动态网络环境下建立 VPN 的安全动态隧道机制

刘 利　胡 鹏　李津生　洪佩琳
(中国科学技术大学电子工程与信息科学系　合肥　230027)

摘　要：随着多种接入方式的出现，许多局域网接入公共网络采用了动态地址的连接，静态配置的虚拟专用网(VPN)便不再适用。本文研究了动态网络环境下如何交换信息、建立 VPN。提出了安全动态隧道机制，定义了动态建立隧道的报文格式，解决了上述问题，并进一步增加了加密认证和抗重播攻击的功能，避免引入的安全隐患。经实验证明，该机制可以安全有效地在动态网络环境下建立 VPN。

关键词：虚拟专用网，隧道，动态网，非对称数字用户数字线路
中图分类号：TP393.08　　**文献标识码**：A　　**文章编号**：1009-5896(2005)08-1310-05

Secure and Dynamic Tunneling Mechanism of Construction VPN in Dynamic Network

Liu Li　Hu Peng　Li Jin-sheng　Hong Pei-lin
(*Dept of Electronic Engineering and Information Science, University of Science and Technology of China, Hefei* 230027, *China*)

Abstract　As emergence of several access methods, many LANs use access of dynamic IP address. Virtual Private Network(VPN)of static configuration is not applicable. Thus, how to exchange information, construct VPN in dynamic network is indicated as new question for research. A secure and dynamic tunneling mechanism is presented. And message of this mechanism is defined. This mechanism can solve above mentioned issue. Authentication and anti-replay function are introduced to avoid secure problems. The result of experiment shows that this mechanism can construct VPN securely and efficiently in dynamic network.

Key words　Virtual Private Network(VPN), Tunnel, Dynamic network, ADSL

1　引言

随着网络技术的迅速普及，越来越多的企业和单位建立了自己的局域网，并且通过各种方式接入 Internet。企业希望能够将分布在各地的局域网通过 Internet 连接起来，迅速安全地传递信息、共享数据。

虚拟专用网(Virtual Private Network，VPN)是在公共网络里建立一个逻辑的、安全的专用连接的技术，这种连接通常称为隧道。以往，企业为了连接分布在各地的局域网时，要利用服务提供商(ISP)的专线(如 DDN)，其费用昂贵。为降低网络的运营费用，利用 Internet 技术构筑内部网的需求日益强烈，IP-VPN(以下简称 VPN)技术在这一背景下迅速发展普及。

VPN 传输数据时，通过 VPN 设备对数据加密形成 Internet 上可以传输的 IP 数据流，利用 Internet 上创建的隧道将 IP 数据流送往目的网络，在另一端使用相应的解密算法对数据进行解密，获得数据。这样，分布在各地使用 VPN 的用户通过 Internet 上的安全隧道传输数据，感觉就像在同一个局域网内一样。

根据不同的需要，VPN 主要分为以下 3 种类型[1]：

(1) 内部网 VPN　将分布在各地的局域网连接建立的 VPN，使得所有的数据可以共享。

(2) 远程访问 VPN　公司总部局域网和远程出差雇员连接建立的 VPN，为移动办公的人员提供服务，或者应用于电子商务。

(3) 外部网 VPN　公司与商业伙伴之间建立的 VPN，提供部分的受限服务。

实现 VPN 的隧道协议主要有第二层转发协议（Layer 2 Forwarding, L2F），点到点隧道协议(Point to Point Tunneling Protocol, PPTP)和第二层隧道协议(Layer 2 Tunneling Protocol, L2TP)，它们主要是远程访问型 VPN 的标准协议。IPSec(Internet Protocol Security protocol)是在网络层上实现认证与加密的安全协议，已由 IETF 标准化。采用 IPSec 技

2004-03-28 收到，2004-07-16 改回
国家自然科学基金(90104011)资助课题

术已被广泛用于第 3 层 VPN 即 IP-VPN，它能够建立隧道，对 IP 应用进行加密和认证。本文主要讨论基于 IP-VPN 的安全动态隧道机制。

文献[2,3]中，主要研究了在网络资源计费不同，费用动态变化的网络环境下，如何选择一条廉价的隧道建立 VPN，以实现费用最少。本文在上述文献的研究基础上，发现不只是费用动态变化需要选择一条隧道，而且随着接入方式的不同，网络的拓扑结构也不同。每次建立 VPN 的时候，都需要获得与以前不同的动态变化的地址，本文提出的动态隧道机制解决了这一问题。文献[5]中提到了 VPN 的安全问题，为了保证在公共网络中 VPN 的安全建立，传输数据，本文进一步改进了上述机制，增加了加密认证和抗重播攻击的功能，解决了公共网络建立 VPN 存在的安全隐患。

