MTL Tofino™ DNP3 Enforcer LSM

A plug-in Deep Packet Inspection (DPI) module that provides real-time validity checking and content inspection for DNP3 traffic.

MTL Tofino™ DNP3 Enforcer

The MTL Tofino™ DNP3 Enforcer Loadable Security Module (LSM) is a plug-in Deep Packet Inspection (DPI) module providing Advanced Cyber Threat and Vulnerability Protection for DNP3 Protocol Communications making sure that the only DNP3 commands your control devices receive are approved commands from authorized computers.

Distributed Network Protocol (DNP3) isIEEE Standard for Electric Power Systems Communications. It's the popular, open utility protocol that emphasizes reliability and less bandwidth usage.

While widely used in power and utility networks, DNP3 also face security vulnerabilities, not only on the slave device, but the master stations as well. Successfully attack a PLC or RTU in a substation and you might knock that station off line. Successfully attack a SCADA master and you can knock a whole system off line.

The MTL Tofino™ DNP3 Enforcer LSM enables deep packet inspection (DPI) capabilities for DNP3 traffic. It ensures that end values are greater than the starting values. If this isn't the case, the Tofino security appliance should drop the packet REGARDLESS of data content. Thus no matter what the attacker puts in his/her payload, or how he/she tried to obfuscate it with techniques like NOP slides, the checks will detect and block the attack. The installation engineer can specify master/slave device pairs between which DNP3 traffic will be allowed to flow. Only correctly formatted DNP3 traffic will be allowed.

DNP3 validation includes checking of common header byte fields, packet lengths, and DNP3 CRC values.

Saves you money through:

- Simplifying compliance to safety and security standards.
- Reduced down time and production losses.
- Lower maintenance costs.
- Improved system reliability and stability.

Unique capabilities:

- Unique deep packet inspection technology for industrial protocols
- Control specialist defines list of allowed DNP3 message type and function codes
- Automatically blocks and reports any traffic that does not match the rules
- Protocol 'Sanity Check' blocks any traffic not conforming to the DNP3 standard
- Supports multiple master and slave devices
- Simple configuration using the Tofino Configurator's graphical user interface

Applications

- SCADA Master Station protection
- Cyber security solution for PLCs, RTUs, IEDs, DCS
- NERC-CIP Compliance
- Electric utility transmission and transmission substation security
- Prevents malware and Man-in-the-Middle attacks

Powering Business Worldwide

Eaton Electric Limited,
Great Marlings, Butterfield, Luton
Beds, LU2 8DL, UK.
Tel: + 44 (0)1582 723633 Fax: + 44 (0)1582 422283
E-mail: mtlenquiry@eaton.com
www.mtl-inst.com

Publication No. EPS DNP2-LSM rev 1 090218
February 2018

FEATURES & SPECIFICATIONS

Supports multiple connections	Multiple master and slave DNP3 devices are supported with a unique set of inspection rules and options for each master/slave connection
Default filter policy	Deny by default: any DNP3 function code 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 DNP3 function codes • Check outstation traffic • Permitted DNP3 Unit IDs • Sanity check enable/disable • CRC check • TCP Reset on blocked traffic (when utilizing TCP transport protocol) • DNP3 exception reply on blocked traffic
Configuration method	Simple configuration using the MTL Tofino™ Configurator (TC).
Throughput	2000 packets per second with full content inspection
Operating modes	All standard Tofino modes supported: • Test: all traffic allowed; alerts generated as per user rules • Operational: traffic filtered and alerts generated as per user rules
Security alerts	Reports security alerts to a syslog server and to non-volatile memory on a MTL Tofino™ Security Appliance.
Certifications	Certified Modbus compliant by Modbus-IDA.
System requirements	• MTL Tofino™ (9202-ETS) Industrial Security Appliance.These new enforcers cannot be run in older systems. They will work for existing MTL Tofino™ (9202-ETS) in the field • MTL Tofino™ Firewall/Event Logger LSM • MTL Tofino™ Configurator
Ordering information	Part number: **9522-DNP3** Name: **MTL Tofino™ DNP3 Enforcer LSM** Visit: **www.mtl-inst.com/product/9202-ets_mtl_tofino_network_security_solution/**

The **MTL Tofino™ DNP3 Enforcer LSM** is a component of the **MTL Tofino™ Industrial Security Solution**

MTL Tofino™ Industrial Security Appliance

Hardware platform that creates Plug-n-Protect™ zones of security on control and SCADA networks.

Loadable Security Modules

Firmware modules that customize the security features of each MTL Tofino™ SA:

- **Firewall:** Monitors and controls industrial network traffic.
- **Modbus, OPC, EtherNet/IP, DNP3, IEC 104 and GOOSE Enforcers:** Ensure compliance, manage connections, and restrict ICS/ SCADA commands.
- **NetConnect:** Provides secure remote configuration over any IP-based network.
- **Event Logger:** Reliably logs security events and alarms.

MTL Tofino™ Configurator (3.2)

Software that provides coordinated security management of all MTL Tofino™ Security Appliances from one workstation or server.

Powering Business Worldwide

Eaton Electric Limited,
Great Marlings, Butterfield, Luton
Beds, LU2 8DL, UK.
Tel: + 44 (0)1582 723633 Fax: + 44 (0)1582 422283
E-mail: mtlenquiry@eaton.com
www.mtl-inst.com

Publication No. EPS DNP3-LSM rev 1 090218
February 2018

EUROPE (EMEA):
+44 (0)1582 723633
mtlenquiry@eaton.com

THE AMERICAS:
+1 800 835 7075
mtl-us-info@eaton.com

ASIA-PACIFIC:
+65 6 645 9888
sales.mtlsing@eaton.com