

Re: Best practices: Two nic's but have hardware firewall

Source:

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.sbs/2006-02/msg05165.html>

- *From:* "SuperGumby [SBS MVP]" <not@xxxxxxxxxxx>
 - *Date:* Tue, 28 Feb 2006 14:35:59 +1100
-

I don't agree with much Tom says, and this article is more than a little 'skewed', but I find it of interest:

ISA Firewall Fairy Tales – What Hardware Firewall Vendors Don't Want You to Know (v1.02)

<http://www.isaserver.org/articles/2004tales.html>

"Child" <SpamFreedawg@xxxxxxxxxxx> wrote in message news:1207duo2biltq46@xxxxxxxxxxxxxxxxxxxxxxxxxxxx

"SuperGumby [SBS MVP]" <not@xxxxxxxxxxx> wrote in message news:edJnsoAPGHA.2176@xxxxxxxxxxxxxxxxxxxxxxxxxxxx

Yes, a Firebox is a real firewall appliance.

But then, you also suggest you have 'Premium'.

It's been a good 18mths since I dealt with a firebox so my info may be out of date. I consider it a good appliance but ISA (only discussed because you are entitled to install it) has the additional function of 'application layer' filtering. The firebox I dealt with was not connected to SBS, and didn't have the option of ISA (three servers and a device which could easily have been replaced by a single SBS Premium, but someone else had already persuaded them otherwise. We picked up support when they dropped the ball). My thoughts at the time were along the lines 'SBS/ISA with the external port connected to the "inside" of the firebox and the "optional" port of the firebox connected direct to the internal network', I did it as a thought experiment but never implemented it, also toyed with the idea of swapping the use of the two firebox interfaces. I see that the 700 product description refers to what was, on the unit I dealt with, the 'optional' port as a DMZ port. To use that I would want a routed public subnet and consider it 'external' to SBS with ISA.

so far I haven't used my "optional port" although i should – i do have a separate WWW server that should be on there.

Re: Best practices: Two nic's but have hardware firewall

I, with my familiarity with ISA, prefer its capabilities (AD integration, logging, reporting) as compared to most firewall appliances. I guess I'm just saying I'm biased. BUT some things become complicated when you have both a device and ISA, terminating a VPN 'inside' the network being one thing.

IMHO you need to make a decision. You have (again IMHO) an _almost_ ISA equivalent available. If you want ISA e-bay the appliance and get a simple NAT router. If I decided to keep the appliance I would (at least at first) go with a single NIC.

I suppose I feel comfortable with my firebox, because I know far more about it than ISA. But perhaps its a good time to learn more about ISA and try to make a more informed decision. Its interesting that my inherent bias is that the firebox, being hardware, is more secure than ISA, being software, however of course, they are both software running on hardware, so thats just silly.

Attach a small switch to one of those firebox interfaces and visitors get full internet access, but the same could be said of a simple NAT router. The firebox however may protect visitors to a greater extent.

Thanks so much for your help. Its been great!