新形势下运营商 DDoS 安全防护解决方案

王奇文

中国电信股份有限公司北京分公司　北京

【摘要】针对网络安全事件愈发频繁，分析探讨了传统 DDoS 防护解决方案的不足，阐述了针对运营商环境下新的混合式解决方案以及实施方法。该方案基于一系列技术论证以及实验得出，并已在某运营商城域网内进行实施部署，实际缓解了城域网 DDoS 防护压力。对于运营商 DDoS 防护解决方案具有较强的参考价值。

【关键词】DDoS；Flowspec；SDN；城域网

【收稿日期】2022 年 12 月 26 日　【出刊日期】2023 年 1 月 21 日　【DOI】10.12208/j.aics.20230003

Solution of DDOS security protection for operators in the new situation

Qiwen Wang

China Telecom Limited Beijing Branch Beijing

【**Abstract**】In view of the increasingly frequent network security incidents, this paper analyzes and discusses the shortcomings of traditional DDoS protection solutions, and expounds the new hybrid solutions and implementation methods for operators. Based on a series of technical arguments and experiments, this scheme has been implemented and deployed in the metropolitan area network of a certain operator, which actually alleviates the DDoS protection pressure of metropolitan area network. It has a strong reference value for DDoS protection solutions of operators.

【**Keywords**】DDoS; Flowspec; SDN; Metropolitan area network

1 研究背景

当前网络安全形势愈发严峻，2020 年 8 月份，AWS 遭遇了目前已知最大的 DDoS 攻击，瞬时攻击流量已达到 2.3Tbps。2022 年 6 月至今，某运营商城域网共遭受疑似 DDoS 攻击 7 万余次，其中攻击时长超过 1 小时的多达 1 万余次，攻击流量超过 10 Gbps 的多达 400 余次。

运营商城域网往往承载着大量重要的党政军客户，同时每年承接各类重要的保障任务。如何在当前环境下，及时高效的应对 DDoS 攻击事件，成为目前急需解决的问题。

2 研究现状

传统城域网的 DDoS 防护方案依赖于专用的防护设备，采用“牵引+回注”的模式对攻击流量进行处置。系统通过 Netflow 协议对网络流量进行采集，对异常流量进行上报，网络维护工程师人工对上报数据进行分析并研判。确认为攻击后，通过 DDoS 专用清洗设备发布防护地址明细路由，由清洗设备对异常流量进行处置，并通过 vpn 路由的方式将处置后的正常流量回注至平台或用户网内。

此方案对于 DDoS 攻击防护的能力完全依赖于清洗设备上联的牵引带宽、以及设备对于异常流量处置的能力。例如某运营商专用 DDoS 清洗设备的防护能力约为 60G，因此当前可以独立处置最大 60 Gbps 的 DDoS 攻击流量。若攻击流量超出此范围，在传统的防护方案下，仅能通过客户或平台的出口链路来承载这些攻击流量。

传统方案下，若需要增加城域网自身的防护能力，只能通过扩容本地防护设备能力并扩容牵引链路。目前一台国产的 100G 防护能力的专用设备大

作者简介：王奇文（1988-）男，浙江人，汉族，中级工程师，硕士研究生，研究方向：IP 网络、网络安全

约需要 25 万元，相同能力的进口设备更是高达 100 万元。通过单纯的扩容防护设备来抵御 DDoS 攻击成本过高，无法满足运营商未来的防护需求。

因此需要一个更加合理的解决方案来满足运营商级别的 DDoS 防护需求。

3 研究内容：

3.1 关于 DDoS 攻击模式的研究

若需要尝试提出新的解决方案，首先需要对 DDoS 攻击的模式进行分析，DDoS 攻击主要可以归纳为以下两类攻击模式：

（1）流量型攻击：

流量型攻击是相对常见的 DDoS 攻击类型，主要是通过技术手段，如反射放大等方式，发送大量的 UDP 数据报文堵塞受攻击主机的出口，以达到拒绝服务目的，由于 UDP 协议无连接的特性，此类攻击通常以突发的大流量灌输的形势呈现。

