

## 使用 Tofino 控制 Stuxnet（震网）恶意攻击的蔓延

本文档详细介绍了如何使用 Tofino 工业安全解决方案，来遏止西门子及非西门子网络环境中的 Stuxnet 蠕虫病毒传播。

### 前情回顾

#### Stuxnet 是什么？

Stuxnet 是一种计算机蠕虫，专门针对使用西门子 PLC 的一个或多个工业系统。这个恶意软件的目的似乎是摧毁特定工业流程。

Stuxnet 会感染基于 Windows 的任何控制系统或 SCADA 系统的计算机，无论其是否使用了西门子系统。该蠕虫只尝试进行修改控制器是模型 S7 - 300 或 S7 - 400 的 PLC。但是，它对所有的网络都具有侵略性，可能对任何控制系统造成负面影响。受感染的电脑也将成为未来恶意攻击的启动点。

#### Stuxnet 的传播途径

Stuxnet 是人们所见过的有史以来设计最为复杂和精心的蠕虫之一。它至少利用了四个之前未知的弱点，具有多种传播途径，对西门子控制系统的开发性上也极其复杂。

遏止 Stuxnet 攻击的难题在于其攻击并感染其他计算机的技术极为多样。它主要通过以下三种途径来进行传播：

- 通过被感染的可移动 USB 驱动器；
- 通过局域网络通信；
- 通过被感染的西门子项目文件。

在这些途径中，它利用了七种独立的机制优势来感染其他计算机。

Stuxnet 同样有一个 P2P

(peer-to-peer) 的网络系统，使得 Stuxnet 能够自动更新，即使它们不能连接回互联网。Stuxnet 还能

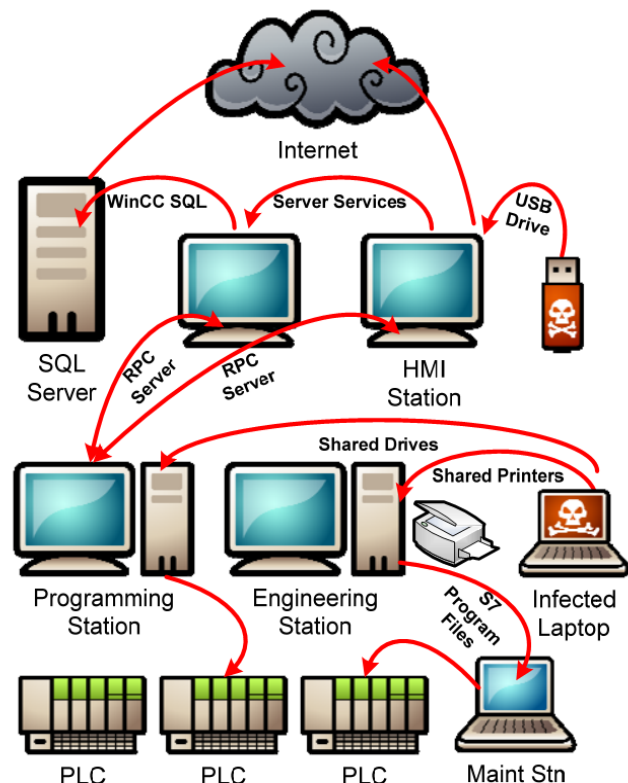


图 1: Stuxnet 的多种传播途径

更多技术了解访问 <http://www.mosesceo.com> OR <http://www.tofinosecurity.com>

基于互联网进行指挥和控制，该机制目前已停用，但可在未来重新启动。

许多人错误地认为，禁用被感染的 USB 驱动器，就可以有效防止 Stuxnet 的风险。很遗憾，这种想法是错误的。Stuxnet 攻击方法的多样性，使得任何企图遏止 Stuxnet 蔓延的行为复杂化，如果要实现有效的安全防护，就必须采用“深度防御”的做法。

针对 Stuxnet 的安全防护设计都必须对其所有传播途径进行遏制，包括 USB 驱动器，网络通信以及被感染的项目文件。本文档重点阐述利用 Tofino 工业安全解决方案来防止 Stuxnet 的网络驱动这一传播途径，同时提供了针对其他传播途径的指导和建议。

