无标题-4

|  |  |  |  |
| --- | --- | --- | --- |
| **绿盟网络流量分析系统**  **产品白皮书**  **【绿盟科技】** | | | |
| ■ 文档编号 | NSF-PROD-NTA-V4.5-产品白皮书-V2.0 | ■ 密级 | 完全公开 |
| ■ 版本编号 | V2.0 | ■ 日期 | 2017/09/19 |
| * 撰 写 人 | 汤湘君 | ■ 批准人 |  |



|  |
| --- |
| © 6/30/18 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，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。 |

|  |  |  |  |
| --- | --- | --- | --- |
| ■ 版本变更记录 | | | |
| 时间 | 版本 | 说明 | 修改人 |
| 2017/9/19 | V2.0 | 更新3.4 | 汤湘君 |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

|  |
| --- |
| 目录 |

[1. 引言 1](#_Toc509409193)

[2. 客户价值 2](#_Toc509409194)

[2.1网络和业务规划相关的问题 2](#_Toc509409195)

[2.2 与网络安全运营相关的问题 3](#_Toc509409196)

[3. 原理介绍 3](#_Toc509409197)

[3.1Flow技术特点 3](#_Toc509409198)

[3.2流量分析原理 4](#_Toc509409199)

[3.3异常检测原理 5](#_Toc509409200)

[3.4接口联动 6](#_Toc509409201)

[4. NSFOCUS NTA产品介绍 7](#_Toc509409202)

[4.1产品概述 7](#_Toc509409203)

[4.2产品架构 7](#_Toc509409204)

[4.3产品特色 8](#_Toc509409205)

[4.3.1 全网状况实时监控 8](#_Toc509409206)

[4.3.2 准确详尽的流量分析 8](#_Toc509409207)

[4.3.3 强大的异常检测功能 9](#_Toc509409208)

[4.3.4 IPV4/V6双栈分析检测支持 10](#_Toc509409209)

[4.3.5 灵活多样的报表展示 10](#_Toc509409210)

[4.3.6 完整的解决方案 11](#_Toc509409211)

[4.3.7 增值运营带来收益 12](#_Toc509409212)

[4.3.8 便捷智能的运维方式 12](#_Toc509409213)

[4.4典型部署 13](#_Toc509409214)

[5. 总结 13](#_Toc509409215)

|  |
| --- |
| 插图索引 |
| 图 3.1 [流量数据的透视](#OLE_LINK1) 5  [图 3.2 基线告警示意图](#OLE_LINK10) 6  [图 4.1 全网监控图](#OLE_LINK11) 8  [图 4.2 绿盟科技三位一体方案](#OLE_LINK13) 11  [图 4.3 典型部署](#OLE_LINK3) 13 |

1. 引言

随着互联网技术的迅猛发展，网络规模空前增长，网络上的应用越来越广泛。网络的多样性给互联网用户带来了的丰富的生活体验，与此同时，网络的复杂性却增加了网络运维的管理难度，使运维人员面临诸多困难。

网络的不断扩张带来的网络协议新变化，无疑增加了网络的复杂性。由于网络地址资源的使用越发缩紧，当前的网络协议IPV4已不能满足互联网用户的需要。IPV6的出现有效解决了IP地址不够用的情况，它能分配的地址空间是现有互联网的1029倍。近年来在专家和政府部门的不断推进下，美国、日本、中国、欧盟等地区都建立了IPV6的骨干网，IPV6的推进已经获得全球共识。IPV6协议的发展，促使网络协议由IPV4向IPV6的进行过渡。过渡阶段，网络中常常出现IPV4/V6双栈并行的情况，加深了网络的管理和异常事件的排查难度。

网络的复杂性还体现在网络中承载的业务不断丰富。为了抢占新的技术变革带来的发展商机，互联网需要向用户提供更大的信息量和多样化的网络服务。云端网络的出现，社交网站的兴起，视频、多媒体技术的迅速发展，各种应用的出现在满足用户多样化的网络需求的同时，也在互相挤占带宽。如何保障正常业务，关键业务的平稳运行，揪出造成了网络拥塞的元凶？只有及时的了解到网络中承载的业务，掌握网络流量特征，才能使网络带宽配置最优化，及时解决网络性能问题。

互联网承载的业务越来越多，消耗的资源也越来越大，全球网络都呈现出一种不断扩张的状态。对于电信级的网络，各个网络节点上的带宽逐年增大，国际出口的带宽以及国内运营商之间飞互联带宽都在成指数趋势增长。对于数据中心，为了保证数据托管业务、专网用户的业务正常运行，在激烈的竞争中给客户提供优质的服务，带宽同样在不断扩充。除了运营商和数据中心，很多行业或政府的专网的带宽也在增加，以满足用户的需求。高带宽的网络环境下，路由设备众多。透视网络状况、及时发现设备故障，根据业务需求合理有效的进行网络规划和设计，常常是摆在运维人员面前的难题。

