

Re: VPN through NAT?

Source: <http://unix.derkeiler.com/Mailing-Lists/FreeBSD/isp/2006-08/msg00021.html>

- *From:* "Jeff Norris" <jeff@xxxxxxxxxxxxxxxxxxx>
 - *Date:* Mon, 14 Aug 2006 12:19:30 -0600
-

Brian,

IPSEC NAT traversal uses UDP 4500? Who implementation? Cisco, Nortel, BSD? I believe 4500 is Cisco's way of doing it, but not all IPSEC vpn clients are the same. I use one that uses UDP port 10000 for nat traversal.

Cheers

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

From: Brian Candler <B.Candler@xxxxxxxxxx>

Date: Mon, 14 Aug 2006 13:30:17 +0100

On Sun, Aug 13, 2006 at 06:28:33PM -0600, Jeff at NorrisTechs wrote:

I assume you have TCP port 1723 forwarding from the internet/dmz to the PPTP host?. That should be enough for most PPTP based VPN clients.

It's can be difficult with IPSEC as you have to forward UDP 500, Protocol 50 and Protocol 51 to / from the VPN client from your NAT router.

If the *clients* are behind NAT, when running IPSEC there should be nothing to do.

IPSEC uses UDP 500 (outbound) to start the key exchange, detects NAT, and then switches to UDP 4500 for IPSEC NAT traversal. It also sends NAT keepalive packets every 20 seconds by default.

So if you have a NAT-aware IPSEC client, it should work with any old NAT firewall without any config changes on that firewall, as long as it allows outbound connections. It was designed to work in hotels etc.

Microsoft's L2TP over IPSEC works just fine for this (with Win2K you need to install a NAT traversal patch). I've no idea about PPTP though. I don't use it, as it's generally considered insecure compared with IPSEC.

I believe some routers have a "PPTP passthrough" mode, which you could try

Re: VPN through NAT?

turning on (or off) to see if it fixes the problem.

Regards,

Brian.

freebsd-isp@xxxxxxxxxxx mailing list

<http://lists.freebsd.org/mailman/listinfo/freebsd-isp>

To unsubscribe, send any mail to "freebsd-isp-unsubscribe@xxxxxxxxxxx"

Sent via the WebMail system at mail.norristechs.net

freebsd-isp@xxxxxxxxxxx mailing list

<http://lists.freebsd.org/mailman/listinfo/freebsd-isp>

To unsubscribe, send any mail to "freebsd-isp-unsubscribe@xxxxxxxxxxx"