

Quidway 金融网络 MPLS VPN 解决方案

利用统一的计算机网络同时开展多种增值业务，是各大银行应用系统的最新发展趋势。将各种传统业务从专有系统环境移植到计算机网络上，不仅可通过计算机网络带来更佳灵活性、兼容性，而且还可以大大扩展服务范围，提高服务质量，降低运营成本。然而同时，网络资源的集中也带来了一系列新的问题，如不同业务系统在同一个网络上承载，如何有效的实现逻辑上的隔离、实现不同类别业务的区别服务等等都是需要仔细设计的环节。

随着中国金融系统网络大集中的逐步实施，网络业务横向集中，网络架构纵向集中的趋势日趋深刻，而业务网络物理统一，逻辑上要求安全隔离的呼声也越来越高，如何在统一的网络平台上高效、安全而经济的实现新一代金融网络的需求，成为金融用户、网络方案供应商、网络设备供应商面临的共同问题。

华为技术有限公司致力于提供面向用户的，可裁剪、可扩展、高效、实施简便的专业化金融网络解决方案，面向上述需求，华为公司推出了基于 Quidway 系列网络产品平台 MPLS 和 IPSEC 技术的一体化 VPN 解决方案。

MPLS VPN 技术概述

MPLS（多协议标签交换）技术最初是用来提高路由器的转发速度而提出的一个协议。但是由于 MPLS 在流量工程和 VPN 这两项在目前 IP 网络中非常关键的技术中的表现，MPLS 已日益成为扩大 IP 网络规模的重要标准。

MPLS协议的关键是引入了标签（Label）交换概念。标签是一种短的，易于处理的，不包含拓扑信息，只具有局部意义的信息内容。

基于BGP4的MPLS VPN技术是一种运营级的VPN技术，在网状网以及需要在同一个IP网络上承载多个相互独立的VPN的时候，MPLS VPN表现出强大的扩展性和高性能。

基于 MPLS 的 VPN 特性必须实现如下功能：LDP（Label Distribution Protocol）标签分布协议，是 MPLS 的信令协议，用以管理和分配标签；MPLS 转发模块，根据报文上的标签和本地映射表进行二、三层间交换；MBGP 和 BGP 扩展，用来传递 VPN 路由和承载 VPN 属性、QoS 信息、标签等内容；路由管理的 VPN 扩展，建立多路由表，用以支持 VPN 路由。

在 MPLS VPN 网络中，有必要引入三个概念：

- ◆ CE（Custom Edge）用户 Site 中直接与服务提供商相连的边缘设备，一般是路由器，也可以是交换机或者主机；
- ◆ PE（Provider Edge）骨干网中的边缘设备，它直接与用户的 CE 相连；
- ◆ P 路由器（Provider Router）骨干网中不与 CE 直接相连的设备。

在运营网中，MPLS VPN 的网络构造由服务提供商来完成。在这种网络构造中，由服务提供商向用户提供 VPN 服务，用户感觉不到公共网络的存在，就好像拥有独立的网络资源一样。同样在金融企业网络中实现 MPLS VPN 业务，对于使用业务的不同类别用户来说，也是完全感觉不到大网存在的。同样，对于骨干网络内部的 P 路由器，也就是不与 CE 直接相连的路由器而言，也不知道有 VPN 的存在，而仅仅负责骨干网内部的数据传输。

所有的 VPN 的构建、连接和管理工作都是在 PE 上进行的。PE 位于服务提供商网络的边缘，从 PE 的角度来看，用户的一个连通的 IP 系统被视为一个 site，每一个 site 通过 CE 与 PE 相连，site 是构成 VPN 的基本单元。一个 VPN 是由多个 site 组成的，一个 site 也可以同时属于不同的 VPN。属于同一个 VPN 的两个 site 通过服务提供商的公共网络相连，VPN 数据在公共网络上传播，必须要保证数据传输的私有性和安全性。也就是说，从属

