NetFlow 能够为网络工程师、容量规划人员和安全部门提供详细的网络利用视图

思科®IT 案例分析/思科网络管理/NetFlow：该案例分析介绍了思科 IT 部门在世界上最大、最复杂的领先企业环境之一——思科全球网中使用 Cisco IOS® NetFlow 技术的情况。思科客户可以借鉴思科 IT 部门在实践中积累的经验，更好地满足类似的企业需求。

“随着融合网络和 IP 技术的普及，提取网络流量特征，以便执行容量规划和异常检测的能力将变得越来越重要。”——思科 IT 网络工程师 Roland Dobbins

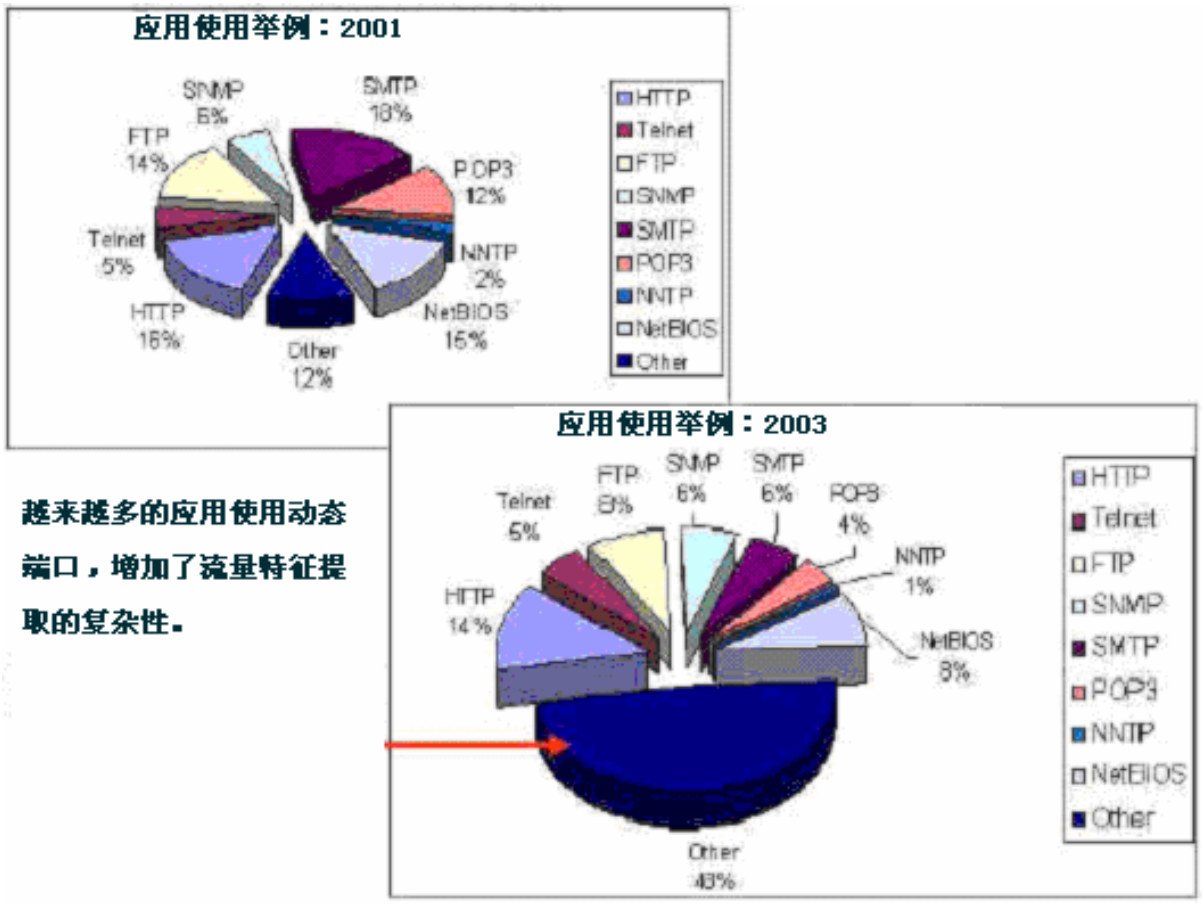
挑战

在思科系统®公司，必须提取 IP 流量的特征，说明流量的流动方式和地点，对提高网络可用性和性能是极为重要的。对 IP 流量的监控有助于执行更加准确的流量规划。它支持资源调整，即适当利用资源，促进企业目标的实现。另外，它不但能帮助 IT 部门确定在哪里应用服务质量（QoS），以便优先处理重要流量，还能在网络安全方面发挥重要作用，使思科能够通过持续流量监控发现拒绝服务（DoS）袭击、网络传播蠕虫及其它意外网络事件。