另一方面，由于网络攻击的成本的技术门槛大幅下降，网络上的DDoS攻击的出现频率和破坏性均在不断增加。各种攻击事件的出现，极易消耗网络资源，可能造成关键业务的中断或网络服务质量大幅降低的严重后果，给运营商、企业和数据中心带来巨大损失。基于安全运维和竞争的需要，及时发现攻击事件，建立一个稳定、安全的网络环境，提供高质量的带宽服务无疑成为重中之重。近年来攻击的手段、方式都在持续改进，如慢速攻击的增加，混合型攻击的增加，针对IPV6攻击的增加等等，仅通过网络扩容的方式并不能真正解决问题。在异常严峻的网络安全形式下，传统的网络管理手段已不能满足运维的需要。

为了在复杂的网络中解决以上提到的各种网络问题，绿盟科技自主研发了网络流量分析产品—NSFOCUS Network Traffic Analyst，以下简称NSFOCUS NTA。基于多年来对网络分析和攻防的研究理解，旨在于提供智能的管理手段，帮助网络运维人员透视网络状况，及时锁定异常威胁，减轻网络复杂性造成的网络运维压力，建立一个平稳、高效的网络环境。

1. 客户价值

网络流量的复杂性给网络的运营维护带来了巨大挑战。绿盟科技网络流量分析产品能帮助网络运维人员全面了解网络状况，解决运维人员通常关心的两大类问题。一类是与网络和业务规划相关的问题，另一类是与网络安全运营相关的问题。绿盟科技网络流量分析产品可以帮助网络管理员纵观网络状况，了解网络成分趋势变化，从容面对网络异常。提供网络运营者安全运维的决策分析与建议，帮助运营商、数据中心等企业提供优质的网络服务，从而增强企业的核心竞争力。下面分别详细列举NSFOCUS NTA给客户带来的巨大价值。

2.1网络和业务规划相关的问题

NSFOCUS NTA能够通过SNMP、Netflow等协议格式采集到网络中路由设备的流量信息，进行多种维度的分析，满足高带宽条件下的实时监控，使网络情况透明化。NSFOCUS NTA围绕与网络和业务规划相关的三个方面进行分析，帮助客户掌握：

* **网络中的流量情况**

NSFOCUS NTA能监控客户网络中的路由设备、关键链路和重要业务的流量，使用户纵观网络状况，帮助用户全面透视网络状况，建立网络整体模型的概念。

* **网络中的流量组成成分**

NSFOCUS NTA能对多达数百种网络应用进行检测分析，展现各种应用的流量及在网络中的占比情况。流量组成分析，使用户对网络成份清清楚楚，知道目前最热的网络应用是什么，最消耗带宽的应用是什么，是否有应用挤占了正常业务的带宽。帮助用户了解网络业务开展情况及占用的网络成本，及时找到网络瓶颈，做出正确的决策优化网络。

* **网络中的流量变化趋势**

NSFOCUS NTA能帮助用户对重点业务进行长期监控，根据业务在不同时期的流量情况，帮助用户建立网络模型。通过对重点业务发展进行价值评估，对网络规划和扩容做出正确决策。

。

2.2 与网络安全运营相关的问题

无论是运营商还是数据中心、金融等其他行业，安全运营无疑都是极其重要的。NSFOCUS NTA能解决运维人员最关心的网络安全运营问题，主要体现在以下几个方面：

* **快速发现网络异常**

NSFOCUS NTA能够7x24小时对全网设备进行实时监控。不但能监控网络设备的物理状况：如路由器接口状态是否正常，CPU、内存状态是否正常，而且能对网络中的流量异常状况：如网络中是否存在攻击事件，是否存在带宽超常等进行实时监控。系统可以根据网络事件的严重程度定义不同的告警级别，网络中一旦出现异常，便会立即触发告警机制。网络管理员可以在故障发生的第一时间获知网络异常信息，在网络故障爆发或扩大前采取相应的防范措施，将故障的影响程度降到最低。

* **定位攻击源和目标**

触发的告警事件中包含着详尽的内容，通过查看告警事件的分析，可以追溯故障发生的时间，地点，原因，是否属于人为的恶意攻击。对于攻击事件，告警属性中包含攻击的流量大小，攻击流量来源，危险程度等信息，帮助网络管理员快速判断并定位故障原因，判断异常对网络状况的影响，及时采取措施进行应急处理。