2　静态 VPN 及问题

内部网 VPN 如图 1 所示，子网 A，B，C 利用 VPN 网关设备在不安全的 Internet 中建立安全的隧道，在此安全隧道中透明传送数据。

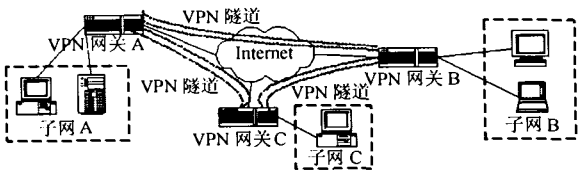

图 1　内部网 VPN 示意图

当前使用的 VPN 是在隧道两端建立人工配置的、静态的、点到点连接，保持硬件设备中的静态路由表，建立静态的 VPN[2]。这种静态配置的隧道需要单独管理，而且网络拓扑的结构很难维持与控制，因此维护的代价很大。

随着 Internet 的发展普及，许多企业的局域网接入了互联网，并将分布在各地的局域网连接构建 VPN。随着 VPN 规模的变大，每次新加入一个局域网，就要对所有的站点作新的配置，因此采用人工建立隧道方式的效率是十分低下的。

非对称数字用户线路(Asymmetrical Digital Subscriber Line，ADSL)能够提供廉价的宽带接入服务，因此许多企业用户选择了拨号 ADSL 接入 Internet，并且仍希望将分布在各地局域网连接建立 VPN。但是，每次拨号连接获得的 IP 地址都是变化的，路由信息也随之变化。而且 VPN 网关可能不是时刻都在工作，有时需要关闭，重新启动后获得的地址和以前的也会不同，这就要求每次建立隧道前修改隧道配置信息。在动态的网络环境里[3]，如何快速地将本地的地址与路由信息通知到隧道对端并获取对端的地址与路由信息，就成了必须解决的问题。并且随着 VPN 规模变大，隧道数目增加，人工维护的代价急剧增加。

目前，正在使用的非对称 ADSL 专线业务的上行速率不超过 512kbps，下行速率不超过 2Mbps。某些企业拥有很多局域网，由这些局域网构建的 VPN 规模较大，需要建立许多隧道连接，单个 ADSL 链路不能满足用户需求，希望能够获得更大的带宽。若是租用更大宽带接入，将要付出很大花费。经济的做法是租用多条廉价 ADSL 链路。于是如何同时使用多条 ADSL 链路构建 VPN 网络，进行负载均衡，成为亟待解决的问题。

本文提出了一种能够快速地自动交换地址和路由信息，以便能够自动创建隧道，并能够综合使用多条链路，进行负载均衡的机制。此外，还提出了在 Internet 上交换信息时经过不安全的公共网络，保证安全地传送信息，安全地建立隧道的解决方案[4]。

3　解决方案

3.1　动态地址更新

当 VPN 网关使用拨号 ADSL 接入 Internet，会自动获得一个全局的 IP 地址，并且获知路由信息。但是，这个地址和路由信息每次都是动态变化的，因此建立 VPN 隧道时应该将这些信息及时准确地通知到对端 VPN 网关，当建立隧道的双方都采用拨号接入方式时，对端的地址也在变化，这就需要首先获得对端网关的地址信息。

本文提出一种机制，使得 VPN 网关有一个唯一标识，并且由可信的第三方机构管理这个标识。VPN 网关每次使用拨号接入时，都会将自己新获得的 IP 地址通知第三方机构进行更新。隧道的对端只需要每次访问这个第三方机构，查找这个唯一标识，获得对方的 IP 地址，然后与之进行通信。如果使用多条链路，有多个 IP 地址，只需要将 VPN 网关的一个地址更新到第三方机构，这个地址通常是网关的默认转发地址。最简单的例子就是 DNS 域名系统，每个 VPN 网关都有一个域名，每次接入时，到域名服务器更新该域名对应的 IP 地址。隧道的对端只需要访问该域名服务器就可以知道更新后的 IP 地址了。但是域名系统更新地址时，没有对更新请求进行认证，可能会带来一些安全隐患，可以采用对更新请求进行加密认证的方法来保证其安全性。

3.2　负载均衡

企业用户的 VPN 网络规模较大，需要建立许多隧道连接时，单个的链路不能满足带宽需要。用户为了以经济的方

式增加带宽，可以同时使用多条链路接入。在建立隧道的时候采用某种调度策略，综合使用这几条链路建立隧道。

调度策略有以下几种：

(1) 轮询　轮询是最简单的调度策略，将 ADSL 链路编号，在建立隧道时依次使用每条 ADSL 链路，使得各个隧道平均分配到每条链路上。这种策略可以用于 VPN 网关刚启动建立隧道的时候。

