

# Re: SBS 3003 Premium – 2 NIC w/ Hardware Firewall

---

*Source:*

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.sbs/2006-07/msg02110.html>

---

- *From:* Blase <Blase@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>
  - *Date:* Sun, 16 Jul 2006 13:16:02 -0700
- 

I'm trying once again to get some clarity on this issue. I now have the X5 properly installed and everything is working fine – I get full access to VPN, remote workplace, rcp over http email, etc. But I am still getting some periodic hits, sometimes 2,500 at a session, where a bot program or something is attempting random login attempts to my server. That is why I opted for the external firewall device in the first place. Apparently the X5 will either not stop that kind of request, or I do not yet have it configured correctly to do so.

Seeing the suggestions from SuperGumby, I wanted to add the ISA protection noted. I never realized I had ISA 2000 as part of my SBS 2003 Premium software, however, so it has never been installed. SuperGumby suggested I not do so, but opt for ISA 2004 instead. So I downloaded ISA 2004 trial to see if I could configure it correctly, until further posts from Marina suggested I should remove it and use only the CD's that are specifically made for SBS 2003.

At this point, all I want to know is how best to get to ISA 2004 for my installation. I have always kept this server patched to the latest updates – so SBS 2003 SP1 has already been installed. Yet if ISA was never installed initially, it was obviously not updated to 2004 when I did the SP1 patch. So the question is how best to proceed. Should I install ISA 2000 from my original product CD's and then run the SP1 patch again? Or is there a better way? Marina's last post simply gave me the link to the SP1 download page. SP1 is already installed – but ISA is not. That is the problem here.

"SuperGumby [SBS MVP]" wrote:

I'm not familiar with the X5 so had a quick look at the manual. Very capable device and possibly a little on the 'overkill' side for someone who already has ISA implemented. I probably would have gone a more simple, and less expensive, 'simple NAT router' instead.

By implementing the X5 in front of a two NIC ISA SBS you need to consider some items.

The device itself has VPN endpoint capability, the manual however also

Re: SBS 3003 Premium – 2 NIC w/ Hardware Firewall

suggests it supports PPTP passthrough. I mention this because I don't know how well the X5 handles it, it may work perfectly, many VPN capable devices interfere with terminating the tunnel at the SBS.

The manual has instructions for disabling the browser proxy settings, disregard these instructions in your situation. You will want your internal clients to use ISA as proxy, it will then send requests through the X5. It is possible to configure ISA to use an 'upstream proxy' but this is not automatically configured, if you had manually configured ISA to use an upstream proxy it is this which should be removed to allow the X5 to 'transparent proxy' requests through it.

The manual seems to suggest that the X5 defaults to 192.168.111.1/24 (/24 is shorthand for a subnet mask of 255.255.255.0, 24 bits) so having your internal network running 192.168.16.0/24 (SBS default) is fine. The external IP address on the SBS should be set to any IP in the 192.168.111.x/24 range, 192.168.111.2 would seem sensible.

your IPConfig should look something like:

```
C:\Documents and Settings\Administrator>ipconfig /all
```

Windows IP Configuration

```
Host Name . . . . . : sbs
Primary Dns Suffix . . . . . : lc.lan
Node Type . . . . . : Unknown
IP Routing Enabled. . . . . : Yes
WINS Proxy Enabled. . . . . : Yes
DNS Suffix Search List. . . . . : lc.lan
```

Ethernet adapter Server Local Area Connection:

```
Connection-specific DNS Suffix . :
Description . . . . . : NetServer 10/100TX PCI LAN Adapter
Physical Address. . . . . : removed
DHCP Enabled. . . . . : No
IP Address. . . . . : 192.168.16.2
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . :
DNS Servers . . . . . : 192.168.16.2
Primary WINS Server . . . . . : 192.168.16.2
```

Ethernet adapter External:

```
Connection-specific DNS Suffix . :
Description . . . . . : Realtek RTL8139 Family PCI Fast
Ethernet
NIC
Physical Address. . . . . : removed
DHCP Enabled. . . . . : No
IP Address. . . . . : 192.168.111.2
Subnet Mask . . . . . : 255.255.255.0
```

Re: SBS 3003 Premium – 2 NIC w/ Hardware Firewall

Default Gateway . . . . . : 192.168.111.1  
DNS Servers . . . . . : 192.168.16.2  
NetBIOS over Tcpiip. . . . . : Disabled

at this point you would run the CEICW with the X5 connected to the external interface. A curiosity here is the choices you take. The most obvious choice would be that you connect through 'A router with an IP address', DO NOT select this, instead taking the choice 'Fulltime broadband connection'. The router choice is, basically, designed for an ISDN or similar 'demand dial' connection.

You should now be able to open the web interface on the X5. You'll need to configure it to connect to your ISP and also set the port forwarding to SBS. For RWW you want to forward 443 (RWW itself), 444(CompanyWeb), and 4125 (RWW's RDP proxy). For PPTP VPN you need TCP/IP port 1723 and TCP\_protocol\_43 GRE, this may be controlled in a single section controlling PPTP passthrough (sorry, I didn't go that far through the manual).

You mention FTP. Do you wish to allow outgoing FTP (in which case I expect nothing need be done on the X5, but you need to turn off the 'read only' in ISA FTP controls) or are you running an FTP server on SBS?

OWA and RPC over HTTPS will also use the port forwarding for 443, same as RWW.

"Blase" <Blase@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message  
[news:226682CA-C78D-42E3-ACFF-38E34E5230EE@xxxxxxxxxxxxxxxxxxxx](mailto:news:226682CA-C78D-42E3-ACFF-38E34E5230EE@xxxxxxxxxxxxxxxxxxxx)

I've had SBS 2003 Premium running for 2 years and recently upgraded to a new server. Wanted to add a firewall appliance for more protection, as we are seeing an increase in random login attempts – sometimes 3000 an evening. The ISA provided software firewall has held to date, but the redundancy seems like a good idea.

Am struggling to get the configuration correct, however. Have the internal NIC appropriately working as 192.168.16.2 defaults. Have a static IP address from our ISP assigned to the external NIC. But I assume I now need to assign the external static IP address to the firewall appliance, using a gateway address to point to the current server external NIC. Is that correct? And if so, what address should it use? Should it be in the same subnet as the internal NIC?

Assuming I get this properly configured, how do I configure the firewall ports correctly (I'm obviously new to firewall setup)? I'm using VPN, FTP, OWA and RPC over HTTP for Outlook in addition to typical internet access. The

Re: SBS 3003 Premium – 2 NIC w/ Hardware Firewall

hardware appliance is a Firebox X5 by WatchGuard, if that matters at all.

Any ideas out there?