Windows Insider

35,000 Subscribers Worldwide

CramSession   StudyGuides   InfoCenter   Discussions   SkillDrill   Newsletters

CramSession

Feature

What's the IIS SMTP Service All About?   Read it

Ask Uncle Bill

Q and A's   Read it

Security Advisories

SQL Extended Procedure Functions Contain Unchecked   Read it
Buffers

News Headlines & Resources

Customizing the Command Prompt in Windows XP	Read it
Watch Out for the Klez.H Worm!	Read it
File Compression Whacks-out Disk Quotas	Read it
Put RIS into Overdrive	Read it
Load Testing Exchange 2000	Read it
How to Configure an L2TP/IPSec Connection Using a Pre-shared Key	Read it
Configuring and Using OWA in Exchange 2000 Server	Read it
ISA Server Exam 70-227 Tutorial	Read it
Make Windows 2000 DNS and BIND Work Together	Read it

Download of the Week

Tiny Key Logger   Read it

Feature

What's the IIS SMTP Service All About?   ▲ to top

Way back when I was a fledgling MCSE wannabe, I had to study for the

IIS exam. For that exam, I was supposed to learn all about the Web Service, the NNTP service, and the FTP service. All those services made sense to me. I could use IIS to create a web site, an NNTP news server, and an FTP server. But one service that never made sense was the SMTP service. What the heck was that for? I read the Microsoft Official Curriculum and many study guides about IIS, but all they did was describe what the various settings were for. NONE of them described when I would ever use the SMTP service.

Of course, you could pass the exams back then without understanding the purpose of the services. To a certain extent, the same is true today. But it always seemed that the SMTP service had some use I could take advantage of, if only someone would show the way!

I didn't realize the value of the SMTP service until I started hosting my own domains and email services. Necessity is the mother of invention! It only goes to show that you don't really understand something until you have to use it yourself.

What good is the IIS SMTP service? There are some less interesting uses, such as providing an SMTP server for a FrontPage site, or providing an SMTP service for some other Web application that needs to send mail. But there are some interesting uses for the IIS SMTP service. The most interesting and powerful application of the IIS SMTP service is that it allows you to take advantage of mail relay.

What is a mail relay? A mail relay is an SMTP server that accepts mail for a particular mail domain, but is not the end point for mail to that particular domain. The mail relay lies between the source (your email client or mail server) and the destination (the SMTP server responsible for mail for a particular mail domain) of a particular email message.

Mail relays are useful for security reasons. You can use a mail relay to prevent spammers from sending mail to your Exchange Server or to domains that you're not responsible for. SMTP servers that accept and forward messages to mail domains they are not responsible for are often referred to as "open mail relays". Spammers can take advantage of open mail relays to spew out their crud. You can also use an SMTP relay to prevent Internet hosts from ever directly interacting with your Exchange Server.

Let's look at an example of how you can use the IIS SMTP service to prevent Internet servers from ever directly interacting with your Exchange server. Suppose you have an Exchange Server on the internal network that receives mail for your domain – mydomain.com. You want all mail for users in the mydomain.com domain to be sent to your Exchange Server. Your Exchange Server is on your internal network, and you use ISA Server as your firewall.

One option you have is to publish your Exchange Server's SMTP service. If you publish the Exchange Server's SMTP service, Internet users will be able to send messages directly to your Exchange Server. This might not be a good idea, because Internet users might be able to exploit your Exchange Server if they have direct contact with it. To prevent Internet users from having direct contact with your Exchange Server, put up an IIS SMTP relay box.

Instead of publishing the Exchange Server's SMTP service, you publish the IIS SMTP Service. When mail destined for the mydomain.com hits the external interface of your ISA Server, the ISA Server will forward the mail to the SMTP relay. The IIS SMTP relay machine gets the mail and forwards (relays) that mail to your Exchange Server.

The Exchange Server's SMTP service receives the mail for a recipient in the mydomain.com domain and never had to interact with an Internet SMTP server. The Exchange Server then can be set up to send outgoing SMTP mail messages to the IIS SMTP relay server and the IIS SMTP mail relay server will forward (relay) those messages to the Internet mail servers.

The trick is knowing how to configure the IIS SMTP Service to properly relay mail. For incoming mail, you want to allow relay only to your own domains. For outgoing mail, you want to be able to relay to ALL domains. If you allow incoming mail to be relayed to all domains, spammers will be able to take advantage of your open mail relay and you'll find your mail server on a "black hole" list and no one will accept mail from your mail server. Not good!

Open the IIS 5.0 Internet Services Manager and right click on the "Default SMTP Virtual Server" node and click "Properties". Click the "Access" tab and then click the "Relay" button located in the "Relay Restrictions" frame. This opens up the "Relay Restrictions" dialog box. The default configuration allows all computers that can authenticate to relay through the server. Authentication requires more overhead than what you really need, so you're better off allowing relay based on IP address. Since you only want to allow your Exchange Server to use the IIS SMTP Server as an open relay, select the "Only the list below" open and click the "Add" button. Select the "Single computer" option and type in the IP address of your Exchange Server. Click "OK", click "OK" again, and click "OK" one more time.