## 防止 USB 驱动器被感染

Stuxnet 利用一种前所未闻的 Windows 快捷方式（如\*.lnk 文件）漏洞，通过 USB 驱动器（即使自动运行已经禁用）来感染计算机。大多数专家分析认为，这将是新型感染方式的起点，虽然其他的感染方式（比如被感染的计算机）仍然有很大的发生可能性。

有关控制 USB 感染途径的更多信息，请参阅文档 AN – 118 “Stuxnet Mitigation Matrix”。

## 防止网络驱动被感染

大多数专家对 Stuxnet 的看法都集中在从受到感染的控制系统里清除它是多么的棘手。一旦进入控制系统，Stuxnet 会迅速在局域网中蔓延，并感染其他计算机。

专家认为，遏制 Stuxnet 快速蔓延的最有效方法是采用 ANSI/ISA-99.02.01 和 IEC-63443 标准中的区级防护，即将网络划分为不同的安全区，在安全区之间按照一定规则（阻止 Stuxnet 用于感染和通信的协议）安装工业防火墙。这样，即使感染了 Stuxnet 病毒，也会被控制在单一安全区的少数设备之中。

## 将控制网络划分为安全区

预防 Stuxnet 的第一步是将控制系统划分为不同的安全区。A 区是一个简单的资产组合，有着基于控制功能，操作要求和危险性等因素的共同的安全要求。

最简单的方法是根据 ISA-95/Purdue 模型建立下列安全区：

- 安全集成系统（SIS）区域
- 基本控制/PLC 区域

更多技术了解访问 <http://www.mosesceo.com> OR <http://www.tofinosecurity.com>

- 管理/HMI 区域
- 过程信息/历史数据区域
- IT 网络区域

这些系统的每一个安全漏洞都会导致不同的后果，所以将它们单独处理十分必要。对于额外的安全性和可靠性要求，这些主要的安全区还可以根据操作功能进一步划分成子区。安全区数量的增加会逐步限制 Stuxnet 蔓延到更少的计算机。一旦发生感染，这样就能大大降低其风险和清除费用。

### 安装 Tofino 安全模块

划分好安全区后，Tofino 工业安全解决方案将用来限制安全区之间的网络通信，该限制仅对系统操作所需要的安全区进行（有关 Tofino 的概述，请参阅本文档的最后一页）。图 2 显示了 Tofino 安全模块（Tofino SAs）在一个石油精炼厂中的典型应用。

