

Re: VPN From W2K/Pro to W2K Server Doesn;t Work Through Firewall

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.win2000.security/2002-06/2575.html>

From: x y (jamescagney90210@excite.com)

Date: 06/26/02

From: "x y" <jamescagney90210@excite.com>

Date: Wed, 26 Jun 2002 06:58:34 -0400

You could try checking your firewall/router/sniffer logs at both ends to confirm that traffic isn't being blocked. My belief is that your NAT solution breaks the VPN.

My understanding is that IPSec AH protocol does not work with NAT devices that do not have IPSec passthrough because the IP header and packet are hashed to confirm that they were not changed in transit. I am not an expert at Windows 2000 NAT, but it appears that it can or does use IPSec AH. I'm not sure in Windows 2000 if or how AH can be turned off and/or ESP used instead.

You could confirm whether NAT is the problem by moving your PC to a different internet connection [such as a dialup modem temporarily], move it outside the NATspace or disable NAT temporarily. If this is the case, the only solution would be to use a different device for NAT.

There is some further explanation of this at <http://online.securityfocus.com/infocus/1519>

"Transports vs. Tunnels

IPSec operates in either one of two modes – transport mode or tunnel mode. Transport mode is meant primarily for protection of upper layer protocols, while tunnel mode protects the IP layer as well. In tunnel mode, used primarily between two gateways or a server and a gateway, the packet has two IP headers, an outer and an inner. The outer header identifies the source and destination endpoints, while the inner contains the original sender and destination addresses, protected by IPSec.

Tunnel Mode

IPSec in Windows was meant mainly for interaction with routers or other IPSec tunnel endpoints. However, as stated, it can be used with L2TP to provide a VPN remote access solution. When this is done, the L2TP headers are encapsulated and protected by IPSec, so if encryption is being used with IPSec, the L2TP headers will be encrypted. The only unencrypted headers will be the outer IP headers (with the destination endpoint IP address) and lower layers.

For details of setting up IPSec tunnels in Windows 2000 (most of which applies to XP also) please take a look at the Microsoft Support Services document How to Configure IPSec Tunneling in Windows 2000. "

"Meron Lavie" <lavie@net2vision.net.il> wrote in message news:uYb5c5IHCHA.2580@tkmsftngp09...

> Steven,

>

> I tried specifying pptp, but it didn't help.

>

> I have all outgoing traffic allowed, and also allow 47 (I enabled logging and see that port 1723 and protocol 47 are succesfully connecting).

>

> Any other ideas? Has anyone ever succeeded in connecting a VPN client in a NATted LAN to an external VPN server?

>

> --

> Meron Lavie

>

>

> "Steven L Umbach" <n9rou@attbi.com> wrote in message

> news:MY3S8.319039\$cQ3.17382@sccrnsc01...

>> Are you trying to use l2tp or pptp? L2tp for the most part does not

>> work with NAT. In your vpn client connectoid properties select pptp as server type instead of "auto" – W2K will try l2tp first by default (assuming

>> W2K vpn server is set up to allow pptp connections). If using pptp your firewall has to allow protocol passage of port 1723 and protocol 47 gre. ---

>> Steve

>>

>>

>> "Meron Lavie" <lavie@net2vision.net.il> wrote in message

>> news:urZ42DIHCHA.2364@tkmsftngp11...

>>> I am trying to access a remote server via VPN.

>>>

>>> The server is W2K/SP2 running ISA.

>>>

>>> My local computer is W2K/Pro with SP2, on a LAN whose gateway is Redhat

>>> Linux v7.0 running an IPCHAINS–based firewall which also performs

>>> NATting/Forwarding. The Linux accesses the Internet through ADSL.

>>>

>>> When I try to connect to the remote server, I get "Verifying Username and

>>> Password", but after about 15 secs it fails with message 721. The firewall

>>> log shows no violations.

>>>

>>> Everyone else succeeds in accessing from their ISP's dialup. I am the

microsoft.public.win2000.security: Re: VPN From W2K/Pro to W2K Server Doesn;t Work Through Firewall

> > *first*
> > > *person to try to access it from an external LAN.*
> > >
> > > *What am I doing wrong?*
> > >
> > > *--*
> > > *TIA*
> > > *Meron Lavie*
> > > *lavie@net2vision.net.il*
> > > *NOTE: THERE IS NO "2" IN MY REAL EMAIL ADDRESS: ANTI-SPAM!!!*
> > >
> > >
> > >
> > >
> > >
> >
> >
>
>
>
>
>