

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

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.win2000.security/2002-06/2737.html>

From: Meron Lavie (lavie@net2vision.net.il)

Date: 06/28/02

From: "Meron Lavie" <lavie@net2vision.net.il>

Date: Fri, 28 Jun 2002 17:42:04 +0300

I've been all over the web, and haven't found a solution. Am I the only person in the universe who is using a Linux Firewall/Gateway with NATting who needs to allow Windows machines on the LAN to run VPN connections to external VPN servers?

Meron Lavie

"x y" <jamescagney90210@excite.com> wrote in message news:eSjcgwSHCHA.1600@tkmsftngp13...

> *I did know you have Linux for NAT and my original suggestions still stand.*
> *I am assuming you are trying to use VPN from a windows 2000 client to a*
> *Windows 2000 server through a Linux router with NAT. Unless your NAT*
> *solution has IPsec passthrough, NAT breaks IPsec AH. This is true*
> *regardless of what vendor you're using for NAT and VPN. I think Windows*
> *2000 uses L2TP and PPTP for VPN encryption, but still uses IPSec including*
> *AH to establish SA connections and to sign packets.*

>

> *No matter what systems you are actually using, I would look in the VPN*
> *settings on your VPN client and attempt to disable AH, possibly replacing*
it
> *with ESP. If your VPN client is Windows 2000, the links I posted are a*
> *first step.*

>

> *"Meron Lavie" <a@b.com> wrote in message*
> *news:#FTWqISHCHA.2280@tkmsftngp12...*

>> *Thank you for your response. Actually, I have a Linux box (Redhat 7.0)*
>> *performing the gateway, routing and NATting. The Linux box itself is*
>> *connected to the Internet via a pptp connection through an ADSL*
>> *connection,*

>> *if that helps explain what's going on. The W2K server doesn't do any*
>> *NATting*

>> *or forwarding – the gateway for all hosts in the network is the Linux.*

>>

>> *Any more ideas given the above info?*

>>

> > TIA – Lavie
> >
> >
> >
> > "x y" <jamescagney90210@excite.com> wrote in message
> > news:#26zFAQHCHA.1600@tkmsftngp12...
> > > 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*

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

> > > >
> > > >
> > >
> > >
> >
> >
>
>