

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

**Source:** <http://www.derkeiler.com/Mailing-Lists/Firewall-Wizards/2003-02/0024.html>

---

**From:** Volker Tanger ([volker.tanger@discon.de](mailto:volker.tanger@discon.de))

**Date:** 02/17/03

From: Volker Tanger <[volker.tanger@discon.de](mailto:volker.tanger@discon.de)>  
To: "'firewall-wizards@honor.ics..." <[firewall-wizards@honor.icsalabs.com](mailto:firewall-wizards@honor.icsalabs.com)>  
Date: Mon, 17 Feb 2003 14:17:16 +0100

Greetings!

Reckhard, Tobias wrote:

> *Back from the weekend, I find my post has stirred up a bit of a debate..*  
>  
> *On Saturday, February 15, 2003 4:11 AM, Rob Payne wrote:*  
>> *On Fri, Feb 14, 2003 at 08:58:41AM +0100, Reckhard, Tobias wrote:*  
>>> *On Thursday, February 13, 2003 3:39 AM, Rob Payne*  
>>>  
>>>> *get in the way of (DNS) security when zones start getting signed.*  
>>>> *(Rhetorical: Has anyone attempted to fit current DNS data plus*  
>>>> *RSA/SHA1 keys and signatures in packets 512 datagrams long?)*  
>>>  
>  
> *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.

Bye

Volker Tanger  
IT-Security Consulting

--  
discon gmbh  
Wrangelstraße 100  
D-10997 Berlin  
Telefon (030) 6104-3307  
Telefax (030) 6104-3461  
[volker.tanger@discon.de](mailto:volker.tanger@discon.de)  
<http://www.discon.de/>

---

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

firewall-wizards mailing list

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

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