一种 IPSec 隧道交换技术研究

A Study of Tunnel – switch Technology Based on IPSec

周云飞　李 欣　（浙江大学 计算机学院 杭州 310027）

摘要：基于 IPSec(IP Security)隧道的 VPN(Virtual Private Network,虚拟专用网)技术在互联网中被广泛应用，它的一种典型应用是在边界设备(如网关,防火墙等)实施 IPSec 隧道,保护子网内所有主机进出子网的 IP 数据包安全。此类应用环境中,IPSec 的保护终止于边界设备,并未在子网内实施保护。但是,在实际应用中,此假设经常受到人们的质疑,因此有必要将 IPSec 的保护从边界设备延伸到子网内主机。为了解决这个问题,引入了隧道交换概念,并提出一种基于隧道交换技术的解决方案,相对于采用物理交换和 IPSec 隧道嵌套两种解决方案,该方案能够实现子网内密文传输,并且数据在安全网关为明文,便于实施安全审计等其它优点。最后,在 Linux FreeS/WAN 的基础上实现了隧道交换技术,测试并验证了该方案的可行性和优点。

关键词：隧道交换 IPSec 延伸隧道

基于 IPSec 的 VPN 技术利用密码学方法在发送和接收方之间构造一个逻辑专用的信息传输通道,来实现点到点的安全通信。IPSec 在 IP 层构造一个安全隧道,保护 IP 数据包,利用该技术可以在公共网络传输私有数据,成本低廉而且能够保证数据的安全。

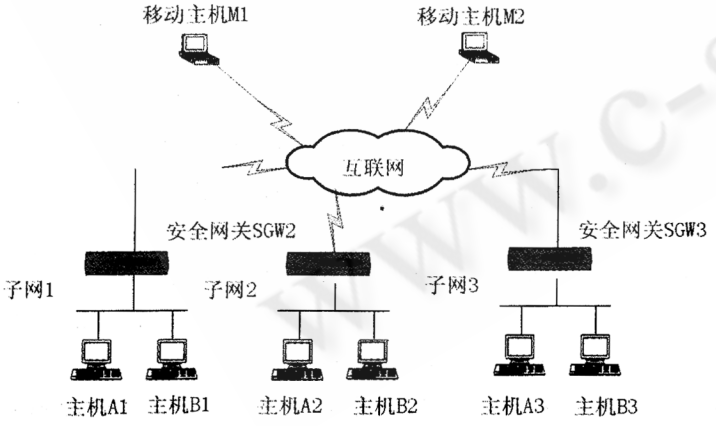

图 1　VPN 拓扑结构实例

图 1 给出的一个网络环境中的 VPN 拓扑结构,它可以看成是这三种典型应用场景的组合。移动主机 M1 和 M2 之间,网关 SGW1 和 SGW2 之间建立 IPSec 隧道;子网 1 内主机 A1 和子网 2 内主机 B2 之间的 IP 通信在公共网络传输过程受到网关之间 IPSec 隧道的保护。移动主机 M1 和安全网关 SGW3 之间建立主机和网关之间的 IPSec 隧道,M1 和保护子网 3 内主机 A3 之间的 IP 通信在公共网络传输过程受 IPSec 隧道保护。

在安全网关的应用场景下,IPSec 隧道终止于网关,所有 IP 数据在保护子网内是以明文方式传输,在子网内部是不受保护的。某些关键数据在子网内传输需要采用安全隧道进行保护。例如公司的驻外地分支机构,存在财务,市场,技术部门主机都在同一保护子网的情况,需要在子网内对财务的通信数据进行保护。

1　通信保护在子网内的延伸

VPN 能够将物理上分布在不同地点的网络通过公用网联接成逻辑上的虚拟子网。隧道能够保护 IP 数据在公共网络传输过程中的安全,但实际应用中会有将通信保护延伸到保护子网内部的需求。如图 1 所示:子网 1 中主机 A1 和安全网关 SGW1 之间的通信数据可能被主机 B1 窃听,为了避免通信数据不被窃听,必须在安全网关和本地子网

