

Re: Firewall and ftp service

Source: <http://www.derkeiler.com/Mailing-Lists/FreeBSD-Security/2001-07/3949.html>

From: Axel Scheepers (ascheepe@surf.iae.nl)

Date: 07/09/01

Date: Mon, 9 Jul 2001 09:29:43 +0200
From: Axel Scheepers <ascheepe@surf.iae.nl>
To: freebsd-security@FreeBSD.ORG

Thank you all for your help! ;-)

I do use kind of a mix of ipf/ipfw/natd at the moment, but that was because I wanted it working as fast as possible (Just switched from modem to cable ;-). Now my first "Wow, I want to do ... and ... and .." feelings are over I want to figure out a nice clean way for doing it. So thank you all for your great responses, you've given me a lot of starting points (ipnat instead of natd) and help (ftp howto ;-)

Thanks,

Axel Scheepers

On Sat, Jul 07, 2001 at 11:38:49AM –0700, Crist J. Clark wrote:

> On Sat, Jul 07, 2001 at 03:32:47PM +0200, Axel Scheepers wrote:

>

> I'll say it again, FTP is eeeevul.

>

> > Hi everybody,

> > I hope I'm not being really off topic with this one but

> > it's been troubling me for a while now.

> > I'm looking for a way to provide acces to an ftpserver, my current

> > network layout looks like this:

> >

> > Cable Modem -----> Gateway -----> http/ftp server

> > |

> > |

> > +-----> private http/ftp/sql server

> > |

> > |

> > +-----> my workstation

> >

> > The gateway does natd and ipf since the other servers have private

> > addresses.

>

> natd(8) and ipf(8) or natd(8) and ipfw(8)? I'd recommend either using,

> natd(8) and ipfw(8) or ipnat(8) and ipf(8), and not mixing and

> matching. There are sometimes reasons to run ipf(8) and ipfw(8) at the

> same time, but when you need to proxy FTP, there is too much room for

FreeBSD–Security: Re: Firewall and ftp service

> *confusion and weird interactions.*
>
> > *The problem now is that whenever I connect to my*
> > *ftp servers from the outside, the server is unable to set up a*
> > *data connection, because it wants to connect on a port > 1024, which*
> > *is blocked by my firewall (and I want to leave it that way).*
> > *Natd does the following:*
> > *natd -redirect_port tcp 192.168.0.5:20 20 -redirect_port 192.168.0.5:21 21*
> > *which redirects the traffic to my public ftp server.*
> >
> > *As I see it there can be 2 problems with this setup;*
> > *1) The server wants to initiate the data connection at a port > 1024 and/or*
> > *2) The server still somehow reports 192.168.0.5 as its address to the clients.*
> >
> > *I have tried to connect with the option passive is off, which I thought*
> > *should force the server to stay on port 21 for the data connection, but*
> > *it didn't work. :(*
>
> *OK, one more time on how FTP generally works. Everyone knows the*
> *client connects to the server on port 21. That's easy. Now as for the*
> *data connection, there are two modes, PORT (active) and PASV*
> *(passive). In PORT, the client tells the server what port it will be*
> *listening on and the _server_ then (usually) connects to the _client_*
> *with a source port of 20 and the arbitrary high port ("ephemeral")*
> *the client gave the server as the destination. In PASV, the server*
> *tells the client what port it will be listening on, usually an*
> *arbitrary high, ephemeral port, and the client then connects with a*
> *ephemeral port source to the ephemeral destination. And we should*
> *point out that in both modes the server and client are passing not*
> *only the port number back and forth, but actually the IP address to*
> *connect to as well.*
>
> *So, the moral of the story is that FTP is an absolute bitch to work*
> *with if you have a firewall or NAT'ing gateway between the client and*
> *server. You need an application layer proxy for the*
> *connection. Redirection alone will not cut it.*
>
> > *Can/will somebody help on getting this done the proper way ?*
> > *I just want to use ipfilter, if possible, and I don't like to install*
> > *a ftp proxy for this.*
>
> *Oops. You are really using ipf(8). IPFilter has an FTP proxy*
> *built-in. However, use ipnat(8) and not natd(8) with ipf(8).*
> --
> *Crist J. Clark cjclark@alum.mit.edu*

--
Met vriendelijke groet,
VIA NET.WORKS Nederland
Axel Scheepers
Operations
phone +31 40 239 33 93

Re: Firewall and ftp service

FreeBSD-Security: Re: Firewall and ftp service

fax +31 40 239 33 11

e-mail eindhoven.beheer@vianetworks.nl

<http://www.vianetworks.nl/>

To Unsubscribe: send mail to majordomo@FreeBSD.org

with "unsubscribe freebsd-security" in the body of the message