对思科而言，保持高网络可用性和性能是非常重要。例如，在思科的总收入中，93%即每分钟 33,000 美元的销售收入都是利用思科互联网连接和内部网实现的。在所有思科产品中，超过 80%的产品生产是由通过思科外部网连接到思科数据中心的合作伙伴完成的。提供支持服务时，大约 80%的服务请求都是由思科客户通过思科技术支持中心（TAC）在线提出的。解决问题时，TAC 工程师一般都通过网络执行远程排障。全球的 55,000 多名员工和合作伙伴依赖全球 WAN 与世界各地的 250 多个站点和远程接入 VPN 相连。重要的思科话音流量、企业视频会议流量和安全摄像机录制的闭路 IP 视频流量通过思科 AVVID（集成式话音、视频和数据体系结构）传输。思科客户希望网络 24 小时可用，因为他们不但要下载 Cisco IOS® 软件和 Cisco® Catalyst® 操作系统（CatOS），还要访问相应的文档。

2000 年，思科几乎只依赖简单网络管理协议（SNMP）监控互联网带宽。虽然 SNMP 有助于容量规划，但无法提取流量特征，而只有了解了特征，才能保证业务连续性，确定是否以增加容量来提高利用率授权，以及评估 QoS 参数是否符合目标服务水平要求等。思科 IT 互联网服务部网络工程师 Roland Dobbins 说：“我们需要更加细致地了解思科带宽的利用方式。”流量特征提取遇到的另一个困难是，许多新应用每次使用的端口都不相同，它们每次都动态选择新端口使用（见图 1）。

