Tofino™ **Firewall** LSM

工业网络通讯的管控核心

完全掌控您的工业通讯网络交通

绝大多数的控制网络在不同的子系统之间很少甚至没有隔离功能。如果网络中的一部分设备因配置错误，硬件故障，或病毒 的原因发生问题，它可以在几秒钟内传播到整个网络，造成你的整个工厂停车。如果您的网络连接没有安全保护措施，即使是冗余的系统也可能会发生主用和备用设备同时故障的情况。

Tofino 防火墙的 LSM （Loadable Security Module）如同是工业网络交通警察，它可以检查出所有有悖于您的控制网络工程师所定义的网络安全规则的通讯内容。所有的违反网络安全规则的名单都将被封锁，Tofino 防火墙将对所有非法的通讯内容都进行封锁并提供报告和记录。

编辑安全规则时使用的都是控制领域人们所熟悉的术语和概念，而且，独特的“Tofino 测试模式”可以让您在没有任何风险的环境下对您的网络进行安全规则的测试。

节约成本措施：

- 在遵守安全原则和安全标准 前提下对实施过程进行简化
- 减少停机时间和降低生产损失
- 更低的培训费用和人员费用
- 提高系统可靠性和稳定性

特有功能：

- 由您的控制团队来定义通讯安全规则，比如指定哪些设备可以使用什么通信协议进行通讯等
- 规则的定义很简单，使用图形化的拖放编辑器就可实现
- 与安全规则相悖的通讯内容会自动被屏蔽并提供报告
- 预先定义超过 50 个 IT 及工 业通信协议
- 预先定义超过 25 个控制器类型
- 预先定义“特殊规则”用于高级过滤和攻击保护

典型应用：

- 将关键设备从安全威胁来源端隔离
- 将各层控制网络配置到独立的安全区域，隔离保护各层网络之间的通讯
- 通过修复已知的协议漏洞来保护控制器

TOFINO®

Tofino™ Firewall LSM

特点及规格

可同时保护多台设备	通过独特的引导和授权设定为每个客户端/服务器建立连接方式实现对主从设备的支持
过滤原则	默认为拒绝：任何不被允许的通讯内容都将被隔离并发出报告
状态追踪	状态封包检测（SPI）
用户可设置的选项	基于 IP 协议： ▪ 源设备：可以设定为指定的 IP 地址、网络或“任何设备（any）” ▪ 目标设备：可以设定为指定的 IP 地址、网络、广播、组播或“任何设备（any）” ▪ 应用协议：任意的单一、系列和（或）端口范围等的组合 ▪ 方向性：输入，传出，双向 ▪ 基于 IP 和非 IP 协议皆可 ▪ 权限：允许，拒绝，允许/有日志，拒绝/无日志
传输协议	支持 TCP, UDP 和 其它非 IP 协议
配置方式	使用 Tofino 中央管理平台（CMP） 可以便捷的进行配置
操作模式	支持所有标准Tofino模式： ▪ 被动模式：允许所有通讯且没有报警 ▪ 测试模式：允许所有的通讯并为每个用户的安全规则生成报警 ▪ 操作模式：过滤通讯内容并为每个用户的安全规则生成报警
安全警报	通过 Tofino Exception Heartbeats 功能在 CMP 上报告被隔离的通讯
认证	▪ MUSIC 2009-1 安全认证 (基础层) ▪ 通过 Modbus –IDA 认证
系统需求	▪ Tofino 安全设备（TSA) ▪ Tofino 中央管理平台（CMP）
订购信息	产品号: **LSM-FW-100** 名称: **Tofino™ Argon Firewall LSM** 更多信息请登录： www.tofinosecurity.com/buy/tofino-argon

Tofino LSM 是 Tofino 工业安全解决方案的重要组成部分之一:

Tofino 安全设备（TSA）

Tofino Security Appliance

通过硬件平台为控制和 SCADA 网络安全建立了即插即用安全保护区域。

可装载安全模块（LSM）

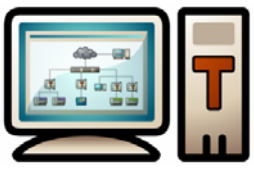
Loadable Security Modules

为 TSA 专门定制的各种可装载安全模件：

- **防火墙**：指导并控制工业网络信息流通
- **Modbus 与 OPC 应用:**深层次的 Modbus 及 OPC 的通讯检测和连接管理
- **安全资产管理:** 追踪并识别网络设备
- **VPN:** 安全的虚拟网络远程通讯
- **事件记录功能:** 可靠的安全事件和报警信息记录

Tofino CMP

通过一台工作站或服务器对所有 Tofino 安全设备（TSA）进行集中组态、管理并进行报警记录的软件系统



TOFINO™
tofinosecurity.com