Remote VPN NAT and FL MGUARD firewall/router

Setting up an FL MGUARD... for a remote VPN NAT

1 Summary

Using the FL MGUARD..., an OEM or equipment supplier can create a virtual private network (VPN) tunnel from their end customer/machine site back to their central location. This allows for direct and secure communication facilitating new program updates, diagnostic and troubleshooting tasks, and other remote maintenance functions.

This paper explains a new feature in the FL MGUARD... called “remote VPN NAT” and how it helps deal with a specific, but common problem faced by machine builders. Specifically, many legacy machines that would benefit from the advantages of remote support through a VPN tunnel lack a default gateway in their network configuration. A default gateway is the IP address of a router, and it allows a machine to communicate with devices “off its network.” For example, in Figure 1, the machine’s PLC has an IP address of 192.168.5.10; while the technician at the OEM office has an IP address of 172.16.20.100. As these two IP addresses are not on the same network, the PLC can respond to the PLC’s communication attempts only if a default gateway is available to “route” the traffic.

Many machine builders, upon originally designing and installing their equipment, assumed they’d never need or want to talk to another network – that is, they were certain they’d always be isolated – and thus, they never included a default gateway in the network configuration of their HMIs, PLCs, I/O and other machine devices. Remote VPN NAT solves this problem by NATing (Network Address Translating) the technician address so that it appears to come from the machine’s own network, that is to say on the 192.168.5 network in the Figure 1 example.

Make sure you always use the latest documentation. It can be downloaded at www.phoenixcontact.net/catalog.
2 Setting up a remote VPN NAT

1. On the machine network side of the VPN (see Figure 1), open the configuration tool, go to IPSec VPN and select "Connections" from the left-side menu. Click the "More" button in the "Transport and Tunnel Settings – Action" column (see Figure 2).
2. Select **Masquerading of remote net** from the “Remote NAT for IPSec Tunnel connections” drop-down box.

3. Enter an open and unused IP address from the machine network in the “Internal IP address used for remote masquerading” field. For the example in Figure 1, the PLC address is 192.168.5.10, so the masquerade address must be on the 192.168.5 network.

4. Click the “Back” button and then click the “Apply” button on the “General VPN” tab.

All traffic that comes over the VPN will now appear to the machine devices to come from 192.168.5.250 (see Figure 3). As this is a local address, a default gateway is not required to respond. The FL MGUARD... will listen to packets coming in to 192.168.5.250, i.e., the NAT address, and translate them back to the actual address of the technician – 172.16.20.100 in the example.

### 3 Limitations

Note that, because of the nature of the “Masquerading,” traffic may only be initiated from the OEM network (technician side). Devices on the machine network cannot start sending unsolicited data but are only allowed to reply to traffic started from OEM network.

Remote VPN masquerading is new in firmware 7.4. Firmware updates can be found at [www.phoenixcontact.com](http://www.phoenixcontact.com).