一种新的 IPSEC穿越 NAT方法

彭近兵 龙 翔 高小鹏 陈贤钦

(北京航空航天大学 计算机学院, 北京 100083)

摘 要: Internet网络层安全协议(IPSEC)和网络地址翻译器(NAT)不兼容,这严重限制了 IPSEC的应用范围. 解决方法必须遵循的原则是既能使 IPSEC数据流穿越 NAT,又不必修改路由器和 NAT,部署方便. 目前存在的3种解决方法都具有局限性:"先于 IPSEC进行 NAT转换"方法难以实现,"特定域 IP通信(RSIP)"方法部署困难,"用户数据包(UDP)封装安全封装协议(ESP)数据包"方法只能部分地解决 IPSEC与 NAT不兼容问题. 在分析现有方法的基础上,提出一种新的解决方法,即 UDP封装 IPSEC数据包方法. 该方法通过 UDP封装 IPSEC数据包,保护原始 IP地址和端口号,消除了 NAT对 IPSEC影响. 详细介绍了该方法的实现思路,进行了可行性和优缺点分析. 通过分析可知,新方法具有明显优点,能够方便、有效地解决 IPSEC和 NAT兼容问题.

关 键 词: IPSEC; NAT; VPN; NAT穿越

中图分类号: TP 393

文献标识码: A 文 章 编 号: 1001-5965(2007) 01-0063-04

New solution for IPSEC passing through NAT

Peng Jinbing Long Xiang Gao Xiaopeng Chen Xianqin

(School of Computer Science and Technology, Beijing University of Aeronautics and Astronautics, Beijing 100083, China)

Abstract The application range of IP security protocol (IPSEC) is badly restricted due to the incompatibility of IPSEC and network address translator (NAT). The rule that must to be followed by the solutions for IPSEC passing through NAT is that IPSEC pass through NAT without any changes to the routers and NAT on the Internet. There are limits to the current three solutions. It can barely be realized to execute the NAT ahead of executing the IPSEC. It is difficult to deploy the realm specific IP (RSIP). The incompatibility of IPSEC and NAT can only be solved partially by user data packet (UDP) encapsulation of the IP encapsulating security payload (IPSEC ESP) packets. A new solution, UDP encapsulation of IPSEC packets, was developed. The new solution eliminates the impact from NAT to IPSEC by protecting the origin IP addresses and ports of the IPSEC packets through encapsulating the IPSEC packets with UDP header. The feasibility of this solution was demonstrated. The analyse shows that the new solution has evident advantages over the others and can remove the incompatibilities between IPSEC and NAT effectively and expediently.

Key words IPSEC; NAT; VPN; NAT traversal

Internet网络层安全协议(IPSEC)和网络地址翻译器(NAT)应用非常广泛. 一方面, IPSEC实现基于 IP数据包的安全保护,为上层协议提供透明的安全服务,在网络安全领域广泛应用,尤其是广泛用于构建 VPN(虚拟专用网); 另一方面, NAT通过将私网地址映射为公网地址,有效地解决了 IPv4地址短缺问题,是当前为解决互联网地址不足而广泛采用的方法. 但是 IPSEC和 NAT不兼容,当 IPSEC数据流穿越 NAT设备时,两者无法协同工作,这严重限制了 IPSEC的应用范围.

1 IPSEC和 NAT原理及兼容性分析

1.1 IPSEC原理

IPSEC由密钥管理和安全协议组成. 密钥管

收稿日期: 2006-01-10

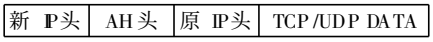
作者简介: 彭近兵(1968-),男,安徽庐江人,博士生, pengjinbing@les.buaa.edu.cn

理由 Internet密钥交换协议(IKE)完成,安全协议包括认证头协议(AH)和安全封装协议(ESP),它们提供不同的保护.

