

Re: Hosting, in or out?

Source:

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.sbs/2008-10/msg00381.html>

- *From:* Leythos <void@xxxxxxxxxxx>
 - *Date:* Sat, 4 Oct 2008 20:40:28 -0400
-

In article <6kq7rlF96019U1@xxxxxxxxxxxxxxxxxxxx>, holz@xxxxxxxx says...

Our client has an SBS 2003 with a SQL server installed, 40 users, the proprietary SQL based application is the core of the business.

A new requirement calls for a report only server, one that will obtain the data from the SQL server and allow outside customers to pull their own status reports. The server will run ASP, .NET framework 3.5, all built with Visual Studio.

I suggested we host it outside on their ISP (he offers dedicated Windows hosting) rather than inside, their developer insists on inside hosting, i guess for ease of development. There is a good Cisco perimeter, however my concern is bandwidth and overall security.

I would like to hear more opinions.

First, hosting the Front-End to a database outside the clients building will be a problem performance, security, etc...

Second, you NEED A REAL FIREWALL, NOT ISA on SBS, you need a real firewall appliance that permits you to make very secure network rules.

SO, lets start with the basics:

Internet (need 2 IP, one for your SBS SSL connection and 1 for your Front-End website SSL Connection).

LAN:

SBS LAN is called PRIVATE or LAN

Web LAN is called RESTRICTED or DMZ

Firewall:

Public: Assign your static IP's to it

LAN: 192.168.x.0/24

DMZ: 192.168.y.0/24

PUB>LAN SSL1, 4124, and other SBS needed ports

Re: Hosting, in or out?

PUB>DMZ SSL2, HTTP (only if needed)

LAN>PUB SSL, HTTP, DNS, etc....

DMZ>PUB SSL, HTTP, DNS, etc... needs to get updates from MS/AV company

DMZ>LAN SQL–Data (TCP 1433) map direct to SBS Server IP, only 1433

LAN>DMZ SSL, FTP – do not open all ports

With this method you can only reach the LAN from the DMZ on the SQL Server Data Port – TCP 1433 – never expose this port outside your LAN/DMZ

This also means that if someone compromises your DMZ that they can't get back into your LAN.

NEVER, NEVER, NEVER allow the Developers to code their queries/connections using the SA database account and never allow them to use Windows Authenticated connections between the DMZ and LAN.

--

– Igitur qui desiderat pacem, praeparet bellum.

– Calling an illegal alien an "undocumented worker" is like calling a drug dealer an "unlicensed pharmacist"

spam999free@xxxxxxxxxx (remove 999 for proper email address)

.