

Re: [fw-wiz] PIX to PIX VPN from within a private network.

Re: [fw-wiz] PIX to PIX VPN from within a private network.

Source: <http://www.derkeiler.com/Mailing-Lists/Firewall-Wizards/2006-03/msg00021.html>

- *From:* "Patrick M. Hausen" <hausen@xxxxxxxx>
 - *Date:* Wed, 15 Mar 2006 09:28:53 +0100
-

Hi, all!

On Mon, Mar 13, 2006 at 06:02:55PM -0500, Greg wrote:

I have a PIX at home and would like to connect via site to site VPN to the PIX at work which I also maintain.

The problem I think I may run into is I have a private network between the internet router and my internal home PIX. The segment between the internet router and the internal PIX is 10.0.0.0/24, the outside interface of the PIX is numbered 10.0.0.1.

AFAIK PIXen with current software (6.3.something) will do NAT traversal for IPSec just fine (using UDP port 4500).

You will have to make sure that your Internet router at home permits and NATs bidirectional traffic on UDP ports 500 (IKE) and 4500 (IPSec) when the session is initiated from the inside. This should be the case for a standard "permit and NAT anything inside -> outside" configuration that is most often used in SOHO setups.

Then it should "just work".

Of course you configure the external IP address of your SOHO router as the peer on the company's PIX. Not 10.0.0.1.

And for most simple SOHO devices in standard configuration you will need to initiate the IKE and IPSec SA from your side. If you want both PIXen to be able to start talking to each other you need to define incoming PAT for ports 500 and 4500 on your SOHO router.

HTH,
Patrick

Re: [fw-wiz] PIX to PIX VPN from within a private network.

Re: [fw-wiz] PIX to PIX VPN from within a private network.

punkt.de GmbH Internet – Dienstleistungen – Beratung
Vorholzstr. 25 Tel. 0721 9109 –0 Fax: –100
76137 Karlsruhe <http://punkt.de>

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