IKE动态协商通信双方的加密/认证密钥及算法等信息,建立安全关联(SA). AH为IP包提供数据完整性、数据源认证和抗重放攻击等保护. ESP为IP包提供数据机密性、数据完整性、数据源认证和抗重放攻击等保护. AH和ESP可单独使用,也可联合使用. AH和ESP都有2种工作模式,即传输模式和隧道模式. 传输模式只为IP的上层信息提供安全保护,隧道模式为整个IP包提供安全保护. 图1和图2分别说明了AH协议和ESP协议在传输和隧道模式下处理IP包的原理.



传输模式下的AH封装

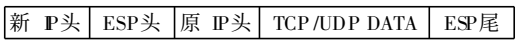


隧道模式下的AH封装

图1 AH封装原理图



传输模式下的ESP封装



隧道模式下的ESP封装

图2 ESP封装原理图

1.2 NAT原理

NAT有3种类型:静态NAT,动态NAT,网络地址端口转换NAPT. 如图3所示,静态NAT将每一个私有IP地址确定地映射到某个合法的公网IP地址;动态NAT将私有IP地址动态映射成NAT网关某个未分配的公网IP地址. NAPT将私有IP地址映射到NAT网关一个合法公网IP地址的不同端口[1].

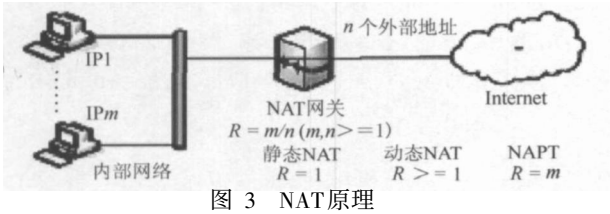


图3 NAT原理

1.3 IPSEC与NAT兼容性分析

IPSEC和NAT间存在的主要兼容性问题是:

AH、校验和、IKE地址标识、重叠的安全策略数据库(SPD)条目和NAT不兼容;IKE固定源端口和NAPT不兼容;IPSEC进入策略检查和地址标识矛盾;有些NAT丢弃非TCP/UDP数据包,使得AH和ESP数据被丢弃;无数据流穿越NAT时,相应映射的保持时间随NAT的实现而不同,可能导致后续数据包无法到达正确目的地[2].

解决IPSEC和NAT兼容问题的方法必须满足以下要求:不修改路由器和NAT,能够快速实现;支持IKE和ESP传输模式穿越NAT;向后兼容,能够检测NAT是否存在,可与现有IPSEC互操作;NAT后多台主机能同时和远程网关建立连接,系统可扩展;对防火墙进行简单配置,就可控制穿越NAT的IPSEC数据流;不给IKE和IPSEC本身带来新的安全问题[3].

2 目前的解决方法

2.1 提前进行NAT操作

最简单的解决方法是在IPSEC操作前,先进行NAT操作获得全局网络地址,可避免冲突. 但在实际应用中,NAT网关往往是基础设施,无法放在IPSEC终端之前,所以该方案局限性大.

2.2 RSIP(Realm Specific IP)

RSIP是IETF(Internet Engineering Task Force)提出的解决方法. RSIP允许主机同时在多个地址域内通信. 当内部主机与外部网络通信时,主机首先向RSIP服务器请求一个合法IP地址,以该地址为源地址构造数据包,然后将数据包封装在以私有IP地址为源地址的报文内传给RSIP网关,网关去掉外面的报头后将报文发送出去[4]. RSIP解决了IPSEC和NAT冲突问题;无需修改IKE和IPSEC协议;同时支持AH和ESP模式. 但是,RSIP也有缺点:要求IPSEC设备实现RSIP的客户端协议;在IKE重建密钥时,要修改IKE源端口,可能无法与现有IPSEC协同工作;要求将NAT网关升级为RSIP网关,耗费较大.

2.3 UDP封装ESP数据包

IETF提出的另一种解决方法. 基本思想是:用UDP封装ESP数据包. 如图4所示,在IP头和ESP数据之间插入一个UDP头[5].

