第32卷 第20期 计 算 机 工 程 2006年10月
Vol.32 № 20 Computer Engineering October 2006
·安全技术· 文章编号：1000—3428(2006)20—0166—02 文献标识码：A 中图分类号：TP393.08

IPSec穿越NAT多用户的一种实现方案

陈熊贵[1]，曹珍富[1]，郭 圣[2]
(1. 上海交通大学计算机系，上海 200030；2. 上海交通大学信息安全学院，上海 200030)

摘 要：网络安全协议（IPSec）和网络地址翻译(NAT)是当前的热点技术，得到广泛的应用。然而IPSec和NAT之间的冲突一直存在，为了解决二者之间的冲突，Ari Huttunen提出了用UDP封装IPsec ESP包，但是这个方案对NAT后多用户接入留下了两种待解决的情况。最近，潘提出了IPSec穿越NAT多用户的解决方案，但是在性能上考虑得不太充分，该文在潘的基础上提出了改进思想，使得在很好地支持多用户的同时性能达到很大程度的提高。

关键词：因特网安全协议；网络地址转换；UDP封装；虚拟专用网

Improvement on New IPSec-NAT Traversal Solution

CHEN Xionggui[1], CAO Zhenfu[1], GUO Sheng[2]
(1. Department of Computer, Shanghai Jiaotong University, Shanghai 200030;
2. School of Information Security, Shanghai Jiaotong University, Shanghai 200030)

【Abstract】Today, both IPSec technology and network address translator(NAT) technology are widely used in the internet, but these also take some problems and conflicts. In reference, Pan puts forward the traversal solution of IPSec-NAT to solve such conflict, however, the performance proposed in his paper is not quite ideal. This paper gives some efficient improvements which are based on Pan[1], and the method works well with multiple clients behind NAT trying to establish IPSec communications with a certain server simultaneously, at the same time, it improves performance to a great extent.

【Key words】IPSec; NAT; UDP encapsulation; VPN

网络安全协议（IPSec）和网络地址翻译(NAT)是当前的热点技术，应用很广泛。

IPSec是在IP层实现数据通信安全的协议，能为上层协议提供透明的服务。IPSec协议主要由Internet密钥交换协议(IKE)、认证头(AH)、安全封装协议(ESP)组成。IKE协议的目的是在IPSec通信双方之间建立安全联盟以及经过认证的密钥材料。AH认证头为数据报文提供数据完整性、数据源认证和抗重放攻击等功能。ESP协议为通过加密数据包，为数据包提供机密性、数据完整性、数据源认证和抗重放攻击。

NAT[5]技术支持多台主机共享一个全局IP地址，能很好地缓解IPv4地址枯竭的危机，常见于接入设备和防火墙中。NAT的原理是对于一般的数据报文，NAT把源IP地址(内部IP地址)和源端口通过一定的映射关系映射成实际的IP地址和端口号。映射完成后，以后从该IP地址端口对上来的数据都进行替换。

在很多时候需要同时用到这两个技术，但是由于NAT修改了IPSec包的源、目的IP地址以及上层的协议端口号，破坏了IPSec报文的完整性，使得这二者之间存在很多不协调的地方[4]。为了解决二者之间的冲突，Ari Huttunen[2]提出了用UDP封装IPsec ESP包。但是这个方案对NAT后多用户接入留下了两种待解决的情况。最近，潘[1]针对NAT后多用户的接入问题提出了新的IPSec穿越NAT的方案。然而潘的方案在性能方面还存在不足，因此本文提出了一种基于潘的改进方法。

1 UDP封装方案及其弊端

UDP[2]封装协议首先在IKE主模式的第1阶段检测通信双方之间是否存在NAT，如果存在NAT，则把原IPSec包完全封装在一个UDP包里，在接收方去掉UDP头处理后还原IPSec包。采用UDP封装的形式，在IP头和IPSec包之间再封装一个UDP头，这样封装后的数据包成为一个普通的UDP数据包，其端口值对NAT可见，就可以进行正确的转换。

