

## Re: [fw-wiz] Allowing DNS servers to operate behind NetScreen 500

*Source:* <http://www.derkeiler.com/Mailing-Lists/Firewall-Wizards/2003-02/0028.html>

---

*From:* Mike Scher ([mscher@neohapsis.com](mailto:mscher@neohapsis.com))

*Date:* 02/17/03

From: Mike Scher <[mscher@neohapsis.com](mailto:mscher@neohapsis.com)>  
To: FWWIZ <[firewall-wizards@honor.icsalabs.com](mailto:firewall-wizards@honor.icsalabs.com)>  
Date: Mon, 17 Feb 2003 10:11:41 -0600 (CST)

On Mon, 17 Feb 2003, Volker Tanger wrote:

- > *Reckhard, Tobias wrote:*
- > > *No, it is not. The reason for my response was that I don't know of any*
- > > *currently relevant reason for DNS responses to be over 512 bytes in size.*
- >
- > *Well, I've seen – and that was not even signed DNS. The idi... ahem...*
- > *programmers of that system (mis)used fake hostnames to hold session-ID*
- > *and shopping basket content. And that easily went beyond UPD packet size*
- > *quite often. Cacheing did not work with that system either.*

Why didn't it respond to TCP? On what little you describe, that arrangement sounds remarkably like the traffic against which firewalls should protect weaker systems. It almost sounds like what a hostile nameserver trying to clear a cache or run it out of memory would do.

Responding generally to the thread from here down (and generally agreeing with Tobias):

If I start stuffing more data in a transaction than the widely-adopted RFC says I should have, am I implementing an experimental RFC or trying a buffer-overflowing attack? Firewall L7 awareness can't be predictive; nor should it accomodate all possible new variations until they become reasonably widespread. There's L4 modes that most firewalls have -- they will accomodate such shenanigans (doing little more for UDP than opening a time-based window of opportunity triggered and renewed by traffic from the allowed initiator).

The basic operating default of a firewall should be strict; yet a good firewall should let an administrator selectively and intelligently allow protocol variance. If you want to mess around with variant UDP protocols, just dumb down the firewall's L7 handling of the protocol in question -- don't encourage the vendor to weaken the established protocol handling by default. Most accomodate this sort of mode.

Firewall-Wizards: Re: [fw-wiz] Allowing DNS servers to operate behind NetScreen 500

Opining that a new protocol can't be rolled out because firewalls will block the new version is the very reason to select a new port for the new protocol. Asking not only vendors but end-users to constantly update firewalls with no known holes just to accomodate every experimental protocol variant is exceedingly unreasonable. As is asking end users to use broadly open protocol compliance checking.

-M

--

Michael Brian Scher		Director, Neohapsis Labs
<a href="mailto:mscher@neohapsis.com">mscher@neohapsis.com</a>		General Counsel
Fax: 773-394-8314		Vox: 773-394-8310

---

firewall-wizards mailing list

[firewall-wizards@honor.icsalabs.com](mailto:firewall-wizards@honor.icsalabs.com)

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