NSFOCUS

黑洞网络流量分析系统白皮书

© 2008 绿盟科技

■ **版权声明**

本文中出现的任何文字叙述、文档格式、插图、照片、方法、过程等内容，除另有特别注明，版权均属绿盟科技所有，并受到有关产权及版权法保护。任何个人、机构未经绿盟科技的书面授权许可，不得以任何方式复制或引用本文的任何片断。

■ **商标信息**

绿盟科技、**NSFOCUS**、黑洞是绿盟科技的商标。

目录

表格索引

插图索引

一. 前言

随着互联网服务的普及，网络上各个环节的带宽越来越大。国际出口的带宽以及国内运营商之间互联带宽都在成指数趋势增长。一些大型城域网的出口带宽都超过了 10Gbps，电信级 IDC 的出口带宽很多也都超过 5Gbps。不仅运营商网络带宽在不断扩充，很多行业或政府的专网的带宽也有很大增加。伴随着带宽的增加，网络上的应用和业务也不断的丰富，如基于流媒体的音视频服务，基于 MPLS 的 VPN 业务等等。与此同时，网络攻击的成本和技术门槛大幅下降，网络上的各种攻击和异常流量大量出现。在这种流量成分日益复杂，异常流量海量涌现的情况下， 对网络流量进行深入分析从而全面了解流量的各种分布以及变化趋势就显得十分必要了。

本文从阐述流量分析的目的入手，概要介绍一下流量分析的一般原理以及通用的技术实现方案，最后重点介绍 绿盟科技骨干网络流量分析解决方案。内容包含如下部分：

- 流量分析的目的
- 流量分析的原理
- 流量分析的技术实现
- 绿盟科技骨干网流量分析解决方案

二. 流量分析的目的

网络流量的复杂性给网络的运营维护带来了巨大挑战，运维人员通常关心的问题包括两大类，一类是与网络和业务规划相关的问题，即关于网络流量成分组成以及地域分布的情况。另一类是与网络安全运营相关的问题，即关于异常流量的种类和数量、来源等情况。流量分析的目的就是解决运维人员这两个方面的问题。下面分别详细列举每一类别所涉及的具体问题。

2.1 与网络和业务规划相关的问题

与网络和业务规划相关的问题基本是围绕三个方面的内容：流量的来源与去向、流量的组成成分、流量的变化趋势。例如：

- 从子网 A 到子网 B 的流量是多少？
- 各个子网间的流量是否平衡？
- 网络出口的流入流出流量是多少？
- 上联电路的负载是否均衡？
- 过去几个月的流量变化趋势如何？网络带宽是否足够？预计什么时候需要扩容？
- 内部网络到外部各个地方的流量的比率?

2.2 与网络安全运营相关的问题

对骨干网的安全运营最大的威胁各种异常流量和攻击。因此与安全运营相关的问题大都是围绕异常流量展开的。运维人员最关心的问题有：

- 谁在访问我们的网络，是否属于攻击？
- 异常流量有多大？都是什么类型的攻击？
- 攻击流量的来源是哪里？
- 网络内部哪些流量被攻击？
- 网络内部是否有向外的攻击流量？

三. 流量分析的原理

任何 IP 网络流量分析的过程都可以大概分为三个环节：数据采集、数据分析、结果呈现。下面分别从这三个环节讲述流量分析的原理。

3.1 数据采集的机制

数据采集的大体上可以分为 Netflow、sFlow、SPAN、SNMP/RMON 四种方式。这些方式是与设备相关的。即某些设备只能支持某一种或几种采集方式。每种采集方式有其固有的优势和局限。下面通过表格对比说明

	工作机制	优势	局限
Netflow	由路由器按照 7 元组条件在缓存中创建流记录，并按照一定触发条	支持此方式的设备较多。可以含有二层的数据信息。不用嵌入到用户电路	路由器在输出流记录的时候会有些延迟（要满足流结束条件后才输出） 。流记

