

Protecting a Modbus PLC with Tofino™ Modbus TCP Enforcer

Application Note #102

AN-102
Version 1.0

Overview

Modbus/TCP is one of the most widely used industrial communication protocols in the world. Modbus started out as a serial protocol running on RS-232 or RS-485 connections, migrating to TCP when Ethernet was deployed on the plant floor.

Like many industrial communication protocols, Modbus has no security features whatsoever – for example, there is no concept of a ‘user name’ and ‘password’ in the protocol to authenticate users or devices that attempt to connect to a Modbus PLC. Any network device can issue commands to a Modbus PLC; these commands can not only read data from the device, but also make changes to it. Needless to say, issuing a command to open a valve or change a pump speed at the wrong time could have disastrous consequences on the plant floor.

A firewall can help protect critical Modbus controllers by restricting which Modbus masters are allowed to communicate with a protected slave device. The Tofino Modbus Enforcer extends this capability by enabling the control engineer to specify a list of ‘permitted’ Modbus function codes and register/coil addresses that may be accessed in each Modbus master/slave connection. In operation, the Modbus Enforcer will examine each Modbus command and response passing between the Modbus devices, and block all accesses that fall outside the limits specified by the control engineer. This goes far beyond the protection offered by a conventional firewall device.

This document provides an introduction to the Modbus TCP Enforcer and shows an example of how it may be used to protect a Modbus PLC.

Example Use Case

In this example, a Modbus PLC is used at a water plant to monitor the level of a holding tank and control the speed of a fill pump. Two PCs communicate with the PLC over the network: an HMI program polls the PLC to provide an operator display, and an engineering workstation is used by the control system engineer to periodically update the PLC’s firmware and ladder logic. Figure 1 shows the network diagram of this portion of the water plant.

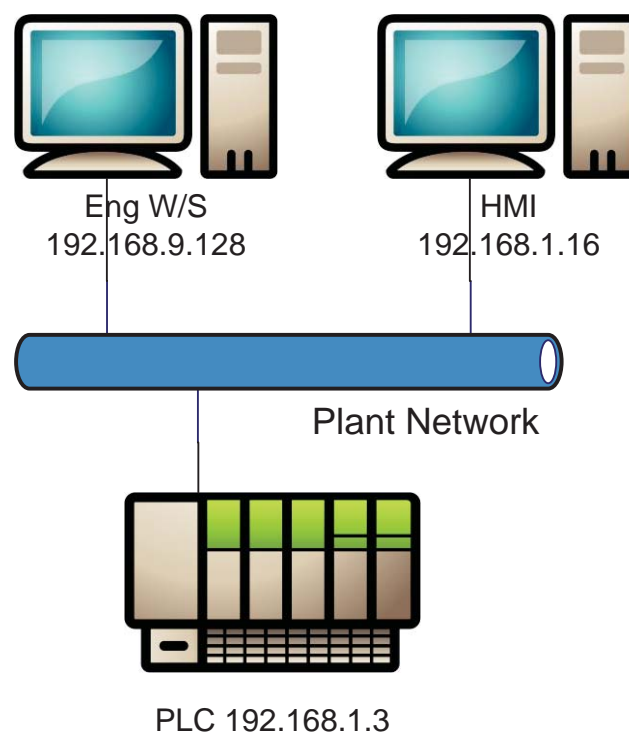


Figure 1: Water Plant Control Network

The following access policies will be implemented for this PLC:

1. The HMI computer is allowed read-only access to the first 100 Modbus holding registers in the PLC

- The Engineering Workstation is allowed read and write access to any of the PLC's holding registers, and may also configure the PLC and upload new ladder logic to it.
- No other network access is permitted to the PLC.

A Tofino Security Appliance is inserted in-line between the PLC and the rest of the network and configured to enforce these access policies. To configure, test and manage the appliance, a PC running the Tofino CMP software is installed. The resulting network is shown in Figure 2.

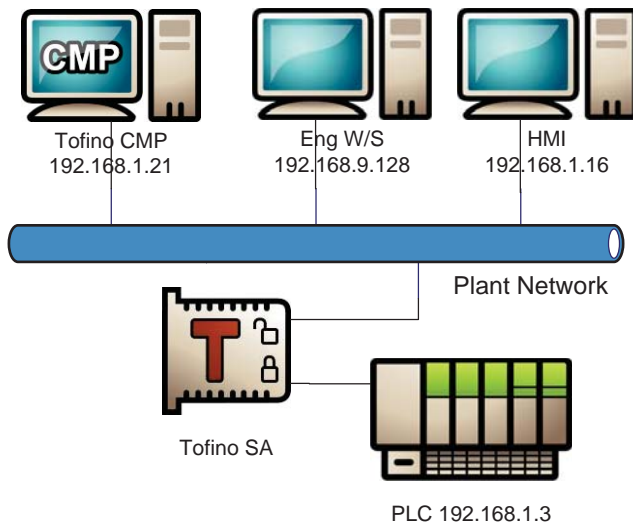


Figure 2: Control Network with Tofino

Configuration in the Tofino CMP

The Tofino CMP enables the user to create a model of the control network by dragging icons from the Nodes view (or by using the Tofino and Asset Discovery features) and dropping them into the Network Editor. It's possible to model the entire network if desired, but only devices that will appear in the firewall rules are required to be included in the network model. As a result, the finished model of the water plant network (Figure 3) is very simple.

