

HP ProCurve TMS VPN解决方案

通过IP或MPLS网络部署TMS VPN

简介	2
业务挑战	2
解决方案概述	2
解决方案	4
为何选择HP ProCurve?	6
总结	7
术语表	7

简介

Web、电子商务、在线游戏等诸多网络服务日益普及，而且越来越多的数据也通过网络进行传输。互联网是一个应用广泛的公共网络，业务交易通常通过互联网等不可信的共享网络进行传输，因此数据安全变得至关重要。

解决方案提供商目前面临的挑战在于提供安全、可靠的网络，并且这些网络要具备更高吞吐率、更低延时和更强的可扩展性。虚拟专用网络 (VPN) 是安全网络的一个重要部分，支持各种规模的企业远程访问站点网络。

HP ProCurve威胁管理软件 (TMS) 可以提供经济高效且基于标准的VPN解决方案，以满足企业不断变化的业务需求。TMS模块可插入ProCurve 5400和8200系列交换机，具备在网络基础架构中轻松进行迁移或安装的部署灵活性。TMS支持IP security (IPsec)、VPN和IPSec上的GRE VPN，以实现安全的网络隧道，并可以在互联网或无线网络等不可信的网络上创建TMS，确保网络两端数据的机密性、真实性和完整性。通过隧道传输的数据经过加密，并且只能通过通信端点解密。TMS提供身份验证机制，用以限制对授权用户的连接和访问。通过TMS VPN隧道传输的数据进入路由后不能予以修改或更改，否则将被TMS VPN丢弃。

VPN是一项应用广泛且不断发展的技术，可通过多种途径从不同层级创建。TMS VPN可以在多协议标签交换 (MPLS) 网络上建立。该网络利用标签标记数据包，然后再根据标签转发数据包。这是一项服务提供商广泛部署的技术。本文将向您介绍不同的TMS VPN解决方案，并解释如何高效应用这些技术提供安全的网络连接。

业务挑战

有了可信赖的专用网络或站点后，企业才能保证专用网络之间传输的数据的机密性、完整性和安全性。这些用户通常需要支持以下两种技术：

- 远程访问 – 允许远程用户使用TMS远程访问功能连接站点网络。远程用户可以通过内置Microsoft L2TP客户

端或ProCurve IPSec客户端连接到部署在站点网络边缘的TMS VPN。

- 站点到站点 – 可以配置两个IPSec VPN网关，以实现两个不同网络间安全的站点到站点通信。例如，可以在两个TMS VPN模块间建立连接。

由于业务区域的多样性，大型企业需要与一个国家乃至全球的多个站点进行安全的网络连接。服务提供商也有这种需求，但在成本、技术可用性和带宽需求方面存在差异。针对业务规模和垂直市场的这些特定需求影响企业选择用以连接站点网络的VPN技术。

TMS VPN解决方案通常由最终用户进行部署和管理，服务提供商可以在自己的网络中提供VPN，因此最终用户无需管理自己的VPN。MPLS-VPN是一项部署在提供商网络中的VPN技术。但是，可变的部署因素会影响最终用户和提供商，例如部署时间、灵活性、每月VPN费用和培训成本。

影响VPN部署的一个因素是将VPN解决方案集成到最终用户使用的整个安全框架中。VPN普遍用于保护站点网络的连接。防火墙和入侵防护系统 (IPS) 等其他技术也广泛用于控制访问和深入检查数据包。对于数据中心数量少但园区数量多的企业，远程站点与数据中心站点间连接的高可用性通常十分重要。因此，拥有高可用性和经济适用性的总体安全解决方案 (包含 VPN) 成为另一热选。以下章节将向您概述TMS VPN解决方案，并介绍它们如何解决最终用户面临的各种挑战。

解决方案概述

专用线路或虚拟电路上的VPN

VPN最重要的一个功能是通过服务提供商网络或互联网连接不同的专用站点网络。在建立此连接的过程中，可通过多种方法建立VPN，以解决来自第1层、第2层或第3层的问题。最近，有些VPN通过租用电信公司的专用电话线物理连接不同的站点。该方法的缺点之一是部署成本高且物理安全站点网络间的连接不灵活，另一缺点是无法建立长距离VPN，因为专用线路存在物理局限性。

