基于SRv6和流量负载的新型高防系统研究

Research on New Advanced Defence System Based on SRv6 and Traffic Load

徐宝辰[1]，余思阳[2]，李长连[1]，李发财[2]，赵　通[1]（1. 中讯邮电咨询设计院有限公司，北京 100048；2. 中国联通智网创新中心，北京 100046）

Xu Baochen[1]，Yu Siyang[2]，Li Changlian[1]，Li Facai[2]，Zhao Tong[1]（1. China Information Technology Designing & Consulting Institute Co.，Ltd.，Beijing 100048，China；2. Intelligent Network & Innovation Center of China Unicom，Beijing 100046，China）

摘　要：

现有的高防DNS引流方式，需用户手动修改DNS域名，SRv6基于路由转发，不需要在每个节点做标签配置，只需要设定SRv6的头、尾节点即可通过路由进行自行选路从而将数据包转发至目标。介绍了SRv6 Policy下unaware SF节点的应用模型，创新性提出在高防及WAF系统下采用SRv6引流的方式将攻击流量引入高防系统进行防护的模型，提供“即插即用”式的高防服务。

关键词：

SRv6；BGP Flowspec；WAF；高防；DNS

doi：10.12045/j.issn.1007-3043.2023.08.009

文章编号：1007-3043（2023）08-0038-04

中图分类号：TN915.08

文献标识码：A

开放科学（资源服务）标识码（OSID）：

Abstract：

The existing advanced defense DNS drainage method requires users to manually modify the DNS domain name. SRv6 is based on routing forwarding and does not require label configuration at each node，it can automaticly choose path through routing to forward data packets to the target only by setting the head and tail nodes of SRv6. It introduces the application model of unaware SF nodes under SRv6 Policy，and innovatively proposes a model that uses SRv6 drainage to introduce attack traffic into advanced defense systems for protection under advanced defense and WAF systems，which could provide "plug and play" advanced defense services.

Keywords：

SRv6；BGP Flowspec；WAF；Advanced defense；DNS

引用格式：徐宝辰，余思阳，李长连，等. 基于SRv6和流量负载的新型高防系统研究[J]. 邮电设计技术，2023（8）：38-41.

0 前言

高防广义上被定义为集成了防御4层（DDoS）+7层（渗透）攻击的高级防御系统，一般以服务器、安全资源池甚至数据中心的形态出现并提供安全服务。对于7层攻击的防护，高防中心内部通常以WAF作为主要防御手段，对扫描、SQL注入、XSS跨站、爬虫等攻击进行拦截，所以高防资源池或者高防数据中心通常以DNS引流为手段，需要防护用户手动修改被防护Web URL的DNS地址指向，将DNS指向为高防系统IP地址，从而将流量引入到高防资源池中来。

本文首先介绍了SRv6的一种应用场景——SRv6 TE Policy+业务链，并结合SRv6 TE Policy+业务链场景深入介绍通过SRv6技术作为流量牵引手段与高防相结合，从而简化了用户接入高防系统的方式，并提出笔者研究的最佳实践。

1 SRv6 业务链的概念与网络架构

1.1 SRv6 业务链的概念

SRv6（Segment Routing）定义为基于IPv6的分段路由，是一种基于Native IP的“隧道”技术。SRv6会将路径上的关键节点或链路定义为每个Segment，Segment

收稿日期：2023-06-08

字段被封装到SRH（Segment Routing Header）中并插入到原始的IP报文前变成新的IP报文头，数据报文会从头节点开始，按照生成的每个Segment组成的路径进行转发。当转发到尾节点的时候，报文中的SRH会弹出，从而暴露出原始的IP头，并按照原始IP报文根据路由进行转发。

