Enable Windows VPN connection when server or client behind NAT

Modern Windows devices do not support L2TP/IPsec connections when the Windows computer or VPN server are located behind a NAT. If the Windows VPN client fails with Error 809 when trying to establish a VPN connection to an MX located behind a NAT, add the "AssumeUDPEncapsulationContextOnSendRule" DWORD value to the Windows registry. This DWORD value allows Windows to establish security associations when both the VPN server and the Windows based VPN client computer are behind NAT devices.

For Windows XP:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\IPSec
RegValue: AssumeUDPEncapsulationContextOnSendRule
Type: DWORD
Data Value: 2
```

For Windows Vista, 7, 8, 10, and 2008 Server:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\PolicyAgent
RegValue: AssumeUDPEncapsulationContextOnSendRule
Type: DWORD
Data Value: 2
```

Note that after creating this key you will need to reboot the machine. For more information, reference the Microsoft Support Knowledge Base.

From:
https://wiki.plecko.hr/ - **Eureka Moment**

Permanent link:
https://wiki.plecko.hr/doku.php?id=windows:net:ipsec_l2tp_no_policy

Last update: **2019/10/31 09:06**