

ICS 33.040.01

M 10



中华人民共和国通信行业标准

YD/T 1909-2009

运营商提供的虚拟专用网安全技术要求

Technique Specification of

Provider Provisioned Virtual Private Network Security

2009-06-15 发布

2009-09-01 实施

中华人民共和国工业和信息化部 发布

目 次

前 言..... II

1 范围.....1

2 规范性引用文件.....1

3 术语、定义和缩略语.....1

4 安全威胁.....2

5 对运营商的安全要求.....5

6 安全技术.....7

7 运营安全防护.....10

附录 A（规范性附录） 三层 VPN 的 PE-PE 数据信息的加密传送.....16

附录 B（资料性附录） 三层 VPN 的 CE-CE 数据信息的加密传送.....18

附录 C（资料性附录） 三层 VPN 几种加密方式的比较.....20

前 言

本标准是 IP 虚拟专用网系列标准之一，该系列标准包括如下标准：

- ◆ 基于网络的虚拟 IP 专用网（IP-VPN）框架
- ◆ 运营商提供的虚拟专用网安全技术要求
- ◆ 基于边界网关协议/多协议标记交换的虚拟专用网（BGP/MPLS VPN）组网要求
- ◆ 基于边界网关协议/多协议标记交换的虚拟专用网（BGP/MPLS VPN）技术要求
- ◆ 公用三层 IP 虚拟专用网（PPVPN）业务技术要求
- ◆ 基于 IP 的二层虚拟专用网（VPN）业务技术要求
- ◆ BGP/MPLS 虚拟专用网测试方法
- ◆ LDP 信令的虚拟专用以太网技术要求
- ◆ LDP 信令的虚拟专用以太网测试规范

本标准的附录 A 是规范性附录，附录 B、附录 C 是资料性附录。

本标准由中国通信标准化协会提出并归口。

本标准起草单位：工业和信息化部电信研究院、上海贝尔阿尔卡特股份有限公司、华为技术有限公司、中兴通讯股份有限公司

本标准主要起草人：吴英桦、田 辉、张立新

运营商提供的虚拟专用网安全技术要求

1 范围

本标准规定了运营商提供的虚拟专用网（PPVPN）在安全技术方面的要求，主要包括 PPVPN 面临的安全威胁、对运营商的安全要求、运营商使用的安全技术、运营安全防护要求等。

本标准适用于单播技术的 PPVPN，不适用于组播技术的 PPVPN。PPVPN 主要指 MPLS VPN。

2 规范性引用文件

下列文件中的条款通过本标准的引用而成为本标准的条款。凡是注日期的引用文件，其随后所有的修改单（不包括勘误的内容）或修订版均不适用于本标准。然而，鼓励根据本标准达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件，其最新版本适用于本标准。

IETF RFC1918（1996） 专用网地址分配

3 术语、定义和缩略语

3.1 术语和定义

下列术语和定义适用于本标准。

3.1.1

用户网络边缘设备 Customer Edge (CE)

用户网络和运营商网络直接相连的设备，可以是主机或者路由器，用户边缘设备“感知”不到 VPN 的存在。

3.1.2

运营商边缘设备 Provider Edge (PE)

运营商网络和用户网络直接相连的设备，负责运营商网络同 VPN 客户网络的交互。PE 处理来自 CE 的数据，并转发到相同 VPN 中的其他 PE，PE 也要能够处理来自网络的到所属 VPN 的站点的资料。PE 能够理解和处理 VPN 用户的私网地址，并提供不同 VPN 用户网络之间的隔离性。

3.1.3

运营商设备 Provider (P)

运营商骨干网络中不和 CE 相连的路由器，负责转发从 PE 发过来的 VPN 数据，如果 PE 之间使用 MPLS 隧道，需要相应的 P 设备支持 MPLS 和 LDP（或 RSVP-TE）信令。如果 PE 之间使用其他隧道机制，P 设备可以不支持 MPLS 和 LDP（或 RSVP-TE），只需要按照该隧道机制的要求支持相应技术。

3.1.4

站点 SITE

VPN 用户的网络，并通过一个 CE 或多个 CE 连接到一个或多个 PE 上。一个 SITE 可能是由位于相同地理位置的一系列主机和网络设备组成，比如一个银行的分理处，也可能是一个地理分布的网络，但作为一个逻辑的整体统一出口和 PE 连接。一个 VPN 由通过公共基础设施连接的多个 SITE 组成。

