How to Manage Remote Field Devices Using VPN

Moxa Technical Support Team
support@moxa.com

Contents

1 Introduction .................................................................................... 2
2 Application Scenario ....................................................................... 2
3 Prerequisites ................................................................................... 3
4 Solution .......................................................................................... 4

About Moxa

Moxa is a leading provider of edge connectivity, industrial computing, and network infrastructure solutions for enabling connectivity for the Industrial Internet of Things. With over 30 years of industry experience, Moxa has connected more than 50 million devices worldwide and has a distribution and service network that reaches customers in more than 70 countries. Moxa delivers lasting business value by empowering industry with reliable networks and sincere service for industrial communications infrastructures. Information about Moxa’s solutions is available at www.moxa.com.

How to Contact Moxa

Tel: 1-714-528-6777
Fax: 1-714-528-6778
Moxa Tech Note  Using the VPN Function in ThingsPro

1 Introduction

As industry professionals keep up with the Industrial IoT trend and enjoy the benefits of valuable data transmission between devices, servers, and databases, they are aware that privacy is a serious concern and industrial systems must be secure to prevent unauthorized access. Moxa ThingsPro gateway enhances security with built-in VPN client and firewall functions, allowing users to set up a secure IoT network architecture for data transmission as well as device configuration and management.

2 Application Scenario

Set up the ThingsPro Gateway as a VPN gateway to manage field devices connected to the gateway from a remote site. Configure a firewall between the control center and field devices to secure data transmission.
**Moxa Tech Note**  Using the VPN Function in ThingsPro

For the purpose of this article, we assume that we have a network setup where a Moxa Iologik-E2242 device connected to a ThingsPro gateway needs to be accessed from a remote site through the VPN tunnel as illustrated in the following diagram:

3  **Prerequisites**

1. A couple of Moxa UC-8112 gateway computers with Internet access, and ThingsPro 2.0 Gateway and SD card installed.
   For information about setting up a Moxa UC-8112, refer to the *ThingsPro User’s Manual*.
2. PC/notebook with Chrome browser, VPN client, and Internet access.
3. Modbus device (e.g., Moxa ioLogik-E2242)
4. VPN server installed at the control center.
4 Solution

To use ThingsPro Gateway to access and configure a remote Modbus device using OpenVPN function, do the following:

1. **Configure the VPN Client on ThingsPro Gateway.**
   a. Access the ThingsPro Gateway web interface by connecting to the following URL on eth1: https://192.168.4.127
   b. Click **GET STARTED**.
   c. Key in the **Email** and **Password** and Click **SIGN IN** to continue.
d. In the ThingsPro Gateway web page, click on the ☰ (Menu) icon to open the main menu.

e. In the main menu, click on the Gateway link and select Network.
f. Click on the **OPENVPN Client** link.

g. In the OpenVPN page, click on the button on the upper right corner of the page and select **Settings** to edit the OpenVPN client settings.
**Moxa Tech Note** Using the VPN Function in ThingsPro

h. **Enable** the OpenVPN client by moving the slider all the way to the right.

i. Click **SELECT** to browse to and upload an OpenVPN configuration file.

j. Click **SAVE**.
   - A message indicating that the OpenVPN client has been successfully updated is displayed.
   - The configuration file should contain the certificate and key information and saved in the *.ovpn format.
   - **Note:** You can click on the (Download) button to view a sample OpenVPN configuration file.

If you want to update the OpenVPN client settings, click on the (Refresh) button. Click on the **DELETE** button to delete the configuration file. To replace the configuration file, click on the (Download) button.

To view the status of the OpenVPN client, click on the (Status) button and select **Status**. The status is displayed in the **Connection Status** field.
2. **Configure the firewall settings on ThingsPro Gateway.**

ThingsPro’s Firewall function is a network address translation (NAT) technique, which is used to make services on a host residing within a protected or internal network available to hosts on the opposite side of the gateway (external network) by remapping the destination IP address and port number to the internal devices.

To configure the Firewall function in ThingsPro Gateway, do the following:

a. In the ThingsPro Gateway menu, click on the **Firewall** link under the Gateway section.
b. Click (Add a rule).

c. Fill in the details.
   
   In this article, we set up the following rule to match the network setup illustrated on page 3 of this document

![Edit rule](image)

- **Internal IP** is the destination IP of a device that is connected to the gateway.
- **Internal Port** is the destination port of a device that is connected to the gateway.
- **External Port** is the external port that is used to forward traffic from a specific external port to an internal host on a specified port.

**Note**

- **Internal IP**
- **Internal Port**
- **External Port**

- **Enable** the rule.
- Click **SAVE**.
3. **Access the ioLogik web interface from a remote PC/notebook.**
   
   Once you connect a PC/notebook to the VPN Server on the remote site, the PC/notebook will automatically be assigned an IP address on the same network subnet as the ThingsPro Gateway. The firewall is configured to forward network requests from port 80 to internal port 80 on the iologik device. You can use the IP 192.168.254.1 to access the iologik web configuration page to monitor and control the device.