

技术白皮书

- 简介 2
 - 当前的安全威胁 2
 - 内部威胁防范解决方案 2
- 网络免疫能力解决方案：定义及其工作原理 2
 - 网络免疫能力解决方案的优势 3
 - 工作原理 4
 - 安全性管理 5
 - 报告 5
 - 灵活部署 6
 - 可扩展性 6
 - 第三方IDS/IPS/UTM设备支持 6
 - 业界领先的保修 6
- 竞争优势 6
- 总结 7

简介

当前的安全威胁

越来越多的网络正在经受着比以前更隐蔽、且不断更新的攻击和威胁，包括病毒、蠕虫、木马和内部破坏等。

《2006年CSI/FBI计算机犯罪与安全调查》显示，超过一半的被调查组织(包括美国企业、政府机构、金融机构、医疗机构和大学)去年都曾遭通过计算机安全事件。去年受到攻击的组织中有将近25%称遭到6次或更多次的攻击。

这些攻击造成了惊人的损失：313个被调查对象共损失了5200万美元，每个被调查对象平均损失167000美元。值得注意的是，只有一半的调查对象报告了遭受的实际损失——人们似乎更加担心对攻击和损失的公开报道，因此很难精确统计这些组织的实际损失。但有一件事是肯定的：网络攻击的范围之广超乎人们的想象。

过去十年中，许多IT管理人员普遍使用的网络安全策略是投资于外网，以防范外部威胁。他们认为所有威胁都来自于外部，外网保护森严的网络是最安全的网络。包过滤路由器、防火墙、应用代理和VPN都是当时采用的技术。

厂商和客户认为他们的网络设计是“外刚内柔”。也就是说，安全策略有意忽视了内部网络边缘安全，同时(由于某种原因)假设内部网络具有固有的高安全性。对于许多组织来说，这种假设与实际情况恰恰相反。

没有足够的内部威胁防护，网络极易受到病毒、蠕虫、用户破坏和其它攻击，从而造成重大的停机、收入损失、最终用户不满意以及IT管理带宽的增加。

内部威胁防范解决方案

客户当前可用的检测网络内部攻击的方法通常价格昂贵、性能有限或安全值较低。

如今，许多客户通过在网络周边设置防火墙、在客户端PC上安装防病毒软件保护网络。不幸的是，他们的网络仍然易于遭受更高级的安全威胁(例如病毒和蠕虫)，因为大部分防火墙不能深入检测病毒特征码，更无法通过网络行为异常检测(NBAD)寻找具有攻击性的网络行为。同样，PC防病毒软件不能做到防范时时的病毒攻击，更不用说有许多客户允许那些未更新防病毒文件的终端用户访问网络。

一些组织使用了昂贵的技术，例如在许多交换机上分别部署IPS(入侵防御系统)设备连接到上行链路上。与交换机网络基础设施架构相比，IPS的成本更高但性能更低，而客户需要通过更有效、更经济的解决方案来了解内部威胁的状态。

ProCurve Network Immunity Manager是一款经济高效的软件解决方案，可针对内部网络威胁进行管理。Network Immunity Manager通过内部攻击检测和外部网络及安全信息，将安全性和网络相融合，以便监测网络是否遭受内部威胁。此外，该软件还可以查明威胁源，并通过网络降低减少威胁。

网络免疫能力解决方案：定义及其工作原理

ProCurve Network Immunity Manager是ProCurve Manager Plus的一个插件模块，为管理内部网络威胁检测和响应提供了一套丰富的工具集。ProCurve Manager Plus和Network Immunity Manager插件构成了ProCurve网络免疫能力解决方案。

ProCurve Network Immunity Manager可以监测网络上的接入点和交换机端口，以便检测内部网络威胁，并允许管理人员设定检测和响应安全策略。

通过将安全流量监测技术(例如 sFlow 和病毒遏制)用于ProCurve交换机，ProCurve Network Immunity Manager可以执行NBAD（网络行为异常检测)检测，并对有线和无线网络中的内部威胁做出响应。另外，Network Immunity Manager还可以将流量远程映射到IDS/IPS/UTM设备，利用病毒特征码匹配方法进行高度可信的已知病毒检测。凭借Network Immunity Manager, IT管理人员可以更有效地防范内部攻击，并获得一套减缓攻击和跟踪攻击者的功能。

