

RE: suggestions on a good firewall

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/security-basics/2003-06/0760.html>

From: chort (chort_at_amaunetsgothique.com)

Date: 06/24/03

Date: Mon, 23 Jun 2003 21:13:48 -0700 (PDT)
To: Ivan Coric <ivan.coric@workcoverqld.com.au>

On Mon, 23 Jun 2003, Ivan Coric wrote:

> Lets take the SMTP protocol for example, fixup SMTP enables the mail
> guard feature which only lets mail servers receive the RFC 821 commands
> of HELO, MAIL, RCPT, DATA, RSET, NOOP and QUIT. All other commands are
> rejected.
>
> If you want to do a similar thing in CheckPoint you will need to
> provide the INSPECT code to do it.
>
> I can netcat through my CheckPoint FW to my mail servers, web servers
> etc. Even do a HEAD request to get a banner of the web server and the CP
> FW does it happily.
>
> cheers
> Ivan
>
>
> >>> Willi Web <Willi.Web@mail4web.de> 06/20/03 10:25pm >>>
> The FIXUP protocol is there to correct irregular behavior in normal
> protocols. For example, the FTP Fixup allows traffic in on port 20
> when
> the traffic originated on 21. The SMTP fixup disallows certain SMTP
> commands that could be used for nefarious purposes. The PIX cannot
> shun
> traffic based on what the FIXUP protocols detect. There is no dynamic
> ACL creation possible.
>
> The PIX is not a true application level firewall. I can send NETCAT
> traffic over HTTP and the PIX will never know. Whereas the Checkpoints
> and Raptors can detect anomalies in traffic, and act on them.
>
> --Chris
>
>

Sorry for jumping in the middle of a thread here, but I wanted to

SecurityFocus BASICS: RE: suggestions on a good firewall

mention what a pain FIXUP SMTP/Mailguard is. It breaks ESMTP and causes nice things like STARTTLS to not work :(If you have a hardend mail gateway, you should NO FIXUP SMTP and enable TLS, strong authentication, etc. Of course, if you are NAT'ing port 25 directly into Exchange, that might be slightly less wise.

--

-chort

AKA Brian Keefer

The thoughts I express are generally piped from /dev/random, needless to say they do not represent my fine employer:
CipherTrust, Inc - www.ciphertrust.com

Evaluating SSL VPNs' Consider NEOTERIS, chosen as leader by top analysts!
The Gartner Group just put Neoteris in the top of its Magic Quadrant, while InStat has confirmed Neoteris as the leader in marketshare.

Find out why, and see how you can get plug-n-play secure remote access in about an hour, with no client, server changes, or ongoing maintenance.

Visit us at: <http://www.neoteris.com/promos/sf-6-9.htm>