3.2 缩略语

下列缩略语适用于本标准:

AS	Autonomous System	自治系统
ATM	Asynchronous transfer mode	异步传输模式
BGP	Border Gateway Protocol	边界网关协议
CE	Customer Edge	用户网络边缘设备
DoS	denial of service	服务拒绝
DDoS	distributed denial of service	分布式服务拒绝
IETF	Internet Engineering Task Force	因特网工程任务组
IKE	Internet Key Exchange	因特网密钥交换
IP	Internet protocol	互联网协定
ITU-T	International Telecommunication Union - Telecommunication Standardization Sector	国际电信联盟-电信标准化部
L2TP	Layer 2 Tunneling Protocol	第2层隧道协议
LAN	Local Area Network	局域网
MPLS	Multi-protocol label switching	多协议标记交换
NAT	Network Address Translation	网络地址转换
P	Provider	运营商设备
PE	Provider Edge	运营商边缘设备
PPVPN	Provider-Provisioned Virtual Private Networks	运营商提供的虚拟专用网
QoS	Quality of Service	服务质量
RADIUS	Remote Authentication Dial In User Service	远程认证拨号用户服务
RSVP	Resource reservation protocol	资源预留协议
SLA	Service level agreement	服务等级协定
SP	Service Provider	服务提供商
TCP	Transmission control protocol	传输控制协议
TOS	Type of service	业务类型
TTL	Time to live	生存期
UDP	User datagram protocol	用户数据报协议
VPLS	Virtual Private LAN Service	虚拟专用局域网业务
VLAN	Virtual Local Area Network	虚拟局域网
VPN	Virtual Private Network	虚拟专用网
VRF	VPN routing/forwarding instance	VPN路由/转发实例
URPF	Unicast Reverse Path Forwarding	单播反向路径转发

4 安全威胁

4.1 概述

PPVPN 网络安全是 IP 网络安全的一个有机组成部分,可从三个维度来分析 PPVPN 网络的安全问题。

网络系统维度的安全性，包括骨干网络设备（P 路由器）的安全性，边缘网络设备（PE 路由器）的安全性和用户接入设备（CE 路由器）的安全性。

网络分层维度的安全性，包括基础 IP 网络层面的安全性，VPN 层面的安全性，用户数据层面的安全性。

安全特性维度的安全性，包括通信安全、访问控制、身份认证、私密性、不可否认性、数据机密性、数据完整性等方面的安全性。

以上三个维度可能受到的安全威胁可细分为来自数据面的安全威胁，来自控制面的安全威胁和来自管理面的安全威胁。

4.2 来自数据面的安全威胁

数据面上的攻击主要是针对 PPVPN 用户数据的，表现为如下几个方面。

4.2.1 未经授权查看数据流

指对 VPN 包进行嗅探，检查包中的内容，这会导致机密信息的泄漏。

当 VPN 数据传送路径上的某个设备被攻击者控制，或者攻击者在 VPN 数据传输路径上插入非法的设备，该攻击者即能够对 VPN 内传输的数据进行拦截和查看。另外一种可能是搭线侦听，直接对链路上的信号进行复制和还原。

这种查看也可能是实施其他类型的攻击的第一步，例如将内容修改后重新发送等。

4.2.2 修改报文

指在 VPN 用户报文的传送过程中将其截获，修改该用户报文后继续传送。此类攻击只针对单个报文的内容，包括长度、报文头和报文净荷，但一般不改变报文的传送顺序等特性。

报文修改攻击一般在 VPN 数据路径上的设备被控制或被插入非法的设备的时候可能发生。

4.2.3 不可信数据流的插入：哄骗和重放

指将不属于某个 VPN 的包发送到该 VPN 中，并使接收者将这些非法包当作合法包接收下来。还有一种方式是将合法报文复制下来，在其后的某个时间重新发送到 VPN 中。

如果 PE 不能严格区分一个来自 CE 的报文属于哪一个 VPN，则可能会发生哄骗。一些 VPN 技术依赖于埠区分，一些 VPN 技术依赖密码学方法（如安全联盟）。VPN 技术不应该依赖地址来判断一个报文属于哪一个 VPN，因为地址容易被仿冒。

