网络路由安全风险与防护对策研究

金宇翔
南京理工大学　江苏南京　100076

摘　要：本文简要描述了大型网络中的路由组织方式和路由协议类型，分析了路由安全事件的主要类型、作用机理和危害影响，并从加强业务体系管理、运用路由监测和预警手段、设置“白名单”路由管控策略3方面提出了防护对策。

关键词：路由安全；路由策略；RPKI

当今世界，网络发挥出巨大的经济、社会和经济价值，网络空间已经成为维护国家主权、安全和发展利益的战略高地。路由作为网络互联和稳定运行的基石，一旦遭受外部势力恶意攻击或是内部人员误操作，轻则业务受损、重则全网瘫痪，其安全问题不容忽视，亟需加强安全风险和应对策略研究。

一、网络路由安全风险

（一）网络路由组织概述

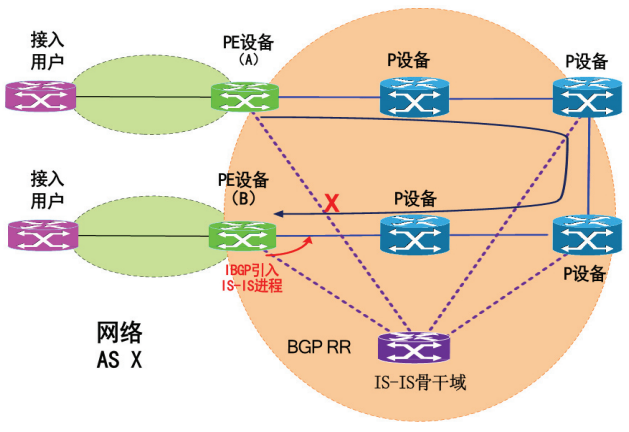
互联网技术（TCP/IP）起源于美国，由美国防部提出并组织研发，采用分布式自主节点和数据包独立传输方式，实现核战争背景下高度抗毁顽存的信息传输能力，路由协议在网络中发挥着传输导航的关键作用，是互联网核心技术。大型的运营商承载网、行业专网和军事网络内部，普遍使用的路由协议包括最短路径优先（OSPF）、中间系统到中间系统（IS-IS）和边界网关（BGP）三大协议，通常采取“拓扑路由+业务路由”分离技术架构，通过IS-IS协议发布PE、P设备环回和互联地址，形成拓扑路由，通过集中设置的路由反射器（RR）反射各PE设备iBGP路由，形成业务路由。大型网络和其它网络通常基于对等原则通过eBGP协议进行跨域路由传递，实现不同组织与网络间互联互通。

（二）路由安全风险

近年来，全球互联网和运营商网络频繁发生网络路由安全事件，造成重大经济损失和国家安全风险。例如，2020年俄罗斯电信运营商Rostelecom大量广播不属于其的IP地址空间的路由宣告，引发前缀劫持。数分钟内，波及Google、Amazon、Facebook等200余家互联网服务提供商。2022年初以来，俄乌间路由异常时间显著增加，据全球路由情报平台GRIP统计，2022年BGP路由安全事件呈现小幅增长，尤其是2022年3月，也同俄乌战争开始的时间恰好吻合。此外，运营商、行业专网中也曾多次出现过人员误操作导致全网性网络中断事件[1]。

我们认为，网络中的路由安全事件绝大多数因异常路由宣告导致，所谓异常路由宣告指网络因偶然（如管理员配置错误）或恶意原因而宣告或传播虚假或违反出站策略的路由信息（如NLRI、AS_PATH），这类异常信息视发布路由条目、扩散范围和安全策略等因素，可能对网络承载业务造成程度不等的失泄密、性能下降、业务中断等危害，严重的甚至造成全网性毁瘫。

异常路由宣告按类型可分为前缀劫持、路径劫持、路由泄露等，按范围分为域间路由异常、域内路由异常等，按照协议类型分为BGP路由异常和IGP路由异常（IS-IS或OSPF）等。以一类典型的运营商网络IS-IS前缀劫持事件分析，如图所示，PE设备、P设备均位于骨干区域内，通过IS-IS协议发布环回地址、互联地址，形成拓扑路由，同时PE设备通过与BGP RR建立iBGP邻居关系，发布接入用户的业务路由信息，实现用户间通信。