于某个 VPN 的 site 发送出来的报文只能转发到同样属于这个 VPN 的 site 里去，而不能被转发到其他 site 中去。同时，任何两个没有共同的 site 的 VPN 都可以使用重叠的地址空间，即在用户的私有网络中使用自己独立的地址空间，而不用考虑是否与其他 VPN 或公网的地址空间冲突，这也是 MPLS VPN 适合多业务多用户网络使用的主要原因之一。

MPLS/BGP VPN的特点

华为公司MPLS/BGP VPN解决方案可以为金融网络提供一种基于网络、易于管理、扩充性好、安全且具有QoS保障、可在任意节点间连接的VPN。

(1) 基于网络，易于管理：这种基于网络的VPN可以完全由骨干网络来实现，不同业务用户可将VPN的管理完全“托管”给骨干网络管理机构，即最终业务网络用户完全感觉不到该业务网与其他业务网络的集成（就像使用物理上独立的一套网络一样），不用了解VPN是如何构造和连接的，由骨干网络管理机构在其网络内构建完成。MPLS VPN可以显著地减少运营商和用户的投资，特别适合于金融企业用户集中多业务网络实现Intranet、Extranet。

(2) 扩充性好：由于基于MPLS/BGP实现，因此很容易对网络节点进行扩充，网络可剪裁性好。

(3) 安全：由于基于MPLS/BGP实现，报文在网络节点构成的MPLS域中采用标签转发的形式进行交换（LSP），因此具有同ATM/FR虚电路相同的安全级别。

(4) QOS: 由于基于MPLS/BGP实现，可以利用MPLS技术特有的CoS、RSVP,流量工程等机制，从而能够为用户实现有QoS保证的VPN。

MPLS/BGP VPN的实现

Quidway MPLS 采用虚拟路由表的方法来实现一个路由器上多个 VPN 的路由表。每一个 VPN 对应一个或多个 VRFs(VPN routing/forwarding instance)。VRF 定义连接到 PE 上的 VPN 成员(一个 site)资格。一个 VRF 包括一个 IP 路由表、一个 FIB(forwarding information table)表、相关联的端口、和一些控制路由的规则和参数。

数据包的路由和交换由 VRF 路由表和单独的 FIB 表所控制，每一个 VPN 对应一个路由表和一个 FIB 表。

一个 PE 路由器可通过静态路由、RIP 或 BGP 从 CE 处得到某一个 IP 前缀的路由，该

前缀是标准 IPv4 的前缀。然后，PE 通过加上一个 8 字节的 RD(route distinguisher)将它转换成为一个 VPN-IPv4 的前缀，该前缀属于 VPN-IPv4 的前缀。通过这种方法，可以使用户地址唯一，即用户使用的是 IANA 规定的保留地址。

用于生成 VPN-IPv4 前缀的 RD(route distinguisher)由 PE 路由器的 VRF 配置命令指定。

MBGP 协议为 VPN 的每个 VPN-IPv4 前缀传递 NLRI(Network Layer Reachability Information)。BGP 实体之间的通信出现在两个地方，AS 内的 iBGP 和 AS 间的 EBGP，PE-PE 和 PE-RR(route reflector)之间为 iBGP，PE-CE 之间为 EBGP。

BGP 协议通过 BGP 多协议扩展(BGP, *Multiprotocol Extensions for BGP-4*)来传递 VPN-IPv4 的路由可达性信息，多协议扩展的 BGP 采用的方法为限定 BGP 的 peer 只能从其它 VPN 的同伴处得到 BGP 路由。

IP 包经过 MPLS 标签交换到其目标地址，其选路的基础是 VRF 路由表和 VRF FIB 表。

PE 路由器为每一个从 CE 路由器学到的前缀产生一个 label，然后将这个 label 作为一个 BGP Communities 属性附加到 BGP 更新中传递出去。当一个源 PE 路由器从 CE 路由器处得到一个 IP 包，它使用从目标 PE 路由器学到的 label 将该 IP 包发送出去。当目标 PE 路由器得到这个 labeled IP 包后，将 label 从 IP 包中去除，作为一个纯 IP 包发送到 CE 路由器。