其易于使用的安全性管理工具将接入点和交换机端口变成安全传感器，提供了网络上的内部威胁活动的可视性，帮助管理人员大幅提高网络可用性。

网络免疫能力解决方案的优势

商业优势

企业需要尽可能保持网络可用性、符合标准要求、保护其在网络硬件和管理工具上的投资，并部署经济的有效解决方案。拥有ProCurve交换机的公司可以从Network Immunity Manager获得以下重要优势。

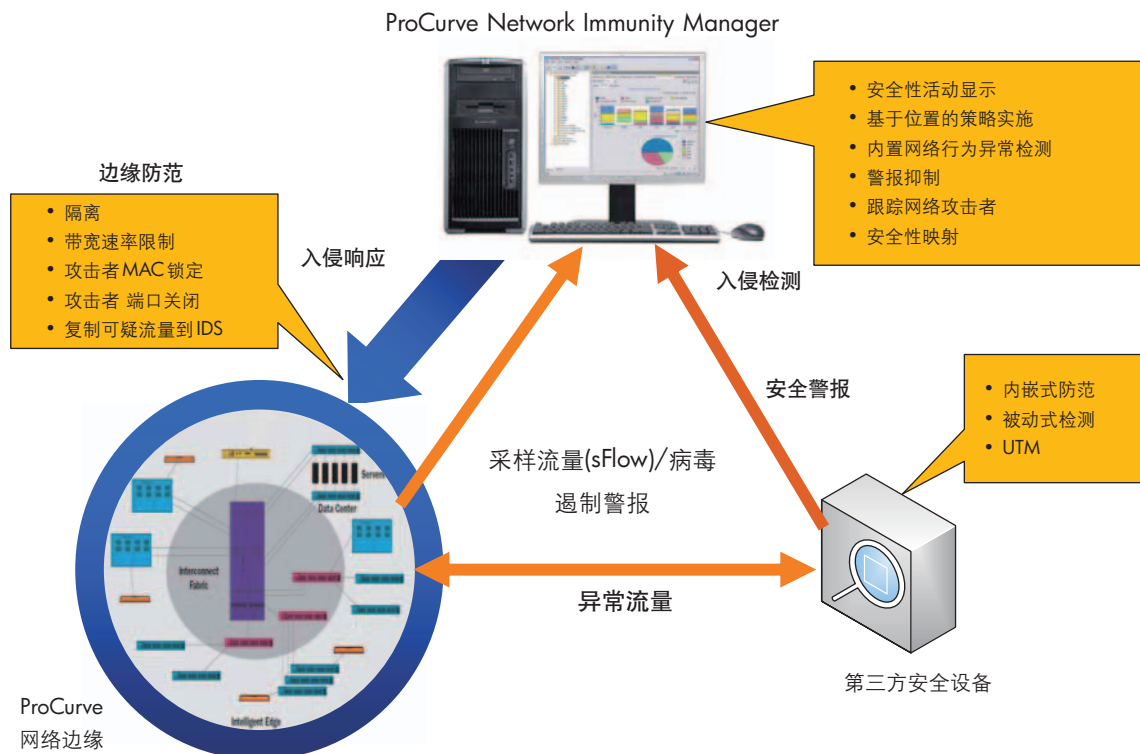
业务需求	ProCurve Network Immunity Manager
最大程度提供网络可用性	检测并自动响应内部网络攻击
可调整、灵活的方法	提供攻击防范策略和活动报告
投资保护	利用内置ProCurve交换机技术将每个端口都变为安全传感器
经济适用性和效率	只需极少的组件即可提供广泛的内部攻击防范功能

IT管理人员优势

IT需求	ProCurve Network Immunity Manager
内部威胁防范	检测网络内的已知和实时的攻击
自动威胁响应	提供一套应对攻击发起者的自动网络攻击减缓对策，包括： <ul style="list-style-type: none"> • VLAN 隔离 • MAC 封锁 • 端口关闭 • 端口带宽速率限制 • IT管理人员电子邮件通知
跟踪网络攻击者(取证)	显示攻击者的IP地址、MAC或DNS名称、攻击者网络访问详细信息(需要Identity Driven Manager)以及用户名(需要Identity Driven Manager)