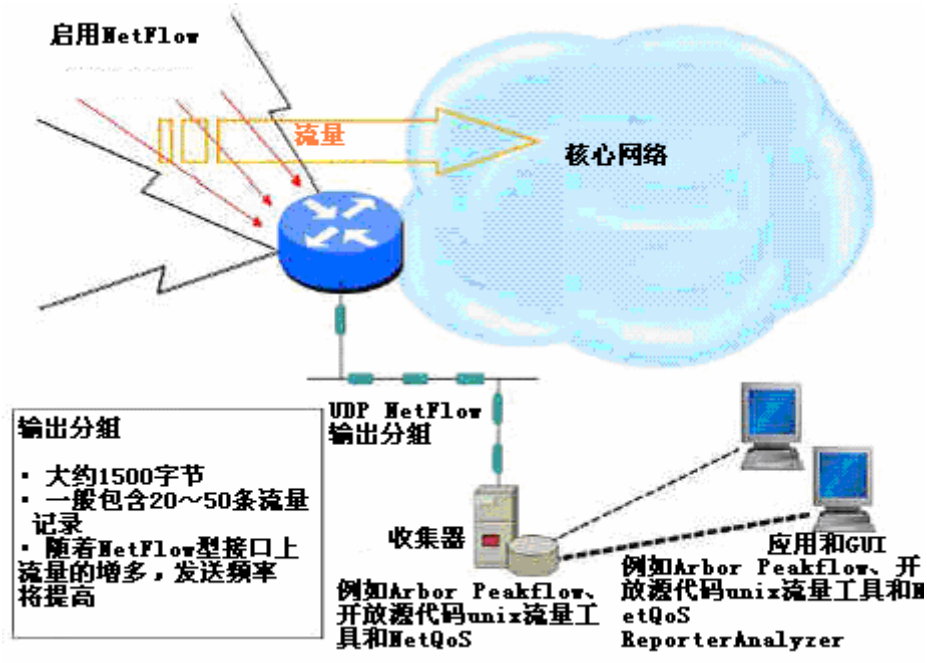
图 1 思科系统公司使用的应用类型的变化



解决方案

思科能够利用 Cisco NetFlow 技术分析和提取网络流量的特征。利用专门开发的应用专用集成电路（ASIC）以及 Cisco IOS 软件和 Cisco Catalyst 操作系统软件的某些专用特性，Cisco NetFlow 已集成到多数思科交换机和路由器中。NetFlow 于 1996 年由思科开发，能够回答网络流量的“对象、内容、何时、何地和何种方式”问题，现在已经成为业界的主要网络计费技术和异常检测技术。2003 年，Cisco NetFlow 9 被选中参与 IETF 标准（称为 IP 流量信息输出（IPFIX）的开发。利用 IPFIX 定义的格式，IP 流量信息可以从输出设备，例如思科路由器，传输到分析数据的收集器应用（见图 2）。为输出数据，路由器将根据源 IP 地址和目标 IP 地址、源端口和目标端口、第三层协议类型、服务类型和输入逻辑接口表示每种网络流量。思科 IT 技术部成员 John Cornell 说：“我们可以将 NetFlow 看成是路由器和第三层交换机控制的遥感设备，它起的是传感器的作用。”

图 2 生成输出分组



入侵检测系统（IDS）和分组窥探软件是用于检查分组内容的微观分析工具，Cisco NetFlow 则是能够实时提取大量流量的特征的宏观分析工具。事实上，思科使用 NetFlow 的一种方式是寻找相应的实例，使 IDS 和分组捕获程序能够在其中提供有用的信息。为说明 Cisco NetFlow 和分组捕获程序之间的区别，Dobbins 用电话帐单做了一个比喻。他说：“NetFlow 用于说明谁与谁通的话、在何时通的话、通话时间有多长、使用的是哪些协议和端口以及总共交换了多少数据量。由于 NetFlow 在说明谈话时并不实际收听对话的内容，因而可以扩展到超大网络。与之相反，分组捕获程序则有点像窃听器，能用于揭示具体谈话的细节。”

解决方案组件

从 Cisco 3700 系列多服务接入路由器到 Cisco 6000 系列 IP DSL 交换机和 Cisco 12000 系列路由器，思科 IT 部门已经在数百台网络路由器、交换机和监控器上安装了 Cisco NetFlow 5。NetFlow 能够提供流经交换机或路由器的每股 IP 流量的信息（见图 3）。当路由器或第三层交换机接收到一股 IP 流量时，NetFlow 将以 NetFlow 数据输出格式输出流，并将其发送到运行分析软件的服务器，例如 Arbor Networks 开发的 Peakflow 软件、NetQoS Reporter Analyzer 或开放源代码工具，例如 splintered.net 开发的 OSU 流量工具。思科 NetFlow 数据报告样例如图 4 所示。