例如，我们计划从A地出发去B公园游玩，打开导航软件，上面显示共有2条路可从A地到达B公园，其中1号路径路程短但比较拥堵，用时较多，2号路径路程长但车流压力不大，用时反而较少。如果从路程角度来计算会选择1号路径，如果从时间长短来考虑会选择2号路径。那么在出发时（A节点）就需要确定选择哪种策略（Policy），这种基于流量工程（案例中为车流量）角度来指定转发策略的方式就是SRv6 TE Policy。

SRv6 TE Policy有3个重要的要素，分别是头端（Headend）、颜色（Color）、尾端（Endpoint）。头端和尾端分别为A、B两地，用来确定SRv6 TE Policy的首尾两端地址，颜色是出行路径的策略，不同的路径会被进行不同的染色动作（在Color字段配置不同的值），需要根据自己的需求选择一条被染色的路径进行报文转发（比如需要利用更短的时间到达B公园的话，就需要选择路径2）。

通过SRv6的封装和Policy的选路，就可以让数据包流向其目标位置。类比图1中的各个地点，假设A地为攻击源、B公园为攻击目标（防护源站），那么高防系统所在的位置就会被置为广场或交叉路口。但是Policy技术只能让数据包经过高防系统所在地点，如何能让数据包真正进入到高防系统进行监测及防护，则需要SRv6 TE Policy+业务链的模型来解决这个问题。

SRv6业务链（SRv6 Service Function Chain，SRv6 SFC）为在SRv6中某些关键节点下挂其他设备（如WAF、防火墙等）提供解决方案。业务链分为控制平面和转发平面2部分，其中控制平面由控制器组成，控制器与下方所管理的路由器建立网络连接，并负责管理路由器状态、下发路由器指令等功能；转发平面即所有SRv6路由经过的网络节点，对于业务链来说分为以下几种设备类型：SC（Service Classifier）、SFF（Service Function Forwarder）、SF（Service Function）、SFC Proxy（业务代理设备）。SFF和SFC Proxy作为SRv6 TE Policy中重要的节点，必然有自己的SID（Segment ID）。重要节点的SID称为Endpoint SID，简称end SID。在业务链中，SFF及SFC Proxy的end SID的类型为end.AS，其作用为暂时剥离SRH暴露Payload转发至指定出接口并缓存Segment List，当流量转发回SFF节点时重新将缓存的Segment List添加至刚才的数据包重新成为SRH。SFC Proxy节点cache SRH过程如图2所示。

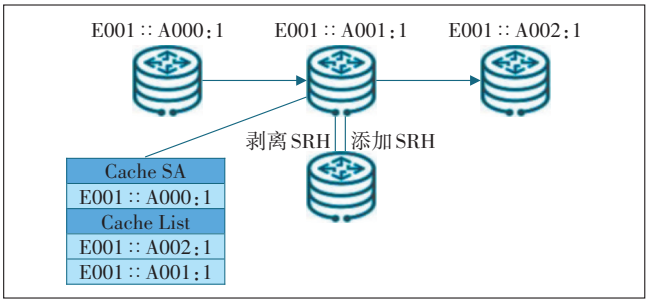

图2　SFC Proxy节点cache SRH过程

1.2 网络架构

业务链可以解决SRv6 TE Policy链路中下挂其他服务的问题，SFC流量走向如图3所示。

流量从R1发起，在R2（Policy头节点）进入业务链，由于下一跳为SFF节点，所以流量并没有按照Segment List向下转发，而是先从SFF转发到其下挂的服务节点SF1和SF2，回到SFF节点后继续转发至R3回到尾节点并弹出SRH头部终结业务链。而当SFF节点下挂的安全服务并不支持SRv6功能时，SFF节点应

