

文章编号:1001-9081(2010)07-1757-03

VPN 中 IPSec 穿越 NAT 的解决方案

杜江,葛洛雅柯

(重庆邮电大学 计算机科学与技术学院,重庆 400065)

(clouddu@gmail.com)

摘要:IP 安全(IPSec)体系结构与网络地址转换(NAT)都是在因特网上得到广泛应用的技术,然而它们之间的不兼容性却制约着基于 IPSec 技术的虚拟专用网(VPN)发展。为解决两者之间的不兼容性,IETF 提出了用户数据包协议(UDP)封装草案。但该草案对于 IPSec 通信双方均在 NAT 之后的情况,则还没提出可行的解决方法。在借鉴 UDP 封装方案和双向穿越 NAT 方案的基础上,给出了一种适应不同情形的 NAT 穿越解决方案,并对方案的可行性进行了详尽的分析。

关键词:Internet 协议安全性;网络地址转换;虚拟专用网;用户数据包协议封装

中图分类号: TP393 **文献标志码:** A

Solution of IPSec NAT-traversal in virtual private network

DU Jiang, GE Luo-yake

(College of Computer Science and Technology, Chongqing University of Post and Communication, Chongqing 400065, China)

Abstract: IPSec architecture and Network Address Translation (NAT) are widely used in the Internet today. However, the incompatibility between them limits the development of Virtual Private Network (VPN) based on IPSec technology. The Internet Engineering Task Force (IETF) proposed a series of drafts based on User Datagram Protocol (UDP) encapsulation to solve this problem. But the solution did not cover the double NAT-traversal in IPSec VPN. According to the methods of UDP encapsulation and double NAT-traversal, this paper proposed a feasible solution to solve the problem of NAT-traversal in different situations, and the feasibility was clarified in detail.

Key words: Internet Protocol Security (IPSec); Network Address Translation (NAT); Virtual Private Network (VPN); User Datagram Protocol (UDP) encapsulation

为了解决 IPSec 与网络地址转换(Network Address Translation, NAT)不兼容的问题, IETF 曾提出了 RSIP (Realm Specific IP)^[1] 以及用户数据包协议(User Datagram Protocol, UDP)封装^[2]两种解决方案。简单来说, RSIP 是将一个拥有合法 IP 的服务器放在私有地址域内, 允许域内主机直接同时在几个地址域内通信。它避免了对 IKE (Internet Key Exchange) 和 IPSec 协议本身的修改, 但是方案的完全实现需要用新的 RSIP 网关代替现有的 NAT 设备, 可行性不大。而 UDP 封装方案只需对 IPSec 和 IKE 的实现作出一些改动, 不需要对现有的 NAT 设备做任何改变。经过改进的 UDP 封装方案已经成为目前条件下较为可行的 NAT 穿越方案。但该方案也有一定的局限性, 它的实现前提是通信双方设备必须有一方拥有公网地址。如果双方均位于 NAT 之后, 处于 NAT 设计的安全性考虑, NAT 只允许由内向外发动主动连接, 而不接受由外部发起的连接请求。因此, 这将导致外部发起的 IKE 协商请求无法经过 NAT 到达内部的响应方。针对上述问题, 下面将探讨一种可行的解决方案。

1 IPSec 与 NAT 的不兼容性分析

NAT 的核心思想是修改 IP 头中的 IP 地址, 但 IPSec 却要保护 IP 包免受非法的修改, 因此将 NAT 和 IPSec 结合使用时便会出现一些问题。两者的不兼容性主要体现在以下三个方面^[3]。

1.1 NAT 对认证报头的影响

认证头(Authentication Header, AH)使用消息摘要算法生成一个散列值, 以保护整个 IP 分组, 包括不变的报头字段(如源 IP 地址和目标 IP 地址)。接收方使用该散列值来验证分组。如果原始 IP 分组中的任何字段被修改, 验证将失败, 接收方将丢弃该分组。AH 用于防止未经授权的修改、信源欺骗和中间人攻击。但根据 NAT 的工作原理, NAT 设备将修改外层 IP 包头的源地址及其校验和, 这样就会使 IPSec 接收方无法认证 AH 分组的真实性和完整性。对于网络地址端口转换(Network Address Port Translation, NAPT)来说, 由于 NAPT 需要 TCP/UDP 端口来对进出的信包或者连接进行匹配, 所以 AH 分组无法跨越 NAPT。由此可见, NAT/NAPT 与 AH 无法兼容。