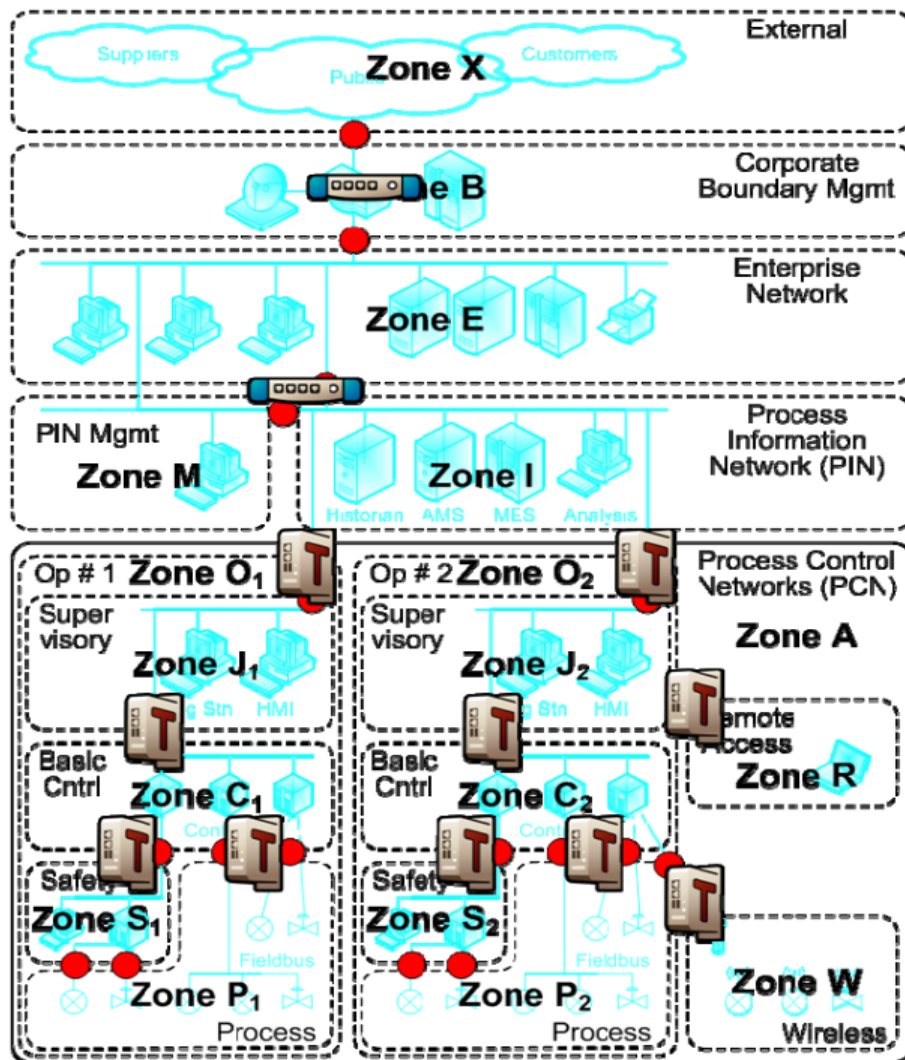


图 2:Tofino 安全模块在安全区间的典型应用

每一个 Tofino 安全模块都可以自定义装载软插件（即可装载安全软插件 LSM），再通过中央服务器（即中央管理平台 CMP）进行组态。遏止 Stuxnet 的蔓延，建议使用以下 LSM：

- Tofino Firewall（防火墙）LSM
- Tofino Secure Asset Management（安全资产管理）LSM
- Tofino OPC Enforcer（OPC 执行）LSM
- Tofino Event Logger（事件管理）LSM

### 对 Stuxnet 使用的通信协议进行阻止

装载 LSM 之后，需要对设备进行组态，来阻止 Stuxnet 在安全区之间通信所使用的协议。以下三种协议尤其需要管控：网页（HTTP）通信协议，远程过程调用（RPC）通信协议，以及西门子系统中的 MSSQL 通信协议。详情见下表。

协议名称	端口号	在 SCADA/ICS 中的基本应用	被 Stuxnet 利用的部分
<b>HTTP(Web)</b>	TCP 80	HMI web clients Historian, web clients	Connection to Internet Control
<b>RPC-DCOM</b>	TCP 135 Random TCP 端口 1024-65535	OPC Classic, Certificate Services, Group Policy	Worm P2P Upgrade System
<b>RPC-SMB</b>	TCP139 TCP445 UDP 139 UDP 445	File and Print Sharing, Event Log, Netlogon, WinCC Web Nav	Open Shares File Share Exploit Print Spooler Exploit
<b>MSSQL</b>	TCP1443	WinCC Client-Server Interaction	WinCC SQL Server Infections

表 1：部分由 Stuxnet 使用和 SCADA 应用服务受影响的协议的名单

### 阻止出站 HTTP 流量

最简单的流量处理即 HTTP 消息，Stuxnet 使用 HTTP 协议在因特网中连接回命令中心。Tofino 防火墙 LSM 默认阻止所有通信协议，因此，除非控制系统需要特定使用 HTTP 协议，否则 HTTP 通信将被阻止。

如果必须使用 HTTP 通信（例如，允许 IT 客户端访问历史数据），应当只限于这一个安全区及相关的 Web 服务器，并且只能进行入站访问。图 3 显示的是允许范围内的 IT 客户端使用 HTTP 访问历史数据的典型设置。注意，Direction（方向）选项设置为“**Incoming（输入）**”，因为 Web 客户端将启动与服务器的会话，且该服务器没有启动区域外会话的权限。