	件定期输出流记录生成包。由专用的采集程序监听路由器发送过来的流记录包，将数据包解码就完成了数据采集的环节。	中，进行采集。主要包含数据包的三层和二层信息。同时也融入了对应的路由信息（如 AS 号、BGP 信息等）。	录不包含包内容信息，无法做深度检验。
sFlow	路由器按照物理端口对随时将采样数据包的包头信息输出	输出信息中包括二层数据，没有流的起止概念，随时将包头信息输出，实时性较好	输出信息都是单个数据包，没有会话的概念，做数据分析时需要做一定的聚合计算。
SPAN	在网络设备上配置镜像端口，用类似 Sniffer 的方式采集来自镜像端口的数据包	输出信息包括应用层信息和数据内容。输出信息的实时性较好	在大流量环境下（接口带宽超过 2.5Gbps）很难满足数据采集的性能要求。部署的可扩展性差，需要在很多点进行部署，造成成本加大。输出信息仅限于数据包自身携带的内容，无路由相关信息。输出信息都是单个数据包，没有会话的概念，做数据分析时需要做一定的聚合计算。
SNMP /RMON	通过 SNMP 查询请求获取数据	采集方法简单，容易实现，数据的呈现比较简单	输出的流量信息内容过于简单，通常只含有总流量的信息。SNMP 的优先级别比较低，容易造成数据丢失。 只能做面向设备的分析，无法做面向业务的复杂分析。

表 3.1 数据采集机制对比

从上面的对比来看，SNMP/RMON 以及 SPAN 方式都无法满足高带宽的网络环境的性能要求和分析需求。因此目前大多数流量分析系统都采用 Netflow 或 sFlow 作为主要的流量采集手段。在某些特殊的情况下，使用 SPAN 方式采集数据。流量统计分析的方法

3.1.2 流量数据所含的信息

无论是那种类型的流量数据，包含的信息都可以分为三类：空间信息、时间信息、技术指标信息。

- 空间信息是流量发生的地点，包括：路由器、物理端口、IP 地址（段）、AS 号、地域名称等。
- 时间信息是流量发生的时间：用分钟、时间片、小时、日、周、月、年 来度量
- 技术指标提供流量的业务特征的信息：应用类型，TCP-flag, ToS, 包大小……

这样流量数据实际上就构成了一个多维数据集。

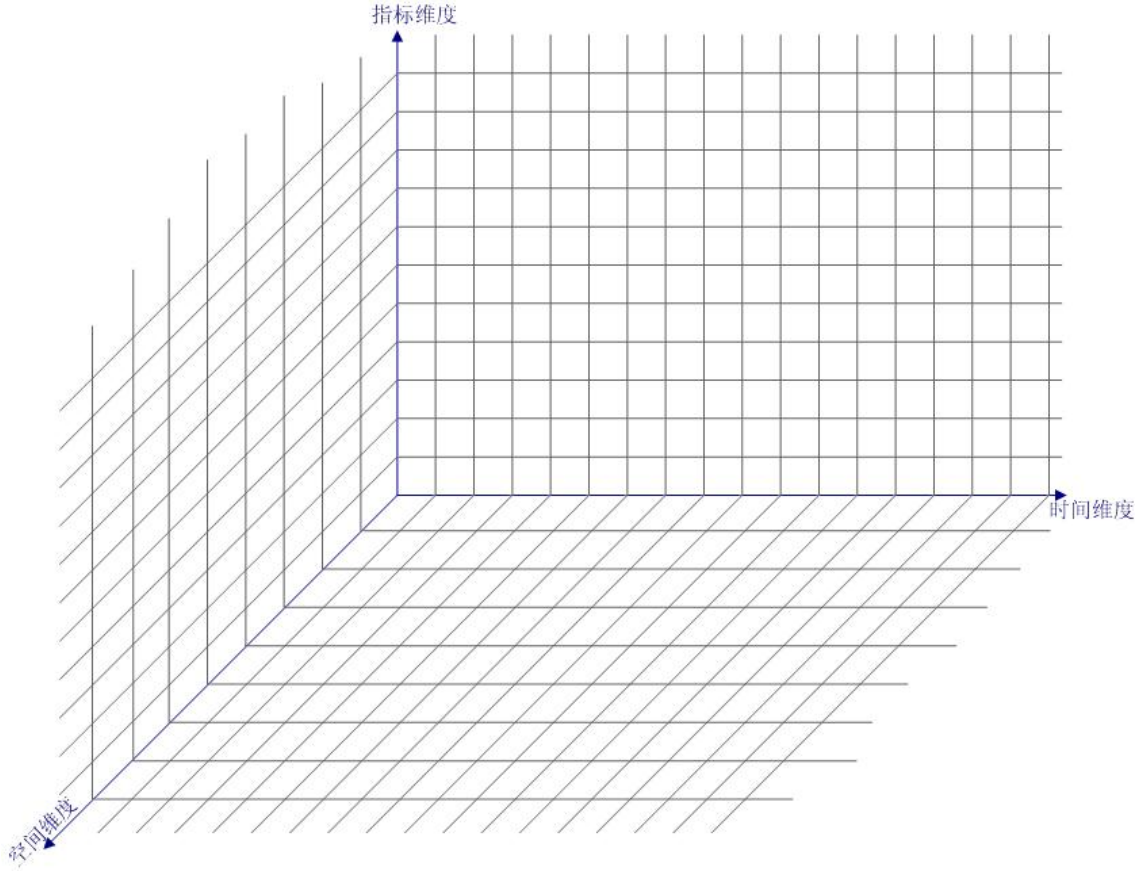

图 3.1 流量数据多维数据集

3.1.3 流量统计分析的过程

所谓流量的统计分析过程，就是在指定的时空范围内，统计流量对不同维度的分布。例如，查看某一天之内，某个路由器上各个端口上的流入、流出的总流量，就是查看指定时间

范围内流量对路由器端口这个空间维度的分布。再例如，查看某段时间内某个端口上流量中各种应用所占比例就是查看指定的时间范围、指定地点流量对应用这个技术指标维度的分布。

