因特网边界 IPv6 ACL 配置实践

（上海期货交易所供稿）

作为本次金融行业 IPv6 改造示范机构，本单位深入贯彻中共中央办公厅、国务院办公厅印发的《推进因特网协议第六版（IPv6）规模部署行动计划》精神，按照一行两会《关于金融行业贯彻〈推进因特网协议第六版（IPv6）规模部署行动计划〉的实施意见》的要求，结合本单位信息技术系统的实际情况，在保障系统安全稳定运行的前提下，稳步推进应用系统与软硬件基础设施的 IPv6 改造，目前已基本完成面向公众的因特网业务系统的 IPv6 改造工作。

当前，网络安全形势日益严峻，在进行 IPv6 改造时，必须保证其安全性不低于传统 IPv4 网络。本单位在部署常规的 IDS、抗 DDoS、流量监测、防火墙等安全防护手段外，在因特网边界路由器部署了 ACL，该 ACL 不仅对业务数据流进行了过滤，也对 ICMPv6 等协议层流量进行了裁剪，目的是在最外层阻隔部分潜在的利用 IPv6 协议进行网络攻击的行为。

本文将对该 ACL 的部署实践进行探讨，由于笔者水平有限，难免出现错误和遗漏，欢迎对此提出批评指正。

一、 网络拓扑简介

本单位因特网生产业务系统主要包括门户网站、行情服务、投资者教育网站等。上述生产业务系统基于单播 TCP 协议向因特网用户提供服务，系统不向外主动发起连接。网络的简要拓扑如图 1（图中的 IP 地址非真实地址，下同）。

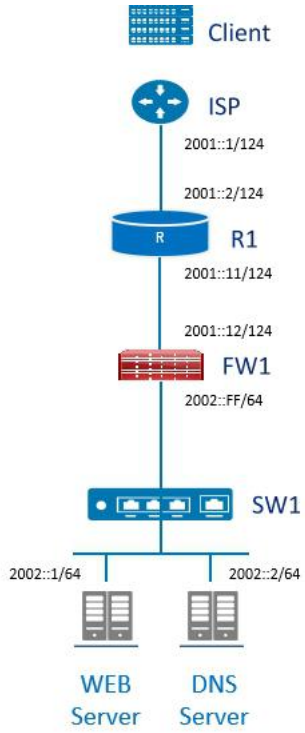

图 1　因特网网络拓扑

网络采用 IPv4/IPv6 双栈模式，其中 IPv6 全局单播地址（Global Unicast Addresses, GUA）由运营商分配（包括业务地址和互联接口地址），因特网边界路由器与运营商节点之间运行静态路由，互联接口地址手工配置。内部应用服务配置 GUA 地址，边界路由器不配置 NAT，把内部应用的路由静态指向防火墙。

二、 IPv6 协议新特性

IPv6 的最初目的是为了解决 IPv4 地址枯竭问题，但是除了提供更多的地址外，IPv6 还推出了一些新的功能和改进[1]，如邻居发现协议（Neighbor Discovery Protocol, NDP）[2]等。NDP 协议对于 IPv6 至关重要，它基于因特网控制消息协议第六版（Internet Control Message Protocol verion 6, ICMPv6）来实现其功能。此外，路径最大传输单元（Path Maximum Transmission Unit, PMTU）发现机制也需要由 ICMPv6 实现[3]。

可见，与 IPv4 网络中 ICMP 协议主要用于网络诊断和测试不同，在 IPv6 网络中 ICMPv6 是一项基础协议，其不仅应用于网络诊断和测试，许多 IPv6 运行所必要的功能都依赖于它，因此必须在每个节点上配置并传递。

然而，这些新的协议栈在丰富了功能特性的同时，由于设计者最初难免考虑得不够周全，网络和系统管理者对其也不够熟悉，因而可能带来了许多不可预见的安全风险。另一方面，从开放式系统互联通信参考模型（Open System Interconnection Reference Model, OSI）角度来看，从 IPv4 演进为 IPv6 最主要的变化在于第三层网络层(Network Layer)。因此，在 ICMPv6 网络协议层面的防护需要网络和系统管理者在 IPv6 网络改造过程中重点关注[4]。

