TippingPoint
a division of 3Com

TippingPoint 5000E 入侵防御系统

数据表

L2 转发性能

- 5Gbps 攻击过滤
- 标准延迟<=1ms
- 并发会话 >=2000,000

(真实世界 TCP/UDP/IP 协议)

- 新建连接 >= 1,100,000/秒

客户端和服务器保护

- 针对操作系统和应用程序的异常行为的防护
- 多路检测手段
- 超越传统的点对点补丁方式

网络架构防御

- 保护 CISCO IOS 漏洞，Microsoft DNS 漏洞和其他操作系统平台
- 提前防御突发性的流量异常和 DOS/DDOS 攻击
- 采用访问控制列表

先进的 DDOS 防御加固

- 3,000,000+ pps SYN 容量
- SYN 高级代理功能(FPGA)
- SYN Flood 防御
- Connection Flood 防御

应用级性能保护

- 增加带宽和服务器的处理能力
- 基于 Rate-limit 的 QOS 流控
  - P2P/IM （MSN,QQ,BT）
  - 使非常规流量正常化

TippingPoint 入侵防御系统（IPS）提供世界上最强有力的网络保护 。TippingPoint IPS 是一种无缝地、透明地嵌入网络的嵌入式设备。当数据包通过 IPS 时，它们能被完全检测出来以判断它们是合法的还是恶意的。这种实时防护是最有效的防止有任何目的的攻击的方法。

TippingPoint 入侵防御系统通过对所有的数据包的检测，在千兆字节速度的水平提供应用防护、执行防护和底层架构防护。应用防护能力提供快速、准确、可靠的对于电脑与网络内部和外部的攻击。通过它的底层架构防护能力， TippingPoint IPS 提供视频组播、VoIP 网络电话底层架构、路由器、交换机、DNS 和其他重要的底层设备的防护，以防受到攻击和反常网络流量的影响。TippingPoint 执行防护能力是用户能够停止无任务的重要应用抢占宝贵的带宽和 IT 资源，因此能够协调网络资源和公司重要应用的执行。

这套系统是建立在 TippingPoint 的威胁抑制引擎(TSE) – 由最新的网络处理器技术和 TippingPoint 自己的一套自定义的专用集成电路所组成的基于硬件的高度专业化的入侵防护平台。以基于专用集成电路的 TippingPoint 威胁防护引擎是一种从网络防护改进而来的重要的技术。通过流水线和大量并行处理硬件的组合，TSE 有能力同时检测一个数据流数千遍。TSE 体系利用了自定义的专用集

400961-001 12/05

先进的威胁防御（灰件）

● VOIP	● 钓鱼
● OS 弱点	● Phishing
● 蠕虫	● 捕鲸
● 间谍软件	● DDOS
● 隔离功能	● P2P
● ZDI	● 病毒

数字疫苗 Digital Vaccine 实时接种

- 动态保护 Zero Day 攻击
- 动态保护 ZDI 漏洞列表
- 自动分发数字疫苗

硬件配置

- 8 * 10/100/1000M(SFP)接口
- 4 * Segment
- 2 * USB 接口
- 1 * Management 管理接口
- 1 * console 控制台端口
- LCD 液晶配置面板

尺寸

- 标准 19”机架结构
- 高度： 3.5 in (8.9cm) 2U
- 宽度： 17.25 in (43.8cm)
- 深度： 18.5 in (47cm)
- 重量： 28.5lbs (13kg)

成电路，一种具有千兆字节基架和和高性能的网络处理器，来执行整个从 2-7 层的数据流的检测。并行处理确保了不管处理多少数据流，数据流在经过 84 微秒后的停顿后通过 IPS 继续向前流动。

安全性和性能兼备的无与伦比的安全平台

TippingPoint 是业界领先的入侵防御系统(IPS)厂商，在安全性、性能、高可靠性以及易用程度上都堪称上乘。作为唯一荣获 NSS 金奖和第一个通过 ICSA 实验室认证的千兆级 IPS，加之其他众多奖项，TippingPoint 定义了基于网络的入侵防御的标准。

主动防御式网络安全

长久以来，网络使用者和管理员被这些麻烦所困扰：网络屡遭攻击后需要进行大量的清理工作但无法彻底清理干净而复发；需要在短时间内紧急为大量的服务器打补丁以避免危害面积扩大；泛滥的 P2P、IM 等“流氓”流量大量侵占了宝贵的带宽使得关键业务中断；DoS/DDoS 攻击致使 Internet 通路堵塞并且导致关键服务器宕机。

入侵检测系统（IDS，Intrusion Detection System）并不能真正解决这个难题，因为 IDS 只能够检测到攻击而不能采取任何主动的防御行为，只适合在某些主要需求为流量监控、分析与回放的情况下部署。

而 TippingPoint IPS 工作于“在线模式”（in-line），即透明地部署到网络当中，对所有流经的流量进行深度分析与检测，实时阻断攻击，同时对正常流量的通过不产生任何影响。

TippingPoint 通过持续地清除有害流量和保证关键应用的优先级实现了对应用系统性能的优化。其高性能和非凡的入侵防御精准度已经重新定义了网络安全，并且从根本上改变了人们保护其组织网络和系统的方式。