内需要进行保密通信的主机之间建立物理或逻辑的通道。

本文提出的基于 IPSec 隧道交换技术能够将隧道延伸到保护子网内部主机，利用 IPSec 隧道保护通信数据，并且避免上文所列举的问题。例如安全网关 SGW1 和 SGW2 建立 IPSec 隧道 $T_{(SGW1,SGW2)}$，保护子网 1 和 2 内主机之间的通信数据，主机 A1 和 A2 之间的通信数据需要实施端到端的保护，需要将通信保护延伸到主机，隧道交换技术将分别建立 IPSec 安全隧道 $T_{(A1,SGW1)}$，$T_{(SGW2,A2)}$ 将隧道延伸到子网内部的主机。如此 A1 发往 A2 的数据在子网 1 内受 IPSec 安全隧道 $T_{(A1,SGW1)}$ 的保护，安全网关终止 IPSec 安全隧道 $T_{(A1,SGW1)}$，并将通信数据封装 IPSec 安全隧道 $T_{(SGW1,SGW2)}$，传送到安全网关 SGW2，它终止安全隧道 $T_{(SGW1,SGW2)}$，并将数据封装 IPSec 安全隧道 $T_{(SGW2,A2)}$ 传送到主机 A2。这样主机 A1 和 A2 之间的安全隧道实际由三条 IPSec 隧道组成，安全隧道在安全网关 SGW1 和 SGW2 上有隧道交换的动作，将通信数据由一个安全隧道交换到另一安全隧道，所以称之为隧道交换。把主机 A1 和 A2 之间的安全隧道称为逻辑隧道，组成它的三条 IPSec 隧道中有两条是子网内主机和本地安全网关之间的 IPSec 隧道，它们将 IPSec 隧道从安全网关延伸到了子网内主机，将这两条子网内 IPSec 隧道称为延伸隧道。而安全网关之间的隧道是在逻辑隧道协商之前就已经存在，并且用来保护数据在公共网络传输过程的安全，将它称为主干隧道。

2 隧道交换技术

隧道交换技术采用分段隧道构成一个端到端的逻辑隧道，利用此逻辑隧道保护两端的 IP 数据包。逻辑隧道是和主机所设置的安全策略相对应，组成逻辑隧道的分段隧道有延伸隧道和主干隧道。

2.1 安全关联协商

为了方便描述，首先给出远端，本地和本机的定义。通过公共网络连接的设备互称远端，局域网连接的设备互称本地，而在同一个设备称为本机。

隧道交换应用环境下，安全关联协商的过程可简单描述如下：远端子网和本地子网通信受到安全网关之间的隧道保护，本地子网内主机需要和远端子网内主机通信实施端到端的通信保护；本地主机向远端主机发起安全关联协商，协商数据需要通过各自安全网关的安全隧道进行数据转发，安全网关能检测到隧道嵌套，并且通知各自本地子网内进行该安全关联协商的主机；主机接收通知，分别协商与本地安全网关之间的延伸隧道，成功之后以本地延伸隧道替换与远端主机之间的嵌套隧道，至此逻辑隧道构成，安全关联协商完成。可见，隧道交换应用环境中，关键是如何检测延伸隧道需求，如何协商延伸隧道。从安全性考虑，接收到的隧道嵌套通知和安全网关配置信息需进行认证，确认它的确由可信任网关发出。另外，为实现逻辑隧道范围内，安全网关和子网内主机之间的通信必须采用延伸隧道保护，在安全网关需要维护隧道交换表，该表确定了哪类通信必须采用延伸隧道保护。

由于引入隧道交换，要求 IKE 实现在有无隧道交换的应用下都能成功协商 SA，因此在标准 IKE 实现基础上需要考虑隧道嵌套的检测、延伸隧道协商和逻辑隧道建立等一系列新的问题。

2.2 逻辑隧道维护

逻辑隧道由延伸隧道和主干隧道构成，每个隧道都有自己的生命期限，当生命期限结束时，需要重新协商 SA，并且更新 SA 属性。当安全策略发生改变，IP 数据不再需要逻辑隧道保护时，需要删除逻辑隧道。由于逻辑隧道是由延伸隧道和主干隧道组成，主机安全策略改变并不影响主干隧道，只需删除延伸隧道。位于逻辑隧道末端的主机由于安全策略的改变，向本地安全网关发出延伸隧道删除通知，并在本机进行延伸隧道删除处理。