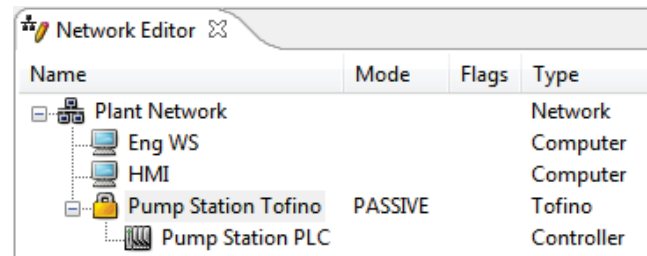


Figure 3: Network Model in the Tofino CMP

Once the model is complete, the Tofino Firewall and Modbus TCP Enforcer Modules must be activated on the Tofino Security Appliance. This is done on the 'Modules' tab of the Tofino icon in the Network Editor.

Creating Firewall Rules

Next, a firewall rule is created to allow communications between the HMI computer and the PLC. A 'Talker' firewall rule is created as follows:

- Double-click on the Water Plant PLC icon to display the PLC's settings, then click on its Firewall tab.
- Locate the HMI icon in the 'Network' view (top left corner of the Tofino CMP), then drag this icon and drop it on the 'Talker Rules' row in the PLC's firewall tab.
- Drag the 'Modbus/TCP' protocol from the 'Protocols' view (bottom right corner of the Tofino CMP) and drop it on the HMI icon in the PLC's firewall tab.

After repeating these steps to create another firewall rule for the Engineering Workstation, the PLC's firewall tab is shown in Figure 4.

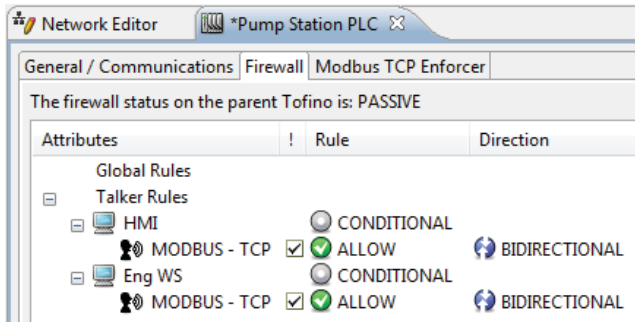


Figure 4: 'Talker' Rules for Modbus/TCP Protocol

Filtering Modbus Function Codes

Once the basic firewall rules have been created to allow Modbus traffic to the PLC, they must be modified to enable the Modbus Enforcer to inspect the network traffic.

On the PLC's firewall tab, double-click the Modbus firewall rules and change the permission setting from 'Allow' to 'Enforcer'. After making these changes, the Firewall tab will appear as shown in Figure 5.

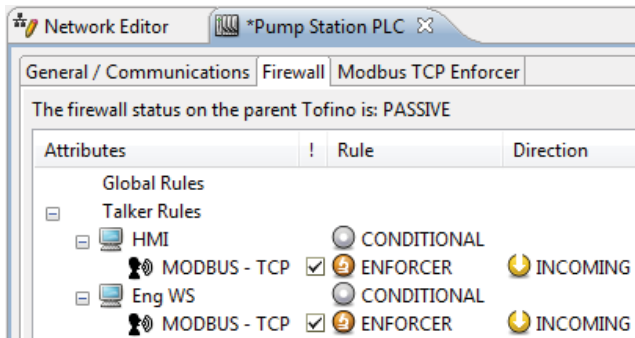


Figure 5: Firewall Rule with 'Enforcer' Permission

The next step is to specify the Modbus function codes and register/coil addresses that should be allowed for these connections. To do this, click on the PLC's 'Modbus TCP Enforcer' tab. Two computer icons, representing the HMI computer and Engineering Workstation, should be visible on this tab. Right-clicking the HMI icon brings up a context menu that allows the addition of a new Modbus function code.

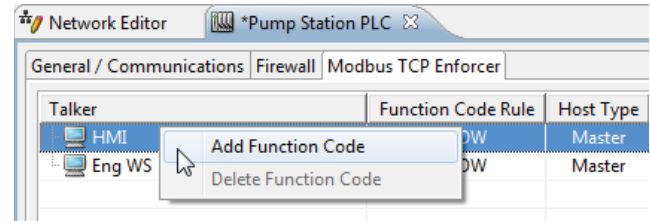


Figure 6: Adding a New Function Code

Clicking on the function code name will display a pull-down list of function codes, which can be used to select the desired function code. A wide range of function codes are supported by the Modbus Enforcer, including all public codes and many proprietary ones as well. Multiple function codes may be added to the list, including multiple instances of the same function code with different address ranges if necessary. The completed Modbus TCP Enforcer tab for our example system is shown in Figure 7.

