

RE: [fw-wiz] Pix LAN-To-LAN Problem

Source: <http://www.derkeiler.com/Mailing-Lists/Firewall-Wizards/2004-06/0139.html>

From: Melson, Paul (*PMelson_at_sequoianet.com*)

Date: 06/21/04

To: "cs 2004" <cskb2004@yahoo.com>, <firewall-wizards@honor.icsalabs.com>

Date: Mon, 21 Jun 2004 08:33:59 -0400

Are you sure that the traffic you are generating is supposed to be allowed? If you are convinced that this is a result of a problem on the remote end, one way to find out might be to run 'debug crypto isakmp' and attempt to bring the tunnel up. If Phase 1 completes correctly, then you can rule out an access-list on your side. In which case, you're probably trying to generate traffic that is denied by a filter on the concentrator.

If Phase 1 negotiation never begins, I would guess that you have an access-list bound to the inside interface (or whichever interface the local VPN traffic arrives on) that doesn't allow the traffic you are attempting to send. I suppose this could also occur as a result of interface security levels if the interface that was assigned to your crypto map had a higher security level than the interface where the local VPN traffic arrives at the firewall. (Though, I have never seen this in production, and I can't imagine a scenario where this would be appropriate.)

PaulM

> -----Original Message-----
> *The tunnel can successfully be established when*
> *initiated by the customer (Concentrator 3030); all*
> *traffic then passes normally. When initiated from our*
> *side (PIX 535) we immediately receive*
> *"IPSEC(sa_initiate): ACL = deny; no sa created" while*
> *running "debug crypto ipsec" and "debug crypto*
> *isakmp". We have other VPN tunnels that function*
> *correctly both from the trusted and untrusted*
> *networks.*
>
> *I have a border router above my firewall and no*
> *filtering on that device.*
>
> *This problem "IPSEC(sa_initiate): ACL = deny; no sa*
> *created" happens everytime , i create a new tunnel,*
> *and dont know what happens, but with every customer i*

Firewall-Wizards: RE: [fw-wiz] Pix LAN-To-LAN Problem

- > *see this error, I tell them to make sure the proxy*
- > *configurations match and UDP 500 traffic allowed on their*
- > *border routers, they do some change and it goes through. But*
- > *for this particular tunnel, I just keep getting the same*
- > *error. Its entirely possible that*
- > *remote end is the problem, however I want to rule out*
- > *possible misconfiguration on my end.*

firewall-wizards mailing list

firewall-wizards@honor.icsalabs.com

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