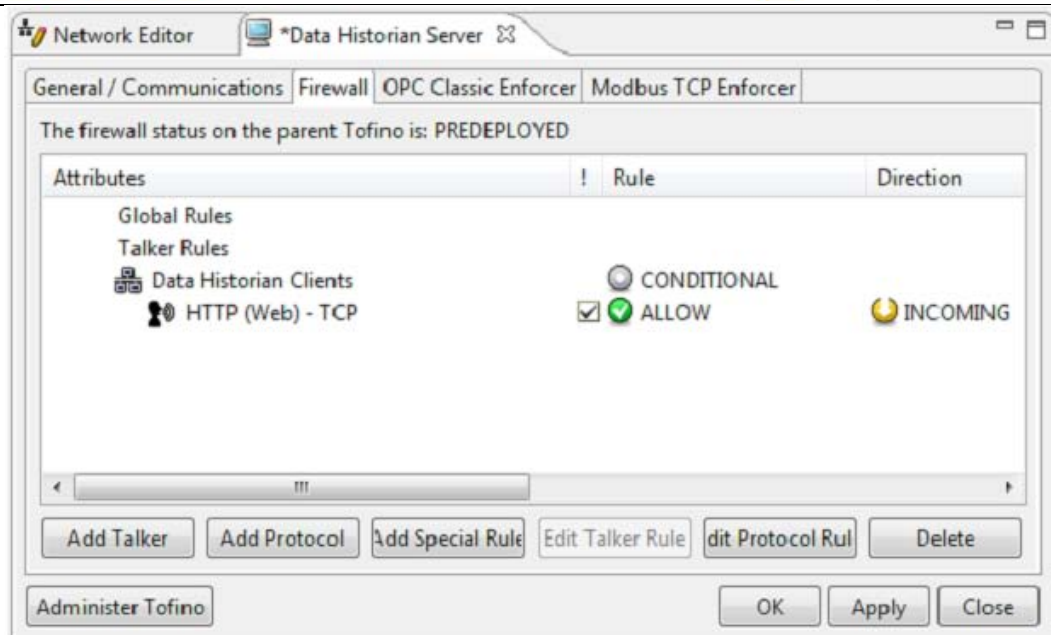


图 3:限制 Web 客户端和历史数据库间的 HTTP 通信

### 阻止 RPC 通信

Stuxnet 大量使用了 RPC 协议，因此必须对这一协议下的通信进行控制。如前所述，Tofino 防火墙 LSM 默认阻止所有通信协议，因此在 RPC 不是必需的情况下，Tofino 安全模块可以直接使用其默认设置来阻止 Stuxnet 在安全区之间的 RPC 通信。

不过，通常情况并没有这么简单。RPC 是 Windows 文件和打印机共享，Microsoft 事件记录，OPC Classic 以及其他大量服务的通用协议。因此阻止所有 RPC 通信可能会对工业流程带来负面影响。

为了最大程度降低对控制系统的影响，应该尽可能同时允许和阻止 RPC 端口。所有标准 RPC 协议的变化都包含在 Tofino 安全模块的协议包中，用户根据自己的需求，进行简单的拖拽操作即可。

要防止 Stuxnet 利用网络传播，首先应该将 NetBIOS 会话服务和服务器消息块协议(端口 139 和 445) 设置为完全封闭或只允许特定服务器。但这也将阻止安全区之间的文件和打印共享，因此这一设定应谨慎进行。

NetBIOS 会话服务和服务器消息块协议必须启用时，可以对特定的服务器进行通信限制。例如，事件日志服务需要对程序和 Windows 操作系统生成的消息进行管理。这些服务使用的协议与 Stuxnet 相同，所以不能完全阻止。具体解决方案是，仅对指定的事件日志服务器进行协议的限制，设置规则如图 4 所示。这种情况下，将由一个全局规则允许事件日志服务器使用 RPC，而其他所有的