流量分析过程还可以用另一种方式来解释。前一节中，我们把流量数据看作了一个多维数据集，流量分析的过程就是根据实际需要从不同的角度去透视这个多维数据集。

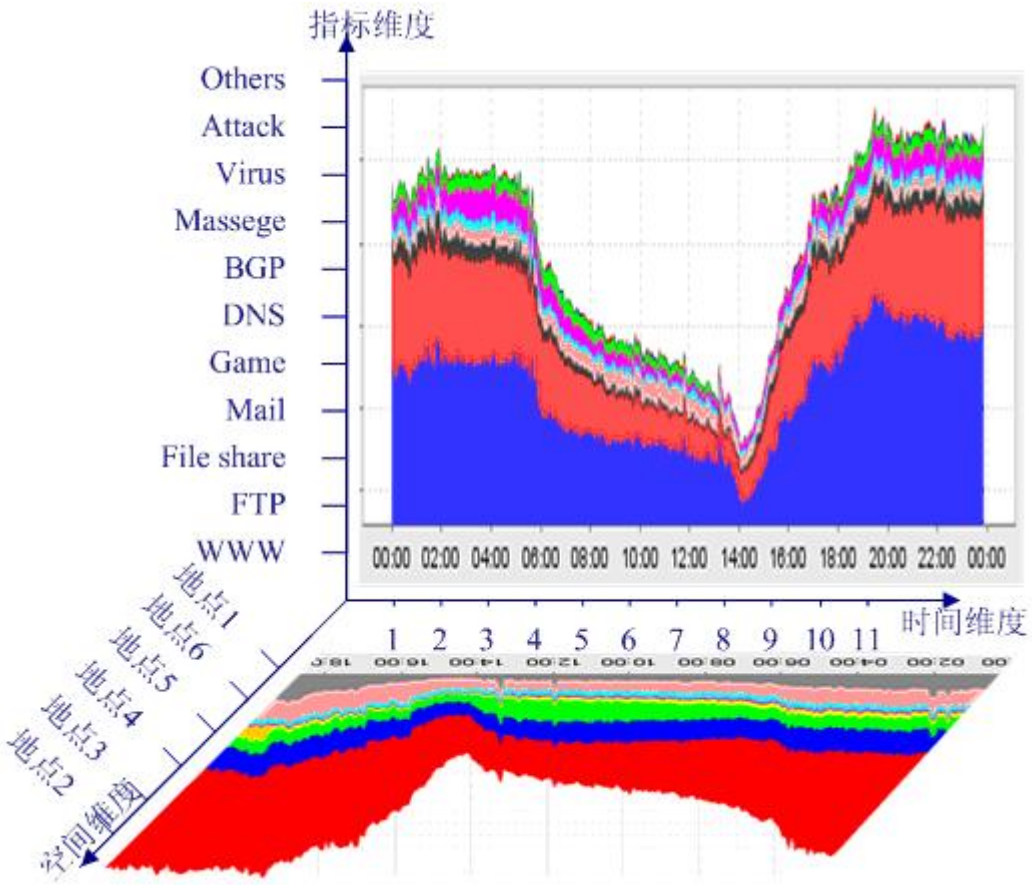

图 3.2　流量数据的透视

3.2 异常流量检测的原理

异常流量的检测分为三个步骤：检测指标实测值的计算，检测指标基线值的计算，实测值与基线值的比较。

每一种检测指标都对应一种或可能的几种攻击。也就是说，有的检测指标是专门检测某一种特定的异常流量的。而有的检测指标出现异常时，则只能判断存在几种可能的异常流量。这种指标就是非特异性指标。

每种检测指标都有自己的基线，但基线的算法是类似的。通常基线算法有两种，一种是周期性基线，一种是移动窗口基线。如果检测指标的正常值的变化趋势有明显的周期性，则

建议采用周期性基线。如果检测指标的正常值没有明显的周期性变化，而且在一个较小的范围内波动，则使用移动窗口基线效果比较好。

四. 流量分析的技术实现

4.1 流量分析系统的一般架构

目前流量分析产品的种类非常多，但是系统架构基本上是一致的。流量分析系统属于网络管理软件，因此在系统架构上仍然遵循网络管理软件系统架构的一般原则。即整个体系分为三层：采集层、分析层、呈现层。

采集层——采集层直接从网元设备获取原始流量数据并进行解码，把解码后的数据交给分析层进行分析计算，通常还会保留一份解码后的流量数据记录的硬盘。

分析层——分析层从采集层获取解码后的流量数据记录开始进行分析计算。通常在计算前需要进行数据的归一化处理。

呈现层——呈现层通过数据接口获取统计分析的结果并呈现在用户界面上。

4.2 技术架构的实现

图 3.3 完整的描绘出一个流量分析系统的实际模型，清晰的显示了流量分析系统各层次组件之间的关系。

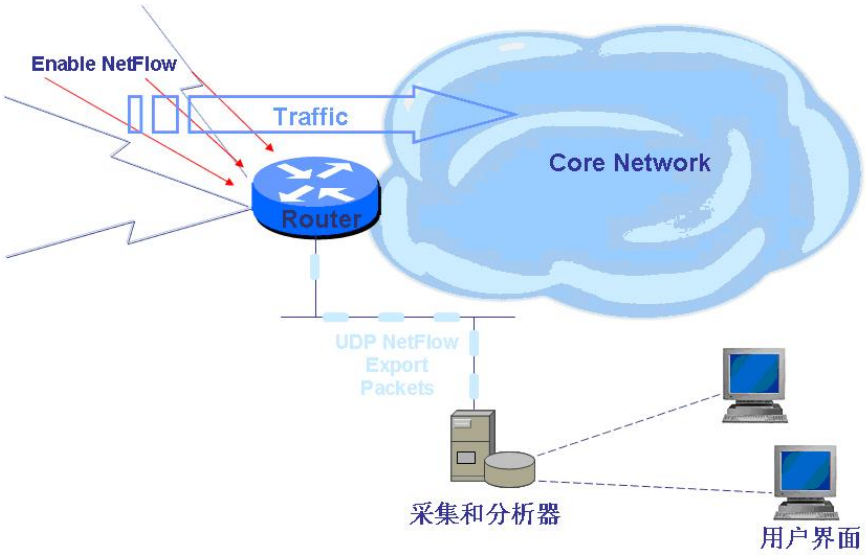

图 4.1 流量分析系统的实现

五. 绿盟科技流量分析系统

5.1 核心功能

5.1.1 异常流量检测

对异常流量的检测是绿盟流量分析系统最主要的功能。骨干网上的异常流量通常分为 6 大类：网络层 DDoS 攻击、应用层 DDoS 攻击、蠕虫传播、P2P 下载、BGP 攻击、用户自定义异常等。绿盟流量分析系统采用了 17 大类，共计 50 多种检测指标，这些检测指标覆盖了全部常见的异常流量：

