

Tofino Content Inspector for Modbus by Byres Security

Content Inspector for Modbus

-

Pre-emptive threat detection

-

Threat termination

-

Threat reporting

Did you know that any device with a network connection to a Modbus controller can potentially CHANGE any of the controller's I/O points or register values? Many controllers can even be reset, disabled, or loaded with new logic or firmware code!

Tofino Modbus TCP Enforcer LSM

Did you know that any device with a network connection to a Modbus controller can potentially CHANGE any of the controller's I/O points or register values? Many controllers can even be reset, disabled, or loaded with new logic or firmware code!

The Tofino Modbus TCP Enforcer is a border guard inspector for Modbus communications, checking every Modbus command and response against a list of 'allowed' commands defined by your control engineers. Any command that is not on the 'allowed' list, or any attempt to access a register or coil that is outside the allowed range, will be blocked and reported by Tofino Modbus TCP Enforcer.

Summary

Saves You Money Through:

-

Reduced down time and production losses

-

Lower maintenance costs

-

Improved system reliability and stability

Features

-

First-ever application of traffic inspection technology to industrial protocols

-

Control engineer defines list of allowed Modbus registers and coils, and limits of accessible register and coil addresses

-

Automatically blocks and reports any traffic that does not match your rules

-

Protocol 'Sanity Check'; blocks any traffic not conforming to Modbus standard

-

Supports multiple master and slave devices

-

Simple configuration and monitoring using Tofino CMP

-

Certified Modbus compliant by Modbus IDA

Applications

-

Oil & gas custody transfer

-

Safety instrumentation systems

-

Historian servers

-

Display-only HMI panels

-

Partner access to telemetry data

Specifications

Supports Multiple Connections

Multiple master and slave Modbus devices are supported, with a unique set of inspection rules and options for each master/slave connection

Default Filter Policy

Deny by default: any Modbus function code, or register or coil address, that is not on the 'allowed' list is automatically blocked and reported

User-Settable Options

The following options may be set on a per-connection basis:

-

Permitted Modbus function codes

-

Permitted register or coil address range (for each permitted function code that accesses registers or coils)

-

Sanity check enable/disable

-

State tracking enable/disable

-

TCP Reset on blocked traffic (only for connections utilizing MODBUS/TCP transport protocol)

-

Modbus exception reply on blocked traffic

Transport Protocols

Both Modbus/TCP and Modbus/UDP supported

Operating Modes

All standard Tofino modes supported:

- Passive: no filtering or alerting
- Test: no traffic filtered; alerts generated as per user-defined rules
- Operational: traffic filtered and alerts generated as per user-defined rules

Security Alerts

Reports blocked traffic to Tofino CMP management console via Tofino 'Exception Heartbeat' mechanism

Certifications

Certified Modbus-compliant by Modbus-IDA

System Requirements

-

Tofino Security Appliance

-

Tofino Firewall LSM

-

Tofino Central Management Platform software

Ordering Information

MTL part number 9520-MBT-G-1 (Tofino Modbus TCP Deep Packet Inspection LSM)

[Download PDF Data Sheet](#)