

RE: L2TP + NAT-T

Source:

http://www.tech-archive.net/Archive/Win2000/microsoft.public.win2000.ras_routing/2004-08/0284.html

From: Michael Thompson (*MichaelThompson_at_discussions.microsoft.com*)

Date: 08/25/04

Date: Wed, 25 Aug 2004 16:17:01 -0700

"I'm using L2TP/IPSec since PPTP does not work through NAT. "

Technically, neither does L2TP. The problem with any VPN technology is that the encryption encrypts the packet, at which point the router (or whatever is providing the NAT'ing for you) can't alter the packet (changing the address/port information) without invalidating the cryptographic checksum.

There are workarounds for this, but they tend to be vendor specific. Microsoft provides basic VPN connectivity in Windows 2000/XP, and you can configure it to use either PPTP or L2TP and they're NAT'able. The Cisco client also works if you're connecting to a cisco VPN concentrator. It all depends on what your company is running. I do this going from home to work with no problems whatsoever using PPTP, have been for months while running SP2 RC1 & RC2 and now final. YMMV.

"Angelo Aldrovandi" wrote:

> *Hi all!*
>
> *I have the following problem.. my WinXP clients can*
> *connect L2TP on our LAN, but they fail from the internet.*
> *I'm talking about the same PCs with the same user account!*
>
> *My configuration is like this:*
>
> *[client with private IP] -> [NAT] -> [internet] ->*
> *[NAT/FW] -> [server]*
>
> *and/or like this:*
>
> *[client with public IP] -> [internet] -> [NAT/FW] ->*
> *[server]*
>
> *I'm using L2TP/IPSec since PPTP does not work through NAT.*
> *On my firewall ("NAT/FW" in the above schema) I have*
> *opened all the needed ports from the internet to my*

- > WS2003 "WAN" interface, as specified by Microsoft:
- > UDP/500, UDP/4500, ESP/IP50 and UPD/1701 (even if it's not
- > always said to be opened).
- >
- > BTW, I have to admit I haven't understood the meaning and
- > usage of the "Internal interface" created by RRAS.. it has
- > a LAN address which is not accessible from the internet,
- > so, can this be the problem?
- >
- > I have Windows Server 2003 and XP SP1 clients. I have a CA
- > and everything is OK with certificates -- I wouldn't
- > connect on the LAN otherwise, I assume.
- >
- > Nevertheless, on the server I get the following two errors
- > (depending on the PC that connects). The first error comes
- > from a NATted client, the second one from a client having
- > a public IP address.
- >
- > *****
- >
- > EVENT LOG ID 547
- > -----
- > IKE security association negotiation failed.
- > Mode:
- > Key Exchange Mode (Main Mode)
- >
- > Filter:
- > Source IP Address <Server LAN IP address>
- > Source IP Address Mask 255.255.255.255
- > Destination IP Address <Client NATted public IP address>
- > Destination IP Address Mask 255.255.255.255
- > Protocol 0
- > Source Port 0
- > Destination Port 0
- > IKE Local Addr <Server LAN IP address>
- > IKE Peer Addr <Client NATted public IP address>
- > IKE Source Port 500
- > IKE Destination Port 6159
- > Peer Private Addr
- >
- > Peer Identity:
- > Certificate based Identity.
- > Peer IP Address: <Client NATted public IP address>
- >
- > Failure Point:
- > Me
- >
- > Failure Reason:
- > Negotiation timed out
- >
- > Extra Status:

```
> Processed second (KE) payload
> Responder. Delta Time 64
> 0x0 0x0
>
> *****
>
> EVENT LOG ID 547
> -----
> IKE security association negotiation failed.
> Mode:
> Data Protection Mode (Quick Mode)
>
> Filter:
> Source IP Address <Firewall public IP address>
> Source IP Address Mask 255.255.255.255
> Destination IP Address <Client public IP address>
> Destination IP Address Mask 255.255.255.255
> Protocol 17
> Source Port 0
> Destination Port 1701
> IKE Local Addr <Server LAN IP address>
> IKE Peer Addr <Client public IP address>
> IKE Source Port 500
> IKE Destination Port 500
> Peer Private Addr
>
> Peer Identity:
> Certificate based Identity.
> .....
> Peer IP Address: <public IP address>
>
> Failure Point:
> Me
>
> Failure Reason:
> No policy configured
>
> *****
>
> What I notice is that on one case the error is in
> the "Main mode" IKE negotiation, the second one on
> the "Quick mode". The first one reveals the server LAN IP
> address, the second one "stops" at the server's public IP
> address. The first one is a "negotiation timeout" error,
> the second one a "no policy configured" error (but since
> the same PC connects if it's inside the LAN, I can assume
> the RRAS policy is correctly defined).
>
> It's already two days I'm making experiments, reading
> stuff and trying to solve this problem, but with no
> success! :( Thanx in advance for your help, it's
```

microsoft.public.win2000.ras_routing: RE: L2TP + NAT-T

> *considered very precious!!*

>

> *With my kindest regards,*

> ** Angelo Aldrovandi*

>

>