- 流量型 DDoS 攻击
- 应用型 DDoS 攻击
- 蠕虫传播
- BGP 攻击
- P2P 流量

绿盟流量分析系统使用动态基线检测异常流量，动态基线分为两种，一种是周期性基线，一种是移动窗口基线。对不同的检测指标，应用不同的基线进行检测。

5.1.2 流量统计分析

网络流量分析系统另一个主要功能是流量的统计分析。统计分析结果可以用实时监控或历史回放的方式展现。流量统计分析可以让用户从各种不同的角度透视网络上的流量。通常的透视角度包括：

- 整个网络（Network）
- 互联运营商(Peers)
- 路由器
- 路由器物理端口
- 地域或子网（用 IP 地址段）
- 客户（用 IP 地址段或端口号定义）

流量统计分析的结果包括：

- 总流量
- Top10 地址流量

- Top10 应用/端口流量
- Top10 自治域流量
- Top10 协议流量

5.1.3 统计报表

统计报表是一种事后的分析工具。统计报表按照其内容分为：

- 流量报表
- 告警报表
- 自定义报表

各种报表按照统计周期的不同，又可以分为年报表、月报表、周报表、日报表。每类报表都包含多种报表模板，这些模板基本可以满足用户的全部需求。

在生成报表之前，允许用户从界面选择一些报表条件，如时间范围，统计周期、报表类型、报表模板等。选定好条件之后就可以生成报表了。

在流量分析页面中可以选择特定监控对象和时间范围，然后把查询结果输出成 PDF、HTML、EXCEL、WORD 等格式的文档，也可以作为一种灵活定制的报表。告警监控和设备监控页面也有类似的报表导出功能。

5.1.4 路由分析

路由分析是运营商用户比较关注的功能，通过分析路由消息和路由表信息，得到关于路由稳定性和合理性的结论。具体的功能包括：

- 不同长度前缀的数量分布：统计路由表中不同长度的网络前缀的数量
- BGP 路由稳定性：根据 RFC4098 中的定义，统计不同路由事件的数量
- 路由数量：统计路由条目数量的变化
- **BGP 包分析：**统计不同 BGP Peer 发生的 BGP 数据包的数量
- **路由震荡分析：**统计不同自治域正在抖动和已被抑制的路由情况（仅分析 EBGP）

5.2 主要特征

5.2.1 先进的基线生成算法

由于异常检测指标的变化特征不同，应该用不同的基线进行比对。系统采用了两种不同的基线。一种是周期性基线，用来检验其变化趋势明显带有周期性的指标，例如端口总流量，某种应用的总流量、某个 IP 群组的流量趋势。另一种是移动窗口基线，用来检测非周期变化的指标。基线值是根据一组历史流量数据利用加权平均和置信区间的算法得到的。超出可信范围的历史数据不参与基线的计算，从而保证了基线的有效性。

5.2.2 丰富的异常检测算法

系统提供的多达 17 大类 50 余种检测指标，每一种检测指标都对应一种检测算法，能够全部覆盖骨干网上的各种异常流量的检测。利用这些检测算法，检测到网络异常包括以下 6 大类包括：

- DDoS 攻击
  - SYN Flood
  - UDP Flood
  - ICMP Flood
  - ACK Flood
  - DNS Query Flood
  - Http Get Flood
  - LAND Flood
  - IGMP Flood
  - TCP Flag NULL
  - TCP Flag 误用
  - Protocol NULL
- 蠕虫事件
  - Code Red
  - 硬盘杀手
  - SQL Slammer
  - 冲击波
  - 冲击波杀手

