

## RE: [fw-wiz] Pix VPN endpoint and split-tunnel

**Source:** <http://www.derkeiler.com/Mailing-Lists/Firewall-Wizards/2005-10/0019.html>

---

**From:** Paul Melson ([pmelson\\_at\\_gmail.com](mailto:pmelson_at_gmail.com))

**Date:** 10/12/05

To: "'Hughes, Chris'" <[Chris.Hughes@thalescomminc.com](mailto:Chris.Hughes@thalescomminc.com)>, <[firewall-wizards@honor.icsalabs.com](mailto:firewall-wizards@honor.icsalabs.com)>

Date: Wed, 12 Oct 2005 10:45:10 -0400

-----Original Message-----

Subject: [fw-wiz] Pix VPN endpoint and split-tunnel

> *I am trying to configure a cisco pix as a vpn endpoint for the cisco vpn client and*  
> *would like to force the client to use the corporate network for internet access. I*  
> *don't want to allow split-tunnel. I cant find any info on how to do this.*  
Is split  
> *tunnel the only way to give a vpn client internet access once they are connected?*

The short answer is yes. PIX-fu rule #1: the PIX is not a router. It can't take traffic that arrives on one interface and pass it back out that same interface, even when the traffic arrives via VPN tunnel. That said, you can sort of solve this problem by having the clients use a proxy server while connected via full tunnel. There may or may not be an elegant way to automate this for your road warriors, but this would really be independent of anything the PIX or VPN client do. (Think login scripts, Group Policy, etc.)

If it's a big enough issue that you're willing to spend time and resources on it, I would recommend looking at the VPN3K concentrators (or ASA 5500?). They can do exactly what you're asking for, plus they possess a number of other features for managing VPN client users that the PIX doesn't have. (Like dynamic VPN profile assignment via RADIUS.)

PaulM

---

firewall-wizards mailing list

[firewall-wizards@honor.icsalabs.com](mailto:firewall-wizards@honor.icsalabs.com)

<http://honor.icsalabs.com/mailman/listinfo/firewall-wizards>