

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

Source: <http://www.derkeiler.com/Mailing-Lists/Firewall-Wizards/2005-10/0020.html>

From: Hughes, Chris (*Chris.Hughes_at_thalescomminc.com*)

Date: 10/12/05

To: "Paul Melson" <pmelson@gmail.com>, <firewall-wizards@honor.icsalabs.com>

Date: Wed, 12 Oct 2005 11:23:47 -0400

That's pretty much what I read. I thought they may have provided a fix by now. As for the workarounds, this is for a business partner network and I've already presented them with the "spend" option and they don't want to.

Another reply I got here from Simon expressed the possibility that PIX 7.x supports this. (split horizon?)

Anybody?

– Chris

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

From: Paul Melson [mailto:pmelson@gmail.com]

Sent: Wednesday, October 12, 2005 10:45 AM

To: Hughes, Chris; firewall-wizards@honor.icsalabs.com

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

-----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

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

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

This email and any files transmitted with it are confidential and are intended solely for the use of the individual or entity to whom they are addressed. This communication represents the originator's personal views and opinions, which do not necessarily reflect those of Thales Communications, Inc. If you are not the original recipient or the person responsible for delivering the email to the intended recipient, be advised that you have received this email in error, and that any use, dissemination, forwarding, printing, or copying of this email is strictly prohibited. If you received this email in error, please immediately notify Administrator2@Thalescomminc.com.

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