当 labeled IP 包在核心骨干部分传递时，其基于 label switching 或 traffic engineered path 进行，一个用户的 IP 包在核心穿行时，携带了 2 层 label:

- 1、第一层 label 指示到正确的目标 PE 路由器;
- 2、第二层 label 给目标 PE 路由器指示，到哪一个其连接的 site 链路。

Quidway MPLS/BGP VPN解决方案

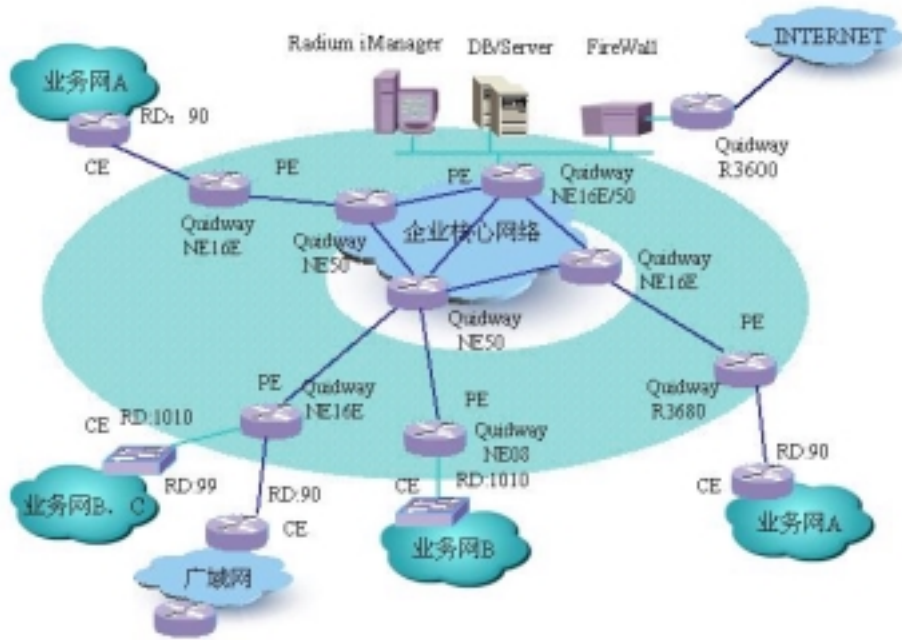


图 1. Quidway MPLS VPN 解决方案

在基于Quidway 产品组建的MPLS VPN网络结构中，所有网络节点以及部分核心骨干层节点都可以设置VPN业务，这些网络节点都作为PE路由器，这些路由器可以是Quidway NE系列路由器也可以是Quidway R3600系列路由器，由于PE节点的特殊性和VPN工作量较大，对于网络结构比较复杂，VPN数量较多的网络，建议全部采用Quidway NE系列产品组建。PE之间的互联可以通过核心骨干层P 路由器进行，也可以直接进行互联。

图示为一个企业集团的内部私网，相对于主干网来说所有的site属于几个VPN，就可以用几个RD来标识，图中假设RD：1010属于储蓄业务用户，而RD：99和RD：90分别属于另两种业务用户，假设是OA和清算等等。作为MPLS VPN的最大特点之一，不同的业务VPN可以使用相同的地址段，这对于结构庞大，地址资源严重不足的集团用户来说，是IP V6以外的另一种可行的地址资源解决方案。

在企业网中心节点上可以设立网管中心，服务器或者 DB 以及 Internet 的出口。

对于中心节点上的共有资源，如 DB 以及金融的大型机等设施，可以通过三层交换机来实现互联，不同的 VPN 通过 PE 不同的 VLAN 子接口接入三层交换机，通过三层交换机访问公共资源，返回的数据报文通过 VLAN 信息进入正确的 VLAN，从而回到正确的 VPN