Bingo! You've configured the IIS SMTP Service to relay all messages sent from your Exchange Server.

You need to allow the IIS SMTP Service to act as an open relay for your Exchange Server because the Exchange Server needs to send SMTP mail to all Internet mail domains. There's no way you can know in advance which domains your users need to send mail to, so the open relay for outbound mail is required.

The situation is quite different for incoming mail. You only want to allow incoming mail for your own domain, mydomain.com. Incoming mail to other domains, such as msn.com or yahoo.com, should not be accepted by your mail relay server. If you allowed the IIS SMTP server to act as an open mail relay for incoming mail, spammers will relay spam through your open SMTP mail relay server and suck up all the bandwidth on your Internet interface. And once a spammer discovers you have an open relay, your server's IP address will be passed around the Internet so that everyone can chow down on your connection.

You need to prevent relay for incoming messages and you can do this by configuring your server to relay only messages destined to your own domain. You can configure "remote domains" for your own email domain and allow mail sent to your email domain to be relayed to your Exchange

Server. Inbound mail destined to other domains is dropped by the SMTP relay.

In the Internet Services Manager console, expand the "Default SMTP Virtual Server" node. Right click on the "Domains" node, point to "New" and click "Domain". On the first page of the Wizard, select the "Remote" option and click Next. On the second page of the Wizard, type in your mail domain name (mydomain.com in this example) and click Finish. Double click on your new Remote Domain name. Put a checkmark in the checkbox for "Allow incoming mail to be relayed to this domain". Then in the "Route domain" frame, select the "Forward all mail to smart host". Enter the IP address of your Exchange Server in the text box under this selection. Make sure to enclose the IP address in brackets, like [192.168.1.254]. The SMTP Service will treat the IP address as a FQDN if you don't put brackets around the IP address.

Now when the IIS SMTP Service on the mail relay server receives mail for mydomain.com, it will forward the mail to the Exchange Server. If someone tries to use your IIS SMTP mail relay server to send mail to hotmail.com, the SMTP mail relay server will drop the request. Cool!

A nice thing about the using an IIS SMTP mail relay server is that you can take down the Exchange Server for maintenance and none of the incoming mail will be lost. If the SMTP Service isn't able to deliver the mail, it will put it in a mail queue and retry sending the mail for up to two days (this is the default setting). Once you bring the Exchange Server back online, the SMTP Server will send the queued mail to the Exchange Server.

You can also set up multiple IIS SMTP Servers for fault tolerance. In our office, we have two IIS SMTP mail relay servers. I created two MX records and gave each record a different weighting. If the preferred SMTP server goes down, external mail can still be delivered to the secondary SMTP mail relay server.

We have carried this mail relay concept one step further, and implemented a IIS SMTP mail relay server on a third machine that has GFI's Mail Essentials spam filter program installed on it. The front-end SMTP mail relay servers accept incoming mail and relay it to the spam filtering SMTP mail relay. After the spam is filtered, the spam filtering SMTP relay sends the mail onto the Exchange Server. If the spam filtering SMTP relay goes offline, the mail is still queued on the front end SMTP mail relay servers.

These are just a few scenarios where you can take advantage of the IIS SMTP Service; there are many others. Once you understand the utility of the IIS SMTP Service, you'll be able to come up with applications of your own. If you use the IIS SMTP Service as a mail relay, or for anything else, drop me a line and let me know what you're doing with it. See ya next week!

This week's feature article by
Thomas W. Shinder,
M.D., MCSE

Ask Uncle Bill

Q and A's

Question:

Hi, Uncle Bill.
I've seen two examples of creating a DNS Caching Only Windows 2000 Server. One example says to use Root Hints and the other says to set a Forwarder. Will either one work? If you Enable Forwarders does this override the Root Hints? Does one take precedence over the other? From what I can tell, they both do the same thing. If the DNS Server can't resolve the name it requests resolution from another server, either the Root Hints server or the Forwarding server. I'm a little confused and any clarification would be greatly appreciated.
--Patcar

Uncle Bill says:

A DNS caching-only server doesn't have any zone files. So, there are two ways the caching-only server can resolve names: using the Internet Root Servers via a Root Hints file, or via a Forwarder. There are a number of reasons to use a Forwarder. One reason is that if you use your ISPs DNS server as a Forwarder, your DNS queries should be resolved more quickly, as the DNS cache at the ISP is much larger than what you might build up on your own server. Another reason to use a forwarder is for security reasons. You can put a caching-only DNS that uses a Forwarder on your DMZ and have your internal DNS server use your caching-only server as a forwarder. That way you insure that your internal DNS server is never contacted by an Internet server.

A caching-only server can use both the Root Hints file and a Forwarder. In this case, if the Forwarder is unsuccessful, the DNS server can perform recursion itself.

