

Tofino™ Firewall LSM

Directs and controls industrial network traffic

Data Sheet

DS-FW-LSM
Version 5.0



Take control of your network traffic

The vast majority of control networks have little or no isolation between different subsystems. If a device misconfiguration, hardware failure, or virus causes a problem in one part of the network, it can spread throughout the entire network in seconds and bring your whole plant down. Even redundant backup systems can fail simultaneously if their network connections are not protected.

The Tofino Firewall LSM is like a traffic control cop for industrial networks, checking all communications on your control network against a list of traffic 'rules' defined by your control engineers. Any communication that is not on the 'allowed' list will be blocked and reported by the Tofino Firewall.

Traffic rules are created using terms and concepts that are already familiar to control specialists. And, the unique 'test' mode of Tofino lets you test your rules without any risk to plant operation.

Saves you money through:

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

Unique capabilities:

- Traffic rules are defined by your control team, specifying which devices may communicate using what protocols
- Rule definition is simple using a graphical drag-and-drop editor
- Traffic that does not match the rules is automatically blocked and reported
- Over 50 pre-defined IT and industrial communication protocols
- Over 25 pre-defined controller templates
- Pre-defined 'special rules' for advanced traffic filtering and vulnerability protection

Typical applications:

- Isolate critical devices from threat sources
- Separate control networks into security 'zones', restricting communications between zones
- Protect controllers with known vulnerabilities

FROST & SULLIVAN

2010 World Customer Value
Enhancement Award
tofinosecurity.com/awards

TOFINO®

Protects multiple devices	Master and slave devices are supported, with unique direction and permission settings for each client/server connection
Filter policy	Deny by default: any network traffic that is not on the 'allowed' list is automatically blocked and reported
State tracking	Stateful Packet Inspection (SPI)
User-settable options	<p>IP-based protocols:</p> <ul style="list-style-type: none"> ▪ <i>Source device</i>: specific IP address, network, or 'any' ▪ <i>Destination device</i>: specific IP address, network, broadcast, multicast, or 'any' ▪ <i>Application protocol</i>: any combination of single, list, and/or range of port numbers ▪ <i>Direction</i>: incoming, outgoing, bidirectional ▪ Both IP-based and non-IP protocols ▪ <i>Permission</i>: allow, deny, allow/log, deny/no log
Transport protocols	TCP, UDP and non-IP protocols supported
Configuration method	Simple configuration using the Tofino Central Management Platform (CMP)
Operating modes	<p>All standard Tofino modes supported:</p> <ul style="list-style-type: none"> ▪ <i>Passive</i>: all traffic allowed, no alerting ▪ <i>Test</i>: all traffic allowed; alerts generated as per user rules ▪ <i>Operational</i>: traffic filtered and alerts generated as per user rules
Security alerts	Reports blocked traffic to the Tofino CMP via Tofino Exception Heartbeats
Certifications	<ul style="list-style-type: none"> ▪ MUSIC 2009-1 security certified (Foundation level) ▪ Certified Modbus compliant by Modbus-IDA
System requirements	<ul style="list-style-type: none"> ▪ Tofino Security Appliance ▪ Tofino Central Management Platform
Ordering information	<p>Part number: LSM-FW-100 Name: Tofino™ Argon Firewall LSM For additional information, visit www.tofinosecurity.com/buy/tofino-argon</p>

Tofino™ Firewall LSM is a component of the Tofino Security Solution:

Tofino 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**: Directs and controls industrial network traffic
- **Modbus and OPC Enforcers**: Content inspection and connection management for Modbus and OPC
- **Secure Asset Management**: Tracks and identifies network devices
- **VPN**: Secures remote communication
- **Event Logger**: Reliably logs security events and alarms

Tofino CMP

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



Copyright © 2010 by Byres Security Inc., All Rights Reserved. All specifications are subject to change without notice.

Your authorized Tofino supplier: