

Re: Firewall question

Source: <http://www.derkeiler.com/Newsgroups/comp.security.firewalls/2003-03/1271.html>

From: Jesper Skriver (harvest@wheel.dk)

Date: 03/15/03

From: Jesper Skriver <harvest@wheel.dk>

Date: 15 Mar 2003 15:43:55 GMT

On Sat, 15 Mar 2003 15:03:55 -0000, Chris wrote:

>

> *"Jesper Skriver" <harvest@wheel.dk> wrote in message*

> *news:slrnb76ehs.16vh.harvest@freesbee.wheel.dk...*

>> *On Sat, 15 Mar 2003 14:26:57 -0000, Chris wrote:*

>>

>> > *I agree. TCP 53 is only used for zone transfers between DNS servers,*

>> > *not DNS lookups.*

>>

>> *Not correct, lookup's will fallback to TCP if the reply cannot fit a*

>> *single UDP packet.*

>>

>> > *Besides, the mail server in question will only need to query MX*

>> > *records when sending out mail if not using a smart host. UDP 53 is all*

>> > *it needs.*

>>

>> *See above.*

>>

>> --

>> *Jesper Skriver, CCIE #5456*

>> *FreeBSD committer*

>

> *When building Firewall-1 firewalls for customers we only ever let UDP 53 out*

> *for hosts that need to resolve DNS and we've never had to let TCP 53 out as*

> *well. In this application I think that UDP 53 will do the job.*

That is a common mistake, please read the below, and take action accordingly

see rfc 1123 "Requirements for Internet Hosts", section 6.1.3.2 say

6.1.3.2 Transport Protocols

DNS resolvers and recursive servers **MUST** support UDP, and **SHOULD** support TCP, for sending (non-zone-transfer) queries.

Specifically, a DNS resolver or server that is sending a non-zone-transfer query **MUST** send a UDP query first. If the

comp.security.firewalls: Re: Firewall question

Answer section of the response is truncated and if the requester supports TCP, it SHOULD try the query again using TCP.

DNS servers MUST be able to service UDP queries and SHOULD be able to service TCP queries. A name server MAY limit the resources it devotes to TCP queries, but it SHOULD NOT refuse to service a TCP query just because it would have succeeded with UDP.

--

Jesper Skriver, CCIE #5456
FreeBSD committer