3. 原理介绍

在了解NSFOCUS NTA产品功能之前先简要介绍一下NSFOCUS NTA的工作原理。NSFOCUS NTA主要是基于Flow的技术，采用DFI的方式网络中的流量情况进行分析检测。

3.1Flow技术特点

以Cisco的netflow为代表的Flow技术是目前流量分析检测领域的主流技术，自1996年问世以来，Flow技术以其高效准确的数据采集方式，低成本高产出的优质网络运维特点，广泛应用于运营商、数据中心、互联网企业等各种路由器和交换机中。同DPI(Deep Packet Inspection)的分析方式相比，NSFOCUS NTA基于Flow的DFI(Deep/Dynamic Flow Inspection)数据采集方式有诸多特点：

* **支持的设备数量众多**

支持Flow采集方式的设备众多，如主流的Cisco、Juniper、Huawei等都有支持Flow格式的设备，能覆盖绝大多数网络中的设备。

* **非嵌入式采集**

不同于SPAN等探针方式的数据采集，基于Flow技术的采用非嵌入式采集方式，不会对现有网络拓扑结构造成任何改变

* **高性能，投资少**

采用先进的数据流采样随机技术，可通过设置合适的采样率，适用于各种类型的带宽环境，单台设备就可满足电信级的高带宽（数百Gbps）环境。而探针的采集数据方式必须基于物理端口，只适用于流量较小的网络环境，投资成本及维护工作量均相对较高。

* **快速响应**

不同于传统的数据采集方式，需要对采集的全包进行解析，DFI的方式处理速度更快，基于Flow的分析方式只需要进行流量特征比对，更利于对网络问题做出快速响应。

3.2流量分析原理

NSFOCUS NTA使用基于Flow的分析方式，支持业界主流的协议，如netflow v5/v9、sflow v4/v5、netstreamv5/v9等，也支持镜像数据通过转换器转为netflow格式进行分析。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。所谓流量的统计分析过程，就是在指定的时空范围内，统计流量在不同维度的分布。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。NSFOCUS NTA提供了一个多维的视角，帮助使用者从不同的角度去透析网络。如图3.1展示了NSFOCUS NTA对网络中流量数据的透视：

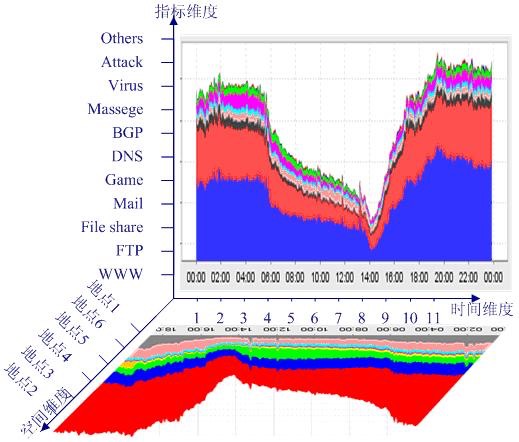


图3.1流量数据的透视

3.3异常检测原理

异常流量的检测分为两个过程：流量数据的采集，流量数据的分析。NSFOCUS NTA基于Flow的采集方式得到网络中的流量数据，获得流的起止、流量等数据信息，并根据不同的对象：如路由器、接口等，按照时间点进行数据聚合，形成基于对象的流量特征模型。

以异常流量检测为目的流量数据分析过程分为三个步骤：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。对流量中符合攻击特征的数据进行统计，根据特征流量是否超出正常范围，判断攻击流量是否存在。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，则能判断存在几种可能的异常流量。无论哪种检测指标都要先有自己的基线，而基线的算法是类似的。NSFOCUS NTA的基线算法分为两种：

* + 静态基线算法

静态基线是一条水平直线，通常是根据经验或是实验测量的结果得来，由于基线水平不变，很难反映客观网络流量的变化。静态基线较大依赖于需要运维人员的自身能力，需要对特征数据大小进行准确配置，阈值配置过高容易导致漏报，阈值配置过低则又容易产生误报，导致真正的攻击事件被淹没。

* + 动态基线算法

动态基线算法在静态基线的基础上开发而来，基于正态分布的理论原理，解决了静态基线配置困难，准确性相对不高的缺点。动态基线配置简单，选取动态基线的生成对象，开启流量自学习功能，经过一段时间对网络特征流量的学习，系统自动生成一条随流量特征变化的曲线。如图3.2展示了静态和动态基线的样式，动态基线是一条更贴近于实际流量的曲线：

