

Re: Please explain port forwarding..

Source: <http://www.derkeiler.com/Newsgroups/alt.computer.security/2004-05/0722.html>

From: Paul H (*nospam_at_nospam.com*)

Date: 05/19/04

Date: Wed, 19 May 2004 17:31:25 +0100

"Leythos" <void@nowhere.com> wrote in message
news:MPG.1b153213f1500f2f98a549@news-server.columbus.rr.com...
> *In article <3AJqc.19\$kK3.9@newsfe6-win>, nospam@nospam.com says...*
>>
>> *"Leythos" <void@nowhere.com> wrote in message*
>> *news:MPG.1b1529e9e252090b98a548@news-server.columbus.rr.com...*
>>> *In article <F_Iqc.15\$kK3.6@newsfe6-win>, nospam@nospam.com says...*
>>>> *I have a NAT router with an SPI and several PCs on a peer network. I*
>>> *have a*
>>>> *good understanding of networks but....*
>>>>
>>>> *I have never been able to get what is really happening with port*
>> *forwarding.*
>>>> *Even though I have usefully configured my router to forward ports, I*
>> *don't*
>>>> **really* know what I am doing.*
>>>>
>>>> *So, If I configure my NAT router to forward port 10,000 to*
192.168.0.26
>> *on*
>>>> *my network does that mean?....*
>>>>
>>>> *Forwarding, means that the port specified that arrives inbound on the*
>>>> *specified public IP address (in case you have more than one) will be*
>>>> *forwarded to the specified internal IP address – no filtering, just*
all
>>>> *data on port X will be forwarded to that IP.*
>>>>
>>>> *So, assuming that you are using a simple NAT router on a DSL/Cable*
>>>> *connection with 1 public IP address:*
>>>>
>>>> *Forwarding –*
>>>>
>>>> *IP Address PORT Enable*
>>>> *192.168.10.200 80 X*
>>>> *192.168.10.200 443 X*
>>>>

alt.computer.security: Re: Please explain port forwarding..

> > > *In the above example, all inbound traffic on your Public IP address for*
> > > *ports 80/443 will be forwarded to the internal IP of 192.168.10.200.*
> > >
> > > *If you had more than 1 public IP and a router that handles it, you can*
> > > *create rules that allow you to specify the public ip, port, internal*
ip,
> > > *port, and enable/disable.*
> >
> > *Thanks for your reply.*
> >
> > *So is port forwarding a security risk?*
> >
> > *If I understand you correctly, **any** packet arriving at my routers WAN*
> > *address destined for port 10,000 will be forwarded straight on to*
> > *192.168.0.26.*
> >
> > *So would someone scanning my network see port 10,000 as open or closed?*
> >
> > *Or if there was a worm going around that tried to get in via port 10,000*
> > *would it get straight through to 192.168.0.26?*
> >
> > *..still confused.. :o/*
>
> *Any data sent to port 10000 will be forwarded directly to the internal*
> *address – there is no filtering, nothing, it just goes directly to it.*
> *it would be considered OPEN to anyone.*
>
> *So, if you opened port 1433/1434 (MS SQL PORTS) and forwarded them to*
> *your MS SQL server, you would be compromised in a short time since there*
> *are still many traces of the SQL Slammer worm running around.*
>
> *If you need port forwarding you need to secure the machine that is the*
> *destination of the forward – meaning that if you were running a web*
> *server behind the router, you had better have locked it down (based on*
> *the Web Server OS vendor suggestions), be running a strong Anti-virus*
> *package, and have changed all accounts/passwords so that they don't*
> *match any accounts/passwords on your other machines.*
>
> *Port forwarding is not a security threat, it's a normal way of doing*
> *business – a threat would be the unsecured machine that is the*
> *destination of the port forwarding. The best rule is that if you don't*
> *know what you are doing, if you don't know how to secure it, if you are*
> *unsure in any way, don't forward.*
>
> --
> --
> *spamfree999@rrohio.com*
> *(Remove 999 to reply to me)*

Thanks a million for this, the penny is starting to drop..:O)

Re: Please explain port forwarding..

alt.computer.security: Re: Please explain port forwarding..

One more thing..

A common reason for a home user to mess with port forwarding is for gaming. Given what I now understand, why should a gamer have to do this? I can understand why exchange or SQL server would need port forwarding but why would a game need this just for multiplayer purposes, especially if he is ****not**** running a server just a workstation and wants to join in the online fun?

Thanks, last question..(promise)

:O)