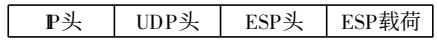


图4 UDP封装ESP数据包

1) 添加IKE标志. 如图5所示,在IKE数据包的UDP头和IKE头之间添加四字节NonESP标志,值为全零. ESP头中前4个字节是SPI字段,实现中,该字段禁止为零. 这样就可区分被UDP封装的ESP数据包和IKE数据包.

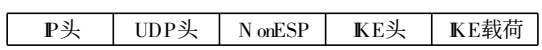


图5 UDP封装IKE数据包

2) 探测. 在IKE协商的第一阶段通过交换Vendor ID载荷确认通信双方能否支持UDP封装,通过交换NAT发现(NAT-D)载荷确认线路上

是否存在 NAT[6].

3) 固定端口. IPSEC端口与 IKE 保持一致, 发现 NAT前后分别用 500端口和 4500端口.

4) 映射保持. 定期发送保持激活报文 (keep alive)以维持 NAT两端的映射.

5) 增加模式. 增加 UDP封装隧道模式和 UDP封装传输模式以标记数据包经过 UDP封装.

6) 调整校验和. 在 UDP模式下, 通信双方在 IKE 快速模式中通过 NAT-OA 载荷传递彼此的 IP 地址, 并利用该地址调整 TCP/UDP校验和.

7) 预设校验和. 将 UDP校验和字段设为零, 接收方不能依赖该零值校验和进行检查.

该方法不修改 NAT设备, 部署比较容易. 但是该方法缺点明显: 不支持 AH 协议; 增加了载荷长度和处理开销; 固定通信端口, 无法实现 NAT后多主机发起通信; 限制较多, 比如 SPI不能为零等; 暴露了 NAT后面的 IP地址.

3　一种新的解决方法

综上分析, RSIP 能很好解决 IPSEC 和 NAT 兼容问题, 但实现和部署难度大; UDP 封装 ESP 数据包方法实现和部署容易, 但只能部分解决 IPSEC 和 NAT兼容问题. 本文提出的新方法, 结合二者优点, 有效地解决 IPSEC和 NAT兼容问题.

3.1　基本思想

1) 用 UDP封装整个 IPSEC 数据包. 格式如图 6所示. 这样, NAT改变外层 IP头后, 内层 IP 头仍保留内部主机 (IPSEC 发送端)原始 IP地址, 当外部主机 (IPSEC 接收端)剥离外层 IP 头和 UDP头后, 就是 IPSEC 报文, 如同未经过 NAT.

2) 标识 IKE 和 IPSEC. 封装 IPSEC 的 UDP 包头与 IKE 的 UDP 包头相同. IKE 数据包和 IPSEC 数据包是由如图 6的四字节标识域区分: IKE 数据包该域为 0, IPSEC 数据包该域为 1.

3) 探测. 在 IKE 协商的第 1阶段通过交换 Vendor-ID 载荷确认双方能否支持 IPSEC 穿透 NAT, 通过交换 NAT 发现 (NAT-D)载荷确认线路上是否存在 NAT. 如果不存在 NAT, 则进行正常 IPSEC 通信; 如果存在 NAT且双方支持 IPSEC 穿透 NAT, 执行 UDP封装 IPSEC 通信; 如果存在 NAT但不支持 IPSEC 穿透 NAT, 则无法通信.

4) 协商. IKE 协商的第 2阶段通过 SA 载荷协商是否采用 UDP封装 IPSEC 数据包及采用的模式.

5) 增加 2种通信模式. 增加 UDP封装隧道模式和 UDP封装传输模式.

6) 发送保持激活报文. 内部主机定期发送保持激活报文 (keep alive)以维持 NAT 两端的映射, 通信对方丢弃接收的保持激活报文.

