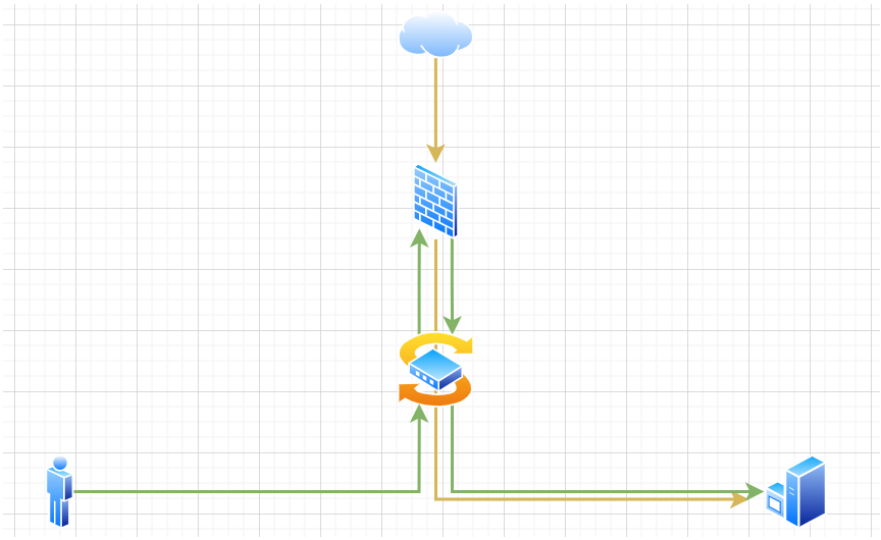
中低端防火墙NAT hairpin问题排查思路

会话同步 NAT 保存上一跳 策略路由 **孔凡安** 2024-01-22 发表

组网及说明

组网简化如下：



功能说明：

NAT hairpin功能用于满足位于内网侧的用户之间或用户与服务器之间通过NAT地址进行访问的需求。

开启NAT hairpin的内网侧接口上会对报文同时进行源地址和目的地址的转换。

上图绿色实线描述了NAT hairpin功能的访问路径，黄色实线描述的路径为正常DNAT的访问路径，即内网中的服务器对外部网络提供对应服务。

本文主要对前者进行探讨。

告警信息

不涉及

问题描述

NAT hairpin出现问题如何进行排查？

过程分析

原理说明：

1. 直接在内网口下配置*nat hairpin enable*，该配置相当于将公网口配置复制到内网口。

流量从内网口进来之后需要会走如下流程：SNAT---安全策略---DNAT---查找路由转发，SNAT后的地址为公网地址。

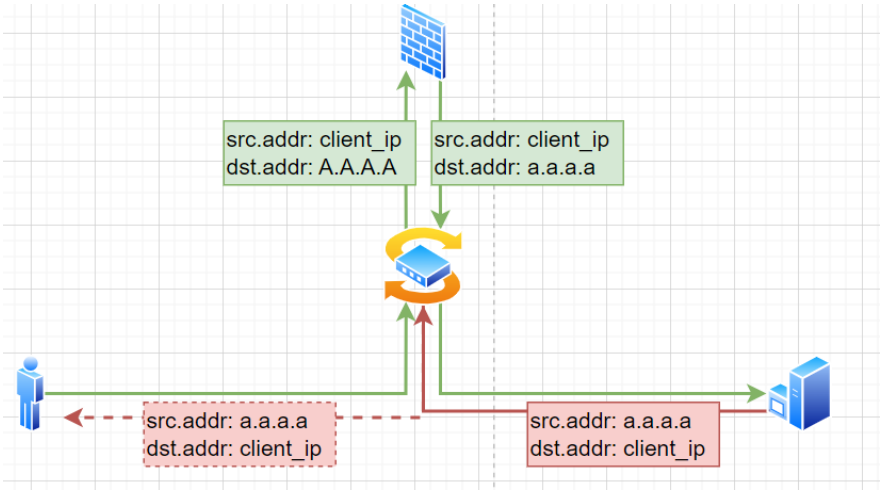
2. 内网口下发dnat+snat配置，举例如下：

```
#
interface Ten-GigabitEthernetx/x/x
 port link-mode route
 nat outbound
 nat server global A.A.A.A inside a.a.a.a

#
```

