

Re: SSH tunneling/port forwarding and stateful packet inspection

Source: <http://www.derkeiler.com/Newsgroups/comp.security.ssh/2004-02/0319.html>

From: steve (*steph19731_at_yahoo.com*)

Date: 02/25/04

Date: 24 Feb 2004 19:07:38 -0800

Richard E. Silverman <res@qoxp.net> wrote in message news:<m2ptc4uvck.fsf@darwin.oankali.net>...
> *This is too vague. State the actual problem you are encountering, with*
> *precise configuration, products involved, and symptoms you are observing.*

Its not a problem per se but I am curious. I don't think actualy products involved are an issue. Lets just speak generally when talking about common firewalls.

However, I think I may have answered my own question already when I was thinking about this earlier today.

The scenario is this – point A – a machine running an ssh client that is tunneling via port 443 to point B – a server running an ssh server on port 443. Point A – the client is using the tunnel to port forward terminal service traffic. My question was, why doesn't the firewall pick this up in SPI because it is not really ssh traffic. However, in doing a packet trace, I saw that the header of the packet really is ssh traffic, but the actual port 3389 (term server) traffic a) encrypted and b) encapsulated. So as far as the SPI functionality of the firewall is concerned, it is SSH traffic.

Does this sound feasible?