中。如果不同 VPN 中的地址段重复（冲突），可以在 PE 的 VLAN 子接口中设置 NAT（地址转换），将其转换到企业网公有地址段中。对于访问 INTERNET 等应用，同样可以采取这种方案。

鉴于目前金融网络结构特点，对于层次较多而且要求高安全性较高的需求，华为公司提供了结合 MPLS+Ipsec 的组合解决方案，全面支持当前金融网络系统的 VPN 网络过渡。

组合解决方案示意如图 2 所示：

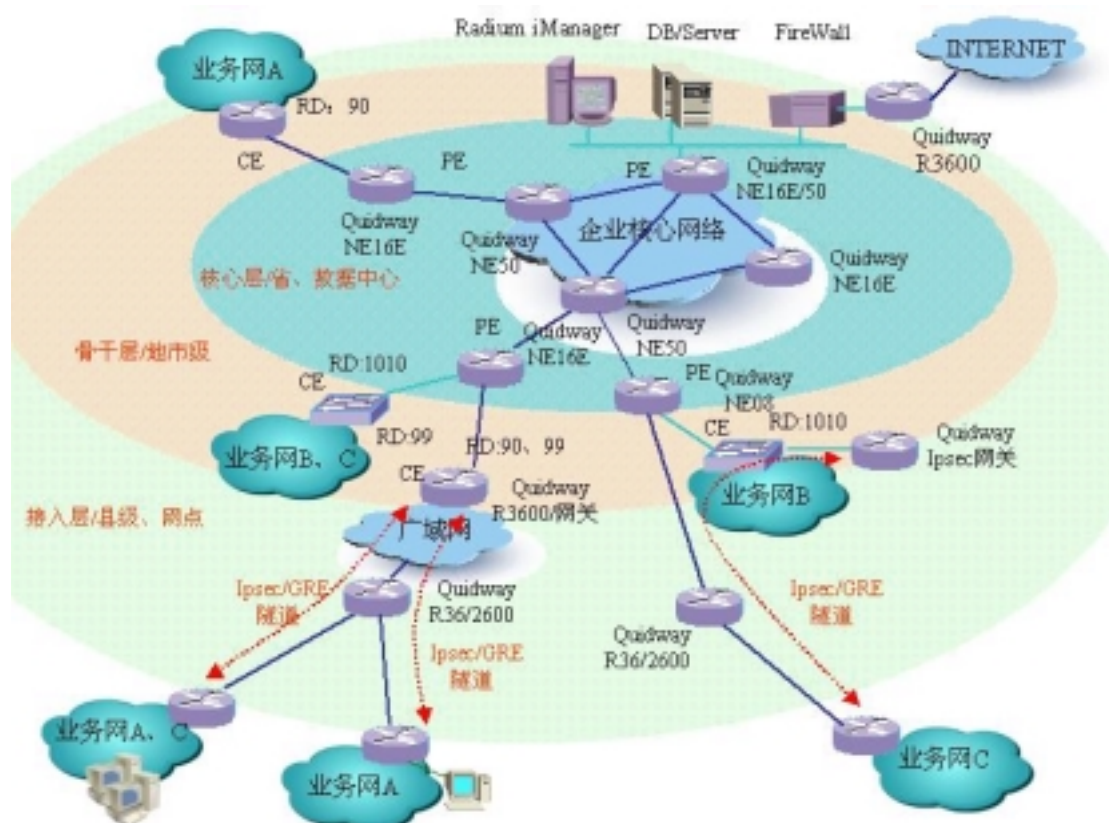


图 2. 组合 MPLS 和 IPSEC/GRE 的解决方案

在对不同的网络层次选择适用的技术的时候，往往不能回避兼顾这样几个方面的问题：

1. 最大程度保证现有设备的可用和其适用效率；
2. 网络的扩展性保证；
3. 网络的安全性保证；
4. 网络的可管理性保证；

与上一部分我们提出的全网 MPLS 相区别，在这一部分描述的解决方案中，我们在边缘网络更多的选择现有通用 VPN 技术，如 L2TP、GRE、IPsec 等。

L2TP、GRE 和 IPSEC 是目前广泛使用的 IP VPN 技术。L2TP 是一种二层隧道协议，目前使用已经较少，GRE 这种三层隧道技术以其广泛的兼容性和维护的简单性，获得了大面积的使用，配合 IPSEC 提供的安全特性，GRE+IPSEC 已经成为隧道 VPN 技术应用的典范。

