

Re: [fw-wiz] PIX, DNS fixups and Zone Transfers

Source: <http://www.derkeiler.com/Mailing-Lists/Firewall-Wizards/2003-05/0202.html>

From: Barney Wolff (barney_at_databus.com)

Date: 05/27/03

To: Bruce Smith <bruce_the_loon@worldonline.co.za>

Date: Tue, 27 May 2003 10:36:22 -0400

On Mon, May 26, 2003 at 09:55:50PM +0200, Bruce Smith wrote:

>
> We've recently implemented a PIX (6.3) firewall setup, resulting in two DNS
> servers that were previously exposed in the outside network being moved
> behind the PIX into the DMZ, and getting 2 new IP addresses, eg 192.168.34.2
> to 192.168.35.2. We mapped the original IP on the outside to the new IP on
> the DMZ via static commands and the proxy arp bits. On the DNS servers, the
> IP's referred to in the forward and reverse zones were been changed to match
> the current setup so that lookups by machines on the DMZ would work fine. So
> far so good. DNS fixup handles the translation of DNS lookups from outside
> perfectly.
>
> Thus arises our problem. Our DNS zones have one primary and 4 secondaries,
> three of which are on separate sites and continents. Now when they do a zone
> transfer of our zones, the mapped IP addresses are NOT changed in the zone,
> so looking up on those zones brings up the new IP address, not the old. That
> IP isn't visible on the 'Net. We hacked around the problem by giving each
> machine two names, eg *dns1.domain.com* and *dns1r.domain.com*. *dns1.domain.com*,
> the address known to the world at large, maps to the old IP.
> *dns1r.domain.com* is the new one. By some careful juggling of several crates
> of eggs, this is working, for the moment. However it is a precarious
> position to be in.

Since NAT actually adds no security, I'd put the nameservers on a DMZ of their own and not NAT between them and the Internet. For internal lookups, I'd use separate internal servers that forward to the DMZ servers for non-internal domains. Or use views to cause the DMZ servers to return different answers for queries from inside. You can still NAT between inside and outside if management insists.

Your nameservers should not be outside the firewall; at least protect them with ACLs that allow only UDP+TCP to port 53 and nothing else. Honor zone transfer requests only from your known secondaries. Allow recursive lookups only from inside hosts.

--

Barney Wolff

<http://www.databus.com/bwresume.pdf>

Firewall-Wizards: Re: [fw-wiz] PIX, DNS fixups and Zone Transfers

I'm available by contract or FT, in the NYC metro area or via the 'Net.

firewall-wizards mailing list

firewall-wizards@honor.icsalabs.com

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