假使网络中IS–IS骨干区域任意一台具有业务路由的PE路由器（如B路由器），错误的在IS–IS进程内配置了引入IBGP路由命令，则会将其拥有的全网业务路由重发布至IS–IS骨干区域内，因默认的IS–IS协议优先级高于BGP协议，则全网任意PE设备（如A路由器）发送至任意用户业务网段的流量，均会被劫持至B路由器，最终因B设备和链路过载导致业务中断。由此分析，骨干域内只要任意1台PE设备错误配置1条命令，即可造成全网业务大面积中断、网络毁瘫，影响之大不可不防。

二、网络路由安全防护对策研究

我们认为，网络路由安全防护应注重技术防护和业务管理双线并举，围绕“白路由”管控目标，构建完善“事前预防+事中监测+事发控制”三层路由防护体系，降低路由劫持发生的概率和影响，确保基础网络运行安全稳定。

（一）加强业务体系管理，杜绝人员误操作

经统计，85%以上路由安全事件均为运维人员无意间的误操作导致，为此需加强业务体系管理，通过组织人员技能培训、严格落实规章制度、提升高危操作审批权限、实行双人交叉验证等风险管控措施，有效杜绝误操作风险。此外，技术手段方面，通过IAM身份管理系统对运维人员合理划分角色和权限，通过Tacacs+等网络设备身份验证协议进行细粒度的操作命令控制，能够有效防止无关人员或低技能人员执行路由策略变更等敏感操作，确保网络稳定运行。

（二）引入路由监测手段，提升态势感知和预警能力

路由协议的监控和异常检测技术也是实时发现处置路由安全事件、感知评估网络运行态势的关键手段，通常包括路由数据采集、数据分析和异常检测、事件可视化呈现等环节。通过部署网络路由信息采集点、构建路由数字孪生体、引入自动化分析、知识图谱、AI人工智能等分析手段，实时采集、感知和监测全网路由，秒级自动判定非法路由发布，派发工单支撑运维人员第一时间介入处置，控制路由安全事件影响范围和持续时间。通过路由监测与感知系统，可提高网络路由的透明性和可审计性，实现路由事件发生时间、发生频率、持续时间以及产生、传播全过程记录，可为攻击检测和防御提供有力支撑，后续随着自智网络、IPv6+、人工智能等技术成熟，结合其它系统还可逐步向路由自配置、自修复、自优化方向演进发展。

路由监测与预警包含多种技术，以基础的路由采集环节为例，具体方式可包括几种：①通过与关键路由器建立IGP、BGP邻居方式，接收路由更新数据，形成特定时刻的周期性“快照”；②通过流量探针等方式提取IGP、BGP协议更新报文，监测路由变化，此方式还可截取恶意的协议攻击报文；③通过BMP、BGP–LS等监测协议获取路由信息。路由数据采集点需结合网络拓扑结构、路由组织等因素合理选取，确保采集数据的全面性、有效性，必要时可通过冗余采集、带外采集等方式保障数据采集的可靠性。

（三）设置路由防护策略，消减异常事件影响

根据不同类型路由异常事件特点和作用机理，提取合法路由特征，据此在网络关键点位预置“白名单”（即默认禁止、按需开放）式路由防护策略，使得网络中即使因误操作或恶意攻击产生异常路由宣告，也能够被防护策略拦截过滤，从而避免因路由劫持造成业务故障，或者大幅降低故障影响范围，通常包括以下几种措施：

1.IGP协议路由过滤策略

针对IS–IS协议或OSPF协议中误引入非法路由并传播至骨干网络的路由异常事件，可以通过在全网P设备、PE设备IS–IS或OSPF协议中配置路由过滤策略，杜绝或大幅降低可能的异常路由影响。