图 3 NetFlow 第 5 版本流量信息

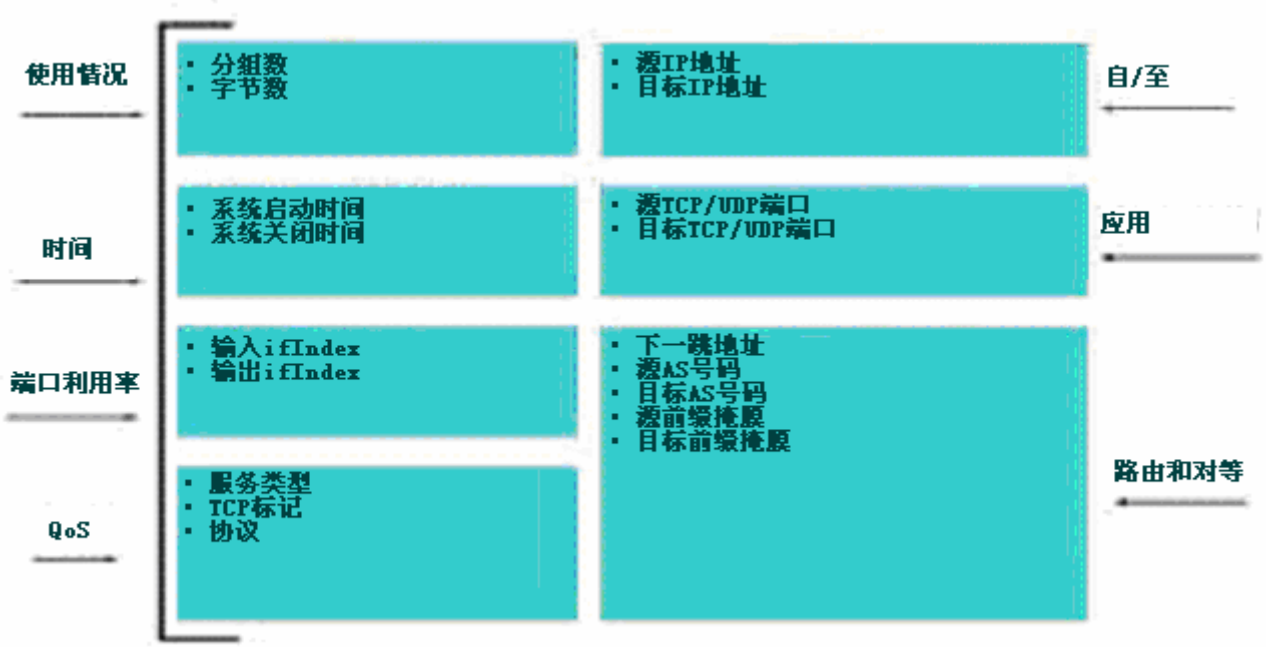
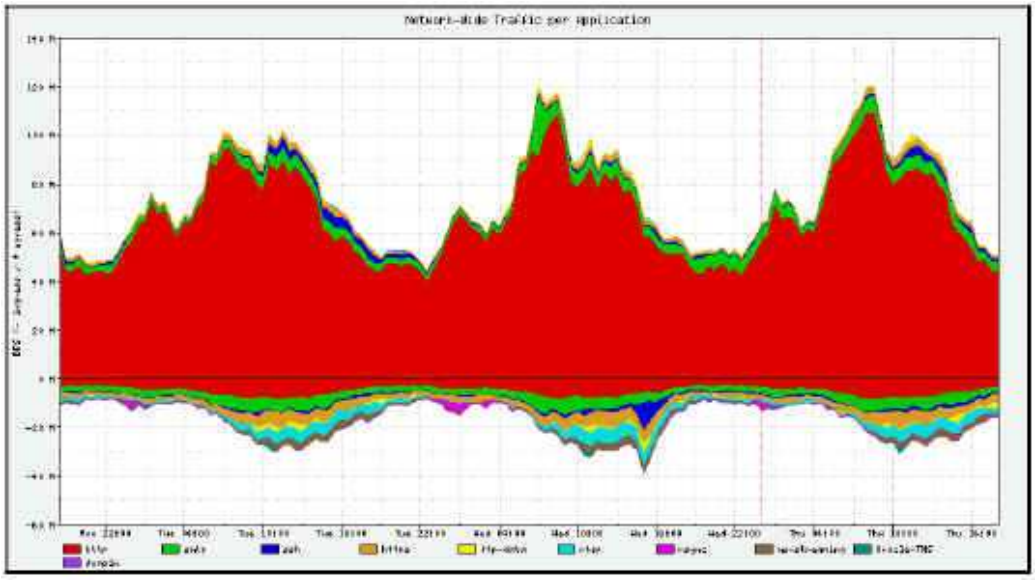


图 4 由 Arbor Networks Peakflow Traffic 绘制的 Cisco NetFlow 数据图，按应用提取的流量特征。



与远程监控（RMON）探针相比，Cisco NetFlow 更适合手机网络流量信息。虽然 RMON 探针也能收集到同样的信息，但必须在需要调查的每个站点和每条链路上都安装独立硬件才行。这是一个缺陷，因为许多站点都难以到达。不仅如此，如果需要调查某路由器上的多条链路，则每条链路上都需要一个探针。由于 NetFlow 属于 Cisco IOS 的

特性，而 Cisco IOS 已经运行在每台服务器上，因此，不但易于安装，还能降低硬件成本。（注：对于思科网络接入模块（NAM），这种说法只有部分正确——NAM 刀片可以安装在 Cisco Catalyst 6500 和 Cisco 7600 系列路由器上，使工程师能够从一个刀片查看机器上的所有端口——但需要添加硬件和安装。不仅如此，Cisco 7200、7500 和 7600 路由器还需要 NetFlow 软件许可证费。）

部署说明

为处理来往流量，思科在思科网络中很多位置都部署了 Cisco IOS 的 NetFlow 特性，其服务的 WAN 接口总数超过 1900 个。思科 IT 项目经理 Michael Chang 提到："如果利用 RMON 探针监控这么多接口，成本上肯定不允许，因为每条链路都需要安装一个探针。"每个位置的信息可以独立使用，也可以与其它网络业务智能结合使用。例如，如果结合使用 Cisco NetFlow 与边缘网关协议（BGP）路由信息，将能够了解思科网络流量的源地址和目标地址，实现与互联网服务供应商（ISP）的最佳对等。我们将在"成效"章节中列举更多的案例。

