

RE: [fw-wiz] Sources for Extranet Designs?

Source: <http://www.derkeiler.com/Mailing-Lists/Firewall-Wizards/2004-02/0199.html>

From: Steven A. Fletcher (sfletcher_at_bcsc.com)

Date: 02/23/04

To: "Firewall-Wizards" <firewall-wizards@honor.icsalabs.com>

Date: Mon, 23 Feb 2004 14:43:22 -0600

My opinion on that would that it's up to the clients to protect themselves. Recently, I set up a connection for a law enforcement customer who would be accessing a county database and a state wide database through this connection. Other county departments would also be accessing this same network. Since I was already putting in a firewall as a requirement for this connection, I included a third NIC so that the internal network would be protected from this other network also.

My theory is that if I can't control anything on that network, then I'm not going to trust it. This applies to the Internet, so why should it not apply to other unfamiliar, untrusted networks? I would spell this out in the partner agreement to alleviate any liability.

Steve Fletcher

Senior Network Engineer, MCSE, Master ASE, CCNA

BCSC Technology Solutions

Phone: (309)664-8129

Toll Free: (888) 764-8100 ext. 129

Fax: (309) 662-6421

sfletcher@bcsc.com

-----Original Message-----

From: firewall-wizards-admin@honor.icsalabs.com

[<mailto:firewall-wizards-admin@honor.icsalabs.com>] On Behalf Of Bob

Alberti

Sent: Monday, February 23, 2004 2:09 PM

To: Firewall-Wizards

Subject: RE: [fw-wiz] Sources for Extranet Designs?

One thing I always wonder about in Extranet designs: how liable are you (the host of the Extranet) if two of your Extranet customers are competitors? If Customer A can hack your Extranet to, for instance, inspect

Customer B's orders, or even to hack Customer B's network, how liable are

you for not providing a more secure Extranet environment?

RE: [fw-wiz] Sources for Extranet Designs?

Firewall-Wizards: RE: [fw-wiz] Sources for Extranet Designs?

Its one thing to protect the host organization from Extranet clients:
its
another entirely to protect clients from each other.

-----Original Message-----

From: firewall-wizards-admin@honor.icsalabs.com
[mailto:firewall-wizards-admin@honor.icsalabs.com]On Behalf Of Wes
Noonan
Sent: Monday, February 23, 2004 1:31 PM
To: 'Baumann, Sean C.'; 'R. DuFresne'
Cc: 'Paul Robertson'; firewall-wizards@honor.icsalabs.com
Subject: RE: [fw-wiz] Sources for Extranet Designs?

> 1.) *If you say you should never allow access to resources on your
> protected or internal network, how do you handle giving access to
> services that reside on machines that cannot be duplicated (i.e.
> expensive mainframes)?*

There are a couple of approaches that I can think of off hand. Approach
1 is
to design the services with extranet connections in mind. Simply put,
maybe
the mainframe isn't the right place to house that resource. This is
probably
not the answer that you want to hear though. Approach 2 is to accept
that
you have a business limitation that is going to force you to implement a
less than ideal security solution. At that point, you mitigate it. What
precise ports need to be opened from the extranet to the internal
resource
and grant *only* that access. If they need SQL access but not NFS access
then make sure that your firewall only permits SQL traffic to pass
between
the two networks. Things like that.

> 2.) *Do most companies require routable address on their extranet?
> Currently we use RFC1918 address for our extranet, but we see that
this
> will become a problem in the future as we add partners.*

Depends. Assuming that you are going to be using firewalls and
advertising
your internal resources as something else (through the use of NAT, etc.)
then you can do that and make the routable addresses what the extranet
partners think they are going to connect with. That being said, you can
pretty much pick any RFC1918 address space at that point and use it in a
similar fashion. The obvious alternative is that someone will need to
change
their address space.

More detailed design you will probably have to pay me for. :-)

RE: [fw-wiz] Sources for Extranet Designs?

Firewall-Wizards: RE: [fw-wiz] Sources for Extranet Designs?

One thing that this scenario really graphically depicts is why separation of resources is such a valuable objective. Sure, it sounds really nice to have all your stuff running on a mainframe running Linux hosts but these are the kinds of security problems you will then run into. (feel free to expand this statement as you see fit – i.e. integrated firewall/ids/content filter/spam control/virus scanning or separate switches vs. VLANs).

HTH

Wes Noonan
mailinglists@wjnconsulting.com
<http://www.wjnconsulting.com>
Hardening Network Infrastructure – A concise how to guide
Available Spring 2004
Order at <http://tinyurl.com/2nof4>

firewall-wizards mailing list
firewall-wizards@honor.icsalabs.com
<http://honor.icsalabs.com/mailman/listinfo/firewall-wizards>

firewall-wizards mailing list
firewall-wizards@honor.icsalabs.com
<http://honor.icsalabs.com/mailman/listinfo/firewall-wizards>

firewall-wizards mailing list
firewall-wizards@honor.icsalabs.com
<http://honor.icsalabs.com/mailman/listinfo/firewall-wizards>