三、 ICMPv6 和 NDP 协议详述

（一） ICMPv6 报文

ICMPv6 的协议号为 58，即 IPv6 报文中的 Next Header 的值为 58，ICMPv6 报文的格式如图 2[3]。

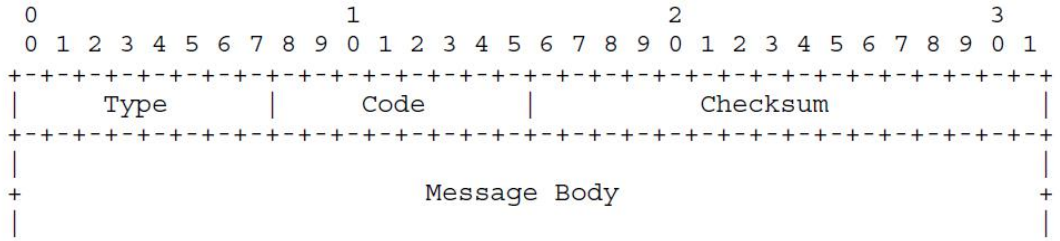

图 2　ICMPv6 报文格式

上述格式中:

- Type 表明报文的类型。
- Code 表示此报文类型细分的类型。
- Checksum 表示 ICMPv6 报文的校验和。

ICMPv6 报文分为“差错报文（Error Messages）”和“信息报文（Informational Messages）”两类，前者的类型号为 0-127，主要用于向源节点报告关于向目的地传输 IP 数据包过程中的报错信息，后者的类型号为 128-255，主要用于提供诊断功能和附加功能。目前已经定义的 ICMPv6 类型可见附表。

RFC 4443 定义了 ICMPv6 协议本身使用的报文类型，包括所有的差错报文 Type 1-4 和信息报文 Type 128-129，以下分别详细介绍。

1. 目的不可达差错报文（Type 1, Destination Unreachable）

中间节点在转发 IPv6 报文过程中，当节点设备发现目的地址不可达时，就会向发送报文的源节点发送 ICMPv6 目的不可达差错报文，同时报文中会携带引起该错误的具体原因。

具体原因由 code 值表示，分为:

Code=0：没有到达目标设备的路由。

Code=1：与目标设备的通信被管理策略禁止。

Code=2：未指定。

Code=3：目的 IP 地址不可达。

Code=4：目的端口不可达。

2. 数据包过大差错报文（Type 2, Packet Too Big）

源节点刚开始向目的节点发送数据报文时，尚不知道全程的 PMTU，源节点首先假设 PMTU 为其出接口的 MTU，发出试探性报文，当路径上某处转发节点的 MTU 小于当前假设的 PMTU 时，该节点就会向源节点发送 Packet Too Big 报文，并且携带自己的 MTU 值，此后源节点将 PMTU 的假设值更改为新收到的 MTU 值继续发送试探性报文，如此反复，直到最后的目的节点。数据包过大错误报文是 Path MTU 发现机制的基础。

3. 时间超时差错报文（Type 3, Time Exceeded）

IPv6 的 Hop limit 机制有点类似于 IPv4 的 TTL，在 IPv6 报文收发过程中，当路径上的设备收到 Hop Limit 字段值等

于 0 的数据包，或者当设备将 Hop Limit 字段值减为 0 时，会向发送报文的源节点发送 ICMPv6 超时错误报文，Code=0。

同时，对于分段重组报文的操作，如果超过定时时间，也会利用 ICMPv6 协议产生超时报文并发送给源节点，Code=1。

4. 参数问题差错报文（Type 4, Parameter Problem）

当目的节点收到一个 IPv6 报文时，会对报文进行有效性检查，如果发现问题会向报文的源节点回应一个 ICMPv6 参数错误差错报文。具体原因由 code 值表示，分为：