收集 Cisco NetFlow 流量的地点以及其使用的分析类型如表 1 所示。

表 1 思科 IT 部门使用的分析软件：数据收集的网络位置和目的

网络位置	分析软件	目的
与 ISP 链路连接的互联网网关路由器	Arbor Networks Peakflow Traffic Arbor Networks Peakflow Dos	按应用执行网络流量分析 建立网络流量与 BGP 路由信息之间的关联 异常检测
面向公众的网络的内边缘的路由器	Arbor Networks Peakflow DoS	异常检测
WAN 核心（汇聚层）	NetQoS ReporterAnalyzer	按应用执行网络流量分析，用于容量规划
WAN 边缘	NetQoS ReporterAnalyzer	按应用执行网络流量分析，用于容量规划
面向公众的网络的核心路由器	splintered.net 开发的 OSU 流量工具	收集历史数据，用于预测和诊断
网络地址转换（NAT）网关	splintered.net 开发的 OSU 流量工具	收集历史数据，用于预测和诊断 审计已执行过 NAT 的地址（"NAT 化"地址）

互联网和安全应用实例

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，包括全部自动柜员机网络和大企业网络。Dobbins 说：“许多机构都认为，他们已经在星期五晚上将 Slammer 阻挡在了互联网边缘之外，但星期一刚上班，却发现网络又遭到了笔记本、VPN 连接及其它直连设备的破坏。”

但是，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。Dobbins 表示：“利用 NetFlow，我们能够深刻了解各种事件及其严重性，因而能及时采取相应的措施。”在思科从 ISP 领域借鉴来的六步方法中，NetFlow 发挥了重要的作用。Dobbins 还说：“它们在内部或通过互联网连接提供内容和服务，因此，为服务供应商开发的许多概念都适用于企业。”Cisco NetFlow 是思科六步安全方法的关键部分，为对付 SQL Slammer，现将这个方法介绍如下：