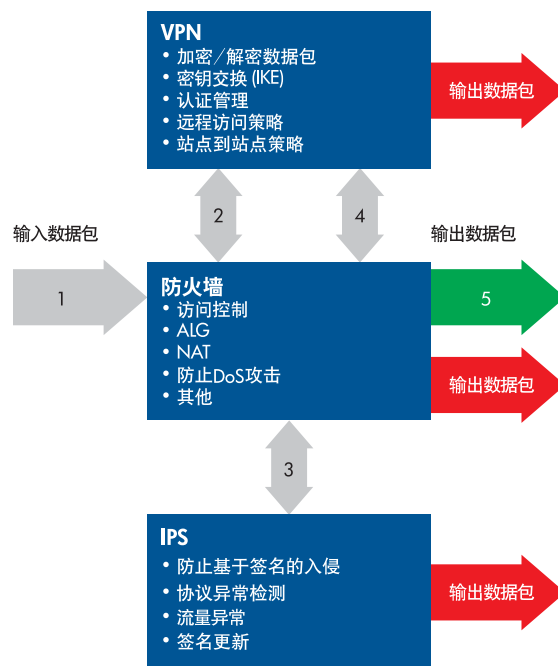
服务提供商要提供专用线路, 在扩展至提供商网络时会遇到挑战。

技术领域日新月异, 而一些用户仍在使用这一解决方案。现在, 有些用户通过租用服务提供商的虚拟电路建立VPN。帧中继和ATM是服务提供商广泛用于实施虚拟电路的两种技术。这些VPN在第2层运行, 并可以在虚拟电路上提供可靠、安全的站点间通信。与租用专线相比, 此方法使VPN能够更灵活地配置和管理虚拟电路。但是这些虚拟电路的价格依然十分昂贵, 部署起来也十分耗时, 而且提供商扩展网络时会遇到技术难题。因此, 租用的专线或虚拟电路均无法提供可行的远程访问解决方案。绝大多数最终用户会利用互联网等公共网络部署VPN, 或者由服务提供商通过MPLSVPN等先进技术在提供的网络中配置VPN。当VPN部署因成本高和灵活性低而不再采用租用专线或虚拟电路时, 以太网或ATM上的IP网络成为提高网络连接性的理想选择。

威胁管理软件架构

TMS可以在一个模块上运行。该模块可添加到ProCurve 5400和8200系列交换机, 并具有防火墙、VPN和IPS功能。下图显示了TMS软件中的高层数据包流和TMS中各组件的功能。TMS具备高可用性, 可充分满足企业用户的需求。例如, 同一机箱中可部署两个模块, 一个作为主设备, 另一个作为备用设备。如果主设备出现故障, 其管理的连接可以顺利切换到备用设备。用户可利用前端GUI或CLI界面配置TMS软件和查看其运行状态。

TMS是一个汇编软件套件, 其独特优势是集成了防火墙、VPN、IPS和高可用性等特性。此内置软件集成降低了管理复杂性。它的另一大优势是在数据中心轻松迁移和安装刀片。对于需要在数据中心部署网络基础架构的最终用户, 可管理性是除成本与稳定性之外的另一重点考虑因素。TMS模块也集成到了ProCurve网络管理软件PCM中, 它可以大大减轻网络管理员管理成百上千个TMS模块的工作负担。



上图显示了指定发送到TMS模块的高层IPSec数据包流。IPSec数据包总是首先进入防火墙组件, 然后防火墙将数据包传送到VPN组件进行加密。加密后的数据包被传回防火墙, 由防火墙针对防火墙策略和DoS攻击等对数据包进行检查。经过防火墙处理后, 加密的数据包被发送至IPS进行签名检查, 然后再次传送到VPN组件进行策略检查, 或根据数据包的要求管理密钥或证书。之后, 可以创建新的数据包, 并将其传回防火墙等待发送。如果其中任一步骤失败, 数据包都会被丢弃。

TMS VPN概述

TMS VPN解决方案以IETF工作组定义的行业标准为基础。通过实施IPSec架构, TMS VPN可确保数据的机密性和完整性, 并支持身份验证和防重播。对于站点到站点连接, 可以建立IPSec隧道或通过IPSec的GRE隧道。TMS可以为远程访问提供IPSec之上的L2TP隧道或IPSec隧道。但是, GRE与L2TP都无法确保数据安全性, 而是利用IPSec保护GRE或L2TP隧道中传输的数据。