这虽然在一定程度上解决了IPSec和NAT之间的矛盾，但是，对于文献[2]提到的两种情况就存在问题：(1)拥有两个相同私网地址但位于两个不同NAT后面的两个主机，隧道模式下会发生冲突；(2)同一NAT后面的不同的主机，在使用传输模式时可能发生冲突。这些冲突的本质都是在于IPSec不能区分NAT后的不同主机，需要一个会话信息来区分不同的会话。

2 潘提出的解决方案

在UDP和ESP之间再插入一层IP封装，最外层的封装提供穿越NAT传输(图1)，中间层封装的IP地址信息作为区分会话的参数，而最内层由IPSec主机处理。实际上也就是建立另一层隧道来传输IPSec包(图2)。

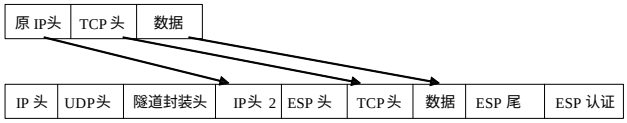

图1 传输模式封装前后数据格式变化

作者简介：陈熊贵(1976－)，男，硕士生，主研方向：网络安全，网络交换；曹珍富，教授、博导；郭 圣，硕士

收稿日期：2005-11-14 **E-mail：**cxg@sjtu.edu.cn

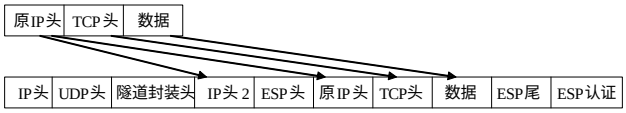

图 2 隧道模式封装前后数据格式变化

在隧道的选取上潘[1]用了L2TP+PPP作为外层封装协议。

3 本方案的实现思想

借用PPPoE[3]支持多用户的思想,在这里把潘提到的隧道封装头改成PPPoE头，由于PPPoE头本身就带有区分Session的Session id，因此这里就不需要文献[1]中说的“ IP头 2 ”了。考虑到在传输模式的时候，缺少“ IP头 2 ”会碰到文献[2]中提到的第 2 种情况，所以对PPPoE协议稍做修改，使它在协议过程中传递server所需要的内部IP地址和port信息。

这里 Session 头格式和协议都是用的类似 PPPoE 协议，不同的是：(1)Payload 存放的不是 PPP 载荷，而是 ESP 载荷；(2)整个从 Session 头开始的数据也不是直接放入以太网包中的，而是封装在 UDP 包中的。这里只是用了 PPPoE 建立 Session 的概念。用 Session 来支持多个 NAT 后面的连接。

正好比 PPPoE 协议只负责 Session 的建立和维护工作，我们这里也是一样。至于安全方面的，还是依靠 ESP 协议来达到。Session 头只负责 Session 的建立和断开，以及传递内部 IP 地址和 port 信息。

具体改进后的封装前后数据格式如图 3，图 4。

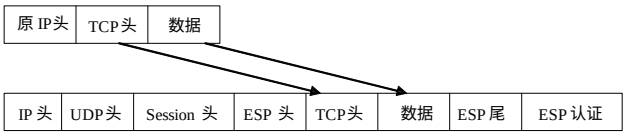

图 3 传输模式封装前后数据格式变化

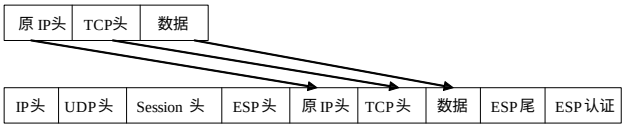

图 4 隧道模式封装前后数据格式变化

Session头的结构[3]如图 5。

VER	TYPE	CODE	SESSION_ID	LENGTH	Payload

图 5 Session头格式[3]

Session 头各字段的意义及取值：

VER|TYPE（1B）：为 0x11，版本和类型信息；

CODE（1B）：Session 发现阶段，用于标识不同的 Session 发现阶段的包类型；

0x09 PADI, 0x07 PADO, 0x19 PADR, 0x65 PADS, 0xa7 PADT

Session 建立后为：0x00

SESSION_ID（2B）：Session id 信息，用来区别不同的 Session，在 Session 发现阶段为：0x0000；

LENGTH（2B）：Payload 域的长度，不包括 Sesssion 头部分；

Payload（长度可变）：Session 建立后，Payload 域为 ESP 包，Session 发现阶段，格式如图 6 所示。

TAG_TYPE	TAG_LENGTH
TAG_VALUE …	

图 6 Session发现阶段Payload域的格式[3]