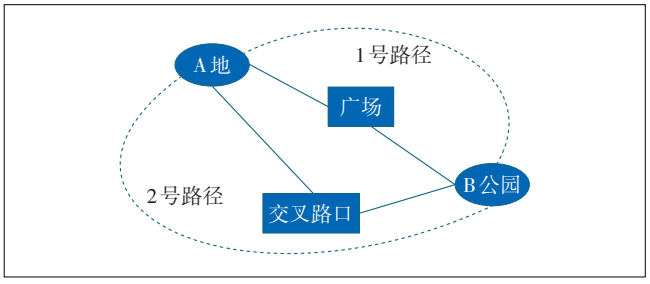

图1　Policy路径选择

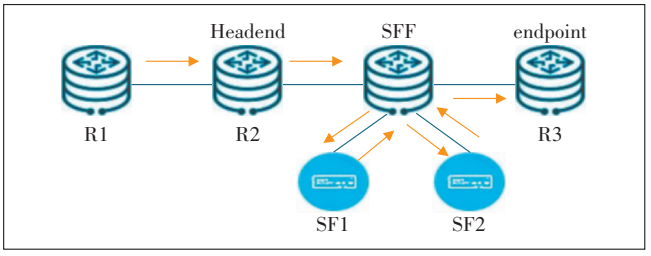

图3　SFC流量走向图

变为SFC Proxy节点，具有代理SRv6并缓存（cache）SRH头部的功能。

2 新型高防设计思路

针对SRv6 TE Policy SFC的特点，可以知道SFF节点下可以下挂任何安全能力，包括具有SRv6功能的安全服务和不具备SRv6功能的普通安全服务，这使得SRv6 TE Policy SFC技术的普适性大大增加。由于现在市面上的安全能力普遍不具备SRv6功能，所以本文以SRv6 TE Policy SFC unaware架构为基础，设计了基于SRv6 TE Policy+流量负载设备的新型高防资源池架构。

新型高防架构分为2个部分：安全资源池外的流量牵引部分以及安全资源池内的流量调度部分。安全资源池外的流量牵引部分以SRv6 TE Policy SFC技术为主，策略路由（PBR或BGP Flowspec）为辅来完成，首先需要将下挂高防服务的路由器SR（Service Router）以及多台高防业务需求区域路由器AR（Area Router）建立SRv6 TE Policy，在建立Policy后，SR承担了SFC Proxy的角色，负责与高防资源池内部对接并将SRv6中携带的Payload转发至高防资源池内。AR利用PBR将所需要防护的业务流量转发至Policy中从而使得被防护流量进入业务链。根据业务链中Segment List流量将会被转发至SFC Proxy节点，SFC Proxy会根据end.AS将Source Address、Segment List缓存并将Payload转发至高防资源池内部，而后将经高防系统清洗后的流量重新加载缓存起来的SRH继续根据Segment List转发至Endpoint。新型高防安全资源池外流量走向如图4所示。

安全资源池内流量主要依靠流量负载设备进行调度。数据报文经过SFF节点后剥离SRH将Payload以及原始报文IP暴露给高防安全资源池内部设备。如果在新型高防资源池出口处部署一台流量负载设备就可以与SFF设备对接，也可以在高防中的WAF接

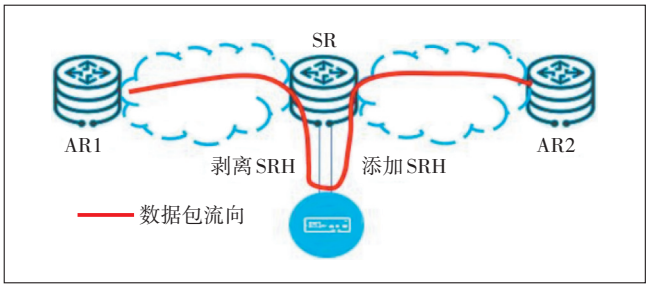

图4　新型高防安全资源池外流量走向

收到流量前通过DNAT将目的地址修改为高防系统的IP，因为WAF只能接收目的地址是自己的数据报文，这样高防中的WAF才能够与流量发起者建立TCP连接。当WAF收到流量后通过自身的代理模式以及WAF的7层防护原理，会将数据包的源地址修改为自身IP地址，而目的地址修改为防护网站所对应的IP地址，随后数据包会根据目的地址查找路由转发至流量负载设备，并继续转发至SFF设备入接口。SFF设备会将报文通过cache list重新封装为SRv6报文并继续根据Segment List转发（SRv6部分详细转发流程已在上文提及，不做赘述）。新型高防安全资源池内上行流量走向如图5所示。

