文章编号:1000 - 582X(2004)03 - 0049 - 04

移动 IP 技术在 VPN 中的应用*

罗 娅,姚家宁,皇甫涛,邹宗惠
(重庆大学 计算机学院,重庆 400030)

摘 要:虚拟专用网络 VPN(Virtual Private Networks)是实现在公网上安全传输私有网络信息的一种技术。作为 VPN 的关键技术之一的隧道技术解决了移动节点的移动性问题。在介绍 L2TP 与 IPSec 这 2 种 VPN 隧道机制的基础上对它们进行了比较,重点介绍了 IPSec 在安全性方面的优势,然后介绍了 VPN 移动用户的问题和 VPN 的 2 种隧道模型,最后分析了利用移动 IP 技术解决 VPN 中的移动用户问题的优点,并与现有方案 VPDN(Virtual Private Dial-up Network)作了比较。

关键词:虚拟专用网;移动 IP;虚拟拨号专网;隧道技术;第 2 层转发隧道协议; IP 安全机制
中图分类号:TP393.01 **文献标识码**:A

虚拟专用网 VPN[1] 是 Internet 迅速发展的产物,它综合了专用和公用网络的优点,允许有多个站点的团体或组织使用公用网络作为其站点之间交流的通道,拥有一个虚拟的完全专有的网络。隧道技术是 VPN 的核心技术。在 VPN 的隧道协议中常用的有 L2TP,IPSec 等,其中 L2TP 虽然已经成为行业标准,但它还存在一些安全隐患。IP VPN 框架中隧道模型分为强制隧道和自发隧道两种,其中强制隧道相对于自发隧道在解决局域网接入的移动用户方面存在有局限性。VPDN 是用于解决 VPN 中的移动用户问题的技术。但 VPDN 是基于 L2TP 和强制隧道的。而移动 IP 技术是在保留原 IP 地址的基础上实现移动用户的通讯问题的技术,它基于第 3 层隧道,可采用自发隧道模型,因此可与 IPSec 结合来解决 VPN 的移动用户问题。笔者将在简要介绍上述技术的基础上讨论移动 IP 在 VPN 中的应用。

1 VPN 的隧道协议[2]

隧道技术是 VPN 的核心技术,它使 VPN 能在公用网络上安全地传输私有数据。隧道技术主要负责将传输的原始信息经过加密、压缩处理、协议封装后嵌套在另一种协议的数据包中,像普通数据包那样进入网络进行传输。有许多种 IP 隧道机制,如 IP/IP、GRE、L2TP、IPSec、MPLS 等。虽然有些协议没有被视作隧道协议,但它们采用的技术措施实际上是相同的,即是从封装包的地址域提取转发信息,将不透明帧作为包载荷通过 IP 网络传输。

1.1 L2TP

L2TP 是一种第 2 层的隧道协议,它的前身是 Microsoft 公司的点到点隧道协议(PPTP)和 Cisco 公司的第 2 层转发协议(L2P)。L2TP 是它们优点的结合,并已成为事实上的工业标准。特别是 L2TP 已成为组建 VPDN 的首选协议。但是 L2TP 也有一些安全性问题:

1)仅对隧道终端实体进行身份验证,无法抵抗地址欺骗。

2)本身不提供加密手段,当数据要保密时依赖其它技术的支持。

3)不对每个数据报进行完整性校验,可能遭受拒绝服务攻击。

后面我们还将谈到 VPDN 在采用 L2TP 与 PPP 协议时存在的数据报丢失的潜在问题。

1.2 IPSec[3]

IPSec 不是单个的安全协议,它提供的是安全算法以及常用结构的集合。其中结构允许一对通讯实体使用任何一种安全算法用以提供通讯安全保证。IPSec 使用的协议包括:封装安全载荷 ESP、验证头 AH、Internet密钥交换 IKE 等。