(2) 链路数据业务量　VPN 网关可以实时监控每条链路的数据业务量，当需要建立隧道时，根据当前流量或是某个时间段内的统计流量，来选择一条负载较轻的链路建立隧道。这种方法可以用于 VPN 网关已经在使用的场合。

(3) 链路的隧道数　VPN 网关根据每条链路已经建立的隧道数目，找到一条隧道数最少的链路使用，建立下一条隧道。这种方法也可以用于 VPN 网关已经在使用的场合。

上述几种调度策略在建立隧道的不同场合时使用。在 VPN 网关刚开始启动时建立隧道，这时还没有数据业务，最好的方式就是采用轮询，把隧道平均分配到每一条链路上去。在建立隧道时，可能隧道对端的 VPN 网关并没有启动，隧道尚不能建立，需要等到对端网关开启时接受请求再建立隧道。这时，本地的 VPN 网关已经工作，并且要不断地监听请求，一旦收到隧道建立请求后，可以采用第 2 种调度策略，选择一条流量较少的链路建立隧道。隧道对端的 VPN 网关有可能关闭，该条隧道就会自动被删除，VPN 网关运行一段时间后，各条链路上的隧道数目可能不再均衡。因此，若再有新的隧道建立时，VPN 网关可以采用第 3 种调度策略，选择一条隧道数最少的链路使用。有时，也可以综合使用以上几种调度策略，或者定义其它的调度策略。

3.3 动态隧道机制(Dynamic Tunneling Mechanism)

如上所述，有了获取动态 IP 地址和链路负载均衡的方法后，便需要一套机制能够在隧道的两端进行通信，告知对方一些必要的信息，然后建立隧道。本文提出动态隧道机制，可以实时传输建立隧道的必要信息，动态地建立隧道，并且定义了通信时传输的报文格式如图 2(a)。建立图 2(a)，隧道所必需的信息包括：

(1) 报文类型(Type)　本文定义了两种报文，隧道建立请求报文(REQ，用于请求建立隧道时使用)，应答报文(ACK，用于接收到请求的隧道对端回应本地信息时使用)；

(2) VPN 网关的标识(Gateway Identity)　这个信息保存在 VPN 网关的隧道配置文件中；

(3) IP 地址(IP Address)　拨号连接后获得的动态 IP 地址，如果使用多条链路，还需要通过调度策略选择一个合适的 IP 地址；

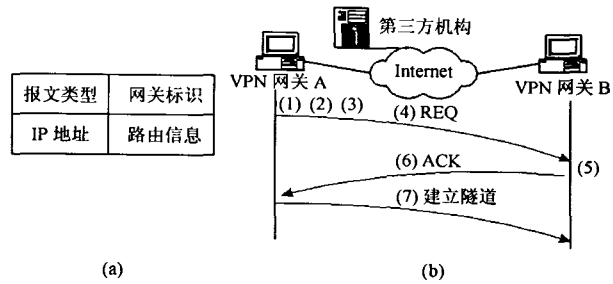

图 2　动态隧道机制报文格式和工作过程示意图

(4) 路由信息(Routing Information)　建立隧道所需要的必要的路由信息，如 VPN 网关的下一跳路由器地址。

本文提出的动态隧道机制(DTM)，步骤如下(如图 2(b)，VPN 网关 A 与 VPN 网关 B 建立隧道)：

(1) 网关 A 首先查询隧道配置文件，获得对端网关 B 的标识，查询到该网关现在的地址，以供通信时使用。

(2) 查询本网关拨号后获得的 IP 地址，如果使用多条链路，使用调度策略选择一个 IP 地址。因为网关 A 只需要将自己的一个地址更新到第三方机构作为自己的通信地址，而网关 A 在建立隧道时，要在多个地址中选择一个，所以有时选择建立隧道的这个地址和网关 A 更新到第三方机构的地址不一样。

(3) 查询本网关的路由信息，例如下一跳路由器地址。

(4) 根据步骤(1)获得的网关 B 的地址，网关 A 向 VPN 网关 B 发送隧道建立请求报文，报文各个域值为：Type 域为 REQ；Gateway Identity 域为 VPN 网关 A 的标识，用来表明是网关 A 发出的请求；IP Address 域为步骤(2)中选择的 IP 地址；Routing Information 域为步骤(3)获得的路由信息。

