木桶原理最适合来描述网络安全问题，如果仅以简单的依靠修修补补提高安全性很难，该提速的时候刻不容缓。

利用 Cisco IDS 4250 传感器改善 Cisco IT IDS 的性能

思科信息安全部门于 2001 年部署了 Cisco IDS 4230 传感器。此次部署不但证实了这种部署方案对思科的价值，还增进了思科对入侵检测的了解。但是，IDS 4230 传感器的性能和管理还有一些局限，为突破这些局限，思科移植到了 Cisco IDS 4250 和 IDS 4250-XL 传感器。

背景

在网络安全领域中，防火墙就好像是坚固的门锁和窗闩一样，能够阻挡他人的非法入侵。事实上，好的安全战略也应该使用入侵检测。与安全大厦内的警报器和摄像机相似，IDS 警报不但能为警卫提供很多详细信息，包括入侵者进入大厦的方法和目前所在的位置等，还能提供必要的数据，帮助警卫确定快速缉拿入侵者的最佳方式，以及将来怎样预防类似入侵的发生。思科内部信息安全（Infosec）部门在思科内部部署了防火墙和 IDS。这些安全设备证明是有效的，例如，2001 年（思科部署入侵检测传感器的当年），全球服务器共遭受了两次灾难性攻击：Code Red 1 和 2（2001 年 7 月）和 NMDA（2001 年 9 月）。在这两次攻击过程中，Cisco IDS 4230 传感器都在几分钟之内就注意到了可疑流量的迅速增加，在一小时之内，Infosec 和 IT 工程师立即采取了相应的措施。

挑战

思科网络和数据中心骨干网由超高速连接组成，多数为千兆位以太网。互联网接入的速度也很高。但是思科原先采用的 Cisco IDS 4230 传感器性能是一个瓶颈。另一个问题是，IDS 4230 提供了很少的管理工具。为自动执行所需的许多管理功能，Infosec 花费了几个月来开发工具，包括更新配置和签名文件、重新启动传感器等（参见附录 1：吸取的教训）。

解决方案和成效

思科 Infosec 已经开始用 IDS 4250 取代 IDS 4230，以便在更大的互联网 DMZ 内支持 500Mbps 的流量。此项工作从圣何塞开始。第一个 IDS 4250 传感器（那时正处于 β 测试阶段）于 2002 年 11 月安装在圣何塞的 DMZ，替换了两个 IDS 4230。替换之后，Infosec 取消了小型 IRSD 传感器不得不实行的流量分割和交换机跨区，简化了体系结构，使 IDS 传感器能够首次“读”所有的网络流量，从而能够更加全面地抵御各种威胁。我们不但能为 IDS 添加双工警报签名，还能为 IDS 4250 传感器部署 Cisco IDS Sensor Software 4.1，这样，思科 IT 不但能享受到这些好处，还能将一台设备配置为多个“虚拟传感器”，更换掉数据中心里的大量 IDS 4230 传感器。这种方法不仅释放了数据中心的空间，还降低了管理成本。

下一步计划

思科 Infosec 计划通过三个步骤升级到最新的 IDS。第一步是将互联网接入点中的 35 个 Cisco IDS 4230 传感器升级为 IDS 4250 传感器，此项工作在圣何塞升级成功之后进行。第二步是将数据中心里的 IDS 4230 升级到 IDS 4250-XL，以便利用其千兆位性能处理通往数据中心的千兆位以太网网关接口。当这些升级都完成时，Infosec 将能够完全取消 IDS 内的流量分割和交换机跨区。第三步是将这些 IDS 4250 传感器移植到最新的 IDS Sensor Software 4.1，以便改善管理，降低虚警率，这些因素是 Infosec 当前 IDS 部署的最大问题（参见附录 1：吸取教训）。目前，Infosec 正在为计划的内升级进行评估 IDS Sensor Software 4.1，具体时间表将由人力资源部和预算审核部确定。

阅读更多详情，请下载PDF文件。