1.3 IPSec 与 L2TP 的比较

第 2 层与第 3 层隧道协议的主要区别在于用户数据是在网络协议栈的第几层被封装的。前面谈到的 L2TP 在安全方面的缺陷使得 L2TP 的控制报文和数据报文很容易受到攻击,例如:通过监听数据报可以很容易地发现用户身份标识符;可以通过发送否认消息报文来攻击隧道和隧道中的 PPP 连接等。另外 L2TP 协议以及要在 VPDN 中一起使用的 PPP 协议提供的认证和加密机制根本不能满足 VPN 的安全要求。L2TP 隧道的认证机制只能提供 LAC(L2TP Access Concentrator)和 LNS(L2TP Network Server)之间在隧

* 收稿日期:2003 - 10 - 20
作者简介:罗娅(1978 -),女,重庆人,重庆大学硕士研究生,主要从事网络技术及网络安全方面研究工作。

道建立阶段的认证,不能保护隧道中的报文。PPP 的加密由于没有提供密钥的有效管理手段,使得加密控制协议 ECP 不能提供对密钥协商过程的保护。L2TP 没有密钥管理机制,但它的认证过程又需在隧道中分发口令,因此存在很大的安全隐患。

IPSec 提供一整套基于 IPv4 和 IPv6,互操作性强、性能好的安全机制。它能提供访问控制、无连接数据的完整性验证、数据内容的机密性保护、抗重播保护等功能。除了前面提到的 AH、ESP、IKE 外,IPSec 还有一些安全机制,如:安全联盟 SA(Secure Association)定义 IPSec 的连接;IPSec 的密钥管理工作由 IKE 完成;IPSec 是一系列在其内部使用认证与加密算法的协议集合,其中 2 种认证和 7 种加密算法已经被定义下来,可满足用户的不同要求。运用 IPSec,用户可以同时使用 Internet 与 VPN 的多点传播功能,而 L2TP 只能执行点对点 VPN 的功能,无法同时执行 Internet 的应用,使用时不方便。

2 VPN 中移动用户的问题

在 VPN 中经常会有移动用户访问专用内部网的情况出现,如公司的出差人员需访问公司数据信息或传回实时信息。由于这样的用户的访问机制的特殊性,在 VPN 中的移动用户问题被作为一个专门的问题提出。

用户从 VPN 中移出而直接连接到公用网中,由此产生并需解决的问题有以下几个:

1)地址问题

首先由于 VPN 中的 IP 地址不能直接在公用网上使用,移动用户在移出 VPN 直接连接公用网时,原有的 IP 地址必须改变。地址的改变使得 VPN 中的安全网关有可能拒绝此主机的访问。这是由于在 VPN 中的安全网关对于出入的 IP 包都要进行处理。所作的处理是以存放在 SPD(安全策略数据库)中的安全策略为标准的。在 SPD 中的配置软件中由于效率原因一般是支持基于 IP 地址的策略配置,通过 IP 地址来确定用户的身份和相关信息。这样对于移动用户改变 IP 地址将会使得访问被拒绝。同时,用户新的地址分配采用什么策略也是需要考虑的。

2)封装与认证等问题

在 VPN 内,传输信息的封装、认证等问题都是由安全网关解决的,在主机上无需配置 IPSec 等协议的程序组件,当由于主机移出了安全网关的保护范围,封装/解包、加密/解密、认证、访问控制等一系列问题必须寻求其它方法解决。

3 强制隧道与自发隧道

强制隧道和自发隧道是在 IP VPN 框架中[4]提出的 2 种隧道模型,现有的隧道技术都采用这 2 种隧道模型。

3.1 强制隧道

强制隧道是指这种情况:一个网络节点(如拨号服务器或者网络接入服务器),作为 LAC,把用户的 PPP 会话通过骨干网伸展到远端 LNS,如图 1 示。这对于向 LAC 发起 PPP 会话的用户 host 来说是透明的。这正是 L2F 规范所支持的一种情况,L2TP 规范保留了这项支持。

