

Re: inbound ssh ceased on 4 servers at same time

Source: <http://unix.derkeiler.com/Mailing-Lists/FreeBSD/isp/2005-06/0005.html>

From: Cody Baker (cody_at_wilkshire.net)

Date: 06/04/05

Date: Sat, 04 Jun 2005 15:31:36 -0400

To: john@day-light.com

Are they really denying the connections or rather just timing out? We had a similar issue a while back where all of our back end servers on a private network were taking forever/never authenticating SSH and a few other services. It turned out that the reverse lookup started failing because in the past our upstream had 10.x.x.x set in their DNS to deliver an nxdomain. Whatever server they had that reverse zone pointed too was either taken offline or setup to drop outside requests making it so when any of our systems on this private network would ssh to another it would try the reverse and sit for minutes waiting for a response. We solved this by adding setting our implementing a DNS server on this private network.

Thank You,

Cody Baker

cody@wilkshire.net

330.874.9030

<http://www.wilkshire.net>

John Brooks wrote:

>Thanks, sounds good to do on the outward facing firewall. These
>four freebsd boxes are protected behind an openbsd firewall so
>none of the brute-force sshd attacks have ever reached them.

>

>All four machines were updated (buildworld) exactly 30 days
>earlier, and all developed this behavior at the same time.
>Seems almost too much of a coincidence. I guess it's time to
>start checksumming binaries with boxes on other networks not
>exhibiting this problem.

>

>--

>John Brooks

>john@day-light.com

>

>

>

freebsd-isp: Re: inbound ssh ceased on 4 servers at same time

>>-----Original Message-----
>>From: Brian Reichert [mailto:reichert@numachi.com]
>>Sent: Saturday, June 04, 2005 12:48 PM
>>To: John Brooks
>>Cc: freebsd-isp@freebsd.org
>>Subject: Re: inbound ssh ceased on 4 servers at same time
>>
>>
>>On Sat, Jun 04, 2005 at 12:10:28AM -0500, John Brooks wrote:
>>
>>
>>>today at about noon, all four freebsd servers on a clients lan
>>>quit accepting ssh connections.
>>>
>>>
>>I've been seeing a lot of brute-force sshd attacks, which leave
>>a lot of connections in an awkward state. I've done this for my
>>primary sshd server, and seems to have alleviated my problems:
>>
>>LoginGraceTime 60
>>MaxStartups 10:30:60
>>
>>
>>
>>>--
>>>John Brooks
>>>john@day-light.com
>>>
>>>
>>--
>>Brian Reichert <reichert@numachi.com>
>>55 Crystal Ave. #286 Daytime number: (603) 434-6842
>>Derry NH 03038-1725 USA BSD admin/developer
>>at large
>>
>>
>>
>-----
>freebsd-isp@freebsd.org mailing list
><http://lists.freebsd.org/mailman/listinfo/freebsd-isp>
>To unsubscribe, send any mail to "freebsd-isp-unsubscribe@freebsd.org"
>
>

freebsd-isp@freebsd.org mailing list
<http://lists.freebsd.org/mailman/listinfo/freebsd-isp>
To unsubscribe, send any mail to "freebsd-isp-unsubscribe@freebsd.org"