Code=0：IPv6 基本头或扩展头的某个字段有错误。

Code=1：IPv6 基本头或扩展头的 NextHeader 值不可识别。

Code=2：扩展头中出现未知的选项。

5. 回送请求报文（Type 128, Echo Request）和回送应答报文（Type 129, Echo Reply）

即通常使用的 Ping 报文。

除此这外，还有很多其他协议也在使用 ICMPv6 传递信息，其中最重要的是邻居发现协议 NDP。

（二） NDP 邻居发现协议

邻居发现协议 NDP(Neighbor Discovery Protocol)是 IPv6 的一个重要基础协议，它使用 ICMPv6 报文实现地址自动配置、邻居地址解析和状态跟踪、进行重复地址检测、重定向

等功能，类似于 IPv4 的 ARP，但比 ARP 功能更多。NDP 协议使用了 ICMPv6 类型 133-137，其详细说明见表 1。

表 1. NDP 协议报文属性

ICMPv6 Type 号	报文名称	发送者	接收者	作用
133	路由器请求 Router solicitation (RS)	节点	所有路由器(组播地址 FF02::2)	主机入网时，请求路由器发送 RA 信息
134	路由器通告 Router advertisement (RA)	路由器	若收到了 RS，则回应给 RS 发送者；其他情况，发送给所有节点(组播地址 FF02::1)	路由器定时发送或响应 RS 请求而定向发送，通告当前本机的链接参数，例如地址前缀、MTU 和 hop limits 等。
135	邻居请求 Neighbour solicitation (NS)	节点	被请求节点	节点请求邻居的链路层地址，同时确认邻居是否仍旧可达。也用于重复地

				址检测。
136	邻居通告 Neighbour advertisement (NA)	节点	若收到了 NS，则回应给 NS 发送者；其他情况，发送给所有节点(组播地址 FF02::1)	回应 NS 请求，告之本机；或主动通告链路层地址变化。
137	Redirect messages (RM)	路由器	节点	路由重定向

1. 通过 RS 和 RA 报文，新入网主机可以获得网段地址前缀和路由网关等信息，再通过重复地址检测（Duplicate Address Detection, DAD）机制，从而可以实现无状态地址自动配置（Stateless address autoconfiguration,SLAAC）。

2. 通过 NS 和 NA 报文，一是可以发现邻居的链路层地址，二是可以实现重复地址检测，三是可以检测邻居状态，发现邻居不可达（Neighbor Unreachability Detection, NUD）。

3. 路由重定向报文则是路由器向节点通告更优路径。

四、 IPv6 因特网边界控制方案

虽然 ICMPv6 协议在 IPv6 网络中具有不可或缺的作用，

但并非所有类型的 ICMPv6 报文在本网络拓扑场景中都具备实际作用。在网络边界对进入网络的 ICMPv6 报文进行裁剪，保留必要的 ICMPv6 报文，丢弃掉在本场景中没有使用的 ICMPv6 报文类型，可以进一步降低恶意攻击者利用 ICMPv6 构造攻击实现的可能性。

通过前两章可以看到，ICMPv6 的四类差错报文均由转发节点或目标节点发向源节点，由于本案例中的网络拓扑为单向提供服务的网络，因此所有会话均由外部 Client 发起，即源节点都在外部，因此在本拓扑的边界接口 inbound 方向正常情况下无需放行 ICMPv6 的四类差错报文。为了便于用户网络检测，可以允许目标为业务服务器地址的 Echo Requset 报文通过，但可以拒绝目标为路由器接口地址的 Echo Requset 报文（因为作为用户只要检测目标服务器是否可达即可，中间节点对其是透明的）；为了自身网络检测需要，允许所有 Echo Reply 报文通过。

另一方面，由于本案例中网络拓扑是固定的，所有 IPv6 地址及路由均手工配置，且不存在多路径的情况，因此在边界可以丢弃 RS、RA 及 RM 报文。但为了与运营商路由器建立并维持邻居关系，NS 和 NA 报文必须保留。