目前 ISP 在解决 VPN 的移动用户问题上所采用的 VPDN 协议,就是基于强制隧道的模型。

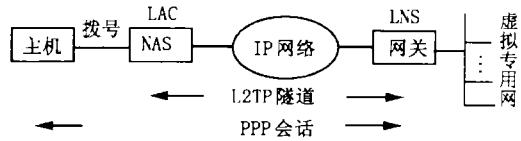

图 1 强制隧道模型

3.2 自发隧道

自发隧道是指这种情况,一个用户通过 host 发起的隧道连接远端站点,不需要中间网络站点的介入,如图 2 所示。PPTP 规范就是基于自发隧道模型的,L2TP 集成了 PPTP 的一部分。就像强制隧道一样,它也有许多不同的应用场合,图 2 中表示的就是用户用 L2TP 或者 IPSec 作为自发隧道接入一个 LNS。

移动 IP 技术就是基于自发隧道的。

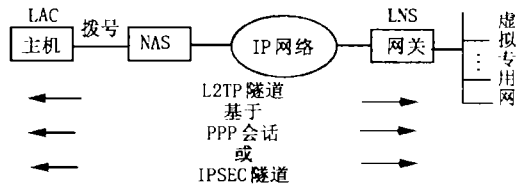

图 2 自发隧道模型

3.3 两种隧道模式的比较

前面已经提到,现在通常对 VPN 移动用户的解决办法大都采用 VPDN 协议的强制隧道模式。在强制隧道模式中,移动用户与 ISP 之间是采用 PPP 拨号直接连接到一个拨号接入网络上。随着网络的发展,大多数的主机将通过小型的以太网、本地区域网接入 Internet。因此 VPDN 的现有模式存在一定的局限性,正受到网络发展的冲击,而隧道的自发模式就可以弥补这方面的缺陷。

但在自发隧道中必须考虑开销问题,特别是需要使用安全性好的 IPSec,当主机是通过低带宽拨入连路连接时,开销显得十分重要。现在的 VPDN 几乎都是建立在 L2TP 上的。但 L2TP 存在很多无法解决的安全问题,常常采用的办法是使用 L2TP 的同时用 IPSec 来保障安全,但无论是在数据平面还是控制平面,开销中包含额外的头。例如 Web 应用将工作在如下的协议栈上:HTTP/T CP/IP/ PPP/ L2TP/UDP/ESP/IP/PPP/AHDLC;而 IPSec 单独使用:HTTP/TCP/IP/ESP/IP/PPP/AHDLC,所以如果使用自发隧道模式,则最好单独使用 IPSec。

4 VPDN 与移动 IP

4.1 VPDN(Virtual Private Dial-up Networks)

虚拟专用拨号网(VPDN)是指利用公共网络的拨号接入网实现的虚拟专用网。它是强制隧道模型的一

种应用。用户通过 PSTD 或 ISDN 拨号到 NAS(即强制隧道中的 LAC),NAS 通过 PPP 将隧道延伸,通过 IP 网络到达网关 GW。VPDN 所采用的隧道层次来说可以是第 2 层,也可以是第 3 层。具体实现 VPDN 的隧道技术有:GRE,PPTP,L2TP 和 MPLS 等。用户由拨号获得动态的地址,以用户名@公司名的方式进行认证。

4.2　VPN 中引入移动 IP[5]

在 VPN 中引入移动 IP 技术的原因有几个:

1)前面已经比较了强制隧道和自发隧道,说明了强制隧道在局域网接入时的局限性,在当前的很多访问技术(接入技术)中,把多个主机连接到以用户为前提的访问设备(接入设备)的最经济的方法就是通过以太网。并且还要尽量保持设备的低成本,同时又要求不改变或很少改变其配置。

2)文中第 3 节中还提到自发隧道如采用 L2TP 再依赖 IPSec 的效率低的问题。如果利用移动 IP 技术可以解决局域网接入、单独采用 IPSec 的问题。