RPC 消息被默认阻止。

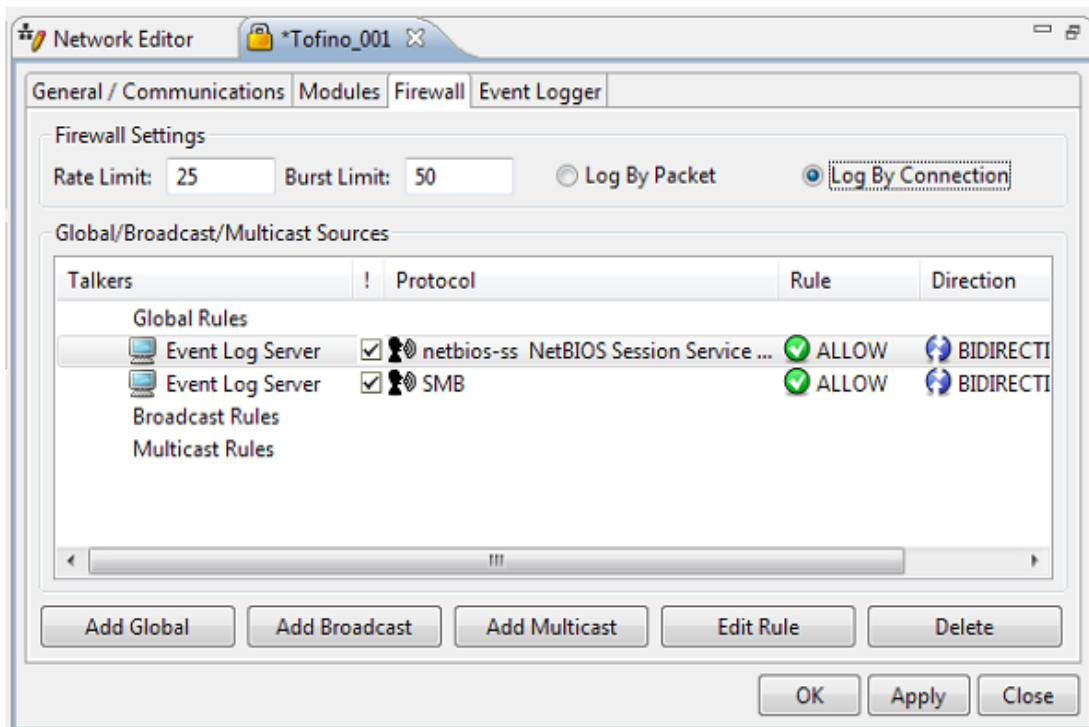


图 4: 限制事件日志服务器使用 SMB 和 NetBIOS Session Service Messages

打印和文件服务器同样需要类似的设置，但最好不要让安全区之间进行共享。最低目标是封锁不受控制的 RPC 流量，因此，在某些情况下，可以对特定服务器（经过仔细修补和感染监测）进行 RPC 限制。与 RPC 相关的协议——NetBIOS 名称服务（UDP 端口 137）和 NetBIOS 数据报服务（UDP 端口 138），在允许的情况下也可以保留，因为 Stuxnet 似乎并没有使用这些服务项。允许通过名称浏览计算机，但不允许文件共享。

如果存在 OPC Classic 通信协议，那么就需要使用 Tofino OPC Enforcer™ 模块来管控其通信。OPC Classic 的核心技术（即 RPC 和 DCOM）在设计之初尚未考虑到安全问题。因此，OPC Classic 采用了动态端口分配技术，使得传统 IT 类防火墙在 OPC 安全防护上毫无用武之地。。

与其它大多数的网络应用程序（如 Web 服务器或 Modbus TCP 的监听）不同，OPC 服务器将 TCP 端口号动态地分配给每个客户端的可执行过程服务对象，OPC 客户端连接到服务器，随之检测到与一个特定对象相关联的端口号，并询问它们应该使用哪个 TCP 端口。由于 OPC 服务器可以使用 1024~65535 间的任意端口，OPC 也就无法方便的使用防火墙——将防火墙设置开放如此庞大的端口数量，等于留下严重的安全漏洞，这种做法是普遍不被接受的。