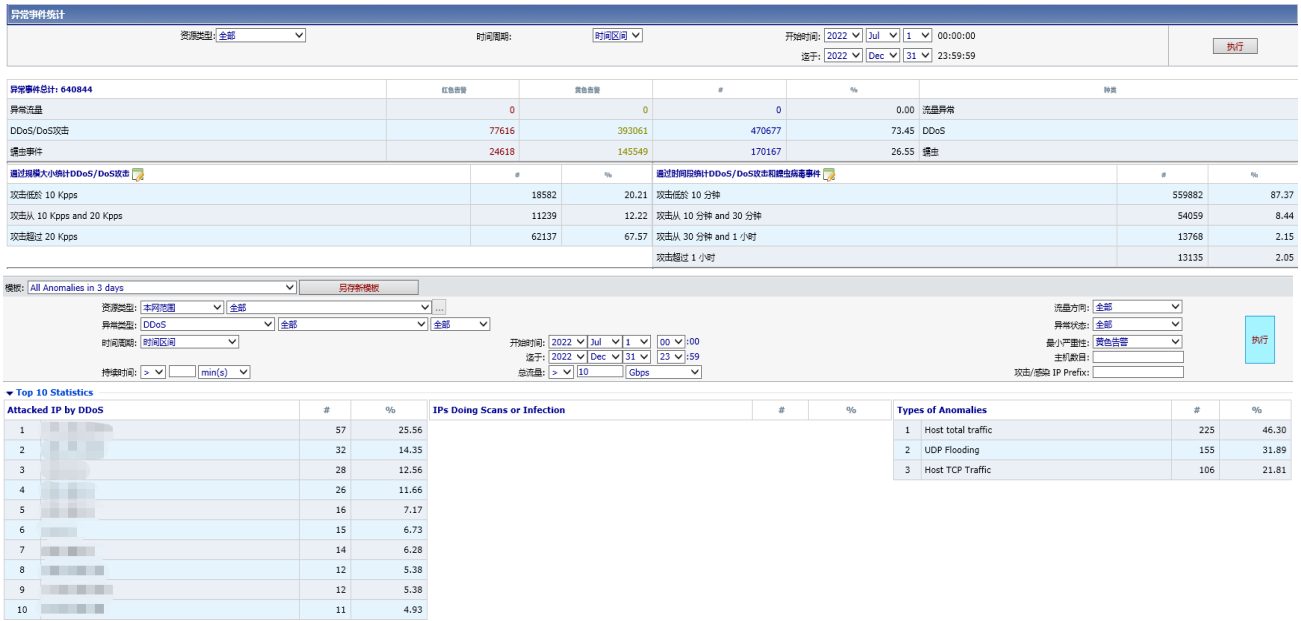

图 1 某城域网 2022 年 6-12 月 DDoS 攻击统计

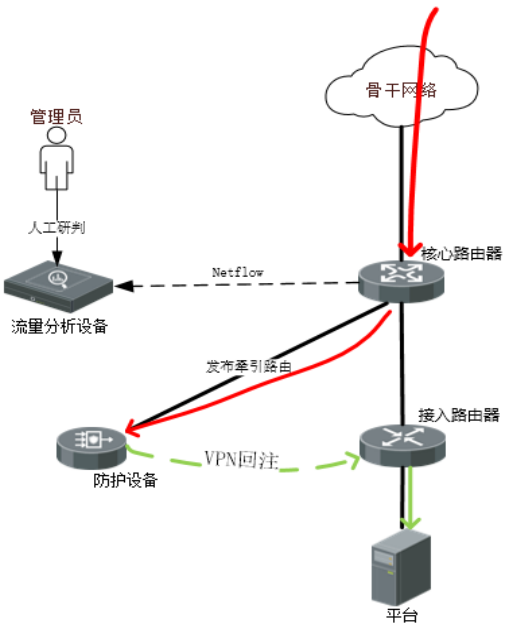

图 2 传统 DDoS 防护方案

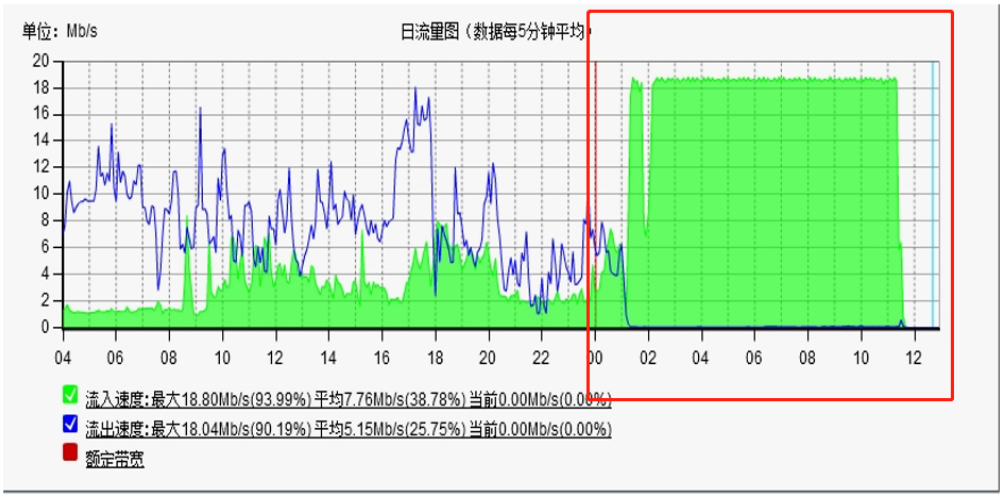

图 2 典型的流量型攻击场景

（2）连接型攻击：

连接型攻击是指通过技术手段，如 TCP 半连接等方式，向被攻击的目的主机发送大量的会话连接，占用目的主机的 CPU 性能，通过使目的主机无法响应其他请求来达到拒绝服务的目的。