3)在 VPDN 中,PPP 通过 L2TP 隧道在 IP 骨干网上传输时存在一个潜在的问题,那就是选择 PPP 参数的不慎会导致频繁地重启动和超时,特别是使用了压缩技术以后。PPP 在采用并行线路地 IP 骨干网中出现上述问题的原因是 L2TP 在传输过程中可能打乱了数据报的顺序而且会产生对数据报的静丢弃。而自发隧道采用的序列号措施则可以解决错序问题。

4)在 2.1 中提到,VPN 网关的认证方式如果是基于 IP 地址方式的,移动用户 IP 地址改变意味着认证方式必然改变,否则节点不能访问 VPN 网内。移动 IP 本身不用改变 IP 地址,因而应用层通讯不用中断。移动 IP 是采用第 3 层隧道的,而 IPSec 协议正是基于第 3 层的,所以采用 IPSec 的移动 IP 是可行的。

4.3　移动 IP

移动 IP 技术支持主机移动的主要思路是:在不改变现有网络路由方式和主机 IP 地址的基础上,提供一种转发机制,使发向移动主机的分组能安全地到达主机地当前节点。而完成转发功能的实体是移动节点的家代理(Home Agent)和其辅助作用的外代理(Foreign Agent)。

4.3.1　移动 IP 技术[6]

当移动主机移入新的网络时,要通过两个过程:代理发现(Agent Discovery)和注册(Registration)。为了实现代理发现,移动 IP 使用现有 ICMP 路由发现定义的路由广告和路由请求消息,移动节点定期发送代理请求(Agent Solicitation),收到代理广告(Agent Adversement)以确定现在所在位置并获得转交地址。然后通过注册请求和注册应答取得与家代理和外代理的绑定。这里要提到转交地址分为 2 种:"外代理转交地址"和"联合转交地址"。地址的不同直接使得隧道的终点不同。前者是用外代理的 IP 地址作为转交地址,隧道的终点是外代理,即外代理参与数据报的拆封;而后者是通过 DHCP 或其它地址分配协议获得的当前网络内的一个独立的地址,隧道的终点是移动节点,即自己对数据报进行拆封。如果存在反向隧道(Reverse Tunneling),意味着反向隧道的起点也不同。

4.3.2　移动 IP 在 VPN 的应用模型

将移动 IP 技术应用于 VPN 中的移动用户通讯,应注意以下几个方面的问题:

1)与 VPN 外部用户的通讯

与一般的移动 IP 不同,对于 VPN 移动用户,整个网络应分为 VPN 内部与外部。移动用户与 VPN 外部的的通讯,由于用户已经获得转交地址,此时采取的方法应与移动 IP 技术一样,移动用户用转交地址与其它用户 VPN 外部的用户采用一般路由机制通讯。对于与一般主机的通讯,移动节点如果想对对方隐藏自己当前的位置,可以使用移动 IP 技术提供的隐藏主机位置的功能。

2)与 VPN 内部用户的通讯

首先,由于各 VPN 采用不同的加密算法、认证机制和安全级别,因此让移动节点的外代理完成对数据的拆封、解密等工作是非常不安全也是不实际的。所以,移动节点往往需要自己完成对数据的拆封和解密。移动 IP 在一般情况下可不采用反向隧道,主机发出的数据不用封装。但移动主机在跟 VPN 内部主机进行通讯时反向隧道就是非常必要的了。对于移动 IP 的反向隧道,很多的路由器都不支持,所以有必要让主机自己作为隧道的起点,发起与 VPN 内部网的隧道。移动主机作为反向隧道的起点也要承担对数据的加密和封装的任务。这样作为隧道的一个端点的主机必须采用"联合转交地址"作为它的转交地址来进行通讯。实际上这就是自发隧道中 LAC 与主机为统一体的模型。这要求移动节点上必须安装相应的软件以支持这些功能,这让移动主机在网络上具有更大的独立性和灵活性。

