

## RE: [fw-wiz] IP migration on "hub" VPN terminus [long]

**Source:** <http://www.derkeiler.com/Mailing-Lists/Firewall-Wizards/2004-03/0133.html>

---

**From:** Melson, Paul (*PMelson\_at\_sequoianet.com*)

**Date:** 03/25/04

To: "Robert L. Wanamaker" <bobw@avantsystems.com>, <firewall-wizards@honor.icsalabs.com>  
Date: Thu, 25 Mar 2004 14:06:57 -0500

> -----Original Message-----

- > (3) add necessary statements for Cisco Secure VPN client to
- > connect from any location, and telnet into the remote pix.
- > (4) Use the VPN client to directly connect to each PIX, and
- > create a separate crypto map entry pointing to the new VPN peer

AFAIK, this can't happen. PIX firewalls won't pass traffic back to themselves on the same interface. This applies to both 3 and 4. If you're connected to the PIX via VPN client and connecting to it via Telnet on its outside interface, you're Telnet connection is almost certainly not encrypted. Set up SSH or PDM (HTTPS) and restrict access to known addresses.

- > (5) Split apart the 515's at the hub; run each in standalone
- > mode, one connected to the old ISP network, and one connected
- > to the new ISP network.
- > (6) Cut the tie to the old ISP. Watch all the tunnels get
- > gracefully rebuilt on the second 515 with little or no impact
- > to users.

Good luck! :)

- > Testing results. I've tested 1, 3, 4 with good results. My
- > only weird results are that Cisco's site has numerous e.g.'s
- > of the VPN client connecting with DES encryption; however, I
- > can only make it work with 3-DES. This is certainly a good
- > excuse for getting the client up to current rev, but am I
- > missing something?

The VPN client has a limited number of supported IKE proposals. If you're using PSK, DES will only work with MD5 and DH Group 2. If you're using RSA certificates, it's MD5 and DH Group 1. There's a handy IKE Proposal table here:

[http://www.cisco.com/en/US/partner/products/sw/secursw/ps2308/products\\_administration\\_guide09186a00800bd991.html#1157757](http://www.cisco.com/en/US/partner/products/sw/secursw/ps2308/products_administration_guide09186a00800bd991.html#1157757)

Firewall-Wizards: RE: [fw-wiz] IP migration on "hub" VPN terminus [long]

- > *Questions. Does this sound feasible? Is there a better way*
- > *to accomplish this cutover?*

My advice is that you should plan for problems. If you succeed in upgrading all 30 506's and cutting over the 515's without incident, you're wasting your life in networking – you belong at a blackjack table in Vegas. To that end, get some external modems and console cables to ship out and coordinate with someone onsite who will be available to plug them in and power cycle things to reduce downtime when it does happen.

Anyway, I don't know enough about your time constraints, external routers/switches, whether or not the 515's are being used for NAT/ACL as well as VPN, and some other details that would be necessary to weigh out all the options. If it were mine to do, though, I would back up and look at whether or not the 515's were worth keeping around. Honestly, if those tunnels are important enough that there's a failover pair there, it might be worth replacing them with concentrators that have better redundancy, performance, and scalability. I'd also reconsider splitting the failover pair if it can be avoided.

PaulM

---

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