

Re: HOW MORE FRUSTRATING CAN THIS GET!!!

Source: <http://www.tech-archive.net/Archive/ISA/microsoft.public.isa/2004-06/0252.html>

From: Tony Su (*anonymous_at_discussions.microsoft.com*)

Date: 06/09/04

Date: Wed, 9 Jun 2004 09:08:35 -0700

OK,
Here is the SBS2000 skivvy...

SBS2K is actually alot easier to modify for varied use because security is more open by default and the IIS architecture is more integrated with traditional Windows architecture. Win2K is the last in a line of IIS which stored its metadata in a BIN file exclusively so you don't have to deal with utilities like SBSIISCONFIG and HTTPCFG.

The most common cause for problems in SBS2K is

– Not running the "To Do" Wizards. In particular, one wizard will re-enable the WAN adapter and another disables WWW socket pooling.

Beyond that, ISA2K configuration on SBS2K is fairly straightforward...

I have my own differing opinions about whether certain configurations are best, but in general the default shouldn't cause problems.

So specifically,
If you're deploying your own website you have three options, they're all possible <after running ALL the "To Do" wizards>...

– Packet Filtering. Simplest but supports only websites on the SBS box and the IIS Webserver is exposed directly. All you do is assign a valid public IP address in the ISM and configure inbound HTTP Server and HTTPS Server packet filters. Note that SBServer already has created these PF for you if you use the default WAN IP. Only PFs, no rules are used with this method.

Whereas Packet Filtering acts as only a screen to filter inbound/outbound traffic to a website on the external

interface, the following Publishing methods employ rules which forward packets from the External interface to the website on a Internal interface.

– Server Publishing. A caveat, never Server Publish your Default Website. You will see this recommended on many websites run by SBS authorities, but it is a mistake. If you choose to Server Publish a website, assign a LAN address which is unused to your website, then Create a Server Publishing rule that maps a WAN address to this LAN address for some particular protocol. Remember to stop/restart your ISA FW Service after making any changes. Compared to the PF method when publishing a website, your Web Server is still exposed but the website can be on any machine in your LAN. Unless you implement a Deny PF which could block Server Publishing, you should not configure or be concerned with PFs.

– Web Publishing. The preferred method with maximum security and performance. When Web Publishing, the User does not talk directly to the Webserver, the User talks to ISA on behalf of the Webserver. If the "conversation" is valid, ISA passes the "conversation" to the Webserver, and invalid traffic is rejected. Not only does the User session never touch the Webserver directly, you can configure caching which permits ISA to return Results lessening the load on the Webserver. To Web Publish, you first have to configure ISA to listen on the WAN address instead of IIS (Incoming Web Listener), then run the Web Publishing Wizard which configures a Destination Set(which describes the WAN interface), an Action (which describes the LAN address), and who this rule applies to (usually anybody). Like the Server Publishing rule, PFs don't enter the picture unless you've blocked access. Like Server Publishing, don't forget to stop/restart the Web Proxy service after making any changes to your Web Publishing rules.

So, this is only a thumbnail introduction which hopefully can clear up some of your confusion regarding what options you have and when rules or PFs are part of the solution and when they aren't.

If you're looking for some good resources for what you're doing, I recommend Harry Brelsford's books on SBServer, particularly his book for SBS2K for introduction to a wide variety of SBS features. Easy to read, I also give it high marks for accuracy, I very rarely read a technical book of its size with less than 3 errors throughout.

HTH,

Re: HOW MORE FRUSTRATING CAN THIS GET!!!

Tony Su

>-----Original Message-----
>"cjobes" <cjobes@nova-tech.org> wrote in message
>news:OdzQl6bTEHA.2944@tk2msftngp13.phx.gbl...
>> *This is the best answer in a newsgroup that I have seen*
for a long time.
>It
>> *really cut to the point. I will check out your link as*
well. Just one
>> *thing – it is an SBS2000 and not an SBS2003 – therefore*
I'm dealing with
>> *IIS5 and ISA2000.*
>
>*They are very different. Hold off till he deals with*
SBS2000 specifically.
>
>--
>
>*Phillip Windell [MCP, MVP, CCNA]*
>www.wandtv.com
>
>
>.
>