其次,在安全性方面,移动 IP 技术本身就有许多安全性措施,例如:家代理与移动节点可以采用缺省算法为 MD5,密钥大小为 128 位的认证。该方法排除了很多潜在的对移动 IP 认证协议的攻击,同时移动 IP 技术也可采用其它的认证算法和认证模式。针对注册请求的重放攻击,移动 IP 还提供了使用时间戳或随机数的重放保护机制。由于移动 IP 技术所采用的隧道技术和 IPSec 的隧道技术都是第 3 层的,这样可以很好地将移动 IP 技术与 IPSec 结合起来。实际上,应用在 IPv6 上的移动 IP 技术 MIPv6 就已经把 IPSec 作为它的安全技术了。

前面讨论的是移动节点与原来所在地的 VPN 的通讯情况,实际上一个 VPN 往往是由多个分支站点组成的。对于有很多分部和合作伙伴的 VPN,移动节点在与原所在地以外的 VPN 站点通讯时可采用以下方法:传给移动节点的数据报可通过家代理接受后用隧道转发给节点。此处实际上是 2 个隧道的串连。将 2 个隧道串连是可能的。如,一个 LAC 发起一个隧道到中继设备,该中继设备作为第一 LAC 的 LNS,同时是后一个 LNS 的 LAC。对于移动节点传出到分部的数据报,也可采用这种隧道串连机制,先传给家代理,家代理拆封后重新封装,通过隧道传到隧道终点。

5 结束语

移动 IP 是基于网络层解决移动问题的方案，当 IPSec 与它结合后，可使它用在 VPN 的移动用户问题上。采用 VPDN 的移动用户通过 NAS(即 LAC)提供与 VPN 内部通讯的隧道连接，但 VPDN 对于通过局域网而非拨号接入的移动用户存在局限性。移动 IP 技术中移动用户可自主的发起与 VPN 中的 GW(即 LNS)的连接。这对于移动用户采用局域网的接入方式与 VPN 通讯是非常方便的。这种模型对于自己建立 VPN 的团体或组织来说比 VPDN 更方便，因为用户不用事先申请 VPDN 业务，不用交纳 VPDN 的费用。而且只要与 VPN 协商好，移动用户可采用任意的隧道，如 IP/IP、GRE 等，因此具有更好的自主性和独立性。

参考文献：

[1] RFC 2685, Virtual Private Networks Identifier[S].
[2] RFC 2003, IP Encapsulation Within IP[S].
[3] 何宝宏. VPN技术综述[J]. 中国数据通信，2002，4:10－14.
[4] RFC 2764, A Framework for IP Based Virtual Private Networks[S].
[5] RFC 2002, IP Mobility Support[S].
[6] RFC 2344, Reverse Tunneling for Mobile IP[S].

Application of Mobile IP in VPN

LUO Ya, YAO Jia-ning, HUANG Fu-tao, ZOU Zong-hui
(College of Computer Science, Chongqing University, Chongqing, 400030 China)

Abstract: VPN is a technology that realizes the security transmission of private information through the public network. As one of key technologies, tunnel technology resolves the mobility problem of mobile nodes. Firstly, L2TP and IPSec have been compared based on these two tunnel principles introduction of VPN. Secondly the advantages of IPSec in security have been introduced. Then, the problems of mobile host and two models of tunnel in VPN have been introduced. Lastly, the advantages of utilizing the mobile IP to resolve the problem of mobile host have been analyzed, and this technology has been compared with VPDN.

Key words: VPN; mobile IP; VPDN; tunnel technology; L2TP; IPSec

(编辑 张 苹)

(上接第 52 页)

Clustering Detection Algorithms for Network Intrusions

YE Fang, WU Zhong-fu, LIU Yong-guo

(Department of Computer Science, Chongqing University, Chongqing 400030, China)

Abstract: Traditional abnormal detection methods need a reference model with a profile of normal action, but building the character profile and specifying threshold of abnormal alarm are difficult. So this paper puts forward intrusion detection in combination with clustering and data processing. This algorithm comes true dynamicly updating the center of cluster and the biggest distance within cluster with fast convergence. The effect is better with the help of pre-processing the data. By means of simulated experiments, this algorithm is proved feasible and efficient for unknown intrusion detection.

Key words: intrusion; network intrusion detection; clustering

(编辑 吕赛英)