

[fw-wiz] L2TP & Split Tunnel –

Source: <http://www.derkeiler.com/Mailing-Lists/Firewall-Wizards/2007-09/msg00052.html>

- *From:* Andrew Andrews <incognito_54@xxxxxxxxxx>
 - *Date:* Thu, 13 Sep 2007 14:24:16 -0700 (PDT)
-

Hello,

This is more of a conversation, looking for input on some issues that have come up while trying to get L2TP IPSEC in place.

The PIX in question (Pix 515 ver 6.3) has been running a VPN in tunnel mode that allowed cisco VPN clients to connect. However, a change in the network layout has the PIX outside interface IP address change to a private address. A Load balancer now sits in front of the PIX. From my reading, i had to change my VPN from tunnel to transport mode. Since the VPN call would be made to the Load balancer interface, which would then NAT to the Outside PIX interface. This NAT process would break IPSEC Transport, and tunnel is what i went with. In so far could someone please tell me if this decision was correct? As the direction i took led me to the next question:

L2TP Transport mode is what i have now deployed in my test environment. Works fine. Except for Split tunneling. L2TP does not support split tunneling. This is what i have read so far and i could be wrong. But so far it does not suport split tunneling. I thus have 2 questions as regards split tunneling:

What are the thoughts on split tunneling and the dangers it poses to a network when enabled, And are there any work arounds to allowing clients connected to the VPN via L2TP access to the Internet?

many thanks for your time.

.a

Tonight's top picks. What will you watch tonight? Preview the hottest shows on Yahoo! TV.
<http://tv.yahoo.com/>

[fw-wiz] L2TP & Split Tunnel –

firewall-wizards mailing list

firewall-wizards@xxxxxxxxxxxxxxxxxxxxxx

<https://listserv.icsalabs.com/mailman/listinfo/firewall-wizards>