考虑 GRE+IPSEC 实施方案的一个目的是在实现私有网的同时兼顾网络的高安全性，正如用户所顾虑的，在敏感数据网，越靠近边缘往往从制度上保证的安全措施越薄弱，而对于金融业务网络，任何数据都是至关重要的，所以，我们有必要在使用安全性较低的内联网平台的情况下，充分考虑 VPN 实施的安全特性。

正如图三显示的，我们在省行以下的 VPN 实施主要依靠两个 VPN 协议进行，与上级 MPLS VPN 的对接实现在 PE 设备（华为 Quidway NE08/16E/3600 设备）上，图中的红色虚线显示了 IPSEC 隧道的起止位置。为了解决 IPSEC 对网络系统的资源占用问题，对于隧道数目较多的网络，可以在 PE 设备旁边配置一台 Quidway R3600 设备作为 IPSEC 隧道网关，在 R3600 上扩展一块（根据需要或者是两块）华为公司出品的网络安全处理器模块，就可以集中、高效的处理来自下级网络各地市、县分支处理点建立的 IPSEC 隧道加解密任务，从而实现安全的 VPN 接入。

在 Quidway 的 VPN 实施建议中，加密算法最高可以选择 3DES 进行，下端地市、县的分理处处于 IPSEC 星型结构的末端，支持此算法不必要使用硬件加密卡。关于 IPSEC 以及相关技术，可以参考华为公司提供的《网络安全白皮书》以及《网络安全解决方案》文档，相关文档可以在华为公司数据通信网站（<http://datacomm.huawei.com>）上获取。

在此方案中，GRE 隧道开始于接入网上端的第一个路由设备，在局域网中，通过 802.1Q VLAN 实现各业务系统的二层隔离。

下面我们看一下数据流的传输流程：

在路由器的入端口，网络操作系统通过 IP 报文的子网信息或者直接依据 802.1Q TAG 进行流的分类，区别普通 OA 和支付数据报文，支付报文直接进入 GRE 隧道，打上 GRE 的隧道报文头，在该路由器上行接口上配置策略，应用 IPSEC，再次封装 GRE 数据流，数据流被 IPSEC 加密，加密后的报文流向广域网，在 PE 节点（隧道对端），IPSEC 报文到达广域网路由器，一种方式是直接解密解 GRE 封装进入 MPLS VPN，另一种方式是通过其以太网口首先流入 Quidway R3600，进行 IPSEC 解密，解密后的报文为 GRE 报文，报文通过以太网回到广域网路由器（NE16/08/3600），广域网设备直接通过 GRE 隧道信息剥离 GRE 报文头，将内部数据送入相应的 MPLS VPN 中，其反向操作类似。

这样，一个全程的 VPN 接续流程完成。

通过在不同网络层面实现不同 VPN 技术的方式，使得金融机构可以作到在对原有网络结构、设备改动尽可能的小的情况下，在各个边缘网络之内，由于结构上的灵活性，可以选择 GRE+IPSEC 的方案，也可以根据实际情况选用其它的 VPN 技术，从中心 MPLS VPN 的工作原理上说，都是可以实现顺利对接，但出于敏感网络对安全特性的严格要求，建议在 VPN，特别是边缘使用的非安全保障 VPN 上实施 IPSEC 的 128 或其以上密钥长度的加密封装以进一步保障安全性。