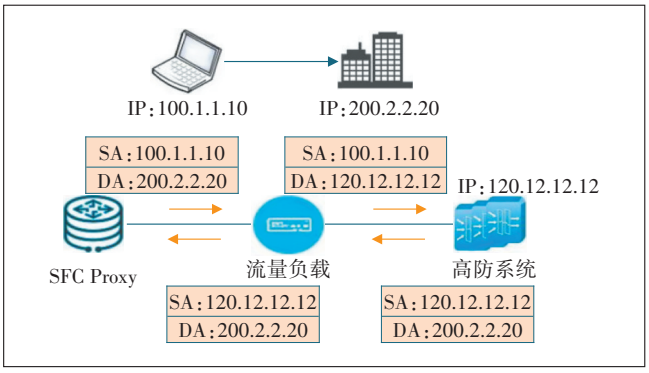

图5　新型高防安全资源池内上行流量走向

当下行数据报文从源站通过路由寻址再次返回高防资源池内时，数据报文通过流量负载设备直接进入高防资源池内WAF中，由于此时目的地址为WAF IP地址，故流量可直接进入WAF中并完成下行流量防护，至此高防系统与目标源站的TCP连接建立完成。数据包经过高防系统WAF后返回流量负载设备，负载设备将此数据包通过SNAT将源地址由WAF地址转换为防护网站地址，并根据路由转发至访问者终端，完成一次完整通信。新型高防安全资源池内下行流量走向如图6所示。

正如前文所述，高防是集成了防御4层（DDoS）+7层（渗透）攻击的高级防御系统，那么4层攻击的防御如何与新型高防的网络架构相结合呢？借鉴于抗DDoS的防御原则，防御手段越靠近攻击源，DDoS攻击的危害就越小，可以将抗DDoS的防御手段尽可能地向流量发起者方向部署。在新型高防系统中，最靠近流量发起者（攻击者）的地点为AR1，所以需要想办法在AR1集成抗DDoS的手段，经过流量清洗后再进入SRv6隧道。传统的抗DDoS流量牵引手段为明细路由

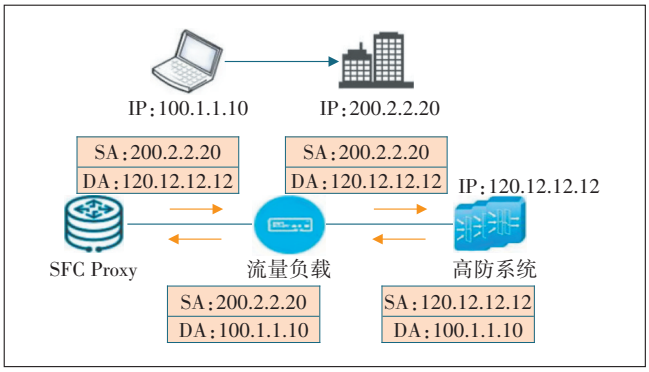

图6　新型高防安全资源池内下行流量走向

转发，即在原主干链路中将要进行清洗的流量通过明细路由的方式将下一跳指向抗DDoS流量清洗设备。流量清洗完成后数据流回注至另一台回注路由器或回注VRF。如果回注VRF配置在AR1上，那么则需要将本地的策略路由删除，并在回注VRF中再次配置策略路由将流量重定向到SRv6 Policy+业务链中。抗D+高防系统完整防护结构如图7所示。