TMS提供以下VPN功能组件:

- 数据包加密和解密
- 密钥管理: 互联网密钥交换 (IKE)、手动密钥管理、PKI

- IPsec NAT穿越
- VPN策略管理: 远程访问策略与站点到站点策略
- 集中星型VPN连接性
- IPsec隧道
- L2TP隧道 (计划通过Radius实现L2TP)
- GRE隧道

支持的加密技术包括:

- 通过预共享密钥、RSA和DSA签名进行的身份验证
- Diffie-Hellman Group 1至Group5
- 加密算法 – DES、3DES和AES
- 数据验证 – 带有ProCurve IPsec客户端软件和Windows XP、Vista L2TP客户端的SHA1和MD5Compatible

IPsec的优势是可以经济高效地部署, 并能够灵活运用目前大多数应用广泛的传输技术: 公共互联网、服务提供商IP主干网和基于MPLS的网络。

MPLS-VPN部署

许多服务提供商都通过MPLS-VPN在提供商网络中部署VPN。MPLS的理念是在数据包网络上模拟电路交换网络, 完美融合了以连接为导向的交换与无连接纯路由服务的优势。MPLS为网络数据包分配短整型标签, 用以描述它们的网络传输方式。MPLS将路由的智能性与交换的出色性能完美结合, 通过现有的本地IP架构、本地IP和ATM, 或混合其他第2层技术使服务提供商获得显著优势。除可扩展性外, 其优势还包括端到端QoS。

MPLS-VRF具有卓越的可扩展性和安全性, 并提供QoS支持, 其复杂性主要存在于提供商的网络, 最终用户无需维护VPN。尽管具有这些强大的优势, 但MPLS依然存在以下缺点:

- 提供商所面临的复杂性 – 致使部署延迟、大量培训和高额成本。
- 用户所面临的不灵活性 – 用户必须依靠服务提供商来配置和部署VPN, 导致最终用户无法使用此项技术。
- 成本 – 最终用户需要投入高维护成本。

- 集成 – 最终用户可能需要将VPN与TMS防火墙、IPsec解决方案等其他安全解决方案相集成。
- 地理因素 – 部分远程站点不一定能访问MPLS网络。对于上述情况, MPLS-VRF不可行。

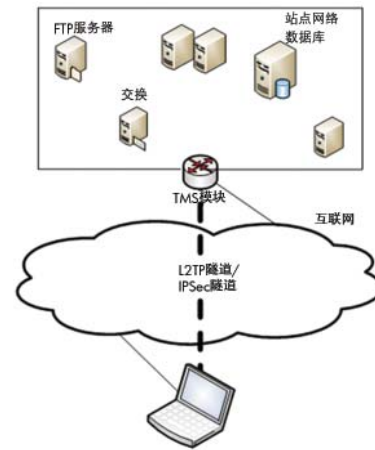
解决方案

TMS远程访问部署

如下图所示, TMS VPN可以提供远程访问解决方案。

远程用户可以连接至服务提供商网络或互联网。用户希望连接的站点网络可能是拥有自身网络地址空间的专用网络。TMS作为连接互联网或服务提供商网络的VPN网关部署在站点网络的边缘。经过部署后, TMS可以用于维护大量专用于其站点网络和远程用户身份验证机制的IP地址。建立L2TP或IPsec隧道后, 远程用户将获得一个用于在站点网络内通信的内部IP地址。

远程用户可以从PC启动ProCurve IPsec客户端软件, 建立一个带有TMS VPN网关的IPsec隧道。为确保远程用户与TMS VPN网关间的连接安全, 隧道需要建立在IPsec之上。建立L2TP或IPsec隧道之后, 远程用户便可以安全地远程访问站点网络。