(5) 网关 B 收到建立请求报文后，根据 Gateway Identity 域获知网关 A 的标识，查询隧道配置文件知道需要建立的隧道名称；由 IP Address 域和 Routing Information 域获得网关 A 的地址和路由信息。

(6) 类似于步骤(1), (2), (3)，网关 B 查询到 A 的通信地址，获得自己的地址信息和路由信息后，向网关 A 发送应答报文，报文各个域值为：Type 域为 ACK；Gateway Identity 域为 VPN 网关 B 的标识，用来表明是网关 B 发出的应答；IP Address 域为网关 B 选择的 IP 地址；Routing Information 域为网关 B 的路由信息。网关 B 根据网关 A 和自己的地址和路由信息，更新本地隧道配置信息，准备建立隧道。

(7) 网关 A 收到网关 B 的应答报文后，根据网关 B 和自

己的地址和路由信息，更新本地隧道配置信息，建立隧道。

使用上述的动态隧道机制，可以在动态的网络环境下建立 VPN，并且能够调度使用多条链路，达到负载均衡的目的。但是，在不安全的 Internet 传递这些通信报文，会导致一些安全隐患。

恶意的攻击者可以伪造报文，向 VPN 网关发送。如果没有任何的加密或认证措施，VPN 网关收到这些报文之后，就会按照伪造的报文上面的地址和路由信息更新隧道配置文件，并按此配置文件建立隧道。结果会无法正确建立隧道，甚至已经建立好的隧道也会受到破坏，从而造成拒绝服务(DOS)攻击[5]。

如果只是对报文进行加密和认证，攻击者也可以截获报文进行重播(replay)攻击。因为 VPN 网关有时重新拨号获得新的 IP 地址和路由信息，需要发送新的报文，以前的报文就过期了，上面的地址和路由信息也就作废了。攻击者对以前截获的报文，不必做修改，就将它发送给对端的 VPN 网关。对端的 VPN 网关收到后，按照这个作废的地址和路由信息更新配置文件、建立隧道。结果不能正确建立隧道，因此这也造成了攻击。

由上面的两点分析，动态隧道机制尚不能在不安全的网络环境里安全的建立隧道，需要增加加密认证和抗重播攻击的功能。

3.4 安全动态隧道机制(Secure and Dynamic Tunneling Mechanism, STDM)

为了增加报文加密认证和抗重播攻击的功能，本文在动态隧道机制的基础上，提出了安全动态隧道机制，并将报文格式做了修改，如图 3(a)。

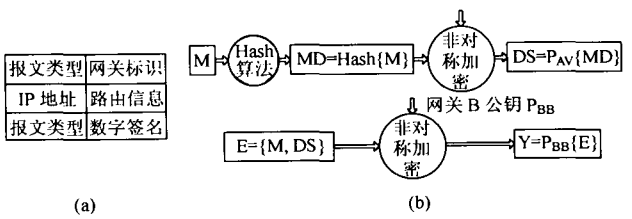

图 3　安全动态隧道机制的报文格式和加密认证示意图

为了抗重播攻击，报文中增加了报文序号，每条隧道对应一个报文序号。VPN 网关在一开始创建隧道的时候将报文序号置为 0，以后每发一次报文，报文序号加 1。VPN 网关重新拨号连接建立隧道时，读取保存的报文序号继续使用，始终保持报文序号递增。对端的 VPN 网关收到报文后，先检查报文序号，和保存的该隧道的序号比较，当收到序号大于以前的序号时，才进行下一步的操作；否则丢弃，不做任何操作。这样，即使攻击者截获了 VPN 网关的报文，再发给对端网关，对端网关根据报文序号就可以判断这是过期的报文，不予理睬，达到了抗重播攻击的目的。

为了增加报文加密认证功能，本文引入了公/私钥加密算法，每一个 VPN 网关拥有一对公/私钥，并可以在可信的第三方机构查询到对端的公钥。如图 3(b)所示，VPN 网关 A 在准备好报文各个域的值后，先使用自己的私钥 P_{AV} 做数字签名，然后再用网关 B 的公钥 P_{BB} 加密发出。VPN 网关 B 收到信息后，解密认证。具体过程如下：

(1) 报文的前 5 个域记为 M={报文类型，网关标识，IP 地址，路由信息，报文序号}，使用 Hash 算法求 M 的 Hash 值 MD=Hash{M}。然后使用网关 A 的私钥 P_{AV} 对 MD 加密得数字签名 $DS=P_{AV}\{MD\}$。