连接型攻击一般以消耗主机资源为主，因此其特点为数据报文密集，但流量不会过高。针对连接型的攻击，多数平台或用户可通过其网内的防护设备，通过技术手段进行处置。

无论攻击类型有何不同，DDoS 攻击，尤其是流量型攻击往往可以分析出相对明确的 IP 报文五元组（源目 IP、端口以及协议），但往往由于清洗设备能力不足而无法进行有效的处置。

3.2 关于 Flowspec 技术的应用

Flowspec 全称为 Flow Specification，在 RFC 5575 中定义了解码的标准程序。 Flowspec 是 BGP 的扩展协议，通过 BGP Updata 报文进行更新。Flowspec 协议最初应用于流量调度的功能，其标准定义了 BGP 路由中的五元组（源目 IP、源目端口和协议）等 12 个属性。

通过 Flowspec 协议，我们可以直接“告知”路由器按需对指定的数据流进行丢弃、重定向或者限速。根据 Flowspec 的这一特性，我们可以利用此协议来通过路由器设备实现部分 DDoS 的防护能力。

前文已经进行过介绍，DDoS 流量型攻击往往会基于明确的 UDP 端口进行实施，通过 Netflow 流量采集分析系统可以采集到明确的攻击流量的五元组信息。因此结合 Netflow 数据针对攻击流量的源目 IP、源目端口以及协议类型进行组合限制，从而通过路由器对对应数据报文进行丢弃，完成 DDoS 攻击的防御工作。运营商核心层路由设备往往具备 T 级数据报文处理能力，因此利用核心层设备处置 DDoS 数据流具备实施的可行性。

综上所述，通过引入 Flowspec 技术，可以代替传统 DDoS 防御设备的部分功能，通过增加新的协议，减少 DDoS 防御系统的成本投入。在合理利用资源的同时，将各系统能力进行最大化利用。

3.3 混合型 DDoS 防御系统解决方案

（1）混合型防御模式

利用 Flowspec 可对 IP 五元组进行精确控制的特点，通过核心层路由器对流量型攻击进行有针对性的限止或者丢弃，可以有效的抵御针对网络层的各类攻击流量。通过利用核心路由器转发高性能，高转发效率的特点，减少对于专用 DDoS 防护设备的依赖。

在使用核心路由器对攻击流量进行处置的同时，保留传统 DDoS 防护设备能力，针对应用层以及部分基于连接的 DDoS 攻击进行处置，补足 Flowspec 技术的防护盲区。

（2）基于 SDN 的智能防御系统

混合防护方案共涉及三套系统：Netflow 流量采集系统、DDoS 防护设备、Flowspec 控制系统。通过采集异常流量-分析研判-策略下发-采集流量恢复状态四部分完成系统的防御闭环体系，在此体系

下，我们可以基于 SDN 的理念引入 SDN 控制器进入此循环内，通过 SDN 控制器对全套流程进行分析控制，智能防御系统简要流程图如下：

整套防御系统 SDN 控制器主要分为六个模块，分别为流量接收模块：用于接收 Netflow 数据流。数据分析模块：用于分析 Netflow’数据，对上报数据按照预设规则进行初筛。异常告警上报模块：对确认为异常结果进行上报，由人工进行二次研判。

Flowspec 模块：针对确认的攻击，生成对应 Flowspec 策略并向核心路由设备下发。

API 接口模块：针对确认的攻击，根据程序生成对应的 API 控制策略，启动专用 DDoS 防护设备。

对比传统的 DDoS 防护系统，SDN 智能防御系统工作拓扑如下图 5：

如工作拓扑所示，新一代的智能防御系统无需对现有网络进行过多的改造，仅需在原有系统功能之外添加一套 SDN 控制设备并与核心路由器、Netflow 采集器和 DDoS 专用防御设备逻辑相连，无需改变原有网络拓扑结构。同时，通过引入 SDN 控制分析能力，可以为维护人员提供更明确的结果输出以及便捷的操作方式，提升了安全事件的相应速度。同时此套解决方案也为日后与骨干网防御系统形成两级控制器体系，实现联动防护成为了可能。