- 震荡波
- 邮件蠕虫
- WinNuke 攻击

◆ 网络误用

- 私有 IP 异常
- Dark IP 异常

◆ 流量超常

- bps 超常
- pps 超常
- 会话数超常

◆ 协议比例异常

- TCP 比例异常
- UDP 比例异常
- ICMP 比例异常
- IGMP 比例异常

◆ 流量分布异常

- 源地址分散度异常
- 目的地址分散度异常
- 端口分散度异常

◆ P2P 流量

- BitTorrent
- 电驴
- 迅雷
- pplive
- P2P 流量(未知应用)

5.2.3 灵活高效的检测

系统的计算引擎的程序结构采用框架和插件模式，这样就在结构上保证了系统的灵活性和高效性。每一种或几种检测算法都对应一种插件。用户可根据自身的网络特征和业务特征加载最适当插件。系统也提供一些预设的插件模板，不同的模板对应不同的典型用户。例如电信运营商的骨干网的运维，对应用层攻击的关注程度就很低，因此在这类用户的环境中，就可以不加载相应的检测插件。

5.2.4 强大的处理性能

通过选用高性能的硬件已经优化计算引擎的程序算法，网络流量分析系统的处理性能最高可以达到每秒处理 8 万条流记录的能力。这个处理能力完全满足电信级骨干网的要求。

5.2.5 即插即用

设备上线以后，只需要非常简单的配置操作，即可生效运行。例如配置监测 IP 地址范围，不需要手工输入，系统直接从备选清单中把拟监测的 IP 地址段勾选上。IP 地址段的备选清单是从路由表中自动提取的。类似的自动过程还有很多，比如对 IP 地址段按照流量趋势的变化规律自动聚合成 IP 地址分类。再比如，路由器物理端口号与名称的对应关系的自动生成。

5.3 部署方式

黑洞网络流量分析产品的部署方式比较灵活，往往根据用户的网络拓扑结构和对流量分析的需求而有一些变化。在运营商的网络环境下，通常会采用下面典型部署方式。

网络出口模式适用于城域网或各种专网的环境中。图中的四个网络出口路由器器之间采用全互联连接。用蓝色线表示。为了避免流量数据的重复采集，出口路由器之间互联的端口不要打开 Netflow。仅将上、下联端口的 Netflow 功能打开。

在有些规模比较小的网络出口可能只有两台，同样遵循上述原则，不打开连接两个路由器的端口上的 Netflow 功能。在性能允许的情况下，可以考虑只部署一台流量分析设备。