**时间**

固定基线（红）

实时流量值（黑）

动态基线（蓝）

**流量**

告警1

告警3

告警2

图3.2基线告警示意图

图3.2中展示了动态基线的三次告警，以流量告警为例，从告警1可看出由于静态基线的特征值通常设置为网络流量的平均值，无法感知网络情况变化，对于部分总是低于平均值的流量若出现异常突增，静态基线算法根本无法感知，更不会产生告警；从告警2、3可看出，静态基线产生的告警，由于基线值和实际值差异较大，无法真实反映流量异常的严重程度，。而动态基线是一条随不同时段的网络状况变化的曲线，更贴近于实际流量情况，特征感知明显，产生的告警更加准确。

3.4接口联动

当设备检测到异常流量时，会产生相应的告警事件，并支持对攻击事件的进一步处理提供四种方案：ADS牵引、BGP牵引、空路由牵引和不牵引。

ADS牵引。通过部署绿盟科技三位一体的解决方案，将NTA检测到的受攻击的目的IP通知给防护设备ADS，并由ADS设备下发牵引通告给路由器进行引流和清洗。

BGP牵引。NTA在部署时可以与路由器建立BGP邻居关系。通过选择BGP牵引可以由NTA向路由器宣告一条BGP路由更新条目，将受攻击的目的IP下一跳指向第三方清洗设备的牵引口。以此实现与第三方清洗设备的联动并对攻击流量进行牵引防护。

空路由牵引。当NTA与路由器建立BGP邻居关系后，如果攻击流量触发了空路由的牵引阈值，由NTA通过BGP向路由器宣告一条路由更新条目，路由器上下一跳为null。因此，当指定目的IP的流量到达路由器并匹配中此条路由时，会被黑洞。

不牵引。对受攻击的目的IP不进行任何牵引操作，路由不更新。

1. NSFOCUS NTA产品介绍

4.1产品概述

绿盟科技网络流量分析系统（NSFOCUS Network Traffic Analyzer, 简称 NSFOCUS NTA）是一款基于Flow技术，在绿盟科技长期对网络流量分析技术的经验积累上，面向运营商、数据中心等市场推出的流量分析检测产品。NSFOCUS NTA给用户提供网络状况的实时监控、网络攻击异常的实时告警，保证用户的网络环境安全。经过多年的发展，NSFOCUS NTA在客户中已经具备良好的口碑，成功案例覆盖国内和国际等多个区域。

4.2产品架构

NSFOCUS NTA的系统架构如图4.1所示，主要的架构分为三个部分，数据采集、分析检测和页面呈现。数据采集层负责对网络中的流量数据进行采集，提供多种主流格式的Flow及SNMP数据采集，并支持将SPAN数据转化成Flow格式进行分析。分析检测层负责对采集到的数据进行多种维度的分析，并通过分析检测判断流量数据中是否存在异常流量，对异常流量成分、来源等进行分析。页面呈现层，负责将分析检测层得到的结果分类在页面上进行呈现，如以告警、报表、日志等方式对分析数据进行筛选聚类，集中呈现。除此以外，还专门设置一个配置管理层对数据、配置、用户等进行集中管理。

4.3产品特色

4.3.1 全网状况实时监控

NSFOCUS NTA通过对网络中的流量数据进行采集和分析，能够对全网络状况进行实时监控，帮助网络管理员建立全网的视角，纵观网络的状况与趋势变化，及时掌握网络负载情况，及网络应用资源的使用情况。

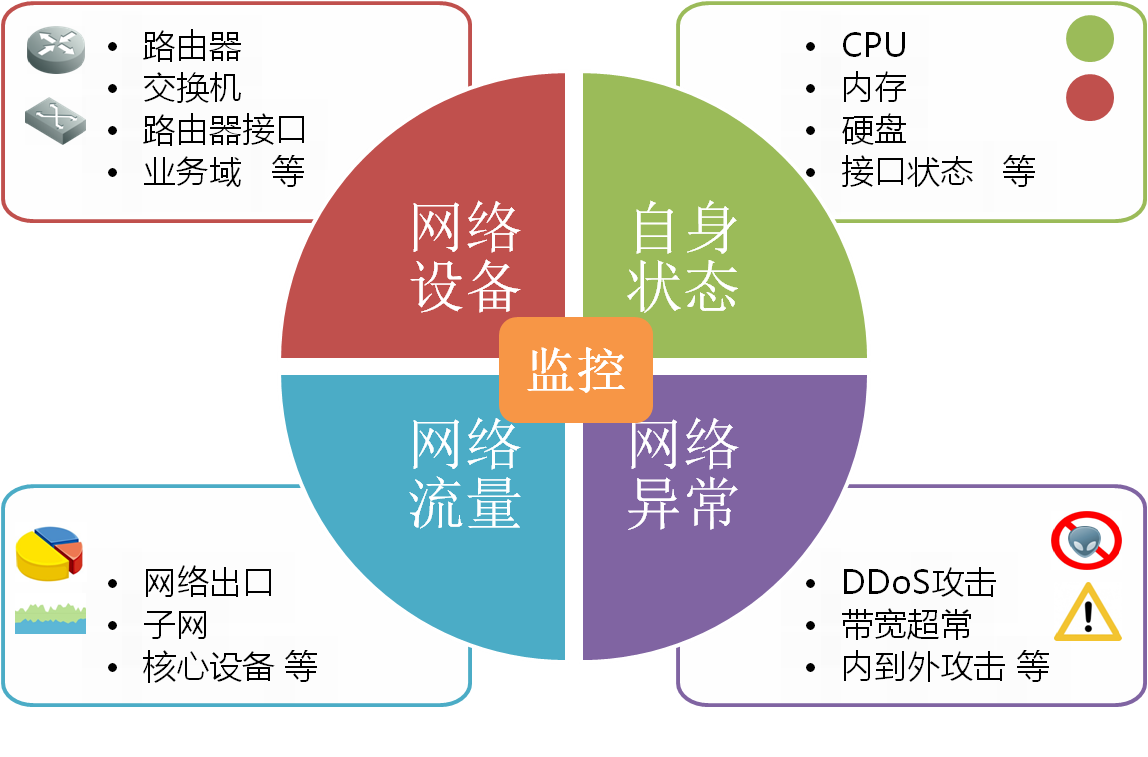


图4.1全网监控图

如同4.2所示，NSFOCUS NTA对全网的状态监控包括四个方面：

1. 网络设备的状态监控：对网络中的路由设备、接口状态、设备流状态进行实时监控，告知网络管理员网络是否畅通，负载如何、性能状况等概括信息。
2. 自身设备的状态监控：对NSFOCUS NTA自身的CPU、内存利用率、硬盘使用率、接口状态、每秒Flow数等进行实时监控，实时提供NSFOCUS NTA的运转信息。
3. 网络流量的状态监控：对网络出口、核心设备、特定子网等网络对象实时监控，提供多维度的流量分析。
4. 网络异常的状态监控：对网络安全运营的各种异常事件进行实时监控，及时发现网络瓶颈，找出网络性能下降的真凶。

4.3.2 准确详尽的流量分析

NSFOCUS NTA基于多年来对Flow数据的检测分析经验，不断改进流数据分析算法，保证应对差异复杂的现网环境均能够提供准确的分析。

网络流量状况监控的对象包括互联网出口、重要业务、特定子网、关键服务器等，分析的维度包括总流量、TOP IP，TOP端口/应用、TOP接口流量等。根据对象在不同维度的关联分析，了解其不同时段网络的成分信息、流向信息、趋势信息。NSFOCUS NTA的最小分析粒度仅为30秒，能实时反映网络流量的变化。系统提供长期的分析数据存储功能，能够存储长达一年的分析数据。基于长期的历史数据分析，很容易建立网络在时间、地域、流向上的分布与趋势特征，帮助运营商和数据中心等机构对业务需求、热点、走向等进行深入挖掘，提供网络决策者对网络的规划与设计的依据。

NSFOCUS NTA的流量分析不仅于此，对于触发告警的异常流量事件，NSFOCUS NTA能够迅速锁定受害IP，从攻击开始到结束，详细记录受害IP所遭受的攻击流量大小、流量组成情况，攻击来源和基于时间的变化趋势，对整个攻击事件发送的全过程进行取证。

4.3.3 强大的异常检测功能

针对网络中的异常状况，NSFOCUS NTA具备强大的异常检测功能，基于绿盟科技自主研发的异常检测算法，确保及时准确的发现问题。NSFOCUS NTA的异常检测功能十分强大，表现在以下几个方面：

* **检测类型丰富，全面覆盖骨干网上的所有威胁**

NSFOCUS NTA提供系统内置以及用户自定义两种的异常特征检测方式，除了系统内置的检测特征，用户可根据自行发现的网络异常特征进行自定义特征告警，系统支持多达128种自定义异常特征检测。异常检测的类型包括：流量超常、带宽超常、DDoS攻击、Dark IP异常、私有IP异常等。NSFOCUS NTA支持的DDoS攻击告警覆盖网络层和应用层，支持如SYN FLOOD、ACK FLOOD、HTTP FLOOD、SIP FLOOD等多达14种攻击事件告警，全面覆盖骨干网上的所有威胁。