1.2 NAT 对封装安全负载的影响

封装安全负载(Encapsulating Security Payload, ESP)并不对 IP 地址进行加密, 但是 NAT 的引入所造成的问题依然存在。由于 TCP/UDP 校验和涉及虚构的 IP 包头, 该虚构包头里含有 IP 源和目的地址, 因此, 当 NAT 设备改变 IP 地址时, 也需要更新 IP 头和 TCP/UDP 头的校验和。然而应用了 ESP 传输模式的 IP 包经过 NAT 设备时, 由于 TCP/UDP 校验和处于加密负载中, 该值在修改了外层 IP 包头后无法被 NAT 设备更新。这样, 当该信包在经过 IPSec 层后被送往上层进行协议处理时, 将会因为 TCP 协议层的校验和错误而被丢弃。

ESP 隧道模式可以和静态或者动态 NAT 相兼容, 因为

收稿日期:2010-01-07;修回日期:2010-02-25。 基金项目:重庆市科委基金资助项目(CSTC2007AB2003)。

作者简介:杜江(1969-),男,重庆人,副教授,硕士,主要研究方向:计算机网络、信息安全;葛洛雅柯(1984-),男,陕西城固人,硕士研究生,主要研究方向:计算机网络、信息安全。

TCP/UDP 检验和只与内层“原始”IP 包头有关,对于外层 IP 包头的修改并不对其造成影响,然而与 AH 一样,在 NAT 存在的情况下,ESP 也无法通过 NAT,NAPT 需要 TCP/UDP 端口来匹配出入的信包,上层端口信息对于 NAT 网关是不可知的,所以 ESP 分组通信将被完全阻隔。

1.3 NAT 对 IKE 的影响

IKE 协商是由来自 UDP 端口 500 的分组建立的,绝大多数 IPSec 实现也都把该端口作为进行 IKE 协商的唯一合法端口。如果该分组经过 NAT 设备后,那么最终的分组端口号将不是期望的端口号,从而使 IKE 协商将不能启动。

2 UDP 封装和双向 NAT 穿越方案

2.1 UDP 封装方案

2001 年 IETF 提出了基于 UDP 封装的 IPSec-NAT 穿越方案来解决 IPSec 与 NAT 不兼容的问题。该方案的核心思想是把 IPSec 包(AH 或 ESP 包)装入一个 UDP 分组中,即在应用了 IPSec 保护的 IP 包的 IP 头和 IPSec(AH/ESP)头之间插入一个 UDP 头,然后让 NAT 或 NAPT 去修改 UDP/IP 分组^[4]。这样,在通信中间系统上看到传输的是 UDP 数据包,IPSec 数据包则作为 UDP 协议的用户数据。然而,原始的 UDP 封装方案只解决了 NAT 设备不支持 AH 和 ESP 通信的问题,它还存在诸如 AH 认证失败、TCP 校验和错误等问题。下面介绍一种改进后的 UDP 封装方案来解决这些问题^[5]。原始方案与改进后方案的数据包封装格式的对比如图 1 所示。

