好的中医，仅仅靠望闻问切就可以诊断疑难杂症。那依靠的是以往对病例的积累、细心的观察理性的分析。对于网络其实也一样，长期的分析、观察积累，即使没有专门的反病毒、防攻击设备，大多数的隐患也能查出来。

NetFlow 为思科内网把脉

思科交换机和路由器所支持的 NetFlow 功能，在竞争激烈的网络市场独树一帜。这一网络监控技术对思科的 IT 部门贡献很大，不仅仅帮助他们管理、优化网络，且在蠕虫病毒爆发时给予他们有力的支持。

挑战

对思科而言，网络的可用性、服务质量至关重要，IT 部门需要有办法 IP 流量的特征，说明流量的流动方式和地点，并进行分析确定网络中存在的服务质量、乃至安全问题。而以往采用 SNMP 监控互联网带宽，无法提取流量特征，无法满足 IT 部门的需求。

解决方案

思科在自己的路由器和交换机上支持 NetFlow 功能，可以实现上述目标。NetFlow 可以统计记录网络中数据包的源目的地址、端口号等信息，将这些信息收集整理分析后，就可以发现网络通信的规律。在思科多数的路由交换设备中，有专门的硬件芯片和软件特性实现 NetFlow。而最新的 NetFlow 9 已被选中参与 IETF 标准，在成为标准前，这一技术已经得到了业界广泛的支持，用户可以找到很多家厂家所提供的收集交换机路由器 NetFlow 信息、汇总分析得软件，用户甚至可以找到开放源代码或者免费的软件来收集分析 NetFlow 的信息。

借助 NetFlow，用户不仅可以发现网络通信的规律，分析这些数据还可以达到入侵检测系统（IDS）的部分能力，实际上由于 NetFlow 在很多 Cisco 设备上采用硬件实现，性能要优于 IDS，结合 NetFlow 和 IDS，可以构成更好的安全监控方案。

多次获益

思科 IT 部门自从在公司内部网络中使用 NetFlow 之后，已经多次获益。

彻底避免 SQL Slammer 蠕虫

2003 年 1 月 24 日，SQL Slammer 蠕虫，也称为 Sapphire，在三分钟之内就传遍了全球，几乎使全世界的网络都出现了故障。思科业务的连续性却没有因 SQL Slammer 而受到损失，IT 部门将成功归功于团队合作、健全的通信计划、强大的网络体系结构以及 Cisco NetFlow 技术的有效使用。NetFlow 配合合作伙伴 Arbor 公司提供的分析管理工具，思科 IT 人员迅速发现了 UDP 端口 1434 出现的大量异常流量。发现潜在问题后，思科进行分析后在所有互联网供应点放置了向内和向外的访问控制列表（ACL），以阻挡这些流量对网络的访问。事故之后的两周内，思科 IT 每天对网络密切监视，确保威胁已被彻底根除。

发现和预防 DoS 袭击及其它意外流量

思科也时常会接收到试图发动 DoS 袭击的流量。利用 Cisco NetFlow 收集分组的源地址、目标地址、协议号、端口号和分组大小，然后将信息发送到 Arbor Peakflow DoS 执行异常检测。Cisco NetFlow 将指导网络设备进行处理。

审计 NAT 化流量

NAT 的内在限制是非互联网路由地址（例如移动员工采用的地址）与公共路由互联网地址之间的多对一关系。Cisco NetFlow 使思科能够审计 NAT 流量，以便排除网络故障，解决方案问题，并执行定期检查，看移动员工是否能够遵守公司制订的网络接入策略。

通过容量规划从托管式 DSL 服务移植到互联网 VPN

2001 年，由于直接 DSL 与 ISDN 接入的成本迅速提高，思科将全球范围内的数千完名远程员工和远程办公室员工转向了远程接入 VPN。为确定是否需要增加容量，思科使用 Cisco NetFlow 与各种开放源代码工具提取现有流量的特征，然后推断未来流量。利用这种业务智能，思科只用了三个月就成功地将 22,000 名用户移植到了 VPN。

检测非授权 WAN 流量

通常情况下，当 WAN 链路上的流量增多时，公司就会投资，执行链路升级。但很多次，思科都避免了昂贵的链路升级。思科的作法是：寻找造成拥塞的应用，如果需要，修改使用策略。

降低高峰期 WAN 流量

当某几条链路上的 WAN 流量迅速增加时，Cisco NetFlow 和 NetQoS ReporterAnalyzer 能够快速找到原因，思科的 IT 人员会发现不好的应用对带宽的消耗。

QoS 指标核实

思科 IT 为数据、话音和视频分配了一定比例的 WAN 容量。分配的依据是每个站点产生流量的理论模型，以及目标 QoS 水平。过去，思科无法核实 QoS 目标是否实现。借助 Cisco NetFlow 就可以得到所有的信息。

分析 VPN 流量和远程员工的行为

利用 Cisco NetFlow，思科 IT 可以方便地发现远程员工的流量，因为这些流量将穿越通用路由封装通道。这种流量分析有助于执行互联网接入容量规划。

核实电信商的服务等级

思科正在运用 NetFlow 功能来测量运营商提供的服务的 SLA。”

计算应用的总拥有成本

在思科内部向大量用户发行新应用之前，思科系统公司都要计算总体拥有成本（TCO）。影响TCO的最大因素之一是WAN。为尽可能准确地估计WAN成本，思科应用开发部率先在测试环境中部署了一个新应用，利用Cisco NetFlow测量向大量用户发行应用时产生的WAN流量有多大，从而更准确地计算TCO。思科IT部门使用NetFlow计算应用TCO的还有当计划将监控系统迁移到IP网络中时、部署Cisco Unity™语音留言系统时、计算来自全球 50,000 部思科IP电话的成本节约、计算思科应用和内容网络系统（ACNS）软件实现的成本节约、制订未来服务计划。

成效

对于思科，Cisco NetFlow 的优点是，不但能保证经济有效地部署应用，还能确保全球的所有员工、客户和合作伙伴随时都可以使用相应的服务。利用 NetFlow 数据，思科 IT 部门不但能防止网络受到病毒侵害或遭到袭击，还能了解当前及未来应用对网络的影响。

未来思科 IT 部门打算进一步提高收集网络数据的价值，并将 NetFlow 的使用扩展到网络的其它部分。

阅读更多详情，请下载PDF文件。