Tofino OPC Enforcer™ 模块使用 Deep Packet Inspection（深度包检测）技

更多技术了解访问 <http://www.mosesceo.com> OR <http://www.tofinosecurity.com>

术自动跟踪和管理 OPC Classic 动态端口的使用情况，从而解决了这个问题。

使得 Tofino 能够被安装到运行有 OPC DA, HDA 或 A&E 通信的网络中，并且无需更改现有的 OPC 客户端和服务器的。

要配置 Tofino OPC Enforcer™模块来允许 OPC 服务器和客户端之间的通信，首先要打开相应 OPC 服务器的防火墙选项卡，然后将 OPC 客户端图标拖放到服务器的 Talkers 列表中，选择“OPC Classic”协议，将 Rule 选项从“Allow”更改为“Enforcer”，如图 5 所示。

更多内容请查阅文档 AN - 105 “Protecting OPC Systems Using the Tofino OPC Enforcer”。

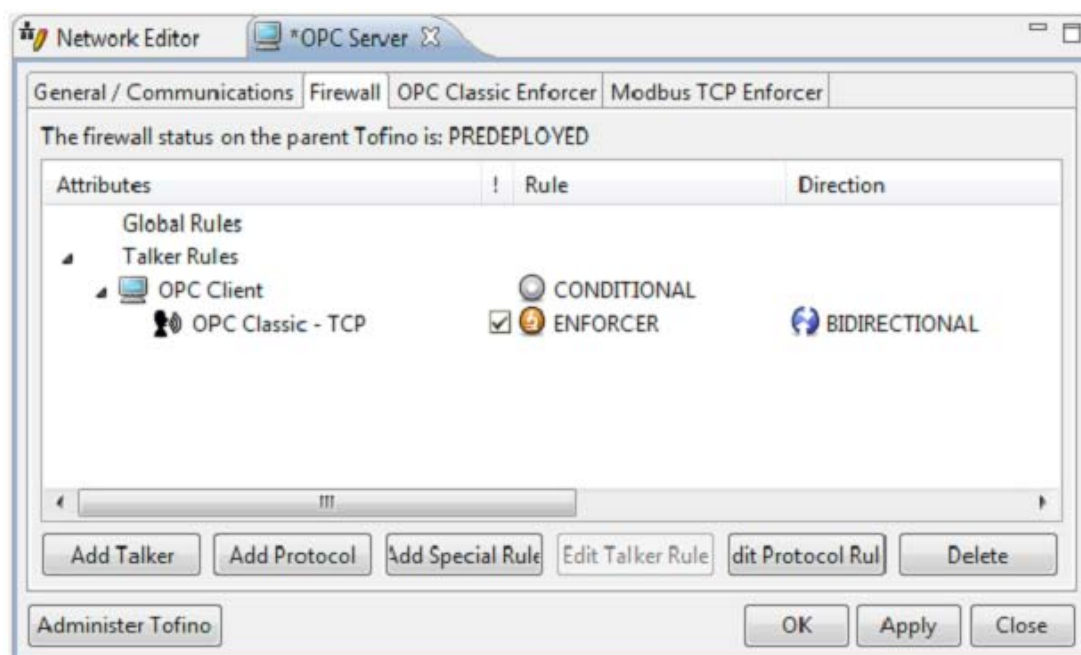


图 5: 使用 Tofino OPC Enforcer 管理 OPC 服务器与客户端之间的通信

### 阻止 MSSQL 通信

对于西门子 WINCC 产品的用户而言，Stuxnet 可以通过使用西门子“内部”系统密码登录 WinCC SQL 服务器来感染计算机，然后自我复制到该服务器并进行本地执行。

最为理想的办法是阻止网络上的所有 MSSQL 通信，不过我们并不建议采用该方法，因为这将阻止 WinCC 客户端接收过程信息。WinCC 的用户可从西门子网站中下载最新的 SIMATIC 安全更新来使用。