重放和修改报文一样，都是比较精密的攻击方式，不同的是，报文修改破坏单个报文的完整性，而重放破坏了一个通信流的完整性。

4.2.4 未经授权删除数据流

指将 VPN 用户数据包在传送过程中删除，这是一种特殊类型的 DoS 攻击。同重放一样，删除也是破坏通信流的完整性的一个方式。

4.2.5 未经授权的业务流类型分析

指嗅探 VPN 包并查看其可以被识别的特征，即使包被加密过也可以查看。根据数据流发送的数量和时间、包的大小、源地址和目的地址等特征，攻击者有可能获得有用的信息。多数 PPVPN 用户较少关注这种类型的攻击，认为其他类型的攻击更需要关注。

4.2.6 VPN 上的服务否认（DoS）攻击

指干扰或阻断合法用户使用服务的攻击。使网络设备不能支持服务、修改设备配置、或者用大量服务请求“淹没”设备都是可能的 DoS 攻击方式。

用服务请求“淹没”设备的攻击被称为资源耗尽型 DoS 攻击,攻击的目标可以是网络中的任何资源,例如链路带宽、包转发容量、各种协议的会话容量和 CPU 处理能力。

资源耗尽型 DoS 攻击的方式是:从 VPN 之外将“淹没”数量的不可信数据发送到某个特定的 PPVPN 数据面上,可能产生的结果是耗尽该 VPN 的可用带宽资源,或者“淹没”了该 VPN 的加密认证机制。

资源耗尽型 DoS 攻击的方式还可以是用业务流将 PPVPN 运营商的通用基础设施“淹没”,这种攻击一般不属于 PPVPN 特定的范畴,除非攻击来自某个具有特权地位的 PPVPN 用户,例如,某个 PPVPN 用户可以独霸网络数据面资源,因此妨碍了其他 PPVPN 用户对资源的使用。

4.3 来自控制面的安全威胁

控制面上,提供 VPN 业务的运营商边界路由器(PE)之间要交换 VPN 路由信息,运营商 IP 网络上的路由器(P)要交换公网路由信息,安全性攻击主要针对的是这两类设备。安全威胁来自两个方面:一方面是攻击者对路由协议进行攻击,非法交换路由信息造成的;另一方面是对路由器设备发动攻击,使路由器无法正常工作造成的。主要的安全威胁表现在如下几个方面。

4.3.1 对网络基础设施的 DoS 攻击

控制面上的攻击可以是针对 PPVPN 运营商使用的控制机制的(例如 IPsec、MPLS 等),也可以是针对通用的网络基础设施的(例如 P 路由器或 PE 路由器)。本规范只涉及与使用 PPVPN 业务有关的 DoS 攻击,其他类型的对网络基础设施的 DoS 攻击不是 PPVPN 特有的问题。

这里主要关注一个 PPVPN 用户的行为引发了 DoS 攻击,对其他用户造成了影响。这种情况是有可能发生的,例如如果允许一个 PPVPN 用户过多占用任意类型的网络资源,其他 PPVPN 用户就会因为得不到资源而影响正常的业务。

4.3.2 通过管理接口对服务提供商设备的攻击

这种攻击包括对服务提供商基础设施的非法访问,例如为了对一个或多个 PPVPN 进行设备的重新配置,或者为了提取信息(统计信息、拓扑信息等)而进行攻击。

这种攻击是通过恶意地进入系统实现的,也可能是由于在 PPVPN 用户自我管理接口上没有做好 VPN 之间的隔离而无意造成的。前一种情况不是 PPVPN 特有的问题。

一些运营商为 VPN 用户提供客户网络管理系统(CNM),客户可以通过 VPN 访问位于公网上的 CNM 服务,这种情况也有可能为恶意用户攻入管理系统提供可能。

4.3.3 对运营商基础设施的社会工程技术攻击

对服务提供商网络的重配置或破坏、不适当地泄漏机密资讯也可能是服务提供商员工的操作造成的。这类操作的结果影响了 PPVPN 业务的运作机制,是 PPVPN 特有的安全攻击。与在 IP 层面“自己提供服务”的 VPN 相比,“运营商提供服务”的 PPVPN 上可能更容易发生这种攻击,这是由 PPVPN 与生俱来的机构的分离(用户、服务提供商)性质造成的。

4.3.4 PPVPN 之间业务流的交叉连接

指破坏 PPVPN 之间的隔离性的事件,表现为如下几个方面:

- ◆ 站点被连接到“错误的”VPN;
- ