

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

Source: <http://www.derkeiler.com/Mailing-Lists/Firewall-Wizards/2003-05/0214.html>

From: Reckhard, Tobias (tobias.reckhard_at_secunet.com)

Date: 05/28/03

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

Date: Wed, 28 May 2003 07:45:32 +0200

Hi Bruce

Just like Barney, I suggest you do away with NAT. I find it to be more of a pain than a gain in many, if not most situations.

You could also switch to djbdns (<http://cr.yp.to/djbdns.html>) and transfer your zones via rsync/ssh. Then the secondaries could strip out the private IP addresses with a simple sed command. Or the Makefile used to construct the DNS database on the primary could create two such databases, one for the primaries and one for the secondaries, by calling sed before tinydns-data. Such is the beauty of combining a non-monolithic DNS suite with UNIX, you can extend it in whatever way you wish. BTW, you could serve the second database via AXFR using axfrdns, too, of course, if your secondaries don't support anything else.

tinydns also supports different records to be served based on the source IP address of the DNS client via RRs being tagged with location codes. This affects AXFR transfer as well, the AXFR client is passed only those records whose location codes match its IP address (as well as those records without any location codes). You could probably use this feature to do what you want while preserving NAT (shudder). Note, however, that djbdns' AXFR behaviour is slightly different from that of BIND in that it transfers the entire domain in question, including all subdomain data in the server's database, while BIND only transfers what amounts to the contents of the zone file in question (tinydns/axfrdns typically has only one database file and does not split zones to different files).

Enough advocacy.

Cheers,
Tobias

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