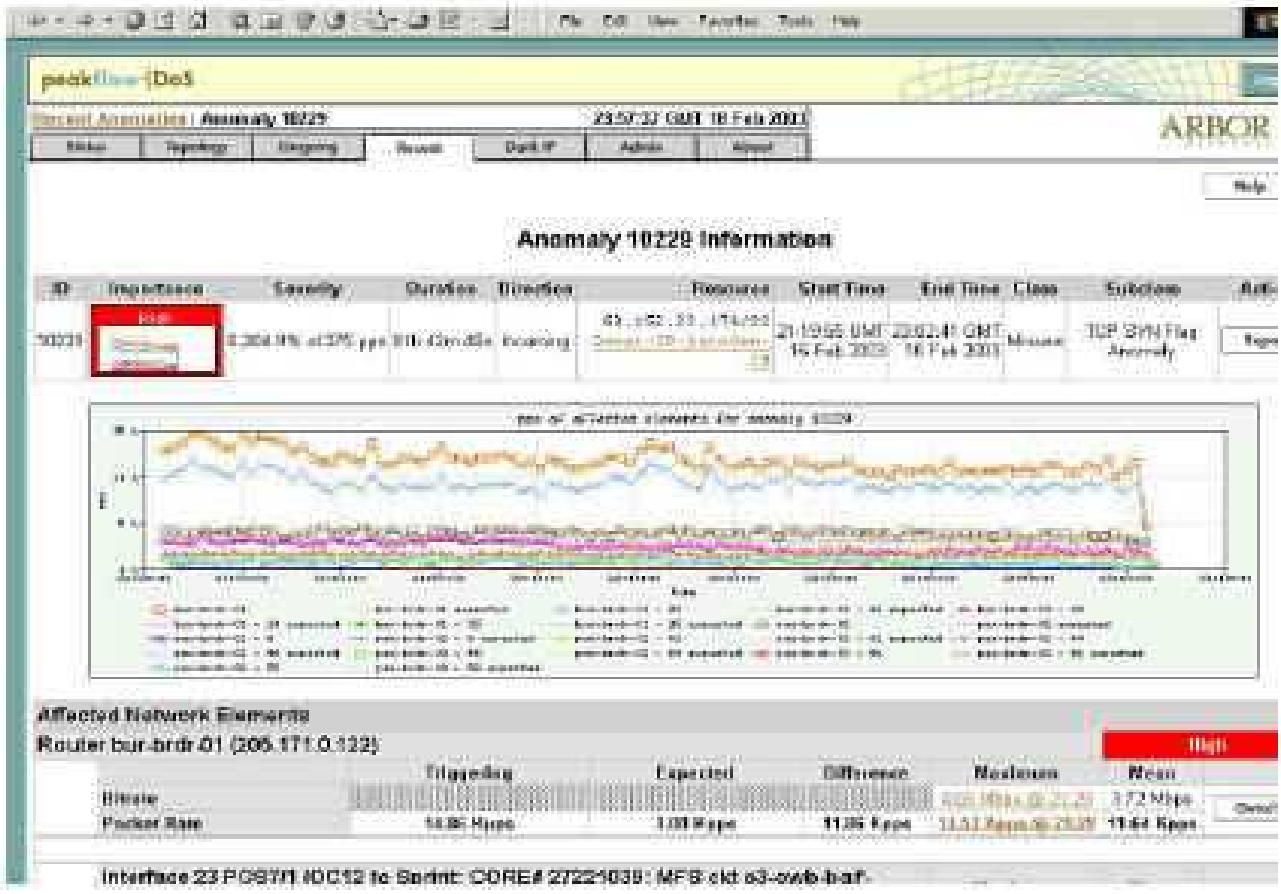
- 第 1 步：准备——发现 Slammer 并采取相应措施的重要一步是在问题发生之前就实施 Cisco NetFlow 和分析软件。由于思科制订了常规网络流量判断计划，因而能够通过流量模式发现恶意袭击。
- 第 2 步：识别——Arbor Peakflow DoS 向思科 IT 部门发出警报，说明 UDP 端口 1434 上出现了大量异常流量。利用 Arbor Peakflow Traffic 查看 Cisco NetFlow 数据，包括历史数据、每秒位率、源地址和目标地址之后，思科立即发现存在意外可疑流量。
- 第 3 步：分类——思科利用 Cisco NetFlow 和 Arbor Peakflow 的输入对各种威胁进行分类。各种异常流量对可用性的威胁各不相同。利用 Arbor Peakflow 解决方案，思科 IT 部门很快就将 Slammer 定为严重威胁。
- 第 4 步：追溯——思科找到了所有潜在的 Slammer 源或矢量。Dobbins 说：“只有通过追溯才能避免受到 Slammer 的伤害。许多其它机构都无法判别间接矢量，例如 VPN 和笔记本电脑，于是在星期一付出了惨重的代价。”
- 第 5 步：反应——发现潜在矢量之后，思科在世界各地的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。Dobbins 说：“为抵御安全威胁，我们不但将 ACL 推广到了世界各地每家思科公司的桌面分布层，还出于战略考虑，在 WAN 骨干网上使用了 ACL。网络专家可能认为这种举措有点过于谨慎，但通过 Cisco NetFlow 和 Arbor Peakflow 发来的信息，我们知道，只有这样才能保证网络安全。”
- 第 6 步：善后——在事故之后的两周内，思科 IT 每天对网络密切监视，确保威胁已被彻底根除。

对 Slammer 的战斗取得了很大的成功。Cornell 表示：“在袭击之后的那个星期一，思科客户就能够全面利用所需的思科资源收拾 SQL Slammer 袭击之后的残局。”

发现和预防 DoS 袭击及其它意外流量

与其它网络公司相似，思科也时常会接收到试图发动 DoS 袭击的流量。DoS 袭击的特征是向网络发送大量分组，这些分组的大小通常不同于普通分组，一般从不可信源地址发往同一个目的地。思科探测和防止 DoS 袭击的方法是，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。异常检测报告样例如图 5 所示。Cisco NetFlow 将指导公司使用微观分析技术，包括 ACL、QoS、由 BGP 触发的单播反向路径转发黑洞以及为 Cisco Catalyst 6500 系列交换机开发的 Cisco NAM-2。

图 5 Peakflow DoS 异常检测报告样例



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。

内部网和外部网应用案例

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。例如，当某办公室的流量迅速增加时，思科 IT 使用 Cisco NetFlow 和 NetQoS ReporterAnalyzer 寻找使流量增加的应用和主机，最后发现罪魁祸首是一个

非授权的 HTTP 应用。当思科向员工重申公司策略，禁止在公司网上传输非授权文件时，这个问题自己消失了。在一个类似的应用中，思科 IT 也使用了 Cisco NetFlow，以便说明公司向商业合作伙伴提供的外部网只支持授权应用。利用部署在思科内部网上的 Cisco NetFlow，公司还可以发现企业信息盗窃现象——例如，当某地在短时间里从某几台服务器下载了大量信息时，就有可能是在盗窃公司信息。

