Tech Note 4 How to add security when connecting to remote field devices web interfaces

Abstract: Heading

This feature is used to add security using HTTPS/SSL encryption and user authentication (user name/password protection) to any web based product connected to the LAN. This document provides a step by step procedure for enabling the SN Proxy feature on the Red Lion Sixnet Series cellular or wired devices (e.g. Topology).

Product:

Any Red Lion Sixnet series SN 6000, RAM 6000, and RAM 9000

Use Case/ Problem Solved:

In many Machine to Machine (M2M) applications the cellular or wired network device is connected to remote field devices that have a built in Web Interface. The remote field devices include managed switches, operator interfaces with virtual interfaces (for remote viewing), supervisory control and data acquisition (SCADA) systems, programmable controllers, security cameras, etc... Web interfaces are typically used to configure, troubleshoot, monitor or control via a remote connection. The most common method used to browse a remote field device web interface is HTTP

http://www.any.com. The data passing between computer and the remote field device is not secure and the information passing between the two points can be compromised because it is not encrypted.

Solution:

Setting up the SNProxy in the Red Lion Sixnet Series cellular or wired devices allows you to connect to the remote field devices via HTTPS (Hypertext Transfer Protocol Secure) e.g. https://www.bank.com, which provides a secure SSL encrypted data path between both devices. One commonly known application where HTTPS is used is between home computers and bank accounts for added security. Another benefit of using the SNProxy is that it improves the overall connection performance.

The SNProxy setup can also enable the User Login feature, which requires the correct user credentials before access is granted to the field device's web interface.

Software:

Internet browser

Firmware:

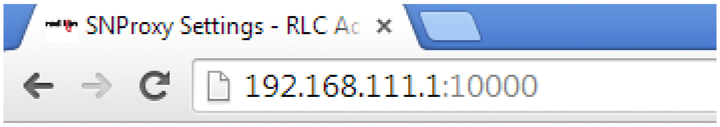
Version 3.12/4.12 or later

Part 1: SNProxy Settings

Procedure:

1. Log into your device (USB link & IP address used below)

   a. Enter the device's LAN/WAN IP, port 10000 into a web Browser

   b. User Name: *admin*

   c. Password: Last six digits of the device's serial number (unless the password has been changed)

   Note: It is strongly recommended to change the default password

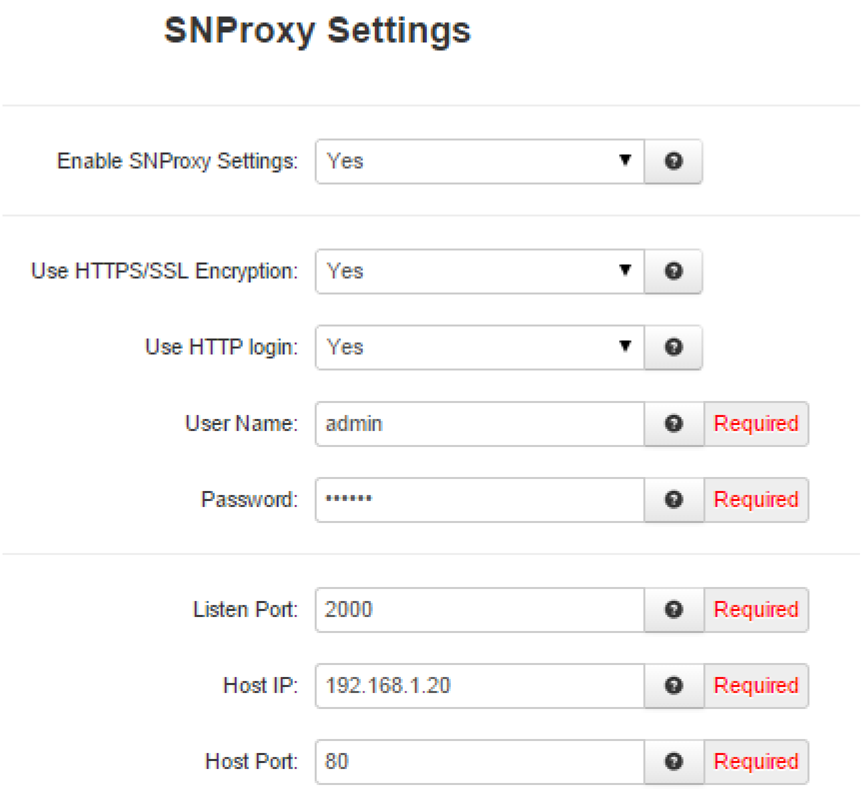
2. Go to **Services** → **SN Proxy Settings**

