

[fw-wiz] VPN Issue with Certs and fragmentation

Source: <http://www.derkeiler.com/Mailing-Lists/Firewall-Wizards/2007-09/msg00041.html>

- *From:* "Bell Simon (RBNA/CIT1.12)" <Simon.Bell@xxxxxxxxxxxxx>
 - *Date:* Tue, 11 Sep 2007 13:48:04 -0500
-

We occasionally have customers call in reporting that they're never prompted for credentials when attempting to connect to the VPN. This happens most often when they're at a hotel/public hotspot. However, if they use a profile based on a preshared key instead of a cert authentication, they connection works w/o issue. I've captured traffic off a failed user and it looks like during a cert auth IPSec tunnel there's a fair amount of packet fragmentation. I'm guessing then that a router in-between is probably just dropping those packets causing phase1 to fail. Has anyone else seen something similar to this? I'm thinking dropping the MTU on either our public interface or on the client directly.

Any other suggestions shared experiences would be great,

Simon

firewall-wizards mailing list
firewall-wizards@xxxxxxxxxxxxxxxxxxxxxxxx
<https://listserv.icsalabs.com/mailman/listinfo/firewall-wizards>