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：欧洲、中东和非洲流量的 55%，以及其它地方流量的一大部分，都来自销售办公室部署的一个新型 PC 备份工具。由于初始备份将通过 WAN 传输大量流量，因而思科 IT 要求员工在夜间执行初始备份。另外，IT 还在 WAN 路由器中编写了基于时间的语句，规定白天的 WAN 链路容量为 10%，夜间则为 50%。当其它应用需要链路容量时，这条语句允许路由器丢弃上述阈值之上的分组。这样做的结果是，思科不但推迟昂贵的 WAN 链路升级，在员工完成大量初始 PC 备份的同时调节了流量，还及时提出了寻求更有效 PC 备份软件的要求。移植到新的备份解决方案之后，思科 IT 部门将使用 NetFlow 统计数据衡量 WAN 流量的减少。

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。Chang 说：“思科 IT 利用 Cisco NetFlow 和 NetQoS ReporterAnalyzer 解决了这些问题，不但能核实是否为每个服务等级（CoS）分配了足够的带宽，还能确认是否存在 CoS 过高或过低的现象。”另外，思科 IT 部门还使用 Cisco NetFlow 和 NetQoS ReporterAnalyzer 检查当话音和视频流量达到高峰水平时，WAN 链路是否丢弃了其它数据流量。例如，从芝加哥到纽约的 OC-3 链路获得了 10%或 15.5Mbps 的带宽，用于传输 IP 话音（VoIP）流量。只需打开路由器中的 Cisco NetFlow，思科 IT 部门就可以看到，即使在高峰时间，VoIP 流量获得的带宽也足以达到 QoS 的要求。

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。通过区分各种远程员工流量，包括话音、电子邮件、Web 浏览及其它应用等，思科可以更好地了解员工的行为，从而提供最佳支持，例如创建时间 QoS 语句，在白天支持更多的话音流量，夜晚则支持更多的数据备份。

为确定远程员工传输的思科 IP 电话和思科 IP 软电话软件流量的相对量，此信息用于市场及 IT 规划，思科 IT 使用 Cisco NetFlow 和 NetQoS ReporterAnalyzer 监控服务类型（ToS）和分组大小位数。所有流量的 ToS 位值都是 5，思科 IP 电话的 IP 流量是每秒 80Kbps（基于 G.711 压缩 codec），软电话流则为 24Kbps（基于 G.729 压缩编译码器）。

核实电信商的服务等级

在美国，思科 WAN 使用租用线路。思科 IT 部门在 WAN 上支持多种服务的情况很容易确定，因为 IT 工程师只需

查看路由器配置就可以核实 QoS 水平。但是，如果像欧洲思科 WAN 那样，WAN 电路是由电信商在共享多协议标记交换（MPLS）网络上供应时，情况就发生了变化：思科 IT 无法检查服务供应商网络内的 QoS 配置。思科 IT 希望能够核实电信商的服务等级现实情况，原因有二。首先，某种流量的 CoS 越高，思科 IT 部门支付给 MPLS VPN 的费率就越高，因此，最好检查服务等级协议是否得到了满足。其次，思科不可低估需要的 CoS 的话音或视频流量，否则必须立即知晓，以便及时升级。思科 IT 部门计划使用 Cisco NetFlow 检查欧州 MPLS VPN 上的抖动和分组损失。Chang 说："收集 QoS 信息不但能检查我们是否得到了合同中规定的 CoS，还能及时为每种 CoS 分配适当的带宽，以支持商业应用的正常运行。"

计算应用的总拥有成本

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（参见"减少高峰期 WAN 流量"）。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。测试并不需要专门的实验室或测试环境，因为应用设计者可以通过配置，让应用在实验中装有 NetFlow 的思科路由器中运行。思科 IT 部门使用 NetFlow 计算应用 TCO 的方法包括：