   a. Select **Yes** to **Enable SN Proxy Settings**

   b. Enable HTTPS/SSL Encryption

   c. Enable HTTP Login
   Enter a desired user name & password for securely logging in to the HMI

   d. Listen Port: 2000
   This can be any port number as it is the port number at which SN Proxy listens
   Host IP: 192.168.1.20 (IP address of the device you wish to connect)
   Host Port: 80 (Port 80 is the default for most web interfaces). Some web interfaces IP port can be configured. Use the IP port that is configured on your device.



SNProxy Settings

Enable SNProxy Settings: Yes

Use HTTPS/SSL Encryption: Yes

Use HTTP login: Yes

User Name: admin Required

Password: •••••• Required

Listen Port: 2000 Required

Host IP: 192.168.1.20 Required

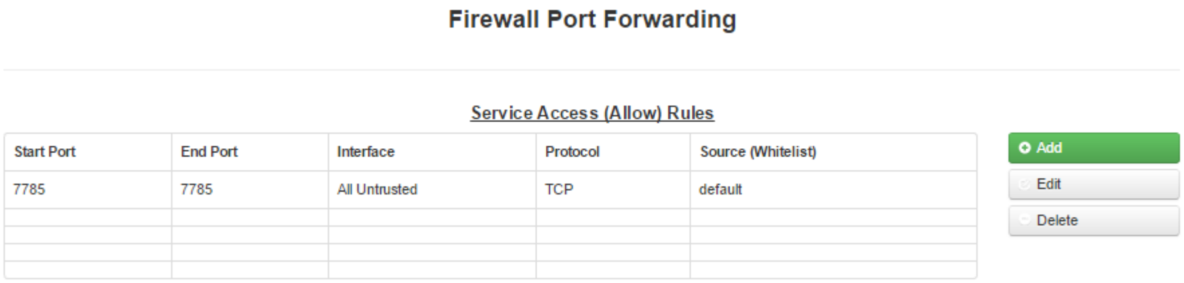
Host Port: 80 Required

3. Click **Apply**.

Part 2: Listening Port Settings

Open port 2000 (or port used as the Listening port in the previous step) in the routers firewall to allow traffic to pass through to the remote web interface.

1. Go to **Networking** → **Firewall** → **Port Allow/Forwarding Rules**
2. Select **Add** in the **Service Access** (Allow) **Rules** table