例如，针对一类常见的、重大的路由劫持案例，即将iBGP业务路由误引入IS–IS协议拓扑路由造成全网业务中断事件，可根据规划中业务路由和拓扑路由地址段的显著区别（通常位于不同的地址空间），在被保护的路由器IS–IS协议中配置路由过滤策略（华为设备为filter–policy），以“白名单”方式仅匹配合规拓扑路由的前缀列表，阻止IS–IS路由表中的可能出现的异常路由条目下发到IP路由表中，因此不会按错误路由转发IP报文，起到本机防护的效果。需要注意的是，根据IGP协议工作原理，异常路由的泛洪过程是不可过滤和阻止的，异常路由仍会扩散至IGP骨干区域，而未配置此路由过滤策略的其它路由器仍会受路由劫持影响，因此该保护策略需要在骨干域的全部路由器上统一实施[2]。

2.BGP协议路由策略

BGP协议主要用于跨域路由交互以及域内业务路由发布，具有较为丰富的路由控制能力，通常可在自治系统边界路由器（ASBR）或路由反射器（RR）等关键设备上加载路由策略实施保护。例如行业内网场景下，可根据不同自治域规划的IP地址段、AS号、团体属性值等，在域间eBGP协议出/入方向加载路由策略，实现前缀列

表、团体属性、起源AS号（AS-Path最右侧）三者绑定，预防跨域路由劫持事件，同样也可在路由反射器上对域内iBGP协议加载路由策略。

通过BGP协议路由策略，可以实施细粒度的路由控制，但在互联网等一些超大规模网络中，因自治域数量多、地址空间范围广，通过路由策略方式存在配置繁琐、易出错、不灵活等缺陷，甚至因设备的ACL容量、可加载路由策略数量有限等原因无法实施，此时需要使用RPKI等技术手段实现风险管控。

3.RPKI（资源公钥基础设施）

资源公钥基础设施（RPKI，Resource Public Key Infrastructure）是旨在提高BGP安全性的方法，它于2007年首次提出，并于2012年作为IETF RFC发布。RPKI建立了一种体系结构，可以为实体定义其合法持有IP地址和ASN，并通过密码学担保方式对授权一个或多个AS为其所持有的IP前缀发起路由起源认证。

RPKI架构其中最为关键的两个部分包括：创建ROA（Route Origin Authorisations，路由源授权）和通过ROV（Route Origin Validation，路由源认证）对BGP路由源的真实性进行验证，从而实现对无效、异常路由过滤。当前各厂商的主流路由器均支持RPKI功能，可以通过路由反射器或自治系统边界路由器等关键设备开启RPKI功能，并部署相关系统实施路由安全防护，具体措施包括：

1.登记注册地址和起源AS绑定关系

针对行业内网等可完全掌控的网络，按照“默认禁止、按需开放”的“白路由”管控策略，将所有用户单位业务网段、对应AS号在IP地址管理系统或其它系统上注册。

2.部署证书签发、证书存储、RP（Relying Party，依赖方）等系统

打通IP地址管理系统和相关系统接口，形成RPKI资料库，RP同步并验证RPKI证书和签名对象，而后将验证有效的ROA（即IP地址前缀和ASN的绑定关系）下放至自治系统边界路由器或路由反射器。当然，针对行业内网等集中管理、完全可控的网络，若能确保注册信息真实有效，也可不部署证书等密码学手段，仅部署RP和相关路由注册和管理系统即可。

3.关键路由器开启RPKI功能

在自治系统边界路由器或路由反射器等关键设备上开启RPKI功能，建立与RP的逻辑连接，接收ROA条目并缓存在路由器中，根据ROA条目对每条BGP路由执行ROV路由源认证。在行业内网中，为实现彻底管住每条路由的“白名单”管控效果，可在RP中添加1条0.0.0.0/0的默认路由并绑定1个实际不使用的虚拟AS号（如AS65535），这样所有未在系统中注册的明细路由均会校验为Invalid状态并不予转发，从而实现异常、非法路由的过滤，保护网络安全。

总结

路由协议是网络互联和运行的核心，路由安全问题直接关系网络运行基础，本文分析了常见路由安全事件类型和作用机理，针对性提出了路由监测预警和安全防护策略，以遏制和消除路由安全风险。

参考文献

[1]邹慧，马迪，邵晴，毛伟.互联网码号资源公钥基础设施（RPKI）研究综述[J].计算机学报，2022，45（05）：1100-1132.

[2]（美）Jeff Doyle，孙余强译.OSPF和IS-IS详解.人民邮电出版社，2014，ISBN：978-7-115-34788-6.