

RE: Help with ipfw rules to allow DNS queries through

Source: <http://www.derkeiler.com/Mailing-Lists/FreeBSD-Security/2001-12/7365.html>

From: Robert D. Hughes (rob@robhughes.com)

Date: 12/26/01

Date: Wed, 26 Dec 2001 14:37:42 -0600
From: "Robert D. Hughes" <rob@robhughes.com>
To: <security@freebsd.org>

If a DNS reply exceeds the maximum size of a udp datagram, it will be sent using TCP so the rule is needed.

-----Original Message-----

From: Thomas T. Veldhouse [<mailto:veldy@veldy.net>]
Sent: Wednesday, December 26, 2001 2:23 PM
To: security@freebsd.org
Subject: Re: Help with ipfw rules to allow DNS queries through

Try replacing your DNS rules with this:

```
# Allow access to our DNS
${fwcmd} add pass tcp from any to ${ip} 53 setup
${fwcmd} add pass udp from any to ${ip} 53
${fwcmd} add pass udp from ${ip} 53 to any
```

Straight out of /etc/rc.firewall. I don't think the first line is really necessary, and in fact, it probably allows zone transfers, so if you don't want these, don't include it.

Tom Veldhouse
veldy71@yahoo.com

----- Original Message -----

From: "X Philius" <xphilius@yahoo.com>
To: <security@freebsd.org>
Sent: Wednesday, December 26, 2001 1:45 PM
Subject: Help with ipfw rules to allow DNS queries through

> *Security Folks,*
> *I have a stand alone server co-located on my employers T1 line. As I*
> *am behind NAT, but not behind a firewall, I have set up ipfw so I can*
> *have *some* control over what gets in and out of my machine. One more*
> *layer in the security onion!*
>
> *My box is set up as a web server, shoutcast server, and Darwin*

RE: Help with ipfw rules to allow DNS queries through

FreeBSD–Security: RE: Help with ipfw rules to allow DNS queries through

> *Quicktime Streaming Video server. I would like to add DNS to the mix so*
> *I can cheaply host domains for my friends and family, but my ipfw rules*
> *are hanging me up. All the rules below seem to work as I would expect,*
> *except for my attempt to allow DNS queries in and out. The current rule*
> *set does not even appear to allow me to access an outside DNS server*
> *(ie the server listed in my resolv.conf), much less allow my machine to*
> *be accessed by others as a DNS server. I started out with the example*
> *'client' rule set, and added holes for SSH, Darwin and the Shoutcast*
> *servers.*
>
> *I do not think this is a factor (it didn't work before my upgrade*
> *either) but I originally set up this rule set under 4.1 Release, and I*
> *am now running 4.4 Release. I believe there were some changes to ipfw*
> *in the transition, but the example rc.firewall looked about the same to*
> *me, so I assume the changes were under the hood.*
>
> *As you can infer from my attempt to add the DNS rules below, I know*
> *there is a UDP and a TCP component to DNS queries, but apparently I do*
> *not have the full picture ;–)*
>
> *Can you suggest a set of rules to allow DNS queries in and out of my*
> *server? As I said, the rest of the rules *seem* to work fine as is, but*
> *if you see anything else I am not doing right I'd appreciate any tips.*
>
> *Thanks in advance!*
>
> *Jason*
>
>
> *# set these to your network and netmask and ip*
> *net="10.1.3.0"*
> *mask="255.255.255.0"*
> *ip="10.1.3.2"*
>
> *# Allow TCP through if setup succeeded*
> *\${fwcmd} add pass tcp from any to any established*
>
> *# Allow IP fragments to pass through*
> *\${fwcmd} add pass all from any to any frag*
>
> *# Allow setup of incoming email*
> *\${fwcmd} add pass tcp from any to \${ip} 25 setup*
>
> *# Allow incoming SSH requests*
> *\${fwcmd} add pass tcp from any to \${ip} 22*
>
> *# Allow incoming HTTP requests*
> *\${fwcmd} add pass tcp from any to \${ip} 80*
>
> *# Allow incoming FTP requests*
> *\${fwcmd} add pass tcp from any to \${ip} 21*

FreeBSD–Security: RE: Help with ipfw rules to allow DNS queries through

```
>
> # Allow incoming POP requests
> ${fwcmd} add pass tcp from any to ${ip} 110
>
> # Allow incoming Darwin requests (also uses port 80)
> ${fwcmd} add pass tcp from any to ${ip} 554
> ${fwcmd} add pass tcp from any to ${ip} 7070
>
> # Allow outgoing UDP connections of Darwin media
> ${fwcmd} add pass udp from ${ip} to any 6970–6975
>
> # Allow incoming Shoutcast requests
> ${fwcmd} add pass tcp from any to ${ip} 8008
> ${fwcmd} add pass tcp from any to ${ip} 8009
> ${fwcmd} add pass tcp from any to ${ip} 7007
> ${fwcmd} add pass tcp from any to ${ip} 7008
>
> # Allow DNS queries out and in
> ${fwcmd} add pass tcp from any to ${ip} 53 setup
> ${fwcmd} add pass udp from any to ${ip} 53
> ${fwcmd} add pass udp from ${ip} 53 to any
>
> # Allow set up of outgoing UDP connections
> ${fwcmd} add pass udp from ${ip} to any setup
>
> # Allow setup of outgoing TCP connections
> ${fwcmd} add pass tcp from ${ip} to any setup
>
> # Disallow setup of all other TCP connections
> ${fwcmd} add deny tcp from any to any setup
>
> # Everything else is denied by default, unless the
> # IPFIREWALL_DEFAULT_TO_ACCEPT option is set in your kernel
> # config file.
> ;;
>
>
> _____
> Do You Yahoo!?
> Send your FREE holiday greetings online!
> http://greetings.yahoo.com
>
> To Unsubscribe: send mail to majordomo@FreeBSD.org
> with "unsubscribe freebsd–security" in the body of the message
>
```

To Unsubscribe: send mail to majordomo@FreeBSD.org
with "unsubscribe freebsd–security" in the body of the message

To Unsubscribe: send mail to majordomo@FreeBSD.org
with "unsubscribe freebsd–security" in the body of the message

RE: Help with ipfw rules to allow DNS queries through