* **快速发现攻击，记录攻击事件全过程**

NSFOCUS NTA能够快速对攻击事件进行响应，最快20秒内就能发出告警通知。告警的级别可按照严重程度预先定义为高、中、低三级，从而触发不同级别的告警。当网络遭受外部攻击时，NTA将从多个维度记录并分析攻击的原因、地点、强度等情况，如记录攻击前后网络流量的变化情况，攻击目标IP的流量变化情况，分析攻击的类型、攻击流量的组成情况等，从而回溯攻击事件发生的全过程，帮助网络管理员定位攻击源。

* **内网的安全保障**

攻击事件越演越烈、呈现多元化的发展趋势，内网、外网都存在发生攻击事件的可能。内部的攻击可能会堵塞网络出口带宽，造成网络瓶颈的严重后果，抵御内网攻击同样严峻。很多机构都已经意识到内网攻击的危险，如数据中心的政策要求，监控内部是否有对外发起的攻击事件；运营商的建设要求，除了知道是否遭受外省的网络攻击，也需要知道省内是否正在发起攻击。应对新的需求，NTA自主研发的智能检测系统，不仅能检测外部攻击，同时也对内部流量异常进行实时监控。根据事先定义的流量阈值，智能判断由内网向外网的访问流量是否超过正常范围，并准确定位内网流量超常的TOP IP。只有抵御网络外部攻击的同时，揪出内部攻击的元凶，全网的安全才能得到保障，NSFOCUS NTA的双向检测功能无疑给用户网络提供了双重的安全保障。

* **智能检测的算法**

由于静态基线配置参数困难，准确性不高。NSFOCUS NTA研发了智能的动态基线生成算法。通过一段时间对学习对象的流量特征分析、建模，智能生成该对象多维度的网络特征。

基线自学习的理论依据是：业务相似流量相似的主机在正常网络情况下，流量大小及特征保持稳态，以此为依据对该主机正常情况下的不同特征进行流量建模，通过一段时间的机器学习得到其正常状态的流量上限。自学习过程中系统自动记录网络的流量变化特征，进行基础数据建模，按照可信范围的数据设置置信区间，通过对置信区间内的历史数据进行分析计算，得到流量的变化趋势和模型特征。为了保证学习的流量特征符合正态分布，系统支持开启日历模式的数据建模，如设置工作日、双休日等日历时间点，针对不同的时间点进行自学习建模。同时系统支持对生成的动态基线进行手动调整，和日历自学习模式相结合，共同保证动态基线的准确性。

* **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。

* **攻击源IP详情查询**

NTA通过与云端NTI进行互联，实时查询攻击源IP详情。快速获取攻击源IP的关联域名、开放端口、ASN等详细信息。NTI数据实时更新，及时将捕获的数据信息更新到数据库中，确保的数据的丰富性和查询结果的准确性，为DDoS攻击的来源分布、防护策略制定提供了有效保障。

4.3.4 IPV4/V6双栈分析检测支持

IPV6的时代大幕正在逐渐开启，互联网向IPV6过渡已经开始进入实施阶段。国内作为IPV6商用主要力量的运营商部分已进入功能验证，大型互联网企业也搭建了自己的实验室平台，用于旗下各个业务进行IPV6的实验和试点。针对网络由IPV4向IPV6的变迁趋势，NSFOCUS NTA积极接应客户需求，产品支持对IPV4/V6的双栈分析及攻击检测，解除客户后顾之忧。

4.3.5 灵活多样的报表展示

为了支撑对分析、检测数据的全方位展示，NSFOCUS NTA开发了灵活的报表系统，可根据需要进行条件筛选、组合，生成多种类型的报表。系统提供实时和历史两种时间维度的报表，支持日/周/月/年及用户自定义时段的报表，一方面满足查看实时监控报表的需求，另一方面提供对历史数据信息的追溯与取证。报表有饼图、柱图、趋势图等展现形式，也支持面积图、折线图的图形自定义。

针对网络的流量状况，系统可以根据关注的不同网络对象进行选择，自定义报表的生成规则，从多维度、多视角对流量数据进行分析、展现。针对网络中的DDoS攻击，系统提供攻击目标、攻击告警次数、攻击流量、牵引情况等信息详细记录，并可根据攻击类型、告警级别、统计对象等进行数据筛选。系统还具备报表组合功能，帮助用户将关注的分析进行组合，生成所需的综合报表。