3 隧道交换技术的实现和性能分析

Linux FreeS/WAN [6] 是 IPSec VPN 在 Linux 操作系统上的实现，是一个开放源码的项目。我们在它的基础上引入并实现了隧道交换技术。修改了 Linux FreeS/WAN 中 IKE 实现，增加了对隧道交换技术的支持；在 IP 包的 IPSec 协议处理中增加了隧道嵌套检测功能和隧道交换表的维护和查找。其中最为关键的是对安全关联协商功能中增加逻辑隧道协商的实现。

搭建一个拓扑结构如图 1 所示的测试环境，移动

主机和安全网关到公共网络的接口是网通宽带，子网内的本地局域网采用 10M 以太网，并且采用共享式集线器实现子网内各设备的连接。连接在公共网络的设备相互之间配置并建立 IPSec 隧道，建立隧道为网状拓扑结构。相互通信的两台主机之间进行 FTP 数据传输，子网 1 内的两台主机 A1，B1 安装 FTP 服务器软件 Serv－U Ver. 5.0，其它子网内主机和移动主机安装 FTP 客户端软件 LeapFTP Ver. 2. 7. 2，此两款软件都自带有流量和实时速率以及传输时间的统计。

性能测试，比较子网内的通信方别采用隧道嵌套，隧道交换和明文传输三种方式，比较它们之间的数据传输速率，并且测试了三种方式中，主机 MTU 设置对传输速率的影响。测试在主机 A1 和 A2 之间，进行 FTP 文件传输测试，测试结果如表 1 所示：

表 1　三种方式下 MTU 值对性能的影响

Packet transfer method in subnet①	Value of MTU② (Byte)	Average rate of traffic③ (KBps)
Plain text④	1420	99
	1300	92
Embedded tunnel⑤	1420	47
	1300	84
Switch－tunnel⑥	1420	98
	1300	92

①子网内通信方式，②主机 MTU 设置，③平均传输速率，④明文，⑤隧道嵌套，⑥隧道交换

结果表明：明文传输和隧道交换的传输速率基本没有差别，原因是子网内为 10 兆以太网，而公共网络的接口速率是整个数据传输的瓶颈，而网关和主机的 IPSec 处理没有成为瓶颈。而 MTU 值对速率的影响比较大，尤其在隧道嵌套情况下 MTU 设为 1420 时，主机之间的通信速率降为明文传输的一半左右，从 IP 包的捕获结果发现安全网关对嵌套的 IP 包封装对该包进行了分片处理，导致了速率明显下降。

采用隧道方式下的 ESP 加密方式，采用以太网作为链路层，根据 ESP 包格式可以估算一次隧道封装需要的占用字节最少为 62 字节（加密填充字节为 0，ICV 字节 32 字节），那么在 1500 的 MTU 的限制下，隧道嵌套将导致 IP 包的有效数据传输效率降低。由于每次嵌套时都需要增加至少 62 字节的长度，所以当长度超过 1500 时需要对数据包进行分片，实际应用中，大部分的网关为了保正高性能，对分片数据包直接丢弃，而不是把它重组后进行处理。所以隧道嵌套在实际应用中会受到限制。

4　结论

实验结果表明本文提出的隧道交换技术能正确将 IPSec 隧道延伸到保护子网内的主机，从而满足保护子网之间的两台主机进行保密通信的需求。相对于其它方案，此方案安全网关需要多进行一次加解密的运算，这将加重安全网关的负担，尤其在追求高性能的场合下将成为瓶颈。但是，随着技术的发展，可以获得的计算能力在不断地提高，而成本却不断降低。在安全性为第一要素的应用中，可以采用高性能硬件平台进行加速，获得需要的性能。

参考文献

1 S. Kent，R. Atkinson. Security Architecture for the Internet Protocol. RFC2401，IETF，1999.

2 S. Kent，R. Atkinson. IP Authentication Header RFC2402，IETF，1999.

3 S. Kent，R. Atkinson. IP Encapsulating Security Payload (ESP) RFC2406，IETF，1999.

4 D. Harkins，D. Carrel. The Internet Key Exchange (IKE) RFC2409，IETF，1998.

5 G. Huang，S. Beaulieu，D. Rochefort A Traffic－Based Method of Detecting Dead IKE Peers，Internet Draft，IETF 2004.1.

6 http://www.freeswan.org.