工作原理

架构



ProCurve Network Immunity Manager是ProCurve Manager (PCM)管理套件的一个插件。Network Immunity Manager和PCM均以软件包形式提供。

攻击检测

以下是利用 Network Immunity Manager 部署攻击检测的两种方式：独立模式或与第三方安全设备联合。

Network Immunity Manager独立模式(NBAD检测)

- ProCurve 交换机通过 sFlow 技术发送采样流量到 Network Immunity Manager, 然后对数据进行 NBAD (网络行为异常检测)检测, 查看其是否遭受内部攻击
- Network Immunity Manager 可以接收 ProCurve 运行病毒遏制软件检测 IP Fan Out 病毒行为的病毒警报信息
- Network Immunity Manager 可以检测下列类型的内部威胁:
 - 实时和已知病毒或蠕虫, 类似: SQL Slammer、CodeRed、Sasser、MSBlaster 等
 - 协议异常, 类似: Land attack、UDP Flood、UDP Bomb 等
 - 搜索扫描, 类似: 端口扫描、fPing、superscan、nmap 等
 - 基于网络的攻击, 类似: DNS Tunneling、Smurf、IP spoofing 等
 - 异常数据包大小, 类似: 死亡之 Ping、Nmap、Netcat
- Network Immunity Manager 的 NBAD 功能并不依赖于那些采用匹配的特征码的防病毒或 IPS 的方式, 而是采用检测病毒、蠕虫或恶意用户的行为特征的方法

第三方安全设备方式

- ProCurve Network Immunity Manager 可接收已部署在战略性位置的部分第三方设备(例如IDS/IPS和UTM设备)的安全攻击警报, 只需发送安全警报到 Network Immunity Manager, 即可利用现有的安全基础设施架构达到操作目的
- Network Immunity Manager 可以利用基于 ProCurve ProVision 交换机的智能远程镜像特性, 将可疑流量发送到安全设备以便进行检查。这样在通知后便可在网络中的任何位置部署安全设备。然后, 安全设备可以检查流量并生成随后 Network Immunity Manager 用于相互关联、减少威胁和记录的警报

响应

- 当安全事件发生时, Network Immunity Manager 可以在多个响应级别进行配置, 对威胁采取从静态的记录事件到多种动态的缓解措施
- 可以配置 Network Immunity Manager, 使其在发生一个或多个异常流量事件时发送电子邮件
- Network Immunity Manager 可以根据 IT 管理人员设定的策略, 按接入点或端口对攻击做出响应。响应的范围包括:
 - 隔离 VLAN 上的攻击者
 - 对发起攻击的端口进行带宽速率限制
 - 封锁攻击者的 MAC 地址
 - 关闭攻击者的端口
 - 镜像异常流量到安全设备
 - 通过电子邮件警告 IT 管理人员发生攻击

安全性管理

ProCurve 网络免疫能力解决方案(ProCurve Manager plus 及 Network Immunity Manager)支持下列安全性管理特性:

- **策略管理** — 根据事件来源、位置、时间、行为和其它警报参数, 利用 PCM 自动管理器创建、管理策略
- **安全事件收集和抑制** — 从监测的异常流量收集安全警告信息, ProCurve 交换机和第三方安全设备通过管理工具产生的安全警报, 并抑制重复警报信息, 以便触发针对重复警报的单一策略
- **安全图示** — 能够以多种时间间隔实时查看网络上的安全活动并采取的相应措施、同时显示攻击者的详细信息
- **白名单(豁免列表)** — 您可以创建一组免除策略的 IP 地址、MAC 和 DNS 名称
- **配置清除** — 策略过期后自动从 ProCurve 交换机和无线接入点撤回响应配置
- **安全性审计** — 利用 PCM 审计日志记录策略配置和网络设备的任意更改
- **ProCurve Manager 集成** — 具有管理 ProCurve 交换机、路由器和无线接入点配置, 以及了解网络拓扑的内置功能