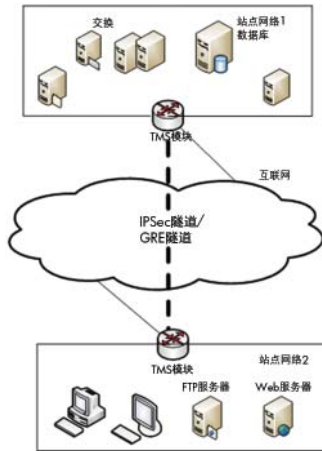


上图显示了远程用户从PC启动VPN客户端, 以连接站点网络VPN路由器 (TMS模块)。下表显示了不同隧道模式支持的VPN客户端。

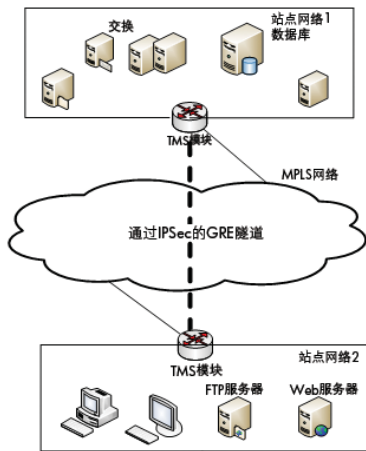
支持的隧道	Windows VPN客户端	Mac VPN客户端
IPsec之上的L2TP隧道	XP/Vista中的内置L2TP客户端	内置L2TP客户端
IPsec隧道	XP上的ProCurve VPN客户端	其他

TMS站点到站点VPN部署

下图显示了典型的站点到站点TMS VPN部署。该图中，一家公司拥有两个站点和两个站点网络。要连接这两个站点网络，需要将两个TMS模块作为VPN路由器部署在站点边缘，并将其连接至服务提供商网络或互联网。可以通过服务提供商网络建立一个隧道，该隧道可以是IPSec隧道，也可以是GRE隧道。借助当前的TMS软件静态配置这两个TMS VPN网关，使其转发指向其他站点网络的数据包。



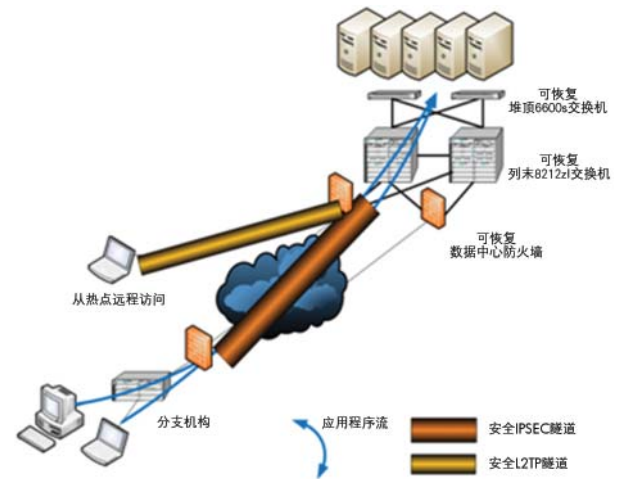
对于IPSec上的IPSec隧道或GRE隧道，上图显示了不必配置VPN或感知VPN的服务提供商网络或互联网。服务提供商网络的路由器可以全部是非VPN路由器。VPN网关（TMS模块）必须经过配置，以支持远程访问或站点到站点VPN。这使得TMS VPN成为一个经济高效、易于部署的解决方案。但是需要注意的是，提供商网络可以是VPN感知网络，并能够配置VPN，如稍后将提到的MPLS-VPN。以下章节将介绍GRE VPN解决方案及其在提供商网络中的部署情况。



TMS VPN防火墙集成

在有关远程访问和站点到站点TMS VPN解决方案的上图中，TMS模块可以直接连接互联网或服务提供商网络。如果直接连接互联网，TMS模块必须有一个可路由的IP地址。通常，如果TMS等模块连接到互联网或服务提供商网络，需部署防火墙，由此保护专用站点网络。除访问控制外，大多数站点网络都有其专用网络地址，并使用NAT将专用地址转换为可路由的IP地址。TMS防火墙组件内置NAT和访问控制支持，因此除VPN外，该模块还可以启动TMS防火墙访问控制和NAT。

下图显示了远程访问和站点到站点VPN配置防火墙和IPS后的典型TMS部署。防火墙符号表示8200交换机或5400交换机中TMS模块提供的防火墙功能。远程用户可以建立一个L2TP隧道，用于访问主数据中心站点的资源。同时，分支机构的用户可以通过IPSec隧道访问数据中心的资源。



