

PIX501 ISA SBS2003 Network Setup Thoughts

Source:

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.sbs/2006-11/msg01343.html>

- From: jimjawn@xxxxxxxx
 - Date: 7 Nov 2006 17:18:33 -0800
-

LONG! Pre-emptive "Thanks!"

Hi All! I'm looking for some recommendations from you fine folks. I've got a customer that develops web software. Recently they've purchased a new server, a copy of SBS 2003 (with ISA 2000 and SQL 2000) for its feature set. Additionally, they've purchased a PIX501 firewall because they wanted a "more secure firewall and VPN solution". This was the setup I was handed.

Currently, my client has 4 public IPs with http and terminal services ports pointing to 3 windows 2000 server boxes and 1 pointing to the SBS server. All of the machines are on the same subnet and win2k boxes do a LOT of things including VMWARE, SQL & Printer & Fax Serving and IIS to name a few.

This is working well. However, my client needs to track where all of their employees are going which presents a problem. Normally, I'd install ISA set it as the default gateway and leave it be, however, by having the default gateway not the SBS server, the clients can essentially "go around". On top of that, the client machines are all laptops. So I can't just create a Group Policy, hide the Internet Connections tab and force them to proxy because they connect at home and need to logon to a separate VPN solution.

I wanted to block port 80 outgoing on the PIX and force the outgoing requests on 8080 but that's not an option (I believe) because I'm serving out web pages on port 80 from win2K, a requirement for their application.

So I move all of the win2k servers to a DMZ like PIX -> DMZ -> SBS -> LAN setup. However, because the win2K servers are running so many critical applications, they need to remain domain members. However, I can't access any of the LAN computers from the DMZ with the default SBS setup and, from the documentation I've read, Microsoft does not support domain members in a perimeter network. Also, I need employees to be able to publish websites on the SBS server but NOT be able to change any of the ISA settings, including site publishing which also presents a challenge.

PIX501 ISA SBS2003 Network Setup Thoughts

So my questions would be:

- 1.) Are there any alternative setups that I should consider for this setup? Modifying only the PIX or purchasing an alternative proxy product that can track where employees browse?
- 2.) Would it make sense to add the DMZ servers onto the LAN using VPN? That way they would show up as members on the LAN and kind of bypass the ISA server right?
- 3.) What would I need to do in order allow all of the DMZ computers get full access to the LAN in ISA if the VPN won't work? Or can I do it with just ISA? I think I'd need a static route somewhere...
- 4.) Is there anyway to disable site publishing and just allow all incoming 80 connections in ISA?
- 5.) Anything else I need to consider?

Whew! As you can see there are a lot of variables and problems that need to be considered and this is by far my most challenging SBS setup. Any help you can provide would rock!

Thanks for reading this and your help.

.