This is generally a bad idea, since it increases the time it takes to get a failure message. However, it does provide a degree of fault tolerance in the event that all your forwarders kick the bucket.

Question:

Hi, Uncle Bill
I have a question about multi-homed PCs. Can you configure a PC that has only one NIC with multiple IP addresses?? If possible, how? Thanks and have a good one.
-–Solhoyun

Uncle Bill says:

Want multiple IP addresses bound to a single interface? No problem! Just open the Properties sheet for your NIC, then click TCP/IP and then click the Properties button. Click the Advanced button, and on the IP Settings tab you'll see an Add button that will allow you to add more IP addresses to the interface. Why would you want to do this? Suppose you wanted to publish multiple SMTP servers on your internal network using ISA Server. You can only publish one service per IP address on the external interface. If one IP address is already using TCP port 25, then you'll need a second IP address to bind TCP port 25 to.

Another example of when you want to bind multiple IP addresses to an interface is when you use Network Load Balancing. You need to bind a primary address, and an address to be used as the NLB interface.

Don't Be Shy!

Got a question about MCSE certification or an event log error that just won't go away? Send it in! We'll be answering a question or two every week. Send your submissions to Uncle Bill **here**.

Security Advisories

SQL Extended Procedure Functions Contain Unchecked Buffers

▲ *to top*

Several of the Microsoft-provided extended stored procedures have a flaw in common: they fail to perform input validation correctly. This makes them susceptible to buffer overruns. Like all the other buffer overrun flaws we've run into, exploiting the flaw could enable an attacker to either cause the SQL Server service to fail, or to cause code to run in the security context in which SQL Server is running.

Read more...

News Headlines and Resources

Customizing the Command Prompt in Windows XP

▲ *to top*

We all have to go into the dark place from time to time. But it doesn't have to be dark! This article shows you how to customize the command prompt window it make it easier to look at and work with. A must read for anyone that spends time at the command line.

Read more...

Watch Out for the Klez.H Worm!

▲ *to top*

This email worm is making the rounds and it can put your private information at risk. Depending on the circumstances, this worm can attach a file on your hard disk to an email sent out to people in your addresses book. If that random file happens to be a text file with your password list then you're really out of luck!

Read more...

File Compression Whacks-out Disk Quotas

▲ *to top*

It's happened to me. Has this happened to you? You want to make sure you don't use up your disk quota so you compress your files. Bingo! You're over quota. But…you still have plenty of space left in your quota. What happened? Check out this article and find out!

Read more...

Put RIS into Overdrive

▲ *to top*

Think that RIS (Remote Installation Service) is just about installing Windows 2000 client machines? Think again! In this article they show you how to deploy your applications using the RIS engine. This is a very cool article if you're into the autoinstall mode.

Read more...

Load Testing Exchange 2000   ▲ to top

Ever wonder why one guy can tell you that his Exchange Server has been running smoothly for 6 months, and another guy says he's lucky to keep it up for two weeks? One of the major reasons for failure is an improperly sized server. Check out this article to learn how to do load testing to insure that you're sized your box just right.

Read more...

How to Configure an L2TP/IPSec   ▲ to top
Connection Using a Pre-shared Key

Want to use L2TP/IPSec but don't want to fiddle around with certificates? You can do use a pre-shared key to connect two Win2k RRAS Servers or a Windows XP and Win2k/Net server using L2TP/IPSec. This Q article has all you need to create the gateway to gateway L2TP/IPSec connection.

Read more...

Configuring and Using OWA in Exchange 2000 Server   ▲ to top

If you use Exchange 2000 and haven't implemented or investigated Outlook Web Access, you're in for a treat! OWA allows you to access your Exchange mail box via a Web interface. Check out this article by Will Schmied to get all the cool details.

Read more...

ISA Server Exam 70-227 Tutorial   ▲ to top

Ricky Magalhaes pulls out the stops in his three-part review of the Microsoft ISA Server exam, 70-227. This is an excellent review of the topics covered on the exam, so you don't want to miss it!

Read more...

Make Windows 2000 DNS and BIND Work Together   ▲ to top

Are you stuck with a BIND server and you need to make it work with your souped-up Windows 2000 DNS server? Don't throw in the towel until you read this article. All aspects of Windows 2000 DNS and BIND are covered here. A must read!

Read more...

Download of the Week

Tiny Key Logger   ▲ to top

Got a whacked out employee, a cheating spouse, or an out-of- control

kid that you need to keep tabs on? Then try out this totally FREE key logger program! Tiny Key Logger keeps track of every keystroke made on the victim's box and stores the information in an unencrypted file on the hard disk. The chump will never know what hit him! Download this goodie for free.

Read more...

Choice from one of these great WIN2K STUDY TOOLS:

- Win 2000 4 Core
- Win 2000 6 Pack
- Win 2000 8 Pack

90-Day money back guarantee.
We also sell separate study tools for all Win2K Exams!

For more information, click here

CramSession
Prepare for Success!