灵活多样的报表系统，全方位满足运维人员的各种需要。

4.3.6 完整的解决方案

绿盟科技针对电信运营商、大型数据中心对Anti-DDoS系统“可管理、可运营”的需求，推出了三位一体的解决方案。该解决方案由异常流量检测系统（NSFOCUS NTA）、异常流量净化系统（NSFOCUS ADS）及管理和取证系统（NSFOCUS ADS M）组成。

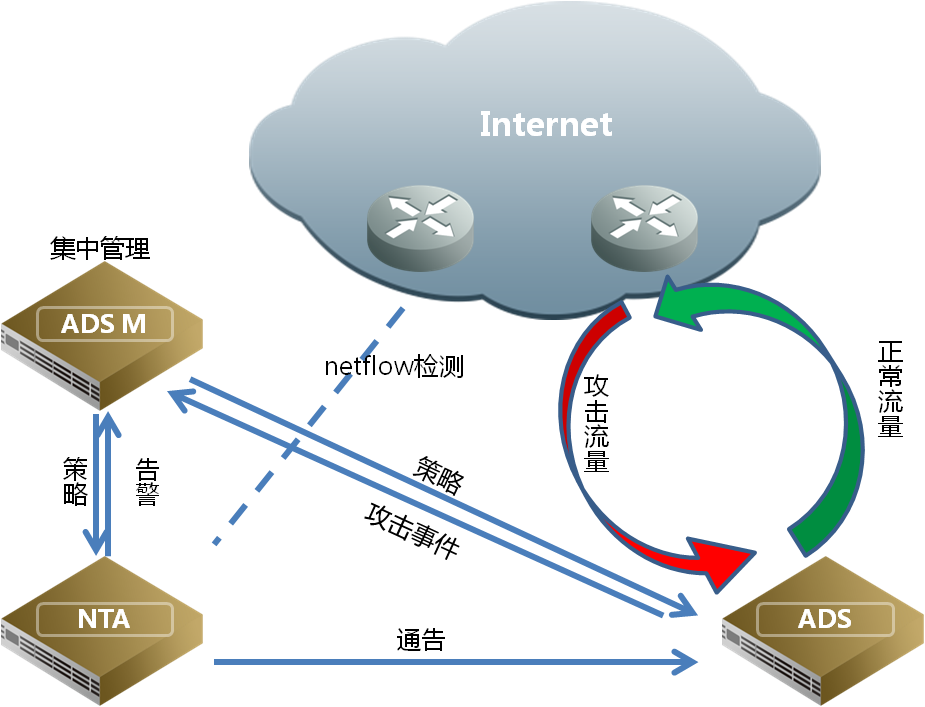


图4.2绿盟科技三位一体方案

NSFOCUS NTA负责进行网络监控、DDoS攻击检测的工作，当发现攻击时，NTA根据预先定义好的规则，智能启动和绿盟抗拒绝服务设备NSFOCUS ADS的联动机制，立刻将异常事件通知ADS。随后由ADS设备启动流量牵引机制，从路由器或交换机处分流可疑流量至ADS设备，在完成DDoS攻击的过滤后， ADS再将“干净”的流量注入回网络当中。另外，NTA还可以通过BGP Flow spec技术与路由设备进行联动，通过静态规格在路由器端对四层攻击进行压制、过滤、限速等，有效分配清洗资源，提高防护效率。

绿盟抗拒绝服务管理中心NSFOCUS ADS M负责对不同网络位置中的多台NTA和ADS设备进行集中监控，对NTA、ADS的策略进行集中管理，提供丰富的报表统一呈现攻击流量发现、清洗的全过程。ADS M更提供用户自服务系统，满足运营商利用DDoS做增值服务的需要。

* + 1. 增值运营带来收益

NSFOCUS NTA针对大客户或关键业务，可按路由器接口、IP（组）、AS号等定义业务域，基于增值运营维度的特性，提供基于业务域的攻击检测、流量分析功能。结合ADS M系列的管理产品，系统可提供特有的运营维护和自服务系统的增值服务平台，从而获取服务收益。运营商藉此对有强烈防护需求的大客户（网吧、证券、珠宝商场、电力、政府、酒店、IPTV提供商等）提供安全防护增值服务，而大客户可通过登录NSFOCUS ADS M开放的自服务界面，查看自己的实时网络流量、应用协议分布情况、攻击防护等关键业务信息。该平台，一方面提高了大客户对其系统安全状况的感知度；另一方面提升客户服务质量和内涵。

* + 1. 便捷智能的运维方式
* 即插即用

NSFOCUS NTA拥有智能的配置系统，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，无需手工输入，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，比如路由器物理端口号与名称的对应关系的自动生成。再比如NSFOCUS NTA先进的动态基线自学习算法，仅需简单配置，就能自动生成各项检查异常的参数特征。

