

Re: Front-end / Back-end Security Question

Source:

<http://www.tech-archive.net/Archive/Exchange/microsoft.public.exchange.design/2005-04/msg00032.html>

- *From:* "Brian Desmond [MVP]" <desmondb@xxxxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Tue, 5 Apr 2005 22:17:50 -0500
-

Hi there,

I'll reply inline.

--

--Brian Desmond
Windows Server MVP
desmondb@xxxxxxxxxxxxxxxxxxxxxxxx

www.briandesmond.com

"-=gu=-" <gu@xxxxxxxxxxxxxxxxxxxxxxxx> wrote in message
news:5E599A97-412F-4C9A-A7A2-6855BE99AA2B@xxxxxxxxxxxxxxxxxxxxxxxx

> Brian and Al, thanks for your responses.

>

> To follow up and give a little more information, we have around 40

> employees

> and perhaps 4 or 5 of them use OWA as their full time email client, the

> rest

> use Outlook 2003 either internally or from outside locations using VPN. I

> fully understand and realize that I am exposed to ears on the wire without

> running https. That is what is driving all this.

>

Yeah so a frontend makes absolutely no sense here. Just get an ssl cert from thawte or somebody (just don't go with verisin) and install it on your backend. That's a big big plus.

> We actually do own a Cisco DMZ switch, and it's never been used. However,

> I

> don't have an interface on my PIX 515 to plug it in. Before my time, the

> company downsized and ended up subletting space to another company. So the

> 2

> interface PIX has been configured for two separate networks, one for my

> company's LAN and one for the other company. Both share the same T1

> internet

Re: Front-end / Back-end Security Question

> bandwidth through this configuration.
>

I've never heard of a cisco dmz switch. I don't know PIX at all, but you can't trunk the switchport going to it and run multiple vlans off the interface?

> These are what I see as my options, comments are welcome:
> a) call Cisco presales and see what a 3 interface PIX would run so I could
> utilize my DMZ hardware. I honestly don't know if a 3 interface model is
> made, but if I were to be able to keep the two networks separate AND set
> up a
> DMZ then I would be able to procede with putting up an Exchange FE server
> in
> the DMZ. We also have a couple of web IIS servers which I would then put
> in
> the DMZ as well.
> b) barring the funds to purchase replacement Cisco equipment and put up a
> DMZ, I could instead put up an ISA server (help me out here...) to
> authenticate the OWA traffic (?). In that circumstance I suppose my cert
> would go on the single Exchange 2003 server? I'm not sure how I would
> utilize
> this.

So I don't know why you want to build this DMZ so badly. I don't think it's useful at all in your situation. The ISA04 box to be a gateway to your LAN for OWA, VPN, etc would be fine. I think Al knows more about ISA94 than I do (I know enough to install it), so I'll leave any ISA stuff to him.

>
> Finally adding insult to injury, we actually have an old ISA 2000 server
> in
> place (currently natted through the pix) which is there to authenticate
> the
> VPN traffic. My predicesor scared the bejesus out of me when I spoke with
> him, he told me it took a really long time to set up and his advice was to
> ghost it to disk and leave it alone, which I have done. I don't know if
> this
> could be used for the above or not. I also believe that being a MS
> partner,
> our program allows us to run a copy of ISA server. Could I build a new ISA
> server and use it for both VPN and OWA traffic purposes?
>

See above. ISA2000 box needs to go esp given this information.

> Obviously I don't have a great handle on this technology and I appreciate
> any help and suggestions you may have. Thanks in advance!
>

No problemo.

- **References:**

- ◆ **Front-end / Back-end Security Question**

- ◇ *From: -=gu=-*

- ◆ **RE: Front-end / Back-end Security Question**

- ◇ *From: -=gu=-*

- Prev by Date: **Databases & Transaction logs on same spindle**
- Next by Date: **Re: Should I use a Front -End server**
- Previous by thread: **RE: Front-end / Back-end Security Question**
- Next by thread: **Should I use a Front -End server**
- Index(es):
 - ◆ **Date**
 - ◆ **Thread**