了解NAT以在IOS和IOS XE路由器上启用点对点通信

目录

[简介](#)
[背景信息](#)
[需要NAT穿越](#)
[用于NAT的会话遍历实用程序](#)
[NAT实施类型](#)
[NAT遍历和对称NAT问题](#)
[问题的解决方案](#)
[摘要](#)

简介

本文档介绍NAT(STUN)服务器对会话遍历实用程序的需求、与STUN服务器相关的网络地址转换(NAT)设置的类型、NAT如何导致此设置中的问题以及解决方案。

背景信息

NAT设备的主要用途是允许局域网(LAN)中具有私有IP地址的设备与公有地址空间（例如Internet）中的设备通信。但是，虽然NAT设备应该允许内部主机与公共空间连接，但是当涉及到点对点(P2P)应用程序（例如VoIP、游戏、WebRTC和文件共享，其中最终用户需要同时充当客户端和服务器来维护双向端到端通信）时，NAT为建立这些UDP连接提供了困难。通常需要NAT遍历技术才能使这些应用正常工作。

需要NAT穿越

Internet上的实时语音和视频通信 是 主流 现在，我们使用支持VoIP呼叫的几种常用即时消息工具(IM)。VoIP最初采用的一大障碍是大多数PC或其他设备都位于防火墙后面并使用私有IP地址。网络中的多个私有地址（IP地址和端口）通过带有 NAT. 但终端设备不知道其公有地址，因此无法在其VoIP通信中通告的私有地址上接收来自远程方的语音流量。

单方面 自地址固定(UNSAF)进程是一些始发终端尝试确定或固定地址（和端口），而另一个终端知道该地址（和端口），例如，能够 u使用协议交换中的地址数据或通告其接收连接的公有地址。

因此，正在讨论的P2P连接是UNSAF进程。 一种常用的P2P应用程序建立对等会话并保留该会话 NAT友好型是指使用可公开寻址的交汇服务器 注册和对等体发现目的。

用于NAT的会话遍历实用程序

根据RFC 5389,STUN提供处理NAT的工具。它为终端提供了一种确定由NAT设备分配的IP地址和端口的方法，该IP地址和端口对应于其私有IP地址和端口。它还为终端提供保持NAT绑定活动状态的方法。

NAT实施类型

据观察，UDP的NAT处理方法因实施而异。实施中观察到的四种处理方法是：

全锥：全锥NAT是指来自同一内部IP地址和端口的所有请求映射到同一外部IP地址和端口的NAT。此外，任何外部主机都可以向内部主机发送数据包，并将数据包发送到映射的外部地址。

限制锥：限制锥NAT是来自相同内部IP地址和端口的所有请求映射到相同外部IP地址和端口的NAT。与全锥形NAT不同，外部主机（IP地址为X）只有在内部主机之前向IP地址为X发送数据包时才能向内部主机发送数据包。

端口限制锥：端口限制锥NAT类似于限制锥NAT，但限制包括端口号。具体而言，只有当内部主机之前向IP地址X和端口P发送了数据包时，外部主机才能将包含源IP地址X和源端口P的数据包发送到内部主机。

对称：对称NAT是指从相同内部IP地址和端口到特定目标IP地址和端口的所有请求映射到相同外部IP地址和端口的NAT。 如果同一主机发送源地址和端口相同的数据包，但发送到不同的目的地，则使用不同的映射。 此外，只有接收数据包的外部主机才能将UDP数据包发送回内部主机。

考虑源(A、Pa)（其中A是IP地址，Pa是源端口）通过NAT设备与目标(B、Pb)和(C、PC)通信的拓扑。

NAT实施类型	Public 源时间 指定给(B、Pb(E)	公共源，目标为(C、Pc(E)	可以目标(例如： (B、Pb))将流量发送到(A、Pa)?
全锥	(X1,Px1)	(X1,Px1)	Yes
限制圆锥体	(X1，像素1）	(X1，像素1）	仅当(A， Pa)首先将流量发送到B时
端口限制锥形	(X1，像素1）	(X1，像素1）	仅当(A， Pa)首先将流量发送到(B， Pb)时
对称	(X1，像素1）	(X2,Px2)	仅当(A， Pa)首先将流量发送到(B， Pb)时

NAT遍历和对称NAT问题

STUN服务器响应STUN客户端发送的STUN绑定请求，并提供客户端的公共IP/端口。现在，此地址/端口 组合由STUN客户端在其点对点通信中使用 信令. 但是，现在， 终端主机 使用相同的私有地址/端口(假设为 已绑定 到公共IP/端口 在STUN响应中提供)NAT设备将其转换为同一IP，但如果是对称NAT，则转换为不同的端口 简单我NTATION 已使用。这会中断UDP通信，因为 信令 已根据p之前的端口。

思科IOS® 路由器' NAT 简单我NTATION 执行PAT时，默认情况下是对称的。 其他e前端，您会看到与这些UDP连接有关的问题 执行ping操作的路由器 NAT.

但是，Cisco IOS-XE路由器执行PAT时的NAT实施不对称。当您发送两个不同的 流具有相同的源IP和端口，但流向不同的目标，源会被NAT到相同的内部全局IP和端口。

问题的解决方案

根据此描述， 很显然， 如果执行 独立于终端 映射。

根据RCFC 4787： 使用 端点独立映射(EIM),NAT会为从同一内部IP地址和端口(X:x)连接到任何外部IP地址和端口。

从客户端上，当终端主机在两个不同的终端窗口中运行**nc -p 23456 10.0.0.4 4000**和**nc -p 23456 10.0.0.5 5000**命令时，如果您使用EIM，将会出现NAT转换结果：

```
Pro Inside global       Inside local            Outside local        Outside global

tcp 10.0.0.1:23456   192.168.0.2:23456  10.0.0.4:40000 10.0.0.4:40000

tcp 10.0.0.1:23456   192.168.0.2:23456  10.0.0.5:50000 10.0.0.5:50000
```

在这里，您可以看到源地址和端口相同的不同流量被转换为相同的地址/端口，而与目标端口/地址无关。

在Cisco IOS路由器上，您可以使用命令启用终端无关端口分配 **ip nat service enable-sym-port。**

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipaddr_nat/configuration/15-mt/nat-15-mt-book/iadnat-fpg-port-alloc.html

摘要

当您使用端口地址转换(PAT)时，Cisco IOS NAT实施默认情况下是对称的，当它传递P2P UDP流量时，可能会引起问题，该流量需要服务器（如STUN）进行NAT穿越。您需要在NAT设备上显式配置EIM才能使此正常工作。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。