

## RE: [fw-wiz] Dynamic routing on a firewall

**Source:** <http://www.derkeiler.com/Mailing-Lists/Firewall-Wizards/2003-11/0099.html>

---

**From:** Ben Nagy (*ben\_at\_iagu.net*)

**Date:** 11/28/03

To: "'Dawes, Rogan (ZA - Johannesburg)'" <rdawes@deloitte.co.za>, <firewall-wizards@honor.icsalabs.com>  
Date: Fri, 28 Nov 2003 17:47:15 +0100

My quick 0.02.

It's a bad idea.

The PIX is a terrible router, for a start, but even so the idea makes my flesh creep. For your scenario, how about using statics with different metrics, or an external load balancing solution (which is the 'standard' way of handling the problem on the Internet interface).

If you do decide to do it, then you can use route filtering per interface to restrict what networks you will allow updates for – this is how it's done in WANs and the Internet (or how it *should* be done ;)

Cheers,

ben

> -----Original Message-----  
> From: firewall-wizards-admin@honor.icsalabs.com  
> [mailto:firewall-wizards-admin@honor.icsalabs.com] On Behalf  
> Of Dawes, Rogan (ZA - Johannesburg)  
> Sent: Friday, November 28, 2003 10:39 AM  
> To: firewall-wizards@honor.icsalabs.com  
> Subject: [fw-wiz] Dynamic routing on a firewall  
>  
> Hi,  
>  
> I just wanted to pick the list's brain with regards to  
> dynamic routing on a firewall.  
>  
> Is it a good idea to allow a firewall to participate in  
> dynamic routing? My first thoughts are that it sounds like a  
> really dangerous thing – you certainly don't want to have  
> routes changing so that a DMZ moves from one interface to a  
> different one, for instance.  
>  
> But if the routing can be controlled so that traffic always

Firewall-Wizards: RE: [fw-wiz] Dynamic routing on a firewall

- > goes through the right interface (but possibly to a different
- > upstream router), that should be OK, I would think.
- >
- > What mechanisms do the various firewalls (mostly interested
- > in Pix and FW-1) have to sanity-check routing updates that
- > they receive?
- >
- > A (simplistic) scenario that could illustrate my concerns:
- >
- > You have a firewall controlling access to third parties
- > (competitors) which provide services to your company. Each
- > party is in their own DMZ. You have dynamic routing enabled
- > on the firewall, since there are two redundant routers for
- > each party in each parties DMZ, and you need to be able to
- > fail over from one to the other.
- >
- > Party A sends a routing update to say that party B is now
- > reachable via Party A's networks. Any packets that you try to
- > send to party B end up going to Party A, where they can be
- > captured, etc.
- >
- > Leaving out the question of how A gets the packets to B
- > eventually, to complete the connection, is this a realistic
- > scenario? How can one protect against something like this,
- > using the abovementioned firewalls, if one still chooses to
- > use dynamic routing?
- >
- > Rogan
- > --
- > "Using encryption on the Internet is the equivalent of
- > arranging an armored car to deliver credit card information
- > from someone living in a cardboard box to someone living on a
- > park bench."
- > - Gene Spafford
- > --
- > Deloitte & Touche Security Services Group
- > Tel: +27(11)806-6216 Fax: +27(11)806-5202 Cell:
- > +27(82)784-9498
- > --
- >
- > Important Notice: This email is subject to important
- > restrictions, qualifications and disclaimers ("the
- > Disclaimer") that must be accessed and read by clicking here
- > or by copying and pasting the following address into your
- > Internet browser's address bar:
- > <http://www.Deloitte.co.za/Disc.htm>. The Disclaimer is deemed
- > to form part of the content of this email in terms of Section
- > 11 of the Electronic Communications and Transactions Act, 25
- > of 2002. If you cannot access the Disclaimer, please obtain a
- > copy thereof from us by sending an email to
- > ClientServiceCentre@Deloitte.co.za.

RE: [fw-wiz] Dynamic routing on a firewall

Firewall-Wizards: RE: [fw-wiz] Dynamic routing on a firewall

> \_\_\_\_\_  
> *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>