此外其他类型的 ICMPv6 报文在本案例单播 TCP 应用的环境均不必要。

五、 配置实践

有一些品牌的路由器支持在全局下选择性接收 ICMPv6 报文的功能，如华为路由器，其命令如下:

```
<Huawei> system-view
[Huawei] undo ipv6 icmp echo-reply receive
[Huawei] undo ipv6 icmp port-unreachable receive
[Huawei] undo ipv6 icmp host-unreachable receive
……
```

本文则采用在边界路由器 R1 与运营商连接的 G0/1 接口 inbound 方向部署 ACL 的方法实现对入网流量进行过滤，如图 3，主要有两点目的：一是本方法更为通用，可适用于各种品牌型号的路由器，二是可以将目的地非本路由器的“途经”流量也进行裁剪。在 outbound 方向则不作限制。

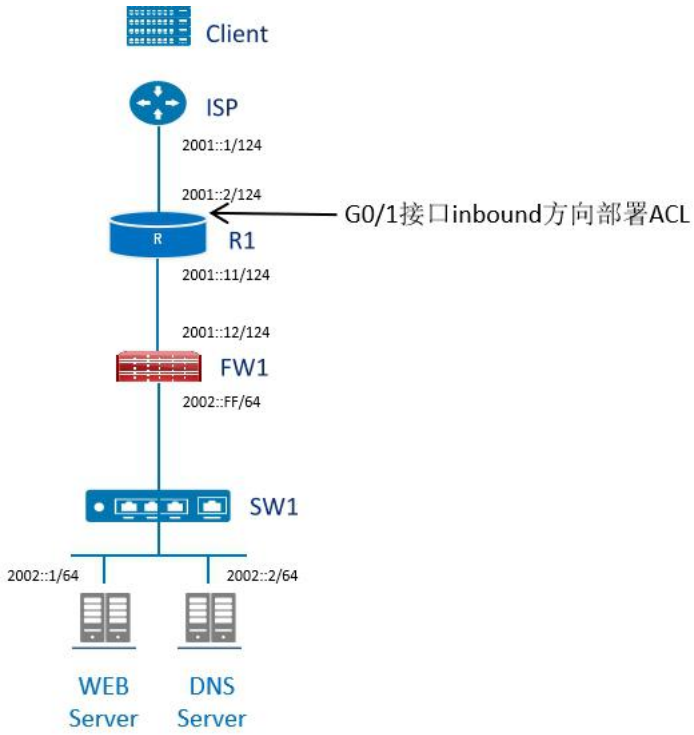

图 3　网络边界 ACL 部署图

（一） IPv6 ACL 配置示例

按上述方案，本案例实际的 ACL 配置如下，经实践部署证明可行:

```
acl ipv6 name INTERNET 1000                                  #  定义 IPv6 ACL
 rule 1 deny ipv6 source ::1/128                             #  拒绝源地址为环回地址的非正常流量
 rule 2 deny ipv6 source FF00::/8                            #  拒绝源地址为组播地址的非正常流量
 rule 3 deny ipv6 source FCE0::/10                           #  拒绝源地址为本地站点地址（Site Local Address）的非正常流量
 rule 4 deny ipv6 source FD00::/8                            #  拒绝源地址为唯一本地地址（Unique Local Address）的非正常流量
 rule 5 permit icmpv6 icmp6-type neighbor-solicitation       #  允许 NS 报文，用于建立 NDP 邻居
 rule 6 permit icmpv6 icmp6-type neighbor-advertisement      #  允许 NA 报文，用于建立 NDP 邻居
 rule 7 permit icmpv6 icmp6-type echo-reply                  #  允许 Echo 响应报文
 rule 8 deny ipv6 destination 2001::/124                     #  拒绝到路由器接口的一切其他数据包
 rule 9 deny ipv6 destination 2001::10/124                   #  同上
 rule 10 permit icmpv6 icmp6-type echo                       #  允许网络检测的 Echo 请求报文通过
 rule 30 deny icmpv6                                         #  拒绝上述以外的所有 ICMPv6 报文
 rule 100 deny ipv6 source FE80::/10                         #  拒绝源地址为链路本地地址（Link Local Addre）的非正常访问流量，由于部分 ICMPv6 报文如 NS、NA 会使用 LLA 进行通讯，因此该策略的排序稍稍靠后
 rule 101 permit tcp destination 2002::1/128 destination-port eq www  #  允许业务流量 1
```

```
 rule 102 permit tcp destination 2002::1/128 destination-port eq 443      #  允许业务流量 2
 rule 103 permit udp destination 2002::2/128 destination-port eq dns      #  允许业务流量 3
 rule 10000 deny ipv6                                                     #  拒绝其他一切数据包
#                                                                         #
interface GigabitEthernet0/1                                             #
 description To_ISP                                                      #
 traffic-filter inbound ipv6 acl name INTERNET                           #  在接口下调用上述 ACL
```