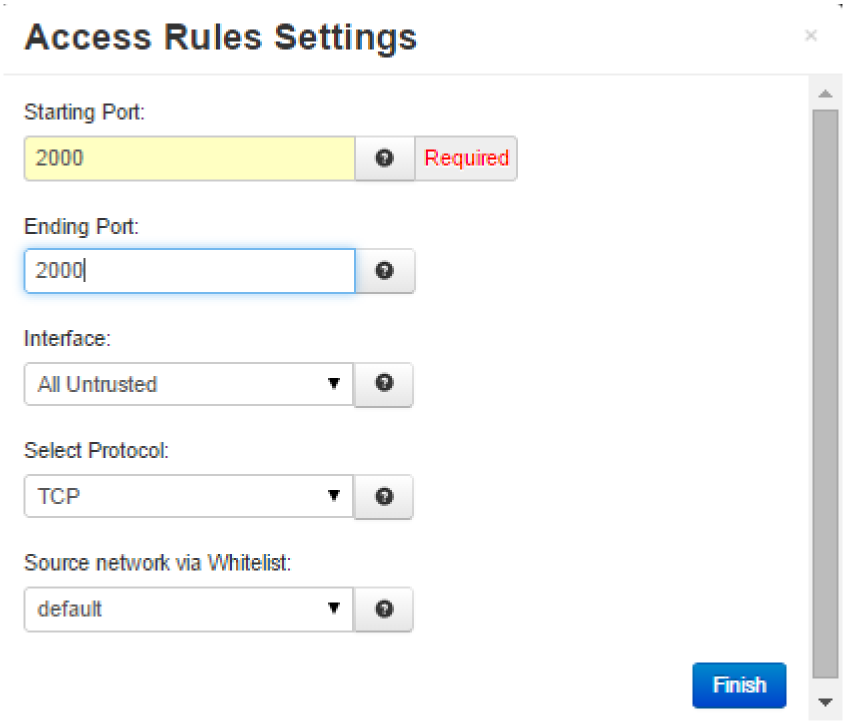
Firewall Port Forwarding

Service Access (Allow) Rules

Start Port	End Port	Interface	Protocol	Source (Whitelist)
7785	7785	All Untrusted	TCP	default

3. Set **Start Port** to: *2000* (Starting Point)
4. Set **End Port** to: *2000* (Ending Point)
5. Set **Interface** to: *All Untrusted*

6. Set **Protocol** to: *TCP* (Selected Protocol)
7. Set **Source (Network via) Whitelist** to: *default*
8. Click **Finish**



Access Rules Settings

Starting Port: 2000 Required

Ending Port: 2000

Interface: All Untrusted

Select Protocol: TCP

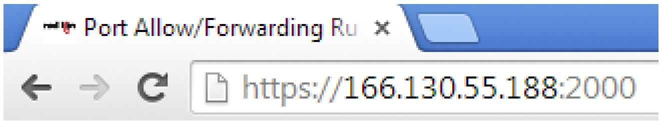
Source network via Whitelist: default

9. Click **Apply**.

The SNProxy configuration is now complete

Verify the SNProxy configuration

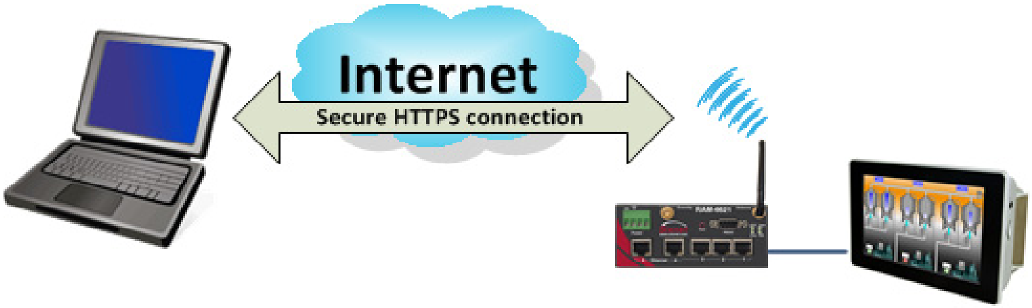
1. Open your web browser and enter the IP address of your device
2. https://your IP address:2000



https://166.130.55.188:2000

3. You should now be securely connected to your device.

Topology/Images:



Disclaimer:

It is the customer's responsibility to review the advice provided herein and its applicability to the system. Red Lion Controls makes no representation about specific knowledge of the customer's system or the specific performance of the system. Red Lion is not responsible for any damage to equipment or connected systems. The use of this document is at your own risk. Red Lion standard product warranty applies.

For questions contact Red Lion Inc. Support at 877-432-9908 or email to support@redlion.net