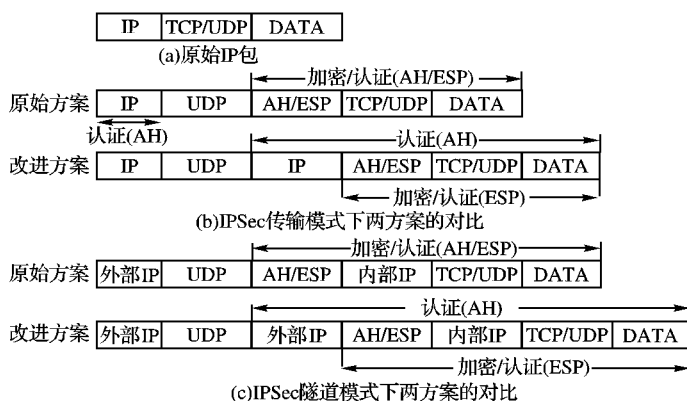


图1 原始与改进后方案的封装数据包的格式对比

从图中可以看出改进后的 UDP 封装方案对 IPSec 所保护的整个 IP 包进行 UDP 封装。而且,AH 认证计算不涉及最外层的 IP 头,这样 NAT/NAPT 对 IP 头部或是 UDP 头部的修改不会对原有 AH 认证产生影响。同时,应用了 ESP 传输模式的 IP 包经过 NAT 设备时,由于 NAT 不对原有 IP 头作修改,所以也就不存在 TCP 校验和出错的问题。本文以下所述的 UDP 封装方案均为改进后的方案。

2.2 双向 NAT 穿越方案

VPN 中双向穿越 NAT 的方案是在参考 P2P 穿越 NAT 方法的基础上提出的。其核心思想是借助双方都信任的第三方来充当通信双方的信息服务器,将 IPSec VPN 建立连接时所需的信息转发给双方,然后 IPSec 双方可通过 UDP 封装方案来实现双向 NAT 穿越。该服务器只在 IPSec 双方不知道对方的情况下转发一些信息。IPSec 双方在得到这些信息后就可以启动 IKE 协商连接,以后便可直接通信而无需再经过信息服务器^[6]。

3 双向 NAT 穿越方案的实现

3.1 IPSec 穿越 NAT 的几种情形

根据 NAT 设备以及 IPSec VPN 在实际网络中部署的位置,IPSec 穿越 NAT 可以分为以下 3 种情形。如图 2 所示。

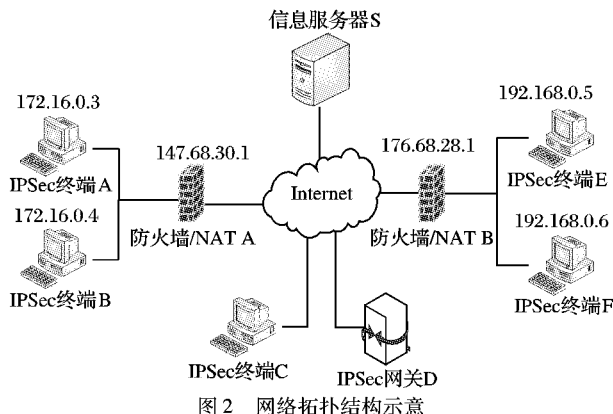


图2 网络拓扑结构示意图

1) IPSec 通信双方之间无 NAT 设备,如图 2 所示中的终端 C 和网关 D。双方进行正常的 IPSec 通信,不需要其他附加方案。此种情况不属于本文的讨论范围。

2) IPSec 通信双方有一方位于 NAT 之后,如图 2 所示中的终端 A 和网关 D。双方采用 UDP 封装方案实现 NAT 穿越。

3) IPSec 通信双方均位于 NAT 之后,如图 2 所示的终端 A 和终端 E。出于 NAT 的安全性考虑,NAT 设备不接受由外部发起的连接请求。此时,双方先采用双向 NAT 穿越方案建立连接,然后便可通过 UDP 封装方案进行 IPSec 通信。

3.2 方案实现的总体思想

在借鉴 UDP 封装方案和双向 NAT 穿越方案的基础上,下面给出一个完整的 IPSec 穿越 NAT 的方案。方案实现的总体流程如图 3 所示。

方案实现的具体步骤如下:

1) IPSec 客户端在启动时访问信息服务器,注册自己的相关信息,并且下载其他 IPSec 客户端的 IP 地址和端口信息等信息。

2) IPSec 客户端参考 IKE 协商第一阶段时的协商数据包,向信息服务器发送源与目的端口都为 500 和 4500 的 UDP 数据包,探测自己是否在 NAT 设备之后。若在 NAT 设备后,则该 IPSec 客户端定时发送 Keep-alive UDP 数据包,以保持自己在 NAT 上的映射不被删除。同时,信息服务器还应记录该客户端经过 NAT 转换后的 IP 地址及 IKE 协商端口号。

3) IPSec 通信发起方根据从信息服务器获取的信息,通过查询响应方信息中是否包含经过 NAT 转换后的 IP 地址及 IKE 协商端口号,以此来判断响应方是否位于 NAT 之后。

