

# Re: IPSEC VPN NAT

---

*Source:* <http://www.tech-archive.net/Archive/ISA/microsoft.public.isaserver/2006-08/msg00182.html>

---

- *From:* "Alex" <nospam@xxxxxxxxxx>
  - *Date:* Wed, 23 Aug 2006 11:28:21 +0200
- 

That would be a workaround. But the configuration is difficult:  
e.g. if two remote workers are in the same hotel then only one can work  
online. The problem is, that I do not know which two persons are behind the  
same nat! So I cannot pre-configure the Clients for different  
IP-Addresses...

Any additional thoughts appreciated!

Alex

"Julian Dragut" <julian.dragut@xxxxxxx> schrieb im Newsbeitrag  
<news:Ocnb1mLxGHA.3436@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>

Alex,

The issue doesn't appear to be feature bug, but rather a config problem;  
however, it seems that there's a quick fix for it:  
add multiple IP addresses to ISA's VPN interface, and ask users from the  
same site to connect to separate IP's. Resource permitting, setup a test  
ISA/VPN and try to reproduce the setup, and start logging the vpn  
connectivity without other production network garbage/noise.

HTH,

Julian

"Alex" <Alex@xxxxxxxxxx> wrote in message  
<news:e1HZe8FxGHA.2448@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>

There is no problem with only one client behind a NAT-Device, but with  
more than one clients!!  
Any suggestions how to get it to work with more than one client at the  
same time?

Alex

"Julian Dragut" <julian.dragut@xxxxxxx> schrieb im Newsbeitrag

Re: IPSEC VPN NAT

news:uEN7qjowGHA.4688@xxxxxxxxxxxxxxxxxxxxxxxxxxxx

<http://www.microsoft.com/technet/prodtechnol/isa/2004/plan/vpnprotocol.msp>

NAT Traversal

There are a number of problems with using IPsec over NAT devices. A NAT device changes packet information during the address translation process. The process can either fail because information needed by the NAT device for address translation is encrypted, or the address translation process can cause the packet to be considered invalid by IPsec. NAT traversal (NAT-T) overcomes these issues to allow IPsec peers behind NAT devices to detect the presence of NAT devices, negotiate IPsec security associations (SAs), and send ESP-protected data, despite the fact that the addresses in the IPsec-protected packets are changed by NAT. For more information, see IPsec NAT Traversal Overview.

To allow ISA Server 2004 and ISA Server 2000 to pass IPsec traffic to a VPN server behind the ISA Server computer, the following is required:

- . The VPN server must be running Microsoft Windows ServerT 2003.
- . The L2TP over IPsec VPN protocol must be used.
- . All VPN clients must be using the IPsec NAT-T VPN client.

Note An IPsec NAT-T client update is available, with improvements to IPsec to better support VPN clients behind NAT devices. For computers running Microsoft Windows® XP Service Pack 1 (SP1) and Windows 2000, a download is available from article 818043, "L2TP/IPSec NAT-T update for Windows XP and Windows 2000," in the Microsoft Knowledge Base. By default, Windows XP Service Pack 2 (SP2) no longer supports establishing IPsec NAT-T connections to servers that are located behind

Re: IPSEC VPN NAT

NAT computers. For more information, see article 885407, "The default behavior of IPSec NAT traversal (NAT-T) is changed in Windows XP SP2, in the Microsoft Knowledge Base."

"Alex" <nospam@xxxxxxxx> wrote in message [news:%232yBeq5vGHA.4576@xxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:news:%232yBeq5vGHA.4576@xxxxxxxxxxxxxxxxxxxxxxxxxxxx)

Hello,

we implemented a VPN solution which uses the L2TP/IPSEC protocol. The ISA Server (ISA 2006 W2K3) is directly attached to the Internet (without NAT). Clients use the VPN without problems, even over a NAT Device.

But if there are multiple clients (XP SP2) behind the same NAT-Device (client side) the second client gets no connection. We also tried different DSL-Routers with features like IPSEC-Passthrough. But there is no different behaviour if this feature is turned off or not. (I think this feature is only useful for Clients that could not use the NAT-T protocol).

Is there a known restriction in the IPSec NAT-T protocol, which would explain that only one connection is possible over the same NAT device???

A.

Re: IPSEC VPN NAT