

## Re: SSH tunneling/port forwarding and stateful packet inspection

**Source:** <http://www.derkeiler.com/Newsgroups/comp.security.ssh/2004-02/0344.html>

---

**From:** steve (*steph19731\_at\_yahoo.com*)

**Date:** 02/26/04

Date: 25 Feb 2004 15:44:53 -0800

res@qoxp.net (Richard E. Silverman) wrote in message  
news:<96aea0e5.0402242202.2aebd7bb@posting.google.com>...  
> > ... *However, in doing a packet trace, I saw that the header of the*  
> > *packet really is ssl traffic, but the actual port 3389 (term server)*  
> > *traffic a) encrypted and b) encapsulated. So as far as teh SPI*  
> > *functionality of the firewall is concerned, it is SSL traffic.*  
>  
> *Your terminology is confused and you want "SSH" here, not "SSL" (these are*  
> *two entirely different protocols) -- but I suppose you've got the idea.*  
> *All the firewall can see is a TCP connection whose contents are entirely*  
> *opaque because they are encrypted. The fact that the connection is being*  
> *to forward traffic between two other TCP connections elsewhere is*  
> *invisible to the firewall.*

My terminology is not mixed up. According to my packet trace, because I have reconfigured SSH to run over port 443 the trace shows it as SSL traffic. Of course the contents are encrypted. This is my whole conclusion why the stateful packet inspection capabilities of the firewall do not blow it going outbound. Because to it, it is just an SSL packet encapsulating SSH data, which of course is encrypted.