### 防火墙组态测试

由于 Stuxnet 使用了众多与控制系统所使用的相同的协议，因此必须确保防火墙规则设置不会影响工业过程。

更多技术了解访问 <http://www.mosesceo.com> OR <http://www.tofinosecurity.com>

Tofino 提供了一个名为 **Test mode** 的操作模式，该模式允许所有的网络流量通过，但会报告 **Operational mode** 下所有被防火墙阻止了的通信。这些报告会在 Tofino CMP 的事件视图中以防火墙异常报警形式显示出来，同时由 Tofino Event Logger LSM 记录（如果已安装）。

**Test mode** 可以用来确认防火墙规则是否无意中阻止了本应启用的通信协议，从而影响工厂运营。就这一功能而言，**Test mode** 绝对是用户的理想选择。我们建议 Tofino 工业安全解决方案的所有装置至在 **Test mode** 下运行至少 24 小时，然后再切换到 **Operational mode**。



**警告：**在对实时运行的控制系统进行配置之前，请务必与系统供应商沟通确认，并在非关键性的系统上做好测试。

## 侦测 Stuxnet 感染情况

Tofino 安全模块安装、组态和测试成功之后，就会提供良好的“Watch-Dogs（看门狗）”功能，一旦出现病毒感染就会立即发出报警信息。具体来说，Stuxnet 会产生大量的流量，Tofino CMP 或 Tofino Event Logger LSM 均可以捕捉这一情况。Stuxnet 企图联系外部 Web 服务器的行为更是极好的标签。

## 针对西门子 Wincc 和 PCS7 用户的其他建议

西门子 WinCC 和 PCS7 的产品在 WinCC 服务器和客户端的通信中大量使用了 RPC，因此阻止安全区之间所有的 RPC 通信可能导致视图丢失或系统失控。Tofino Test mode 可用于监测允许西门子 RPC 通信的规则。



**警告：**设置防火墙规则之前，西门子产品用户请首先联系您的西门子代表，或查阅西门子文档“**Security concept PCS 7 and WinCC**”。

西门子产品用户面对的是一种不面向其他系统用户的传播路径，即感染 STEP 7 程序文件。遗憾的是，这一漏洞并未得到有效的缓解。

## 更多信息

Windows 系统补丁的其他参考信息，USB 驱动器的管理及其他 Stuxnet 防护主题，敬请登录以下站点查询：

[tofinosecurity.com/stuxnet-central](http://tofinosecurity.com/stuxnet-central)

主要内容有：



- AN-118: Stuxnet Mitigation Matrix
- 白皮书：《控制系统专家分析西门子 WinCC/PCS7 Stuxnet 恶意攻击》
- 西门子恶意软件信息和软件更新链接
- 其他工业资料链接

## Stuxnet 概述

Stuxnet 是一个设计复杂，极具攻击性的计算机蠕虫病毒，可以感染任何控制系统中的计算机。尽管西门子产品用户避免 Stuxnet 感染的要求最为迫切，但同样不能忽略 Stuxnet 对其他产品和控制系统产生的负面影响。

遏止 Stuxnet 在控制网络蔓延的关键是维持工业系统安全、可靠和稳定。Tofino 工业安全解决方案可以降低 Stuxnet 病毒的诸多恶性影响，同时保护您的工业网络免受其他形式的意外或恶意攻击。

Tofino 工业网络安全解决方案包括以下组成部分：

<p><b>Tofino安全模块（TSA）</b></p> <p>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。</p> 	<p><b>可装载安全模块（LSM）</b></p> <p>为 TSA 专门定制的各种可装载安全模块：</p> <ul style="list-style-type: none"> <li>▪ <b>防火墙：</b> 指导并控制工业网络信息流通</li> <li>▪ <b>Modbus 与 OPC 应用：</b> 深层次的 Modbus 及 OPC 的通讯检测和连接管理</li> <li>▪ <b>安全资产管理：</b> 追踪并识别网络设备</li> <li>▪ <b>VPN：</b> 安全的虚拟网络远程通讯</li> <li>▪ <b>事件记录功能：</b> 可靠的安全事件和报警信息记录</li> </ul>	<p><b>Tofino中央管理平台CMP）</b></p> <p>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</p> 
--	---	--