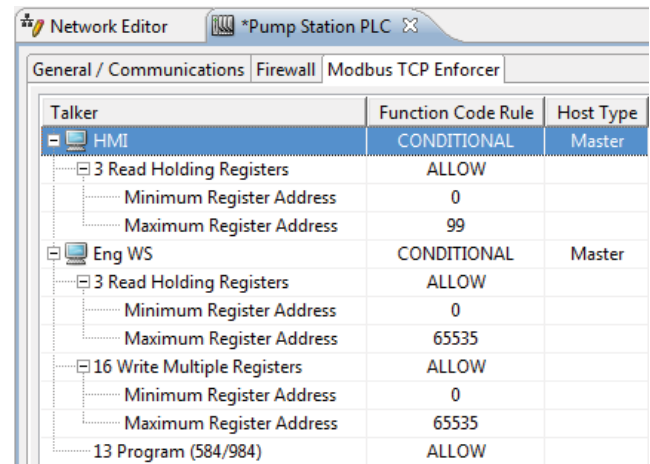


Figure 7: Completed Modbus Enforcer Rules

Testing the Rules

Tofino's unique 'Test' mode allows all network traffic to pass through the security appliance, but generates alarm messages for any traffic that would have been blocked if the device was operational. This permits testing firewall and Modbus Enforcer rules with no risk of accidentally blocking traffic that must be allowed through for correct plant operation.

The Tofino's operating mode is set using the pull-down control at the bottom of its 'General/Communications' tab. In Test mode, any disallowed traffic will generate an Exception Heartbeat message that is displayed in the Tofino CMP Event view. Double-clicking on an Exception Heartbeat will display more details about the heartbeat, as shown in Figure 8.

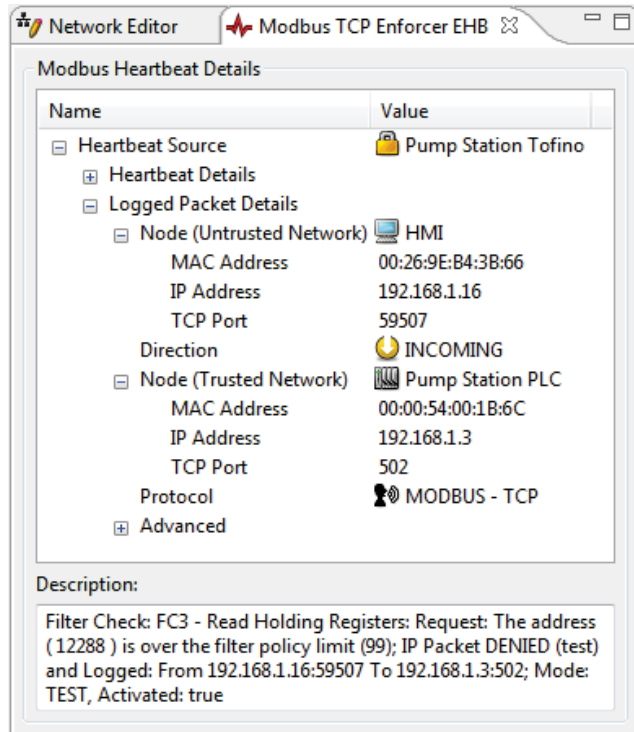


Figure 8: Modbus Enforcer Exception Heartbeat

By monitoring the exception events and editing the firewall and Modbus Enforcer configuration, the user may ensure that all required system traffic can pass through the Tofino SA without generating alarms. After testing is complete, the Tofino SA may be deployed in Operational mode to enforce the rules that have been configured.

Modbus Enforcer Options

Several options are available to control how the Modbus Enforcer manages each Modbus connection.

'Sanity Check' causes the Modbus Enforcer to check the Modbus commands and responses for compliance with the Modbus protocol specification. This option may be turned off when using devices that are known to be non-compliant with the specification.

'Reset' and 'Exception' control how the Modbus Enforcer responds when an individual Modbus command is disallowed by the user's rules and must be blocked. If 'Exception' is enabled, then a Modbus exception response is returned to the Modbus master device to indicate a data error. If 'Reset' is enabled, a TCP reset is sent to both the Modbus master and slave devices to terminate the TCP connection. (TCP only - this option has no effect on Modbus/UDP connections.) These options may be enabled simultaneously, in which case the TCP reset and Modbus exception response will be sent in the same packet. If neither option is set, then the packet will be dropped and no notification will be sent to either Modbus device. The default settings (both options enabled) are appropriate for most applications.

The last option, 'State Tracking', causes the Modbus Enforcer to track the command and response packets between the Modbus master and slave devices to ensure that they match up – i.e. checking that every command packet results in one, and only one, response packet. This prevents certain types of attacks that might otherwise be possible from a compromised or spoofed slave device.

Summary

The Tofino Modbus TCP Enforcer is quick and simple to configure, and offers dramatic security and reliability improvements for any industrial control system that uses Modbus/TCP. In addition, Tofino's Test mode allows the entire security solution to be tested in-circuit before deployment to ensure that it will operate as intended.



BYRES SECURITY INC.
TEL: 1 250 390 1333
TOLL FREE: 1 877 297 3799 (N. America)
EMAIL: sales@tofinosecurity.com