Re: DMZ / Firewall question

Source:
http://www.tech−archive.net/Archive/WinXP/microsoft.public.windowsxp.network_web/2006−03/msg00127.html

- *From*: "Mike Lloyd−Jones" <mike@xxxxxxxxxxx>
- *Date*: Fri, 3 Mar 2006 08:19:46 −0000

Hi
Apologies, it is an FXV538
(http://www.netgear.co.uk/vpn_firewall_router_fvx538.php)
We are using ADSL, and the reason we want this PC/server to be "local" is so that we don't have to upload what are very large files across a 256k upstream link.
I guess the question is if we attach the PC to the DMZ port (192.168.10.x) can we still access it from the LAN (192.168.0.x) ?
Thks

"Chuck" <none@xxxxxxxxxxx> wrote in message
news:d6pe0292qukub3iuquad321buc4g5mjafr@xxxxxxxxxx

> On Thu, 2 Mar 2006 18:53:02 −0000, "Mike Lloyd−Jones" <mike@xxxxxxxxxxx>
> wrote:
>
> > "Chuck" <none@xxxxxxxxxxx> wrote in message
> > news:483e02dpvrco33t7jv9nldbprrau6me3l9@xxxxxxxxxx
> >
> > > On Thu, 2 Mar 2006 09:00:28 −0000, "Mike Lloyd−Jones"
> > > <mike@xxxxxxxxxxx>
> > > wrote:
> > >
> > > > Hi
> > > > Not strictly related to XP, but maybe
> > > > someone can help ?
> > > >
> > > > Have a Netgear DSL modem/router with a
> > > > DMZ port.
> > > > LAN side of the router has a number of XP
> > > > PCs.
> > > > We want to connect a PC to the router so it
> > > > is publicly accessible to

> the
> Internet for customers to download files.
>
> Guess we have 2 options:
>
> 1) Port forwarding to allow FTP or whatever
> through, directed to that
> PC.
> Problem here is that since the PC is still
> connected to the LAN this
> opens
> up a potential security risk to the rest of the
> network

You are correct. NAT routers are great security when all that
you do is
surf
the Internet. When you need to run an Internet server from a
NAT router
LAN,
you have to open a hole in the router, and this will indeed
expose your
LAN.

> 2) Connect the PC to the DMZ port on the
> router. This keeps it secure,
> but
> we still need to be able to copy files to this
> from the LAN side (for
> customers to download). Can a route
> generally be configured from the LAN
> to
> the DMZ which is "one−way" so that we can
> copy files up to DMZ computer
> but
> no access the other way?

On most NAT routers (and here the model of the Netgear
might be useful)
the
"DMZ" is really just a virtual server port, protected by the
firewall
components
(if your router has any such), and connected openly to the
rest of the
LAN. No
routing or firewall rules are necessary, or are possible.

In most domestic DSL LANs, you will find it best to host any server offsite.
Security, as noted above, is not easily done with a typical DSL modem / router.
Asynchronous DSL, which is what most DSL is, provides for most bandwidth to support surfing of the Internet (downward bandwidth). What little bandwidth in the other direction (upward) is generally taken up by surfing, and if any surfing is going on the upward bandwidth (which is what your customers will depend upon for their downloads) is unlikely to be available in any reliable amount.
Some DSL services explicitly prohibit servers for this reason.

In short, you can connect a server to your modem / router. Depending upon the model, you may or may not be able to do this without exposing your LAN.

Thanks for the reply
It's a Netgear FVX318. We want a PC connected to it's DMZ port so we can upload files to it from the LAN PCs and so that external customers can access those files..
Mike

OK, Mike,

Do you maybe have a FVS318? I can't find anything about an FVX318.

From what I'm reading about the FVS318, is that it is not a simple NAT router, it's more of a firewall with NAT built in. That should make your DMZ an actual

separate VLAN, potentially, and you should indeed be able to put an Internet
server on one port, and have that server isolated from the others.

I'll stand firm with my advice about using DSL (do you have ADSL or SDSL?) for
serving data across the Internet. Co located servers are similar in concept to
edge hosting, they move the traffic closer to the clients. Many ISPs provide co
location, in various autonomy and service levels, for reasonable prices.

But, if you do go with your personally hosted server, you can make your LAN
secure while doing the hosting.

--
Cheers,
Chuck, MS-MVP [Windows - Networking]
http://nitecruzr.blogspot.com/
Paranoia is not a problem, when it's a normal response from experience.
My email is AT DOT
actual address pchuck mvps org.

.