报告

ProCurve 网络免疫能力解决方案可以提供包括安全策略报告和攻击者跟踪的报告。网络免疫能力解决方案支持下列报告特性:

- **数据挖掘** — 生成以网络、攻击者和警报为基础的报告同时具有多种程度的颗粒度信息
- **定制报告** — 从 PCM 数据库模式生成报告, 帮助您符合标准要求。欲知标准符合报告的详情, 请参见 ProCurve 白皮书“持续的标准符合性” (www.procurve.com)

灵活部署

ProCurve Network Immunity Manager支持多种使用模式，使部署更加灵活：

- 网络行为异常检测和响应 — 利用Network Immunity Manager检测未知或零天攻击，并减缓ProCurve网络边缘的威胁
- 主动入侵防范和响应 — 利用嵌入式IPS/UTM设备防范攻击；利用Network Immunity Manager减缓ProCurve网络边缘的威胁
- 被动入侵检测和响应 — 利用嵌入式IDS/UTM设备检测攻击；利用Network Immunity Manager减缓ProCurve网络边缘的威胁

可扩展性

ProCurve网络免疫能力解决方案为小型或大型交换机和接入点范围提供更广泛的覆盖。

- 监测 — 监测有线和无线网络中高达10000个边缘节点

第三方IDS/IPS/UTM设备支持

Network Immunity Manager支持下列第三方IDS/IPS/UTM设备：

- Cisco IPS 4200系列传感器
- ISS Proventia G系列IPS设备(支持日期：2007年6月)
- Fortinet UTM设备(支持日期：2007年7月)

业界领先的保修

- 90天介质保修(软件)

竞争优势

ProCurve Network Immunity Manager拥有一个简单、高效且经济适用的架构，可以为有线和无线网络提供广泛的内部威胁防护，其多个组件采用了ProCurve交换机中的安全监测技术。

ProCurve Network Immunity Manager具有许多不同于竞争产品的独特优势：

- 提供有线和无线支持。其它解决方案只能在有线或无线环境下发挥作用，但不能在全部两种环境下实施
- 充分利用交换机和接入点基础设施架构的安全功能。许多ProCurve基础设施架构设备都附带内置sFlow取样技术和/或病毒遏制功能
- 可提供一套丰富的响应选项，而大部分竞争对手的响应对策非常有限
- 具有更低复杂性和更高安全性。ProCurve的技术更直观、更易于使用

总结

ProCurve Network Immunity Manager是ProCurve主动防御安全策略中的防御部分，可建立可信赖的网络基础设施架构。ProCurve Network Immunity Manager与ProCurve访问控制解决方案(例如Identity Driven Manager)一起为连接用户的网络边缘提供安全性。ProCurve Network Immunity Manager通过检测和响应网络内部威胁避免网络受到内部威胁。

超值的**ProCurve**网络免疫能力解决方案可为您提供以下特性：

- 大幅提高网络可用性
- 利用很少的组件即可提供经济适用的高效可扩展解决方案
- 提供内部威胁管理
- 提供全天攻击保护
- 充分利用ProCurve交换机的当前投资
- 提供跟踪攻击者功能
- 为有线和无线网络提供更广泛的内部威胁防范

ProCurve Network Immunity Manager可以根据客户的个人需求部署适用的安全解决方案。

欲了解有关ProCurve

Networking产品和解决方案的
更多信息，请访问我们的网站：

www.hp.com.cn/network

欲了解更多信息，请电话垂询当地惠普销售办事处或离您最近的惠普授权经销商。

惠普售前支持热线： 800-820-2255
惠普售后支持热线： 800-810-3888
惠普客户反馈/投诉热线： 800-810-0039

或请访问：www.hp.com.cn
www.hp.com.cn/network

© 2007 Hewlett-Packard Development Company, L.P. 本文所含信息如有更改，恕不另行通知。
惠普产品与服务的全部保修条款在此类产品和服务附带的保修声明中均已列明，本文中的任何
信息均不构成额外的保修条款。惠普对于本文中所包含的技术或编辑错误、遗漏概不负责。

P/N: 4AA1-0788CHP, 2007年9月中国印刷

