IPSec VPN 双边穿越 NAT 解决方案探讨①

Solutions to IPSec VPN Double NAT-Traversal

张爱科 (柳州职业技术学院 信息工程系 广西 柳州 545006)

摘 要： 鉴于 IPSec VPN 双边穿越 NAT 的现象广泛存在和目前 IETF 尚未对此提出任何可行的解决方案这一现状，本文提出了三种方案，并详细介绍了 IPSec VPN 通过各独立网络上的代理服务器实现双边 NAT 穿越和借助双方信任的中间服务器实现双边 NAT 穿越这两种方案的具体实现过程。

关键词： IPSec VPN NAT 双边 NAT 穿越

1 引言

基于网络安全协议(IPSec)的虚拟专用网络(VPN)技术和网络地址转换(NAT)技术[1]是当前网络中应用广泛的两种优秀技术。IPSec 协议在 IP 层实现数据的通信安全，为上层协议提供透明的服务，是 VPN 技术的安全基础。NAT 技术很好地解决了 IPv4 网络因设计缺陷引起的 IP 地址短缺问题，同时隐藏了内部网络地址信息，具有一定的安全保障。

在实际应用中，基于 IPSec 的 VPN 技术和 NAT 技术经常需要在网络中并存，然而，IPSec 和 NAT 这两种针对不同问题的协议在兼容性上存在先天不足。IETF 针对 IPSec 穿越 NAT 制定了一系列的标准和草案，其中 UDP 封装格式可以在一定程度上较好地解决 NAT 穿越的问题[2]。但是，实现该标准的前提是必须有一端的设备地址是公网地址，如果 VPN 设备两端都在 NAT 后面，都是私有地址，IPSec VPN 需要双边穿越 NAT。当双 NAT 存在时，由于出于安全性考虑，NAT 只允许由内到外主动发起连接，而不会接受由外向内的主动连接，因此造成 IKE 的主动协商包无法经过 NAT 到达响应方，这是 IPSec VPN 双边 NAT 穿越的技术难点所在[3]。对于这一难题，IETF 并没有给出任何可行的解决方案，这对我国这种 IP 地址匮乏、大量使用 NAT 设备的环境来说有很大的影响。

针对上面的问题，下面探讨一些方案来解决。

2 映射静态地址

在公网地址宽裕的的情况下，可以通过 NAT 作静态地址映射。在这种情况下，NAT 设备在 VPN 设备的私有地址和公网地址之间建立一一映射，使得此 VPN 设备能被处于 NAT 后面的另一台 VPN 设备找到，从而协商并建立 VPN 通道。如果两边的公网地址都宽裕，可以考虑都为内部的 VPN 设备作静态映射，这样双方都能主动发起连接进行协商并建立 VPN 通道。

在作静态映射时，需要把端口也作相应的映射，因为 VPN 协议的协商端口是 UDP 端口 500，在 NAT 环境中是 4500。如果映射时未作端口映射，会造成 VPN 协商无法成功。

这种方案只是把私有 IP 地址隐藏起来，对内部网络提供一定的保护作用，并不能节省宝贵的全局 IP 地址资源，因此在实际应用中并不多见。

3 通过代理实现NAT穿越

组网示意图如下图 1 所示：

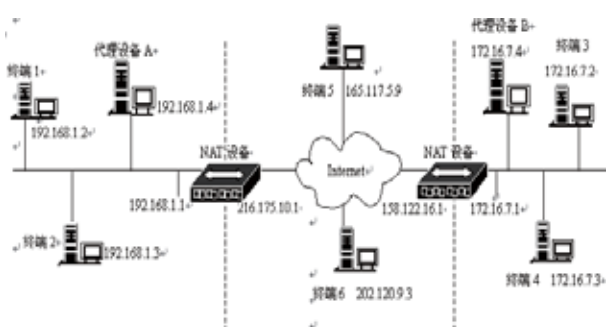

图 1 通过代理实现 NAT 穿越

① 基金项目:2008 年度广西教育厅科研项目(200808LX240)
收稿时间:2009-01-09

这里我们借鉴了交互式连通建立 ICE(Interactive Connectivity Establishment)的方法[4]，在每个独立的网络上分别设置代理服务器，通过这些代理服务器来完成通信通道的建立。通过代理实现 NAT 穿越的具体过程如下。