流量从内网口进来之后会走如下流程，DNAT---查找路由转发---安全策略---SNAT---查找路由转发，需要注意SNAT之后地址为内部私网地址。

此处略微展开一下，为何下发要添加snat配置呢？我们来看下如果不配置snat会发生什么？



源地址是client_ip，目的地址是A.A.A.A的报文经过防火墙NAT转换为，变成源地址是client_ip，目的地址是a.a.a.a。最终到达内部服务器。
内部服务器回应报文，源地址是a.a.a.a，目的地址是client_ip。在经过中间核心交换机的时候查找路由报文被直接转发到client端。
client收到这个报文会如何处理呢?
答案不言而喻，那就是丢弃。因为客户端请求的目的地址并非a.a.a.a，而是A.A.A.A。二者无法对应。
SNAT配置目的就是为了让核心将回程流量送到防火墙，会话还原之后将报文转发到客户端。该配置和服务器负载功能下发SNAT地址池配置原因是一样的。

3. 使用全局NAT（nat global-policy），举例如下：

```
#
nat global-policy
#
 rule name test
  description test
  source-zone Trust
  destination-ip host A.A.A.A
  action snat easy-ip
  action dnat ip-address a.a.a.a
  counting enable
#
```

流量从内网口进来之后会走如下流程：DNAT---查找路由---安全策略---SNAT---查找路由转发，SNAT之后的地址同样为内部私网地址。

无论是上述那种方式转换，在了解基本原理的前提下出现问题首先定位到对应NAT配置，查看对应NAT会话看NAT转换是否正常（*display session table ipv4 source-ip X.X.X.X destination-ip Y.Y.Y.Y verbose*（一定要带上verbose！））。
如果没有会话调整下筛选条件，防止遗漏；调整之后还是没有大概率可能被安全策略阻断。
有对应会话情况下查看NAT转换是否正常，Responder方向是否作了snat和dnat转换，如果均有对应转换则关注报文发送接口是否准确。
现网最常遇见的问题都是路由问题，报文从公网口发出导致业务不通。此处需要关注内网口是否有策略路由配置。

单纯查看会话无法看出问题的话，则需要进一步写acl进行debug排查原因。acl对应的rule尽可能包含所有的转换过程，示例如下：

```
client_ip----A.A.A.A（双向）
snat地址---A.A.A.A（双向）
snat地址---a.a.a.a（双向）
client_ip----a.a.a.a（双向）
```

如果对NAT hairpin转换过程不了解，建议以上rule均添加到对应acl中。常见的debug如下：

```
 <FW>debugging ip packet acl 3XXX      # 查看报文具体从哪个接口，哪个slot上来和发出的情况
 <FW>debugging ip info acl 3XXX        # 如果有丢包则会打印信息丢包的具体模块，
```

如果没有丢包则不打印
<FW>debugging aspf packet acl 3XXX # 如果报文状态不合法，则会显示被aspf丢弃，需检查流量来回是否一致
<FW>debugging security-policy packet ip acl 3XXX # 如果是对象策略则用object-policy，如果是包过滤则用packet-filter
<FW>debugging nat packet acl 3XXX #查看nat会话情况
如果没有会话，但是debug有报文上来，还需要收集：
<FW>debugging session session-table event acl 3XXX # 可以查看会话被删除的具体情况

解决方法

解决方案：

了解NAT hairpin实现原理，梳理流量转发路径，确保报文转发接口正常。

建议在内网口配置保持上一跳功能，对应命令如下：

ip last-hop hold命令用来开启转发保持上一跳功能。

undo ip last-hop hold命令用来关闭转发保持上一跳功能。

【命令】

ip last-hop hold

undo ip last-hop hold

【缺省情况】

转发保持上一跳功能处于关闭状态。

【视图】

三层以太网接口视图

三层以太网子接口视图

Dialer接口视图

以太网通道接口视图

Serial接口视图

【缺省用户角色】

network-admin

mdc-admin

vsys-admin

【使用指导】

接口上开启保持上一跳功能后，当该接口接收到正向流量的第一个IP报文，设备会根据流量特征以及上一跳信息，建立相反方向的快速转发表项，当反向流量报文到达设备进行转发时，可以直接通过该快速转发表项指导报文进行转发。

可以通过本命令对设备上支持IPv4转发保持上一跳功能的接口进行配置，也可以在系统视图下通过**ip global last-hop hold**命令对全局进行配置，只要全局和特定接口中有一个保持上一跳功能处于开启状态，则特定接口的保持上一跳功能开启，全局和特定接口的开关全部关闭，接口的功能才能关闭。

保持上一跳功能依赖于快速转发表项的建立，对于以太网类型的链路，如果上一跳的MAC地址发生变化，对应的快速转发表项需要重建才能使保持上一跳功能正常工作。

本命令不适用于MPLS组网中。

【举例】

开启转发保持上一跳功能。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ip last-hop hold
```