新 IP头	UDP头	标识域	原 IP头	IPSEC载荷

图 6　改进的 UDP封装格式

3.2　通信流程

假定网关为 NAPT 类型, 网络连接如图 7所示. 通信流程如下: ① IKE 探测、协商. 如图 8所示, 由内部主机发起, 在第 1阶段通过交换 Vendor-ID 载荷确认双方能否支持 IPSEC 穿透 NAT, 通过交换 NAT发现 (NAT-D)载荷确认线路上是否存在 NAT设备; 在第 2阶段通过 SA 载荷协商通信模式. ②内部主机出站处理. 如图 9中消息 1 ~ 4所示, 进行 IPSEC 封装, 源地址为本机地址, 目的地址为外部主机地址; 用 UDP 封装 IP包, 设置标识域的值为 1; 用 IP封装整个 UDP数据包, 源地址为本机地址, 目的地址为外部主机地址. ③外部主机入站处理. 如图 9中消息 7~ 9所示, 数据包经过 NAT 网关到达外部主机时, 源 IP地址为 NAT网关地址, 目的地址为外部主机地址, 源端口被修改; 去除外层 IP报头和 UDP报头; 数据包送往 IPSEC 层, 根据标志域区分 IKE包和 IPSEC 包, 进行相应处理. ④外部主机出站处理. 如图 10中消息 1~ 4所示, 进行 IPSEC封装, 源地址为外部主机, 目的地址为内部主机; 用 UDP封装整个 IP数据包, 目的端口为内部主机原始源端口经 NAT改变后的端口号; 设置标志位; 对整个 UDP数据包进行 IP封装, 源地址为外部主机地址, 目的地址为 NAT网关地址. ⑤内部主机入站处理. 如图 10中消息 7~ 9所示, 数据包经 NAT 网关到达内部主机, 目的地址变为内部主机地址, 目的端口变为内部主机原始源端口; 内部主机去除外层 IP报头和 UDP报头; 后续的处理过程



图 7　实验中的网络连接状况

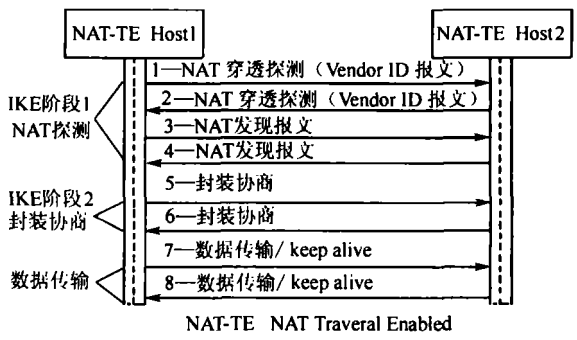


图 8　IKE 探测、协商示意

同外部主机入站处理. ⑥NAT映射保持. 内部主机定期发送保持激活报文, 外部主机丢弃收到的保持激活报文.