Quidway VPN解决方案的安全性保障

(1) VPN的安全保护

VPN直接构建在公用网上，实现简单、方便、灵活，但同时其安全问题也更为突出。企业必需要确保其VPN上传送的数据不被攻击者窥视和篡改，并且要防止非法用户对网络资源或私有信息的访问。在MPLS VPN网络中，使用标签形式进行报文的转发，具有和ATM/FR虚电路相同的安全级别，可以保证通常应用的数据安全。

在安全性要求很高的场合可以应用加密隧道则进一步保护了数据的私有性、完整性，使数据在网上传送而不被非法窥视与篡改。

例如用户VPN中的用户需要有很重要数据通过VPN网络发送，可以通过IPSEC配置加密隧道选择性传送，加密隧道可以在用户路由器CE设备及其以下设备上配置。

(2) 访问Internet的安全防范

1、地址转换

发地址转换，用来实现私有网络地址与公有网络地址之间的转换。地址转换的优点在于屏蔽了内部网络的实际地址；外部网络不可能穿过地址代理来直接访问内部网络。

支持带访问控制列表的地址转换。通过配置，用户可以指定能够通过地址转换的主机，以有效地控制内部网络对外部网络的访问。结合地址池，还可以支持多对多的地址转换，更有效地利用用户的合法IP地址资源。

Quidway 支持

2、包过滤技术

IP报文的IP报头及所承载的上层协议（如TCP）报头的每个域包含了可以由路由器进行处理的信息。包过滤通常用到IP报文的以下属性：

- IP的源、目的地址及协议域；
- TCP或UDP的源、目的端口；
- ICMP码、ICMP的类型域；
- TCP的标志域

表示请求连接的单独的SYN

表示连接确认的SYN/ACK

表示正在使用的一个会话连接

表示连接终断的FIN

由这些域的各式各样的组合形成不同的规则。比如，要禁止从主机1.1.1.1到主机2.2.2.2的FTP连接，包过滤可以创建这样的规则用于丢弃相应的报文：

- IP目的地址 = 2.2.2.2
- IP源地址 = 1.1.1.1
- IP的协议域 = 6 (TCP)
- 目的端口 = 21 (FTP)

其他的域一般情况下不用考虑。

Quidway 支持基于接口的包过滤，即可以在一个接口的进出两个方向上对报文进行过滤。

Quidway 同时支持基于时间段的包过滤，可以规定过滤规则发生作用的时间范围，比如可设置每周一的8:00至20:00允许FTP报文，而其余时间则禁止FTP连接。在时间段的设置上，可以采用绝对时间段和周期时间段以及连续时间段和离散时间段配合使用，在应用上具有极大的灵活性。使用包过滤防火墙规则，可以根据网络的特点和数据包经过网络的特点，灵活的设计不同的安全规则，来保护网络的安全。

参考方案组网图1。

在VPN解决方案中，包过滤防火墙可以设置在各个业务VPN的出口，也可以设置在整个企业网的出口，在拒绝互通的不同应用共同访问的资源出口节点设置包过滤策略是非常必要的。

(3) 防火墙的安全保护

防火墙是保护一个网络免受“不信任”的网络的攻击，但是同时还必须允许两个网络之间可以进行合法的通信。防火墙具有如下基本特征：

经过防火墙保护的网路之间的通信必须都经过防火墙。

只有经过各种配置的策略验证过的合法数据包才可以通过防火墙。

防火墙本身必须具有很强的抗攻击、渗透能力。

防火墙可以保护内部网路的安全，可以使受保护的网路避免遭到外部网路的攻击。硬件防火墙应该可以支持若干个网路接口，这些接口都是LAN接口（如Ethernet、Token Ring、FDDI），这些接口用来连接几个网路。在这些网路中进行的连接都必须经过硬件防火墙，防火墙来控制这些连接，对连接进行验证、过滤。

由于防火墙具有的特性，防火墙可以设置在私有网路的边界出。例如Internet的出口处、重要内部局域网的出口处等。这样可以更大的程度上保护这些私有网路的安全。