GRE/IPSec VPN的优势

IPSec VPN和GRE VPN的主要优势：

- 基于标准 — 确保与其他VPN网关厂商和VPN客户端的出色互操作性，保护最终用户的投资。
- 易于部署 — 无需更改现有IP网络的基础架构，即可在现有的任一IP网络中轻松部署。
- 地理因素 — 利用互联网时，IPSec/GRE VPN隧道不受地理因素的限制。
- 安全性 — IPSec有助于确保数据保密性，可通过一套灵活的加密和隧道机制保护网络上传输的数据包。通过数字证书或预共享密钥对用户进行身份验证，不符

合安全策略的数据包无法通过隧道。GRE隧道没有用于保护自身的GRE隧道加密或身份验证机制,但是可以利用IPSec (传输模式) 保护数据传输。

能会影响对TMS VPN解决方案或其他VPN解决方案的选择。

IPSec/GRE VPN也有其局限性,存在的两个缺点包括:

- 1 需要全网格VPN站点时服务提供商网络和VPN客户的可扩展性问题
- 2 服务质量 (QoS) 问题

下表从几个方面归纳了TMS VPN解决方案的优势:

- 1 部署 (成本、时间、地理因素、灵活性)
- 2 安全性支持: 数据机密性
- 3 组播支持
- 4 可管理性
- 5 集成
- 6 适应VPN发展趋势

为何选择HP ProCurve?

虚拟电路上的VPN、互联网上的IPSec VPN、MPLS-VPN等VPN技术具有截然不同的部署特性和优势。每种技术都有其满足客户需求的优势和领域。许多不同的因素可

TMS IPSec和VPN解决方案的一个优点是,能够适应以太网进入WAN空间的VPN发展趋势。TMS根据防火墙分区和VLAN管理安全性,并自然地适应这种长期发展趋势。

组件		TMS IPSec VPN	TMS GRE VPN
部署	成本	低	低
	时间	短	短
	地点	边缘,本地环路	边缘
	灵活性	高	高
	维度	不受限制	不受限制
	远程访问	是	否
安全性	站点到站点 VPN	是	是
组播支持		强	GRE/IPSec的安全性强
可管理性		无	待定
集成	单一设备管理	便于用户使用的UI	便于用户使用的UI
	与网络管理软件相集成	是	是
VPN发展趋势: 以太网进入WAN空间	集成了防火墙/NAT/IPS	内置	内置
	具有高可用性	内置	内置
		适合该发展趋势	适合该发展趋势

总结

以下是各种优势的简短总结。

- 1 TMS VPN是一个远程访问解决方案, 而MPLS-VPN还不适合作为远程访问解决方案。
- 2 对于站点到站点VPN, TMS VPN是MPLS-VPN的替代解决方案, 可降低成本, 缩短部署时间, 并且不受提供商的限制。
- 3 TMS VPN解决方案非常灵活, 因为它们独立于基本的IP网络。可以利用此优势在站点网络中创建更精细的粒度, 从而进一步增强安全性。
- 4 TMS VPN甚至可以部署在一个或多个MPLS网络上。在这种情况下, 可以把MPLS网络当作一种 WAN 技术。

术语表

- **转发等价类 (FEC)** — FEC是一组可用同一方式 (例如同一路径或相同的转发处理方式) 转发的IP数据包。
- **标签** — 一个简短而定长的连续物理标识符, 用于识别FEC, 通常在本地有效。
- **MPLS域** — 一个运行MPLS路由和转发的连续节点集合, 同时也包含在一个路由/管理域内。
- **MPLS边缘节点** — 连接MPLS域和一个域外节点, 因为该节点不运行MPLS和/或因为它在不同的域中。请注意, 如果LSR有一个不运行MPLS的相邻主机, 则该LSR是一个MPLS边缘节点。
- **MPLS出口节点** — MPLS出口节点属于MPLS边缘节点, 用于处理 MPLS 域输出的流量。
- **MPLS入口节点** — MPLS入口节点属于MPLS边缘节点, 用于处理进入MPLS域的流量。

科技以推动业务成效为本

欲了解详情, 请访问: www.hp.com.cn/network

© Hewlett-Packard Development Company, L.P. 2009年版权所有。本文信息如有更改, 恕不另行通知。惠普产品与服务的全部保修内容在此类产品和服务附带的保修单中明确说明。本文所含信息不得视为额外的保修承诺。惠普对于本文所包含的技术或编辑错误、遗漏概不负责。

2009年6月 4AA2-6702CHP