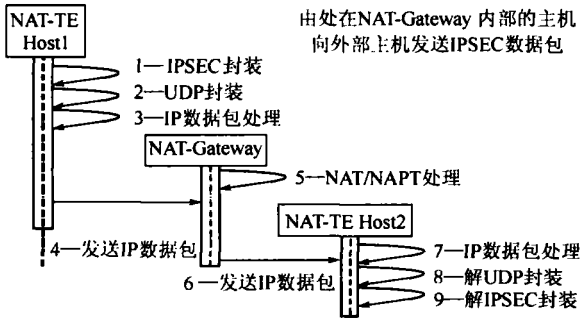


图 9 内部主机向外部主机通信流程示意

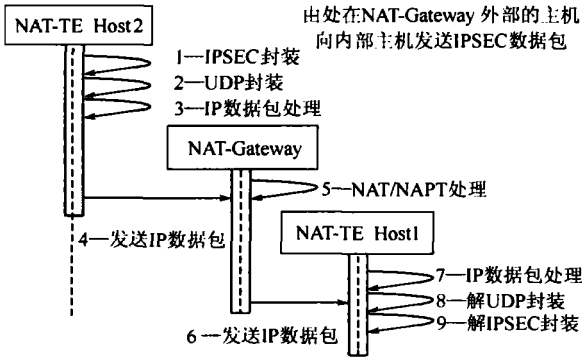


图 10 外部主机向内部主机通信流程示意

3.3 可行性分析

IPSEC和 NAT冲突是因为 NAT改变 IPSEC报文的 IP地址和端口号, 破坏了 IPSEC报文的完整性, 同时与 IKE固定通信端口相矛盾. 本方法通过 UDP封装 IPSEC数据包, 保护原始 IP地址和端口号, 消除了 NAT对 IPSEC和 IKE的影响, 使 NAT对 IPSEC和 IKE透明, 因而能解决 IPSEC与 NAT冲突问题. 本方法满足本文第 1.3节所述的 IPSEC穿透 NAT解决方法必须满足的要求. 原因是: 本方法不改变 NAT设备和路由器, 易于实现和配置; 本方法中, NAT对 IPSEC透明, 所以支持 IPSEC的所有模式; 必要时才进行 UDP封装 IPSEC通信, 否则进行正常 IPSEC通信, 所以本方法具有后向兼容性, 能与现有 IPSEC实现互操作; 本方法不改变通信目的端口, 与防火墙的兼容性同 IPSEC一致.

本方法暴露了 NAT后面内部主机的 IP地址, 但是, 这不会带来新的安全隐患. 原因有 2点: ①在没有 NAT的情况下, IKE和 IPSEC通信也不保护 IP地址, IP地址以明文传送. ②NAT虽然可以在一定程度上隐藏内网的主机身份和拓扑, 但是这并不能带来更多的安全性, 因为攻击者可以通过特定的手段探知内网的拓扑结构及 NAT网关内部主机的操作系统[7].

3.4 优缺点分析

如表 1所示, 与 RSIP方法相比, 本方法具有易于实现和部署, 能与现有 IPSEC协同等优点, 但增加了载荷长度, 暴露了 NAT后 IP地址; 同 UDP封装 ESP数据包方法相比, 本方法具有支持 IPSEC所有模式, 能与现有 IPSEC协同, 支持 NAT后多主机, 无实现限制等优点.

表 1 IPSEC穿越 NAT方法比较

方法特性	RSIP	UDP封装 ESP数据包	UDP封装 IPSEC数据包
实现和部署	难	易	易
支持模式	AH和 ESP	ESP	AH和 ESP
与现有 IPSEC协同	不能	不能	能
支持 NAT后多主机	支持	不支持	支持
实现的限制	少	多	
暴露了 NAT后 IP地址	不暴露	暴露	暴露
增加了载荷长度	增加	增加	增加

4 结束语

IPSEC和 NAT不兼容严重制约了 IPSEC的使用范围, 亟需解决. 本文提出的 UDP封装 IPSEC数据包方法消除了导致 IPSEC和 NAT冲突的根源, 能有效解决 IPSEC与 NAT的冲突问题, 支持 IPSEC的所有协议 (AH / ESP) 和模式 (传输 /隧道), 易于实现和配置. 但也有不足, 一是增加了带宽开销, 二是暴露了内部网的 IP地址.

参考文献 (References)

[1] Srisuresh P, Egevang K. Traditional IP network address translator[EB/OL]. 2001-01[2005-11]. http://www.ietf.org/rfc/rfc3022.txt

[2] Aboba B, Dixon W. IPSEC-NAT compatibility requirements [EB/OL]. 2004-03[2005-11]. http://www.ietf.org/rfc/rfc3715.txt

[3] Kent S, Atkinson R. Security architecture for the internet protocol[EB/OL]. 1998-11[2005-11]. http://www.ietf.org/rfc/rfc2401.txt

[4] Borella M, Grabelsky D. Realm specific IP: protocol specification[EB/OL]. 2001-10[2005-11]. http://tools.ietf.org/html/rfc3103

[5] Huttunen A, D Burro L. UDP encapsulation of IPSEC packets [EB/OL]. 2005-01[2005-11]. http://www.ietf.org/rfc/rfc3948.txt

[6] Kivinen T, Volpe V. Negotiation of NAT-traversal in the IKE [EB/OL]. 2005-01[2005-11]. http://www.ietf.org/rfc/rfc3947.txt

[7] Honeynet Project. Know your enemy: passive fingerprinting [EB/OL]. 2002-03[2005-11]. http://project.honeynet.org/papers/finger

(责任编辑: 张 嵘)