(1) 第一步：代理设备发现过程。在设备启动完成之后，代理设备首先会查找本网络的邻居网络的代理设备。如图 1 所示，代理设备 A 和代理设备 B 之间互为邻居网络。找到邻居网络的代理设备之后，就会在 NAT 设备上建立起会话，这样代理设备之间的通信通道就建立起来了。由于 NAT 设备上建立的会话有一定的生命周期，所以互为邻居的代理设备之间在会话生命周期内将会通过保活数据包来维持这个会话的生命周期。

(2) 第二步：代理设备间的 NAT 类型侦测过程。互为邻居的代理设备之间建立起通信通道之后，接下来要做的一件事就是互为邻居的代理设备之间的 NAT 类型的侦测。NAT 类型的侦测可以采用试探法和最高匹配原则来进行。如代理设备 A 首先按试探规则发送不同的数据包，再由代理设备 B 根据收到的数据包返回相应的信息。代理设备 A 按最高匹配原则确认邻居代理设备之间的 NAT 类型，并将侦测的结果发送给代理设备 B。

(3) 第三步：通信终端间通信的 NAT 类型判断过程。终端发起的连接请求首先发送给所在网络的代理设备，代理设备确认目标终端所处的位置，如果目标终端是处于本网之内，则代理设备直接建立起终端间的通信通道；如果目标终端不属于本网络，则根据预先建立起的网络路由找到下一个可能接收处理的代理设备，并将连接请求和该连接的 NAT 类型转发给该代理设备，重复这一过程，直到找到目标终端所在网络的代理设备。这个连接请求可能通过多重 NAT 设备才能到达目标网络，在这个过程中 NAT 类型按照最高适应原则传递。如图 1 所示，如果终端 1 向终端 4 发起连接请求，则连接请求发送的过程分别是终端 1、代理设备 A、代理设备 B、终端 4。代理设备 B 最终按照最高适应原则确认连接的 NAT 类型。

(4) 第四步：通信终端间的通信通道建立过程。确认了终端连接的 NAT 类型之后，将会由代理设备根据不同的情况在通信终端之间建立通信信道。如图 1 所示，如果终端 4 首先向终端 1 发起连接，假定终端 1 和终端 4 之间的 NAT 类型为完全圆椎形 NAT。终端 4 发送连接请求到代理 B，代理 B 将 NAT 类型和连接请求通过预先建立的通信通道(在第一步就已经完成了代理设备之间通信通道的建立)发送给代理 A，代理 A 再将连接请求和终端 4 的公网地址转发给终端 1，终端 1 收到后发送响应给终端 4 的公网地址。这样双向的通信通道就建立好了。

通过代理实现 NAT 穿越不需要升级或更换原有网络的设备与终端，将实现穿越的任务交由代理来完成，简化了对终端的要求，可以实现所有类型 NAT 的透明穿越。但由于每个私网内都需要设置一个代理设备，增加了组网成本，每个数据流都需要代理进行转发也在一定程度上降低了通信效率。

4　通过中间服务器实现NAT穿越

组网示意图如下图 2 所示：

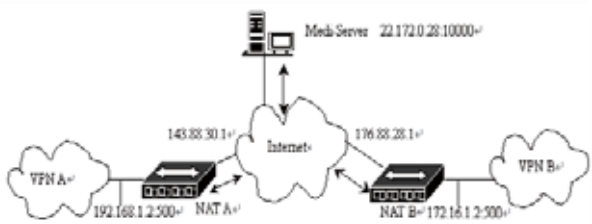

图 2　通过中间服务器实现 NAT 穿越

这里我们借鉴了 P2P 通信机制[5]，通过一个受信任的第三方充当通信双方的服务器，使得 IPSec VPN 双方在中间服务器的协助下建立起点对点的会话以直接进行 P2P 通信。通过中间服务器实现 NAT 穿越可经过以下步骤来完成。

(1) 第一步： VPN A、VPN B 各自发起与中间服务器 S(Medi-Server S)的通信会话。假设 NAT A 为 VPN A 与 S 之间的会话分配了端口 50000，NAT B 为 VPN B 与 S 之间的会话分配了端口 30000，那么 NAT A 为此会话建立的映射是 192.168.1.2:500<—> 143.88.30.1:50000，NAT B 为此会话建立的映射是 172.16.1.2:500<—> 176.88.28.1:30000，VPN A、VPN B 从 S 处获知的对方的公网 [IP 地址:端口] 对分别为[176.88.28.1:30000]和[143.88.30.1:50000]。