系统提供了一个部署工具集，包括抓包工具、PING、路由器接口方向判断工具、检测范围生成工具等。可以大大简化部署操作

* 高性能，便捷运维

NSFOCUS NTA通过选用高性能的硬件以及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。网络管理员只需管理一台NSFOCUS NTA设备，即可监测电信级的高带宽网络环境，极大减轻了运维人员的工作压力。

* 专家级的运维支持

绿盟科技拥有网络安全运营多年的实践经验及专业的专家队伍，可提供快速的现场防御支持及攻击防御咨询/部署/培训等服务，不仅帮助客户建立坚固的防御系统、提供防御支撑，还帮助客户建立起专业的攻击防御团队。同时NSFOCUS NTA还支持接入绿盟科技云端ESPP平台，绿盟攻防专家可基于此技术接口进行7x24小时的安全值守，提供实时攻防响应服务。

4.4典型部署

对于电信运营商的城域网或各种专网的环境，NSFOCUS NTA通过接收网络核心路由器的Flow信息，对网络流量信息进行综合统计分析。 在大型行业、大企业园区等网络环境下，运维人员需了解出口网络以及各个子网的流量状况。每个接入路由器可以通过部署NSFOCUS NTA C系列产品将镜像的网络流量转换成Netflow数据，再进行全面的流量分析。以下是NSFOCUS NTA在运营商城域网、大型行业专网的的典型部署图：

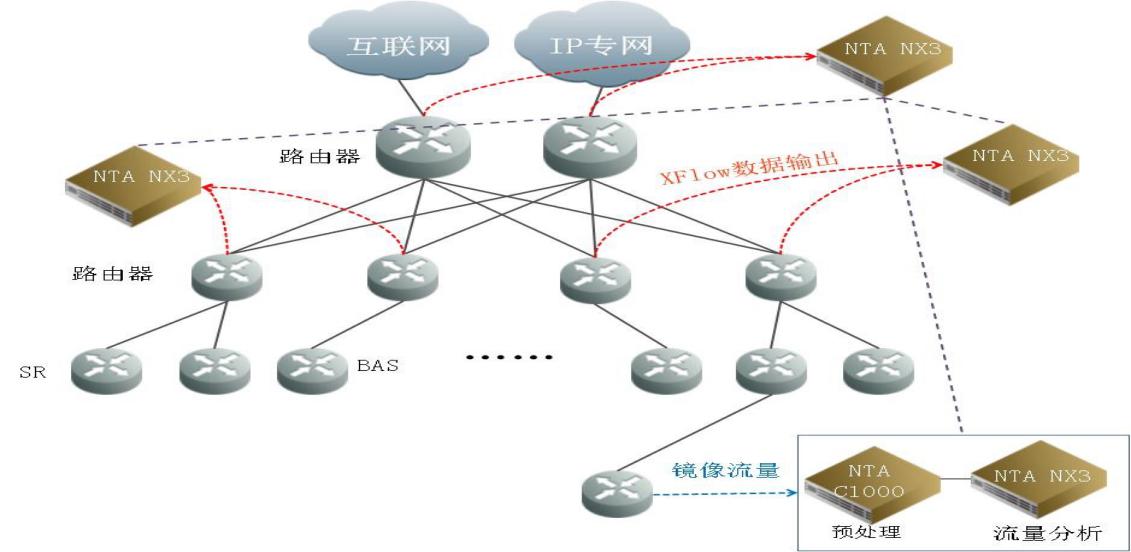


图4.3典型部署

1. 总结

随着互联网技术的迅猛发展，网络情况变得越来越复杂，IPV4向IPV6协议的过渡，应用的增加，带宽的扩张都不同程度增加了对网络的监控难度。而伴随着网络的发展，网络的安全形势也越来越严峻， DDoS攻击等各种网络异常事件严重威胁了数据中心、运营商等企业的利益。传统的网管工具无法监控电信级的大流量网络状况，不能详细分析复杂网络情况下的流量成分及发展趋势；面对越演越烈的DDoS攻击事件，更无法快速锁定攻击的来源和目标以及攻击的类型。

绿盟科技的网络流量分析产品可监测电信级的大流量网络带宽，具备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，能够及时有效的分析出DDoS攻击异常并产生告警，有效减轻网络复杂性造成的运维压力。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，多维度的流量分析统计结果，给予网络规划、业务规划方面的决策建议。有效帮助网络管理员便捷运维，保障网络的安全性，提供企业核心竞争力。