others know how useful this tip was via the rating scale below. Do you have a useful Exchange Server or Microsoft Outlook tip, timesaver or workaround to share? [Submit it to SearchExchange.com.](#) If we publish it, we'll send you a nifty thank-you gift.

[Rate this Tip](#)

To rate tips, you must be a member of searchExchange.com. [Register now](#) to start rating these tips. [Log in](#) if you are already a member.

[Submit a Tip](#)

Share - [Digg This!](#)  [Bookmark with Del.icio.us](#)

EXCHANGE RELATED LINKS

Ads by Google

[Outgoing Mail - SMTP](#)

Want the ultimate solution for sending your email?

www.authsmtp.com

[Free Mail Server Download](#)

POP3/IMAP4/SMTP: IMail Server Protection from spam and viruses.

www.ipswitch.com/imapserver

[Add Email Disclaimers](#)

Add legal disclaimers and signatures to Exchange Server

www.maildisclaimer.com

[Looking for a Static IP?](#)

Run your server from Cable or DSL! Host your own Web, FTP, VPN, DVR

www.tzo.com

[Sendmail, Inc.](#)

Anti-spam, anti-virus and other add-ons for the sendmail MTA

www.sendmail.com

RELATED CONTENT**Spam and Security Tips**

- Microsoft hotfix offers selective Exchange IMF filtering
- How to move an SSL certificate between Exchange servers
- Are out-of-office messages a security hazard?
- How to enable automatic Exchange IMF updates via Microsoft Update
- Should you turn off your network's outbound SMTP (port 25)?
- How to display IMF's Spam Confidence Level (SCL) rankings in Microsoft Outlook
- How to enable the Exchange Server Intelligent Message Filter on authenticated SMTP connections
- Excessive Exchange Server NDRs destroy DNS
- Optimize your DNS blacklists with BL-Monitor
- Freebie antiphishing tool verifies domain information

Exchange Server Administration Tips

- Exchange Server 2007: 32-bit versus 64-bit hardware
- When Exchange ActiveSync won't download mailbox items to mobile devices
- Backing up Exchange Server with Microsoft System Center Data Protection Manager
- Registry hacks that improve Exchange Server and Active Directory performance
- Optimizing Exchange Server archiving for email attachments
- Global catalog server best practices for Exchange Server
- Why HTTP can hurt Exchange ActiveSync attachments
- Troubleshooting Exchange Server global catalog issues
- Event ID 9031 issue when deleting Exchange Server mailboxes
- Proper patching procedures for front-end/back-end Exchange Server setups

Spam Prevention and Management

- McAfee products vulnerable to code execution flaw
- Image-based spam scams on the rise
- Image spam paints a troubling picture
- Exchange Intelligent Message Filter
- Masking an email's source IP address
- Exchange Server security essentials
- Microsoft hotfix offers selective Exchange IMF filtering
- Microsoft anti-malware suite ready to go
- Antispam crusade backfires; Blue Security shuts down
- Spammers hijack authentication mechanisms to send malware
- Spam Prevention and Management Research

RELATED RESOURCES

- 2020software.com, trial software downloads for [accounting software](#), [ERP software](#), [CRM software](#) and [business software](#) systems
- Search Bitpipe.com for the latest [white papers](#) and [business webcasts](#)
- Whatis.com, the online [computer dictionary](#)

DISCLAIMER: Our Tips Exchange is a forum for you to share technical advice and expertise with your peers and to learn from other enterprise IT professionals. TechTarget provides the infrastructure to facilitate this sharing of information. However, we cannot guarantee the accuracy or validity of the material submitted. You agree that your use of the Ask The Expert services and your reliance on any questions, answers, information or other materials received through this Web site is at your own risk.

[HOME](#) | [NEWS](#) | [TOPICS](#) | [IT KNOWLEDGE EXCHANGE](#) | [TIPS](#) | [ASK THE EXPERTS](#) | [WEBCASTS](#) | [WHITE PAPERS](#) | [WINDOWS IT DOWNLOADS](#) | [CAREERS](#)

[About Us](#) | [Contact Us](#) | [For Advertisers](#) | [For Business Partners](#) | [Reprints](#) | [RSS](#)

SEARCH

SEARCH

SearchExchange.com is part of the TechTarget network of industry-specific IT Web sites

CIO AND IT MANAGEMENT

[SearchCIO.com](#)
[SearchSMB.com](#)
[Whatis.com](#)

STORAGE AND DATA CENTER

[SearchStorage.com](#)
[Search400.com](#)
[SearchDataCenter.com](#)

WINDOWS AND DISTRIBUTED COMPUTING

[SearchWinIT.com](#)
[SearchExchange.com](#)
[SearchSQLServer.com](#)
[SearchWindowsSecurity.com](#)
[SearchWinComputing.com](#)
[SearchServerVirtualization.com](#)
[Labmice.net](#)
[SearchOpenSource.com](#)
[SearchDomino.com](#)

NETWORKING

[SearchNetworking.com](#)
[SearchVoIP.com](#)
[SearchMobileComputing.com](#)

SECURITY

[SearchSecurity.com](#)

APPLICATION DEVELOPMENT

[TheServerSide.com](#)
[TheServerSide.NET](#)
[SearchAppSecurity.com](#)
[SearchWebServices.com](#)
[SearchVB.com](#)

ENTERPRISE APPLICATIONS

[SearchCRM.com](#)
[SearchDataManagement.com](#)
[SearchOracle.com](#)
[SearchSAP.com](#)
[2020software.com](#)



[TechTarget Expert Answer Center](#) | [TechTarget Events](#) | [TechTarget Corporate Web Site](#) | [Media Kit](#) | [Site Map](#)

Explore [SearchTechTarget.com](#), the guide to the TechTarget network of industry-specific IT Web sites.