(2) 第二步：Medi-Server S 向 VPN B 发送请求，请求 VPN B 往 VPN A 方向“打洞”。由于 NAT 不允

许外网主机主动访问内网主机，所以一个消息能从NAT 外部进入 NAT 内部的前提条件是 :该消息的源[IP 地址:端口] 对与某一个先前由 NAT 内部向外部发起的会话的目的[IP 地址:端口]对匹配。如果此时 VPN A 直接发送消息给 VPN B，由于目前由 NAT B 内部向外部发起的会话中只有 VPN B 与 S 之间的会话，这一会话的目的[IP 地址:端口]对是[22.172.0.28:1000]，而 NAT B 接收到的消息(来自VPN A、途经NATA)的源[IP 地址:端口]对是[143. 88.30.1:50000]，两者不匹配，所以 NAT B 通常会将这一消息丢弃。现在我们需要在 NAT B 上打一个方向为 143.88.30.1:50000(即 VPN A 的外网地址)的洞，这样 VPN A 发送到 176.88.28.1:30000(实际地址是 143.88.30.1:50000)的信息，因为 NAT B 上已经有了这洞，就能顺利进入 NAT B 内部到达 VPN B 了。

(3) 第三步：VPN B往 VPN A 的外网 NAT A 地址[143.88.30.1:50000]发消息(我们称之为打洞消息)。该消息将使得 NAT B 上留下对应于[143.88.30.1:50000]的标志信息(我们称之为“ 洞 ”，发消息的过程称为打洞过程)，此后来自[1143.88.30.1:50000]的消息就可以进入 NAT B 内部，至此完成了 NAT B 到 NAT A 上的 “ 打洞 ” 工作。该消息的源端口号与发往 Medi-Server S 的端口号一致，NAT 只是再次创建一个会话，不分配新端口，而是用原来分配的端口号 30000。NAT B 为此会话建立的映射是 172.16.1.2:500<—> 176.88.28.1:30000。

(4) 第四步：由通信发起方 VPN A 发送一个协商包到[176.88.28.1:30000]。由于 NAT B 已经建立了 176.88.28.1:30000 到 172.16.1.2:500 的映射关系，因此该协商包可以顺利进入 NAT B 内部到达 VPN B。此后从 VPN B 发往[143.88.30.1:50000]的消息因为有了 “ 洞 ” 和 143.88.30.1:50000 到 192.168.1.2:500 的映射，也可以顺利进入 NAT A 内部到达 VPN A 了。至此，位于 NAT 后的 VPN A 和 VPN B 就实现了双边穿越 NAT 进行 P2P 通信而无需 Medi-Server S 的介入了。

为了维持端口映射，我们让 VPN A、VPN B 定时向 Medi-Server S 发送特定的数据包，该数据包经过 NAT 时，NAT 将自动延长相应映射的生存期从而使映射得以维持，此类包的发送间隔必须小于 NAT 为端口映射分配的生存期[6]。

该方案使位于 NAT 设备之后的主机之间实际交换数据时真正实现双方的 P2P 通信，保证了网络的通信效率，是一个健壮而可靠的解决方案。只是需要在 IPSec VPN 双方之间架设一个中间服务器，但该服务器的配置要求不高，实际组网时还是容易实现的。

5 结束语

基于 IPSec 的 VPN 以其能够提供简单、廉价、安全和可靠的 Internet 访问隧道而备受青睐，而由于 IP 地址短缺， 许多 VPN 设备都部署在 NAT 之后，需要双边穿越 NAT 的情况普遍存在，但对于双边 NAT 穿越的问题目前仍无标准可循。本文探讨了几种可能的解决方案，用户可以根据自己的实际情况作选择，更多的研究和探索还有待今后在实际的工作中进行。

参考文献

1 RFC-1631-1994.The IP Network Address Translator (NAT).

2 IETF Draft.Considerations for Selection of Techniques for NAT Traversal, 2005.

3 高玲,祝翔. IPSec VPN 双 NAT 穿越设计.电子测量技术, 2006,29(1):67－68.

4 石友康.下一代网络的核心软交换技术.电信科学, 2002,18(1):39－44.

5 RFC-1661-1994.The Point-to-Point Protocol (PPP).

6 徐向阳,韦昌法. 基于NAT 穿越技术的 P2P 通信方案的研究与实现.计算机工程与设计, 2007,28(7):1559－1561.