

Re: hardware firewall

Source: <http://www.derkeiler.com/Newsgroups/comp.security.misc/2004-01/0081.html>

From: Leythos (void_at_nowhere.com)

Date: 01/07/04

Date: Wed, 07 Jan 2004 19:13:28 GMT

In article <btjh6f\$2c5p\$1@nyheter.ipsec.se>, phn@icke-reklam.ipsec.nu says...

> Leythos <void@nowhere.com> wrote:

> > In article <bt9sk\$28l4\$2@nyheter.ipsec.se>, phn@icke-reklam.ipsec.nu

> > says...

> > > Leythos <void@nowhere.com> wrote:

> > > > In article <qbbnv4f9ndk2lfs59iavup2no8t3ctf64@4ax.com>,

> > > > chris@nospam.com says...

> > > > On Mon, 05 Jan 2004 23:20:42 GMT, Leythos <void@nowhere.com> wrote:

> > > > [snip]

> > > > >To be honest, you might be better off purchasing a copy of Windows 2000

> > > > >Server and using a Linksys Router with NAT. The cost of a good firewall

> > > > >that will also provide IP restrictions will cost more than the Server

> > > > >software and a simple NAT router.

> > > >

> > > > Have you priced W2K Server lately?

> > >

> > > > Yes, Server 2000 standard will run on any beefy workstation and is only

> > > > \$700 US. It can be purchase for less if you are a non-profit or a

> > > > educational member. You can also subscribe to the MSDN, if you are a

> > > > developer of MS products you should already have this, and install

> > > > anything they make.

> > >

> > > I can obtain a linx server AND HARDWARE for \$700

>

> > And it would not help him at all – he's developing on a IIS platform the

> > comment was about firewalls and security based on his question. He

> > wanted to restrict the site to specific IP's.

>

> > Shure it would have helped him. The discussion was (read yourself)

> > about installing a hardware firewall outside his wintendo boc)

he wanted to limit the connections to his Windows development web server to specific IP's, and I pointed out that he could do it with server 2000 without purchasing any firewall. Since he would probably want to continue to develop, 2000 server is a great platform.

> > \$700 does not buy much in the way of quality hardware.
>
> We don't live in the same world. I can purchase a DELL dimension 2400
> for 2 790:– Svedish crowns (divide by 7) I need to add
> memory and one NIC .

Nope, we don't – the 2400 is a VERY LOW END system that has little performance until you ADD a lot to it. The base system from Dell has limited performance.

I know Dell systems quite well, I spec'd more than 200 of them last month and am installing over \$328K worth of them next week.

[snip]

> > What down time – he's already on a MS Platform, so there is no downtime.
> > I would assume, from your comment, that you've never run a Windows based
> > server on anything, or that you've never run it on a quality hardware
> > platform.
>
> I mean down-time of an additional windows machine, which needs to
> be rebooted for each and every service-pack installed. How often
> do they come ? My *BSD machines has been "secure" from the CD
> and are often running (yes running with zero downtime) for years.

He doesn't need an additional machine, and not every service pack requires a reboot – in fact, there have not been that many service packs out for a while. SP4 for 2000 has been out for a long time and security updates, while common, don't always require a reboot.

For his development purpose, a reboot once a week is nothing.

How about addressing how long it's going to take him to learn BSD or RH or any other flavor before he can start being as productive as he currently is?

As for downtime, until it was replaced by a Windows 2000 server OS, I had a NT 4 PDC running 24/7 in a factory that had more than 2 years UP-TIME on it. It's not the OS, it's what you know.

> > Why didn't you address the downtime needed to install, learn, reinstall,
> > configure, reconfigure, etc... a Linux install that the user has no
> > experience with.
>
> That can be bought for less money then a windows license. Look for
> "packced linux-based firewalls"

No one is disputing that most Linux installs are free, I never did. I said that cost of setting it up, maintaining it, converting to that platform, the cost of being down while learning it, is NO FREE.

[snip]

> > *Um, you need to look a little deeper – those 99% are mom and pop shops
> > and home users. I would venture a guess and say that professional IIS
> > installs from hosting companies are as secure a Apache and Java based
> > solutions.*
>
> *I guess that mom&pop shops runs on all kind of hard–software. In fact
> they do.*
>
> > *It's nice that you can pull the numbers that you want to see without
> > understanding them.*
>
> *What did i not understand ? Please specify !*

That 99% of those 99% are home users, mom–pop ISP, and others that don't really understand what security is. If you look at the professional installations of IIS / Windows Servers, very few of them are compromised. It's almost always a case of a developer or home user installing and not updating or securing their systems.

> > > *So, considering he appears to be a MS platform developer, a box like you
> > > suggest makes no sense for him unless he wants to abandon the MS
> > > platform.*
> > >
> > > *http != MS*
>
> > *I never said it was, I said that if he's doing IIS, which means he's
> > almost certainly doing ASP, then your solution would not work.*
>
> > > *I always love how people say that Linux is free – but they never
> > > consider the cost of conversion for the apps, technicians, support
> > > centers people, etc... And they always said it can run on an old P200
> > > system, BS, to run a "server" acting as a decent box you need at least a
> > > P3 with good drives and memory to match.*
>
> > *I see you forgot to address this one.*
>
> *No, but it's irrelevant to running a firewall. GUI is bloaty, and
> to little memory will make linux and *BSD system slower.*

And it does not address his problem or what he wants, it only addresses what you wanted to say. His problem is that he wants to limit connections by IP, and he develops websites on a Windows platform. With the server version he can do that with no additional hardware – he could replace his 2000 Professional OS with 2000 Server and do what he wants.

> > > *I have a RH 9.1 install running on a Celeron 466 with 512MB of RAM and
> > > 30GB of drive space and opening office on it is slow as hell, and most
> > > times it looks like it's locked up. On a P4 it screams.*
>

- > > *I see that you forgot to address this one too.*
- >
- > *What should i say ? What does 'top' tell you about lack of memory ?*
- > *What unneeded daemons are running ? Of course anything will run faster*
- > *on a P4 – is that surpricing ?*

Ah, but you didn't say anything about limiting it – you listed a large group of services that could run on a lowly PC and I said BS. Heck, you even added another computer to his development network just to do something that the OS can already do.

I suppose you didn't know that the 120Day Eval Version of Windows 2000 server is free too.

--
--
spamfree999@rrochio.com
(Remove 999 to reply to me)