4) 依据 3.1 节所述的 IPSec 穿越 NAT 的不同情形,采用不同方案实施 NAT 穿越。

3.3 双向穿越 NAT 的具体步骤

下面将以具体实例详细描述双向穿越 NAT 的步骤。如图 2 所示,假设 IPSec 终端 A 欲与 IPSec 终端 E 通信。

1) 终端 A 向信息服务器 S 发送与终端 E 通信的请求消息。假设在 3.2 节步骤 2) 时,NAT A 为终端 A 与信息服务器 S 之间的会话分配的端口为 40000,则在 NAT A 上为此次会话建立的映射为 172.16.0.3:500 ↔ 147.68.30.1:40000。同

理 NAT B 为终端 E 与信息服务器 S 之间的会话分配的端口为 50000, 则 NAT B 为此次会话建立的映射为 192.168.0.5:5000↔174.68.28.1:50000。此时, 双方可以从信息服务器那获知对方的公网 IP 地址以及端口号。

2) 信息服务器 S 向终端 E 发送消息告知终端 E 向终端 A 发送消息, 以便终端 A 可以向终端 E 发起 IKE 协商请求。由于 NAT 不允许外部主机向 NAT 后的主机发起主动连接, 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 地址和端口号, 与先前 NAT 内部向外发起的会话的目的 IP 地址和端口号匹配。如果此时, 终端 A 向终端 E 发起 IKE 协商连接, 则会因为 NAT B 终端 E 没有向终端 A 发起的会话映射 (只有终端 E 向信息服务器 S 发起的会话映射), 从而丢弃该 IKE 协商数据包。

3) 终端 E 向终端 A 的公网地址 (147.68.30.1:40000) 发送消息。此时将会在 NAT B 上留下目的地址和端口号为终端 A 的公网地址 (147.68.30.1:40000) 的标志信息, 以后终端 A 发送的消息便可以进入 NAT B 内部, 到达终端 E。该消息的端口号与发往信息服务器 S 的端口号一致, NAT B 只是再创建一个会话, 不分配新的端口号, 而是使用原来的端口号 50000。NAT B 为此次会话建立的映射 192.168.0.5:500↔176.68.28.1:50000。发送消息完毕之后, 终端 E 通知信息服务器可以让终端 A 发起 IKE 协商。

4) 端 A 在收到信息服务器 S 的反馈信息, 被告知可以向终端 E 发起 IKE 协商。则终端 A 向终端 E 发起 IKE 协商请求。此时, 由于上步已经在 NAT B 上建立了 176.68.28.1:50000 到 192.168.0.5:500 的映射, IKE 协商包便可以顺利穿越 NAT B 到达终端 E。同理, 终端 E 发往终端 A 的消息因为有了在 NAT B 和 NAT A 上存在的相关映射也可以顺利到达。

5) 双方通过 UDP 封装方案来进行 IPSec 通信。采用 UDP 封装穿越 NAT 主要包括 IKE 协商、对外出数据包的封装、对进入数据包的解封装和定时发送 Keep alive 数据包这四个过程。图 4 简单描述了 UDP 封装方案穿越 NAT 的流程。