TAG_TYPE（2B）：Session 发现阶段 TAG 的种类；有下面这些类型：

0x0000 End-Of-List, 0x0101 Service-Name, 0x0102 AC-Name, 0x0103 Host-Uniq,

0x0104 AC-Cookie, 0x0105 Vendor-Specific, 0x0110 Relay-Session-Id,

0x0203 Generic-Error 0x0201 Service-Name-Error 0x0202 AC-System-Error

TAG_LENGTH（2B）：TAG_VALUE 的长度；

TAG_VALUE（长度可变）：当前某种 TAG 类型的值。

这里和 PPPoE 协议的第(3)个不同之处是：在协议的过程中，对于 TAG_TYPE = 0x0103 (Host-Uniq)，可以约定在该 TAG_VALUE 的最后 6 个字节指定内部 IP 地址和 port 号。这样解决了对传输模式的支持问题(因为传输模式 ESP 载荷中不包含内部 ip 头)，同时节约了文献[1]中提到的在中间层“ IP头 2 ”。建立 Session 的协议交换过程只要 4 个包传输就够了，而如果在数据的传输过程中每个数据包都包含 IP 头，这个开销将是很大的。

Session 的建立过程(图 7)：

(1)client 端发送 PADI 信息给服务器端，其中的 Host-Uniq 域包含了内部 ip 地址和 port 信息；

(2)在 server 端收到 PADI 后，回复一个 PADO 给 client；

(3)client 收到 server 回复的 PADO 后，发送 PADR 给 server；

(4)当 server 收到 PADR 后，为当前 Session 分配一个 Session id 号，给 client 发送 PADS 信息；

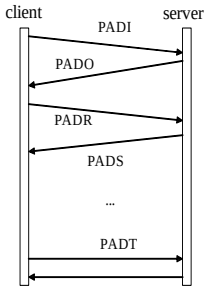

图 7 Session 的建立过程

(5)当 client 收到 PADS 信息的时候，Session 就已经建立起来了；

(6)然后进行 Session 阶段的数据传输；

(7)等数据传输结束后，client 或者 server 发送 PADT 信息，服务器将删除该 Session。

在 Session 建立完成后，Payload 域的内容为 ESP 载荷，CODE 为 0x00。Session 建立后，在 client 端保存 Session id 号，在服务器端为该 Session 建立一条记录。

服务器系统中保存的 Session 表字段如图 8 所示。

session_id	outer_ip	inner_ip	outer_port	inner_port	time

图 8 服务器系统中 Session 表字段

下面对各字段的意义进行说明：

session_id：用来唯一确定一个 Session（也是这张表的主键）；

outer_ip：经过 NAT 转换后的真实的 ip 地址；

inner_ip：局域网内部 ip 地址；

outer_port：经过 NAT 转换后的 port 值；

inner_port：未经 NAT 转换的 port 值；

time：定时器，如果超过一定的时间没有数据往来，断开当前的 Session 连接。

这样，对于文献[2]提到的第 1 种情况：拥有两个相同私网地址但位于两个不同 NAT 后面的隧道模式，就可以通过 outer_ip 值进行区别了，因为外网的 IP 地址是唯一的。对于文献[2]提到的第 2 种情况：同一 NAT 后面的不同的主机，在使用传输模式时的冲突。我们就可以用 inner_ip 值加以区别，因为同一 NAT 后的不同主机，内部 IP 地址应该是唯一的。这样，我们就可以区分不同的用户，为不同的用户分配不同的 Session id 值。

4 和潘实现方式比较的优点

(1)节约了头长度，现在我们用的 Session 头只要 6B，而 L2TP 头为 12B，因为考虑到这个头在每个数据包中都存在，所以长度的缩短还是很重要的；

(下转第 182 页)