(2) 将 DS 添加到 M 之后，{M,DS}即为如图 3(a)所示的报文，记为 E={M,DS}。使用网关 B 的公钥 P_{BB} 对 E 加密得 $Y=P_{BB}\{E\}$。将 Y 发送给 VPN 网关 B。

(3) VPN 网关 B 收到 Y 后，使用自己的私钥 P_{BV} 解密 Y 得 E={M,DS}。

(4) 网关 B 使用 Hash 算法求得 M 得 Hash 值 MD'，再使用 P_{AB} 解 DS 获得 MD，比较 MD 和 MD'来验证报文是否来自于合法的报文发送者以及报文的数据完整性。

VPN 网关使用 SDTM 构建 VPN，可以在动态的网络环境中安全有效地交换信息，建立隧道，解决了本文前面所分析的问题和安全隐患。并且，上述的加密认证方法可以应用于前面分析的 DNS 域名系统的安全问题。

4　实验

本文采用了 FreeSWAN 软件作为搭建 VPN 网络的基础，并在 3 台机器上配置了该软件作为 VPN 网关，构成了如图 1 的实验环境。FreeSWAN 是一个免费的、公开源代码的 VPN 软件。

每台 VPN 网关采用 ADSL 拨号接入 Internet，并且有两台机器使用两条 ADSL 链路。每个网关之间配置一条 IPSec 隧道，在 VPN 网关连接的内部网中的机器配置内部地址。使用本文提出的动态隧道机制(DTM)开发了实验程序，并配置到各个 VPN 网关上。开启 VPN 网关后，检查隧道连接情况，可以正常建立隧道，并且使用两条链路的网关按照调度策略实现了负载均衡，各个内部网中的主机可以通过隧道进行通信。此时，没有任何的安全措施，我们使用 VPN 网关 C 作为攻击者，假冒网关 A 向网关 B 发送伪造的报文，网关 B 因此更新了隧道配置，导致了隧道断开，造成了 DOS 攻击。

我们又使用 VPN 网关 C 进行重播攻击实验，首先截获网关 A 发送的请求报文，再将网关 A 重新拨号，获得新的 IP 地址与网关 B 建立隧道，然后网关 C 将 A 的已经过期的报文发送给网关 B，又导致了隧道断开。

然后，我们使用 SDTM，对程序进行了修改，增加了报文序号和加密认证功能。VPN 网关之间的隧道仍然可以正常建立，并且以上的攻击手段已经不再有效，经实验证明使用 SDTM 可以安全有效地在动态网络环境里建立 VPN。本文提出的 SDTM 开发出软件，已经应用于众多企业组建 VPN。

5 结束语

Internet 的开放性导致了攻击者可以对网络的任何地方进行攻击，即使使用了性能极强的加密技术建立 VPN 隧道，攻击者仍可能从局域网接入点进行攻击。随着企业上网、电子商务等的需要，VPN 技术有着广阔的应用前景。伴随着新的网络技术出现，对于 VPN 技术又提出了新的要求。本文针对拨号接入方式的动态网络环境下如何安全建立 VPN 的问题，提出了安全动态隧道机制(SDTM)，解决了如何根据动态获取的 IP 地址来更新 VPN 的隧道配置、建立隧道，并讨论和解决了由此引入的新的安全问题，为局域网接入点提供了安全保护。

参 考 文 献

[1] Venkateswaran R. Virtual private networks. *IEEE Potentials*, 2001, 20(1): 11 – 15.

[2] Huan Liang, Kabranov O, *et al*.. Minimal cost design of virtual private networks. Proceeding of the 2002 IEEE Canadian Conference on Electrical and Computer Engineering, 2002, vol.3: 1610 – 1615.

[3] Anerousis N. Dynamic virtual network dimensioning in cost-sensitive environments. Global Telecommunications Conference, 1999. GLOBECOM '99, 1999, vol.2: 1511 – 1516.

[4] Metz C. The latest in virtual private networks: part I. *IEEE Internet Computing Magazine*, 2003, 7(1): 87 – 91.

[5] Ramanujan R, Kaddoura M, *et al*.. VPNshield: protecing VPN services from denial-of-service (DoS) attacks. DARPA Information Survivability Conference and Exposition, 2003, Proceedings , 2003, vol2: 138 – 139.

刘 利： 男，1983 年生，博士生，研究方向为通信协议和网络安全.

胡 鹏： 男，1981 年生，博士生，研究方向为通信协议和网络安全.

李津生： 男，1937 年生，教授，博士生导师，研究领域为下一代网络体系结构.

洪佩琳： 女，1961 年生，教授，博士生导师，研究领域为网络策略控制和信息安全.