在运营商的环境里，NTA SP2000 通常会与 ADS(抗拒绝服务系统)集群设备一起组成一个抗 DDOS 的解决方案。或者是作为 IP 综合网管系统的一部分。

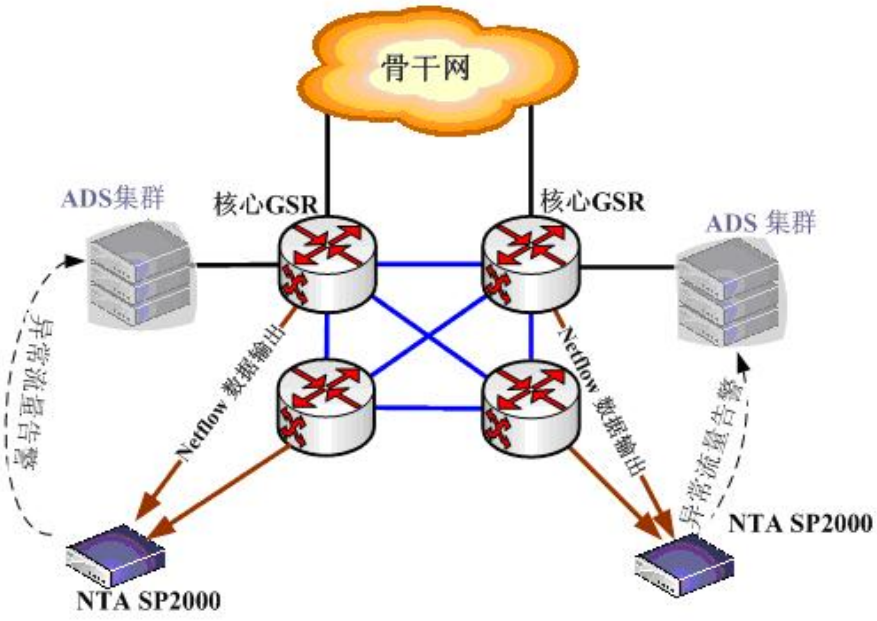

图 5.1　运营商环境下典型部署图

在企业办公网的环境下，分为两种情况：用户网元设备支持 Netflow，用户网元设备不支持 Netflow。对于支持 Netflow 的情况，按类似运营商的方式部署。对于不支持 Netflow 的情况，需要增加一个叫做 NTA CT600 的设备。

图 5.2　企业网环境下典型部署图

在园区网的环境下，用户可能关心各个子网间的流量，且分布层设备也不支持 Netflow，需要把每个接入层路由器的上联端口的流量镜像到 NTA CT600，NTA CT600 把流量转换成

Netflow 数据并发送给 NTA SE2000。如果分布层设备支持 Netflow，则不需要 NTA CT600，接入层设备直接打开 Netflow 功能，直接向 NTA SE2000 发送 Netflow 数据。

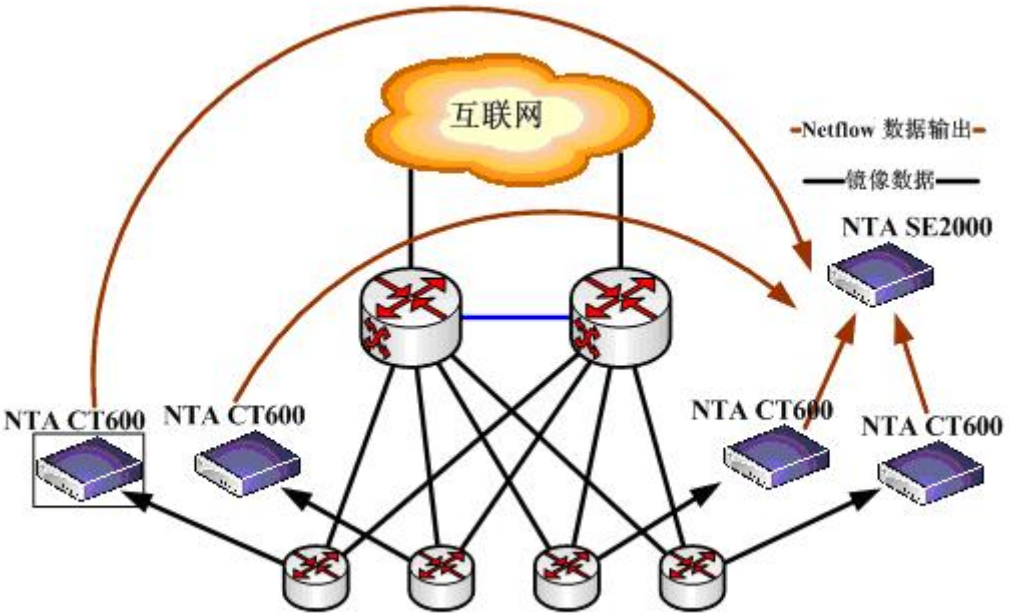

图 5.3　园区网环境下典型部署图

六. 结论

随着网络异常流量的类型和大小不断增加，网络流量的成分越来越复杂。传统的网管工具不能详细分析流量的成分组成和发展趋势，更无法快速锁定异常流量的来源和目标以及异常流量的类型。日常运营维护以及未来增值服务需要，只有在骨干网络上部署专业的流量分析系统才能满足。

绿盟科技的网络流量分析产品提供了业界领先的异常流量检测能力，通过多种机制的分析检测以及灵活的部署方式，绿盟的产品能够及时有效的分析出异常流量并发出告警。

绿盟科技的网络流量分析产品还提供丰富的统计分析功能，为用户透视流量数据提供了多种视角。对流量的统计分析结果有助于解决用户在业务规划和网络容量规划、流量工程等方面的诸多问题。