（二） 存在出向访问需求情况下的配置示例

若存在出向访问需求，即内网有节点作为客户端主动向外访问因特网资源。笔者认为在这种场景下需要在 ACL 中增加放行必要的 ICMPv6 四类差错报文，另外再放行必要的回包报文。仍旧以刚才的拓扑为例，配置调整如下（增加 rule 11-18,31-32）：

```
acl ipv6 name INTERNET 1000                                              #  定义 IPv6 ACL
 rule 1 deny ipv6 source ::1/128                                         #  拒绝源地址为环回地址的非正常流量
 rule 2 deny ipv6 source FF00::/8                                        #  拒绝源地址为组播地址的非正常流量
 rule 3 deny ipv6 source FCE0::/10                                       #  拒绝源地址为本地站点地址（Site Local Address）的非正常流量
 rule 4 deny ipv6 source FD00::/8                                        #  拒绝源地址为唯一本地地址（Unique Local Address）的非正常流量
 rule 5 permit icmpv6 icmp6-type neighbor-solicitation                   #  允许 NS 报文，用于建立 NDP 邻居
 rule 6 permit icmpv6 icmp6-type neighbor-advertisement                  #  允许 NA 报文，用于建立 NDP 邻居
 rule 7 permit icmpv6 icmp6-type echo-reply                              #  允许 Echo 响应报文
```

```
rule 8 deny ipv6 destination 2001::/124                    #  拒绝到路由器接口的一切其他数据包
rule 9 deny ipv6 destination 2001::10/124                  #  同上
rule 10 permit icmpv6 icmp6-type echo                      #  允许网络检测的 Echo 请求报文通过
rule 11 permit icmpv6 icmp6-type Network-unreachable       #  允许回送不可达差错报文 Network-unreachable
rule 12 permit icmpv6 icmp6-type Host-admin-prohib         #  允许回送不可达差错报文 Host-admin-prohib
rule 13 permit icmpv6 icmp6-type Host-unreachable          #  允许回送不可达差错报文Host-unreachable
rule 14 permit icmpv6 icmp6-type Port-unreachable          #  允许回送不可达差错报文 Port-unreachable
rule 15 permit icmpv6 icmp6-type Packet-too-big            #  允许回送 Packet-too-big 差错报文
rule 16 permit icmpv6 icmp6-type Hop-limit-exceeded        #  允许回送 Hop-limit-exceeded 差错报文
rule 17 permit icmpv6 icmp6-type Unknown-next-hdr          #  允许回送 Unknown-next-hdr 差错报文
rule 18 permit icmpv6 icmp6-type Unknown-ipv6-opt          #  允许回送 Unknown-ipv6-opt 差错报文
rule 30 deny icmpv6                                        #  拒绝上述以外的所有 ICMPv6 报文
rule 31 permit tcp tcp-flag established                    #  允许主动向外发起 tcp 访问的回包
rule 32 permit udp source-port eq dns destination 2002::2/128  #  允许dns 服务器向外发起dns 递归查询的回包
rule 100 deny ipv6 source FE80::/10                        #  拒绝源地址为链路本地地址（Link Local Addre）的非正常访问流量，由于部分 ICMPv6 报文如 NS、NA 会使用 LLA 进行通讯，因此该策略的排序稍稍靠后
rule 101 permit tcp destination 2002::1/128 destination-port eq www  #  允许业务流量 1
rule 102 permit tcp destination 2002::1/128 destination-port eq 443  #  允许业务流量 2
rule 103 permit udp destination 2002::2/128 destination-port eq dns  #  允许业务流量 3
```

```
 rule 10000 deny ipv6                                    #   拒绝其他一切数据包
#                                                        #
interface GigabitEthernet0/1                             #
 description To_ISP                                      #
 traffic-filter inbound ipv6 acl name INTERNET           #   在接口下调用上述 ACL
```

