Tech Note 1 How to access remote field devices through a cellular device

Abstract:

Port forwarding can be used to remotely access multiple IP addressable devices over the Internet using a single cellular device. This document details the steps to implement this functionality.

Product:

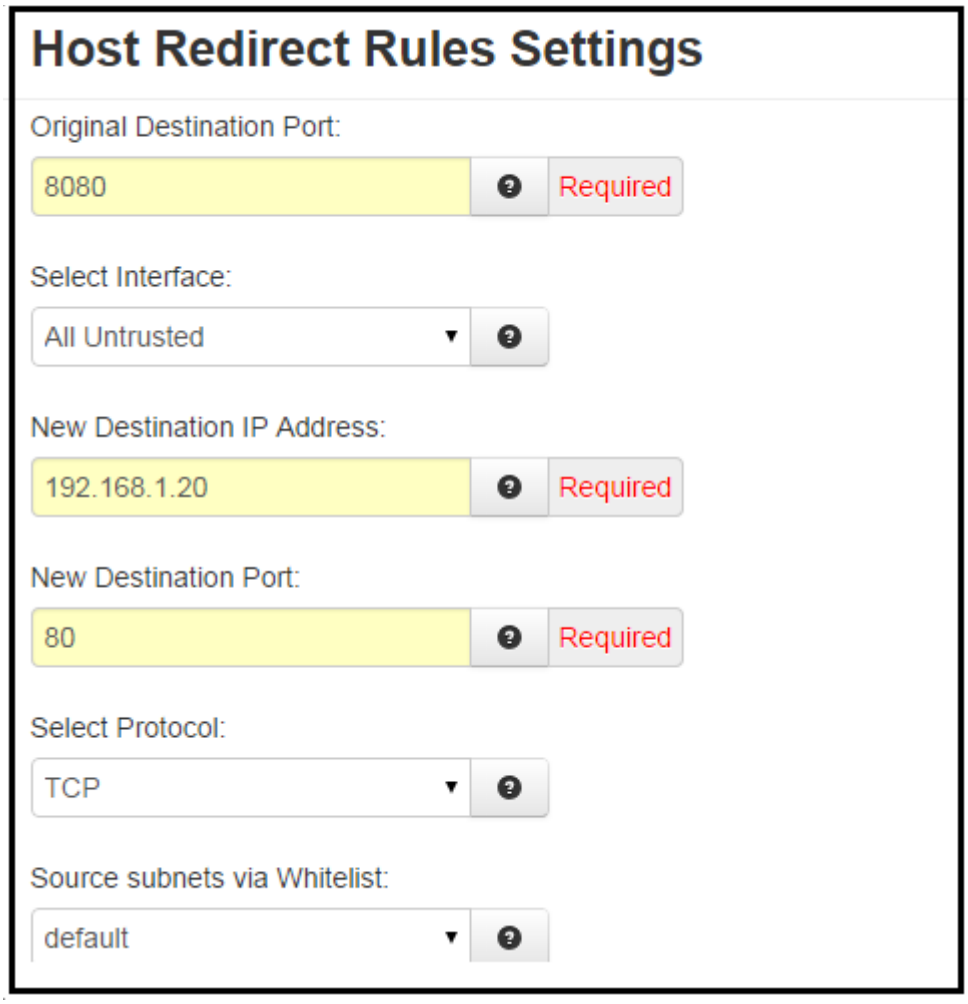
Any Red Lion Controls Sixnet Series SN 6000, RAM 6000, and RAM 9000

Use Case/ Problem Solved:

Host Redirect (Port Forwarding) Rules allow multiple devices such as Human Machine Interfaces (HMI), programmable controllers, and remote telemetry units (RTU) that have different IP addresses on a LAN (Local Area Network) to be accessed at a single Internet IP address.

Procedure:

1. Log into the SN/RAM interface using a Web Browser
2. Enter the device's LAN/WAN IP, port 10000 into a web browser
3. Eg: 192.168.0.1:10000
4. **User Name:** admin
5. Password: Last six digits of the device's serial number
6. Go to **Network** → **Firewall** → **Port Allow/Forwarding Rules**
7. Scroll down to **Host Redirect** (Port Forwarding) rules
8. Click **Add**.
9. Setup the port forwarding rule in the popup window that appeared.
   a. **Original Destination Port:** Enter the port that an external device will remotely connect to. This is the port that will be open on the specified interface. For example, by default Modbus uses port 502. This would match the New Destination Port unless there are multiple end point devices listening on the same port.
   b. **Select Interface:** Click on the pull down menu to select the interface on which to open the specified port. It is recommended to use the default setting.
   c. **New Destination IP Address:** Enter the IP Address of the device (e.g. HMI, PLC, or RTU) that the incoming connection will be redirected to, which must be in the same subnet as the router's LAN interface… example? … reference?
   d. **New Destination Port**: Enter the port that the incoming connection will be redirected to (for example, Modbus port 502). This is the port number of the device behind the router.
   e. **Select Protocol**: Choose the protocol type for this port's data. TCP or UDP.
   f. **Source subnets via whitelist**: Select a whitelist name, a list of allowed external IP addresses, from the list of names available in the drop-down list box provided. Whitelists may be viewed or defined via the **Networking** → **Firewall** → **Subnet Whitelist Rules** screen. It is recommended to use the default.
   g. Click **Finish**.



10. Click **Save**. The port forwarding rule is set on the router.

Disclaimer

It is the customer's responsibility to review the advice provided herein and its applicability to the system. Red Lion 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 Support at 877-432-9908 or email to support@redlion.net