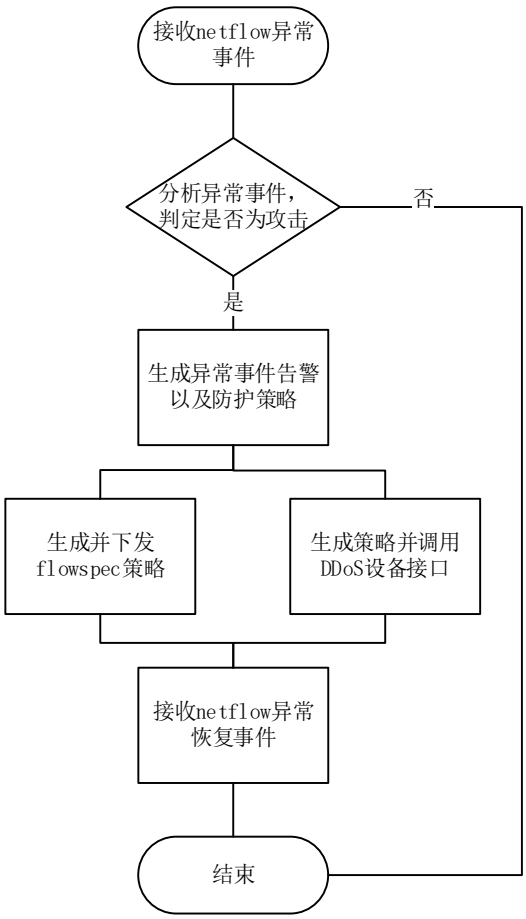

图 3 SND 智能防御系统工作流程图

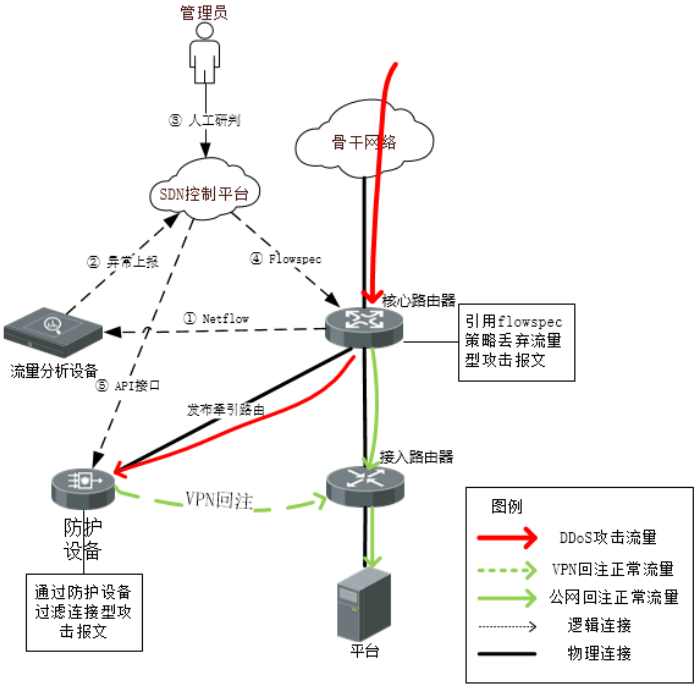

图 4 SDN 智能防御系统工作拓扑

4 结论

目前某运营商城域网已经按照本文中混合防御模式进行了部署，同时也在联合设备厂家启动了对于智能防御系统 SDN 模块的论证开发工作。在此体系架构下，该城域网利用仅 60Gbps 清洗能力的专用 DDoS 防御设备，实现了理论值 1.6T 的 DDoS 攻击的防御能力。同时由此系统衍生的自服务平台已将清洗服务能力产品化，为客户提供了有力的支撑和保障。未来随着 SDN 架构不断的成熟，智能防御系统还能进一步融入网络智能化的体系中，形成一套及网络运营、网络安全、云网融合于一体的智慧网络生态系统。

参考文献

[1] 网络安全法背景下网站安全管理与防护对策[J]. 余晖.农业工程技术,2021(30)

[2] 做好安全测评 加强网站安全建设[J]. 刘燕.理论学习与探索,2017(01)

[3] 网站安全风险及解决方案分析[J]. 侯俊东.数字传媒研究,2020(11)

[4] 亲历 DDoS 应急的回溯与心得分享[J]. 高杰欣.网络安全和信息化,2022(02)

[5] 云计算中 DDoS 攻防技术研究综述[J]. 岳猛;王怀远;吴志军;刘亮.计算机学报,2020(12)

[6] DDoS 攻击的发展与防御综述[J]. 王印玺;黄华雪.现代计算机,2021(02)

[7] 基于机器学习的DDoS攻击检测关键技术研究[J]. 方友志;谭坤淋.网络安全技术与应用,2021(06)

[8] 基于DDoS攻击的检测与防御实验系统的设计[J]. 丁智;肖宇.安徽电子信息职业技术学院学报,2021(03)