六、 总结

本案例实践采用在网络边界部署 ACL 的方法，对从因特网进入网络的 ICMPv6 等协议层流量进行适当裁剪，既保证正常业务不受影响，又可提升内部系统抵御安全风险的能力。

七、 附件

[1] S Deering, R Hinden. Internet Protocol Version 6 (IPv6) Specification[OL].[2022-3-9]

https://datatracker.ietf.org/doc/html/rfc8200

[2] T Narten, E Nordmark, W Simpson, et. Neighbor Discovery for IP version 6 (IPv6)[OL].[2022-3-9]

https://datatracker.ietf.org/doc/html/rfc4443

[2] A Conta, S Deeringand, M Gupta. Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification[OL].[2022-3-9]

https://datatracker.ietf.org/doc/html/rfc4443

[4] Scott Hogg. IPv6 Security[M]. San Francisco:Cisco Press,2009:15-70

[5] IANA. Internet Control Message Protocol version 6 (ICMPv6) Parameters[OL].[2022-3-9] https://www.iana.org/assignments/icmpv6-parameters/icmpv6-parameters.xhtml

附表 ICMPv6 报文类型汇总[5]

type	name	Reference
1	Destination Unreachable	RFC 4443
2	Packet Too Big	RFC 4443
3	Time Exceeded	RFC 4443
4	Parameter Problem	RFC 4443
5-99	Unassigned	
100	Private	RFC 4443
101	Private	RFC 4443
102-126	Unassigned	
127	Reserved for expansion of ICMPv6 error messages	RFC 4443
128	Echo Request	RFC 4443
129	Echo Reply	RFC 4443
130	Multicast Listener Query	RFC 2710
131	Multicast Listener Report	RFC 2710

132	Multicast Listener Done	RFC 2710
133	Router Solicitation	RFC 4861
134	Router Advertisement	RFC 4861
135	Neighbor Solicitation	RFC 4861
136	Neighbor Advertisement	RFC 4861
137	Redirect Message	RFC 4861
138	Router Renumbering	RFC 2894
139	ICMP Node Information Query	RFC 4620
140	ICMP Node Information Response	RFC 4620
141	Inverse Neighbor Discovery Solicitation Message	RFC 3122
142	Inverse Neighbor Discovery Advertisement Message	RFC 3122
143	Version 2 Multicast Listener Report	RFC 3810
144	Home Agent Address Discovery Request Message	RFC 6275
145	Home Agent Address Discovery Reply Message	RFC 6275
146	Mobile Prefix Solicitation	RFC 6275
147	Mobile Prefix Advertisement	RFC 6275
148	Certification Path Solicitation Message	RFC 3971

149	Certification Path Advertisement Message	RFC 3971
150	ICMP messages utilized by experimental mobility protocols such as Seamoby	RFC 4065
151	Multicast Router Advertisement	RFC 4286
152	Multicast Router Solicitation	RFC 4286
153	Multicast Router Termination	RFC 4286
154	FMIPv6 Messages	RFC 5568
155	RPL Control Message	RFC 6550
156	ILNPv6 Locator Update Message	RFC 6743
157	Duplicate Address Request	RFC 6775
158	Duplicate Address Confirmation	RFC 6775
159	MPL Control Message	RFC 7731
160	Extended Echo Request	RFC 8335
161	Extended Echo Reply	RFC 8335
162-199	Unassigned	
200	Private experimentation	RFC 4443
201	Private experimentation	RFC 4443
202-254	Unassigned	

255	Reserved for expansion of ICMPv6 informational messages	RFC 4443