- 将监控摄像机系统升级到 IP 闭路电视（CCTV）系统。思科安全部（负责远程监控 270 多个思科站点的 2000 多台安全摄像机）计划通过 WAN 传输偶而点播的视频，因而正打算将园区网 MAN 视频流量从专用光纤向共享千兆位以太网 LAN 转移。通过收集和分析实验室中的 Cisco NetFlow 数据，安全部证实，IP 流量不会造成城域网和 WAN 流量激增。
- 通过 WAN 部署 Cisco UnityTM 语音留言。Cisco NetFlow 数据能够保证，部署 Cisco UnityTM 语音留言需要的流量不会超过分配给话音流量的 WAN 带宽。
- 计算来自全球 50,000 部思科 IP 电话的成本节约。思科 IT 管理层希望定量计算从传统话音网络移植到 IP WAN 后的成本节约。利用 Cisco NetFlow，思科 IT 部门可以测量各位置之间的 WAN 话音流量，然后利用这些数据估算通过公共交换电话网传输这些流量的成本。
- 计算思科应用和内容网络系统（ACNS）软件实现的成本节约。思科 ACNS 服务器在思科 IT WAN 上保存最终用户附近的高速缓存和预选择内容，以减少 WAN 流量，提高访问速度。另外，思科 IT 部门还利用 Cisco NetFlow 确定从 WAN 下载的流量大小，以便估算成本节约。
- 制订未来服务计划。在思科 IT 部门继续部署未来服务的过程中（例如，Oracle 11.i 和 Cisco Unity 是可能会影响 WAN 的两个大应用），他们将继续使用 NetFlow 捕获实验室和试用网络数据，以确定与这些新服务相关的所有 WAN 的影响及其成本。

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。Cornell 表示："Cisco NetFlow 能够帮助我们提高对网络流量的洞察力，使我们不但能抵御 DoS 攻击以及其它形式的意外流量，正确应对各种网络威胁，还能收集宝贵的应用使用数据，更好地执行容量规划。"

下一步

下一步，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。

思科 IT 部门的容量规划网络工程师 Keith Brumbaugh 说：“随着收集的 NetFlow 历史数据的增多，容量规划将变得越来越容易。如果拥有足够的历史数据进行比较，我们就能够更容易地看到历史发展趋势。不仅如此，我们还将能够了解公司网络的正常流动情况，从而更快地捕获异常流量。”

一开始，思科 IT 部门先在小范围内利用 Cisco NetFlow 逐渐地收集信息，从互联网网关开始发展到 WAN 和外部网网关。John Cornell 谈到：“我们收集的重点是从互联网到内部网，以及从内部网到互联网的流量信息。”Roland Dobbins 补充说：“以后，我们不但要把 NetFlow 的使用逐步扩展到内部网中，还要将容量规划扩展到园区网 LAN，尤其是数据中心 LAN，以及这些数据中心 LAN 与互联网之间的连接点中。”

以后，思科将把 Cisco NetFlow 的使用从公共网扩展到内部网。Dobbins 说：“随着无线网和 VPN 通道的建立，网络边界的消失，内部网的安全性成为 IT 安全部关注的最重要的问题。如果能对内部网和桌面网边缘的流量提取特征，就能够检测到正在产生恶意流量或试图非法访问资源的主机。”另外，思科还希望将用于互联网连接的容量规划方法扩展到思科 WAN 上的内部网。

Dobbins 指出：“无论是企业还是政府机构，只要是负责任的机构，需要通过网络的有效利用来实现资源调整、容量规划和安全性。融合网络和 IP 电话将不断普及，通过网络流量特征提取执行容量规划和异常检测的能力将变得越来越重要。对思科而言，NetFlow 完全能够实现这些功能。”

如果想阅读关于其他商业解决方案的思科 IT 案例分析，
请访问 Cisco IT@Work：www.cisco.com/go/ciscoitatwork

注：

该出版物介绍了思科在部署自己开发的产品之后获得的好处。文本描述的结果和好处是多种因素作用的结果。思科并不能保证在其它地方也能获得类似的结果和好处。

思科以真实面目提供该出版物，思科不提供任何明确或隐含的保证，包括隐含保证可销售性，或者适合某种目的。某些国家的法律不允许否认明确或隐含的保证，因此，该否认声明可能并不适用于您。

思科系统（中国）网络技术有限公司

北京
北京市东城区东长安街1号东方广场
东方经贸城东一办公楼19～21层
邮编：100738
电话：(8610)85155000
传真：(8610)85181881

上海
上海市淮海中路222号
力宝广场32～33层
邮编：200021
电话：(8621)33104777
传真：(8621)53966750

广州
广州市天河北路233号
中信广场43楼
邮编：510620
电话：(8620)85193000
传真：(8620)38770077

成都
成都市顺城大街308号
冠城广场23层
邮编：610017
电话：(8628)86961000
传真：(8628)86528999

如需了解思科公司的更多信息，请浏览http://www.cisco.com/cn