

## Re: DNS ACL ?

**Source:** <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2005-11/0186.html>

---

**From:** Richard C Lewis ([mrlew1\\_at\\_earthlink.net](mailto:mrlew1_at_earthlink.net))

**Date:** 11/14/05

To: John Hally <[JHally@epnet.com](mailto:JHally@epnet.com)>

Date: Sun, 13 Nov 2005 20:19:09 -0500

Whenever a DNS server returns a response of over 512 bytes it will set the Truncation bit to tell the requesting server to reissue the same query over a Virtual Circuit (TCP connection). This is normally seen with requests for web server information for large server farms. If you block TCP/53 to your DNS server you *\*MAY\** not experience any problems, but the problems will likely occur on the requesting side of someone seeking your information. If you do not have a lot of systems with the same name on multiple IP addresses or multiple CNAMEs or a large mail server farm you *\*MAY\** come out okay. Just keep in mind that your DNS system will not be functioning the way it *\*should\** be... but then we wouldn't have a need for security professionals if everything did what it *\*should\**...

You can limit your exposure by reducing who can perform zone transfers via the allow-transfer option and use the query-source option to control the port used for your outgoing queries. Coupled with router/firewall ACLs you can seriously limit the TCP connections to your DNS server.

*attached mail follows:*

---

To: "'pen-test@securityfocus.com'" <[pen-test@securityfocus.com](mailto:pen-test@securityfocus.com)>

Date: Fri, 11 Nov 2005 08:35:06 -0500

Hello All,

I need a sanity check regarding DNS ACLs. For external facing DNS servers you need to allow only udp/53 inbound, correct? I know tcp/53 is used for zone transfers and requests/replies greater than a certain size, but they shouldn't typically happen for general dns queries correct?

SecurityFocus Penetration: Re: DNS ACL ?

Thanks in advance!

---

Audit your website security with Acunetix Web Vulnerability Scanner:

Hackers are concentrating their efforts on attacking applications on your website. Up to 75% of cyber attacks are launched on shopping carts, forms, login pages, dynamic content etc. Firewalls, SSL and locked-down servers are futile against web application hacking. Check your website for vulnerabilities to SQL injection, Cross site scripting and other web attacks before hackers do! Download Trial at:

[http://www.securityfocus.com/sponsor/pen-test\\_050831](http://www.securityfocus.com/sponsor/pen-test_050831)

---

---

Audit your website security with Acunetix Web Vulnerability Scanner:

Hackers are concentrating their efforts on attacking applications on your website. Up to 75% of cyber attacks are launched on shopping carts, forms, login pages, dynamic content etc. Firewalls, SSL and locked-down servers are futile against web application hacking. Check your website for vulnerabilities to SQL injection, Cross site scripting and other web attacks before hackers do! Download Trial at:

[http://www.securityfocus.com/sponsor/pen-test\\_050831](http://www.securityfocus.com/sponsor/pen-test_050831)

---