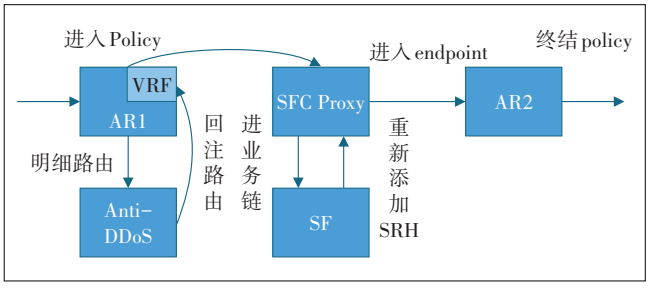

图7　抗D+高防系统完整防护结构

3 新型高防的优势与应用场景

3.1 新型高防的优势

新型高防系统与传统高防系统相比，具有以下几方面的优势。

a）被防护网站无需修改DNS域名指向，对于SaaS化安全服务厂商来说可以为用户提供“即插即用”式的高防服务。

b）可根据链路状态为用户提供不同等级的安全服务，由于链路采用了SRv6 TE Policy技术，所有Segment List包含的节点都可以以不同的Color进行染色操作，不同Color的链路可以根据用户需要进行不同的选择，为用户的SLA提供了更高级别的保障。

c）资源池内部的调度方式更加丰富，对于支持SRv6的安全设备，可以通过SFF节点直接进行流量调度，对于不支持SRv6的设备，也可以通过下挂其他流量调度设备进行流量负载以及流量编排功能。

3.2 新型高防的应用场景（云安全服务商）

对于云安全服务商来说，由于资源限制，高防中心或高防IDC不会在每个地区都进行部署建设，新型高防系统架构可以让流量调度手段更加丰富，使用SRv6进行流量牵引无疑是更好的选择，新型高防对于客户的接入性也更加友好。云安全服务商可以在运营商设备下挂载自己的网络设备及高防。当有用户需要接入高防系统的时候，可以先通过BGP将明细路由发送至运营商设备，将目的地址为防护用户的流量牵引至云安全服务商自有网络设备，然后通过策略路由或Flowspec的方式将流量重定向至SRv6 Policy中，从而通过新型高防系统网络架构完成用户的安全防护。

4 结束语

近年来，随着IPv6技术的发展以及国家对于IPv6技术的推进，越来越多基于IPv6的技术应运而生，SRv6就是其中之一。本文利用SRv6技术原理，结合现有技术及安全能力，将分布式部署的各种安全能力通过SRv6 TE Policy业务链技术整合到一起，更好地做到了资源整合、云网安一体等功能。同样，随着网络技术的发展，安全话题会越来越成为人们关注的焦点。利用优势技术，使网络安全能力越来越方便地接入普通用户的环境也是需要探索的重点之一，这样才会有更多的人使用安全防护能力，才能保证人们的资产越来越安全，越来越不会被侵犯。

参考文献：

[1] 推进IPv6规模部署专家委员会. SRv6技术与产业白皮书[EB/OL].[2023-06-06].https://www.waitang.com/report/31200.html.
[2] 骆兰军. IP网络系列丛书 SRv6[EB/OL].[2023-06-06].https://support.huawei.com/enterprise/zh/doc/EDOC1100193023.
[3] 郭泓伟. SRv6业务链的研究与应用实践[J]. 江苏通信，2023(2)：47-52+28.

作者简介：
徐宝辰，毕业于西安电子科技大学，学士，主要从事网络安全产品的研发工作；余思阳，毕业于北京邮电大学，工程师，硕士，从事网络安全体系规划及产品研究工作；李长连，毕业于西北工业大学，高级工程师，主要从事网络安全技术方向的研究工作；李发财，高级工程师，主要从事网络安全前沿领域研究、网络安全产品产品规划、架构设计及指导研发落地工作；赵通，毕业于中国农业大学，硕士，主要从事网络安全产品及安全技术方向的研究工作。