

Re: Using putty to debug ssh through a firewall

Source: <http://www.derkeiler.com/Newsgroups/comp.security.ssh/2007-08/msg00101.html>

- *From:* NightStrike <nightstrike@xxxxxxxx>
 - *Date:* Mon, 20 Aug 2007 19:05:08 -0000
-

On Aug 20, 1:32 am, NightStrike <nightstr...@xxxxxxxx> wrote:

On Aug 18, 9:46 am, Jacob Nevins <jac...@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote:

NightStrike <nightstr...@xxxxxxxx> writes:

I currently use ssh to access things outside of a firewall.

[...]

debug1: SSH2_MSG_KEXINIT sent

And it just hangs there until the connection times out. Any ideas on what might be causing a hang at that stage?

KEXINIT messages can be quite large. Guess: could it be <http://www.snailbook.com/faq/mtu-mismatch.auto.html>?

It's possible, but I don't think so. I will post tomorrow similar information but where I force SSH v1 protocol. There will be a similar hanging point. What would be a good tool to use to see if a KEXINIT message is in fact being transmitted, however slowly?

Here is the output of a version 1 attempt:

```
$ ssh -1 -vvv -p 23 aaa.bbb.ccc.ddd
OpenSSH_4.6p1, OpenSSL 0.9.8e 23 Feb 2007
debug2: ssh_connect: needpriv 0
debug1: Connecting to aaa.bbb.ccc.ddd [aaa.bbb.ccc.ddd] port 23.
debug1: Connection established.
```

Re: Using putty to debug ssh through a firewall

```
debug1: identity file /cygdrive/c/Documents and Settings/User/.ssh/  
identity  
type -1  
debug1: Remote protocol version 1.99, remote software version  
OpenSSH_4.6  
debug1: match: OpenSSH_4.6 pat OpenSSH*  
debug1: Local version string SSH-1.5-OpenSSH_4.6  
debug2: fd 3 setting O_NONBLOCK  
debug1: Waiting for server public key.
```

And then it just hangs like always...

.