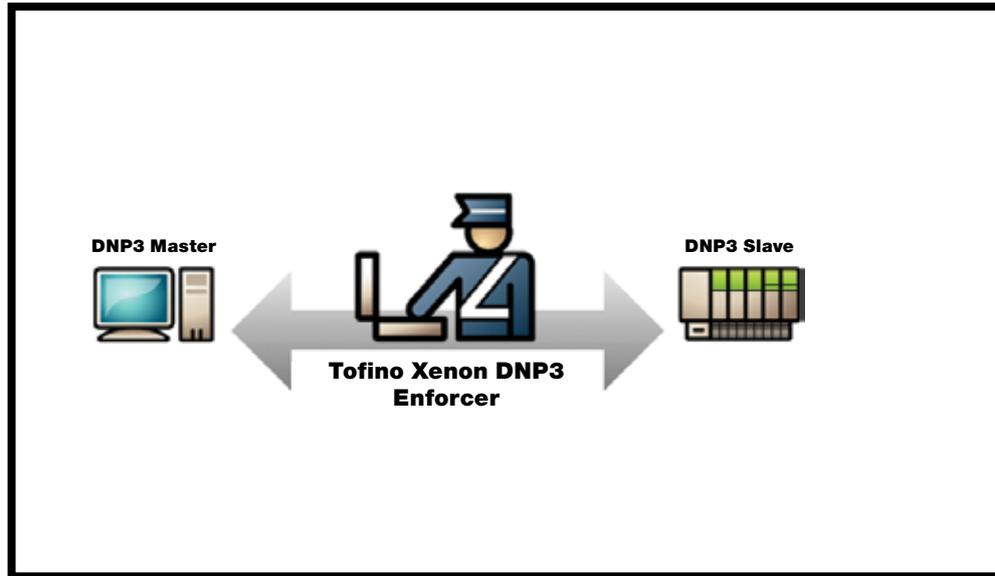


PB00058

Tofino Xenon DNP3 Enforcer Loadable Security Module (LSM)

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



The Tofino Xenon DNP3 Enforcer LSM makes sure that the only DNP3 commands your control devices receive are approved commands from authorized computers.

Advanced Cyber Threat and Vulnerability Protection for IEC 104 Protocol Communications

Distributed Network Protocol (DNP3) is IEEE 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 Tofino Xenon 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

**Be certain.
Belden.**

Tofino Xenon DNP3 Enforcer LSM

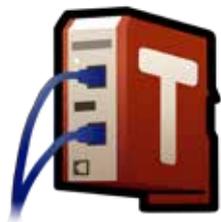
Features and Specifications

Type	Description
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: <ul style="list-style-type: none"> • 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 Tofino Configurator
Throughput	2000 packets per second with full content inspection
Operating modes	All standard Tofino modes supported: <ul style="list-style-type: none"> • 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 Tofino Security Appliance
System requirements	<ul style="list-style-type: none"> • Tofino Xenon Industrial Security Appliance. These new enforcers cannot be run in older systems. They will work for existing Tofino Xenons in the field • Tofino Firewall/Event Logger LSM • Tofino Configurator
Ordering information	Part number: LSM: 942-140-006 Name: Tofino Xenon DNP3 Enforcer LSM For additional information, visit www.belden.com/products/industrialnetworking/security/tofino-xenon.cfm

Tofino Xenon DNP3 Enforcer LSM is a component of the Tofino Security Solution

Tofino Xenon 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 Tofino SA:

- **Firewall:** Monitors and secures industrial network traffic
- **Modbus, OPC, EtherNet/IP, DNP3 and IEC 104 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

Tofino Configurator (3.0 and higher)

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

