

# Re: More DMZ

---

*Source:*

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.sbs/2006-07/msg00627.html>

---

- *From:* "JosephByrns" <josephbyrns@xxxxxxxx>
  - *Date:* Thu, 6 Jul 2006 14:25:46 +0100
- 

From your reply I, think I am doing most of what you list, that I can do

with SBS2003. Without buying a new exchange server I don't think there is anything I can do about getting exchange out of the network. I already have Exchange aware AV for instance.

This may be a stupid question, but out of curiosity, how do users get the email off the Exchange server in the DMZ? Do you set up a rule in the firewall to allow them to get it directly from the Exchange server, or do you somehow synchronise the DMZ Exchange with another one in the LAN?

As for point 3, I currently allow access by RWW, but will consider the PPTP/IPSec part (which I am assuming means setup a VPN?)

Thanks AGAIN for your help.

"Leythos" <void@xxxxxxxx> wrote in message  
[news:SH7rg.11254\\$Eh1.6672@xxxxxxxxxxxxxxxxxxxxxxxxxxxx](news:SH7rg.11254$Eh1.6672@xxxxxxxxxxxxxxxxxxxxxxxxxxxx)

In article <#xvpZCNoGHA.4728@xxxxxxxxxxxxxxxxxxxxxxxx>, josephbyrns@xxxxxxxx says...

I now have a new firewall in place (DFL-700), with a new DSL modem (DSL-300) on a single NIC SBS2003 (which I believe is secure enough, with the firewall). I am about to use the DMZ port on the firewall to add a webserver.

It occurs to me that there are other ports available to internet (other than the DMZed port 80), such as Remote Desktop, port 25 for email and exchange on https. These ports are directly available through the firewall to the LAN, i.e. not being routed through the DMZ port. While I may have secured the webserver my concern is that these other ports are making the system vulnerable.

## Re: More DMZ

Are my concerns warranted and if so what are my options?

Any exposed, meaning any ports that you expose to the public, are a risk at some level.

I never allow port 80 inbound to the LAN, only to the DMZ servers.

I allow SMTP to a server in the DMZ, but it's a single dedicated Exchange server that has no active directory connection to the LAN server/networks – yea, this is a pain, it requires double entry in that you create a user in the LAN network and then have to create the same user in the DMZ Server, but I never allow them to manage passwords in the exchange server in the DMZ and I use some very strong passwords. This has to benefits – it means that all email stays in the DMZ, provides OWA via SSL in the DMZ, and it means that "I" control email passwords – it also means that I have the firewall set to remove almost every email attachment to standard users, the AV Exchange aware scanner doing full email scans BEFORE it reaches the Exchange service, spam and other filtering.... If the Exchange server is compromised it doesn't impact the LAN.

I also do a lot of other non-standard things, but I've never had a facility compromised.

While you can't do this with SBS, you can do a lot of the basic security measures:

- 1) SMTP – you have to allow it if you want email
- 2) SSL – if you want to allow web mail you need to allow it
- 3) Remote connections – RWW or setup firewall to act as PPTP/IPSec server and then map users through firewall to specific services on LAN
- 4) All public access in a real DMZ

Don't allow access from the DMZ to the LAN, or restrict it to a specific IP/Port.

As for the ports, you need to map them from WAN to Network by IP/Port, which means that they can't be mapped anywhere else.

Yes, they will be a risk, but you have no way to expose them and not assume some risk.

--

spam999free@xxxxxxxxxx  
remove 999 in order to email me