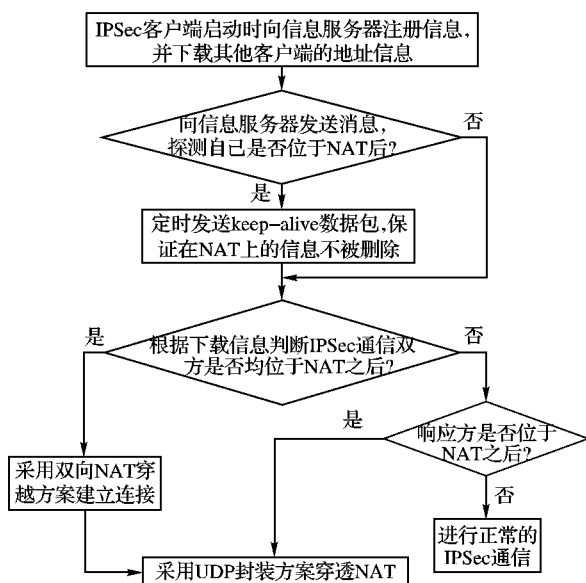


图3 方案实现的总体流程

4 方案的可行性分析

4.1 易操作性

方案的实施只需在公网上架设一个信息服务器, 对服务器的配置要求也不高, 只需对 IPSec 和 IKE 的实现作出一些

改动, 而不需要对广泛使用的 NAT 设备作任何修改, 具有较强的可操作性。

4.2 向后兼容和互操作性

方案具有向后兼容性, 能与现有的 IPSec/IKE 实现进行互操作。方案能够自动检测是通信双方之间是否存在 NAT, 还能判断通信对方的 IKE 实现能否支持 NA(P)T 穿越, 以使通信双方在必要时才使用 NA(P)T 穿越支持。

4.3 安全性

方案的实现需在公网上架设的第三方服务器, 这一中间实体便成为了最易遭受攻击的环节。基于这一点, 可参考 IKE 通信并结合认证中心 (Certificate Authority, CA) 认证机制加以保证, 对于可预见到的篡改、重放及中间人攻击, 可以实现较好的防范机制。同时, UDP 封装方案对 IKE 协商作出了改进, 增强了安全性。例如: 将第一阶段探测 NAT 存在的 NAT-D 载荷放在第三对消息中, 因为第三对消息的内容除消息头外都是经过加密、验证处理的, 这样可以防止 NAT-D 载荷的内容受到中间人攻击。

4.4 性能效率

改进后的 UDP 封装方案比原始方案增加了一个 IP 头部, 多了 4 B。增加的传输开销与所传输的 IP 数据包大小有关。在进行较大数量的数据通信时, IP 数据包的大小由路径的最大传输单元 (Maximum Transmission Unit, MTU) 决定, 路径的 MTU 越大, IP 数据包也越大, 所增加的开销比例越小。以低速链路 (如: 点对点链路) 和宽带链路 (如: 以太网) 为例, 其 MTU 分别为 296 B 和 1500 B, 对应的传输开销比为 1.35% 和 0.27%。可见, 由此引起的额外传输开销相对较小, 对整体的性能效率影响不大。

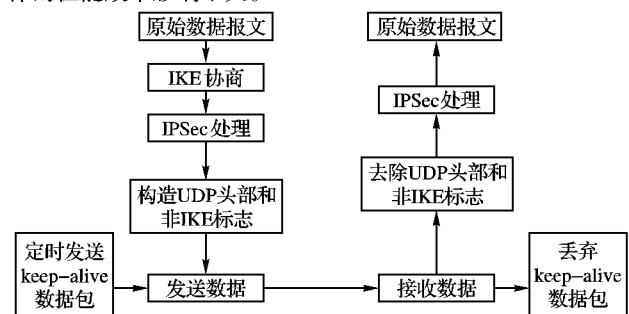


图4 UDP封装方案穿越 NAT 的简易流程

5 结语

IPSec 与 NAT 在本质上存在一定程度的冲突, 所以 NAT 的广泛存在极大地限制了 IPSec 技术的推广, 因此, 寻求解决两者不兼容的方案势在必行。然而由于 NAT 自身设计的限制, 目前的解决方案对于通信双方均位于 NAT 之后的情形还没有给出很好的解决办法。本文在参照 UDP 封装方案以及双向 NAT 穿越方案的基础上, 给出了一种完整可行的解决方案。

参考文献:

- [1] BORELLA M, GRABELSKY D. Realm specific IP: Protocol specification, RFC3103[S], 2001.
- [2] IETF draft: IPsec over NAT Justification for UDP encapsulation 2001 [S], 2001.
- [3] ABOBA B, DIXON W. IPsec - NAT compatibility requirements, RFC3715[S], 2004.
- [4] HUTTUNEN A, DIBURRO L. UDP encapsulation of IPsec packets, RFC 3948[S], 2005.
- [5] 张永平, 万艳丽. VPN 网络中 IPSec 穿越 NAT 的研究[J]. 计算机应用与软件, 2008, 25(1): 250-252.
- [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[J]. 计算机工程与设计, 2007, 28(7): 1559-1561.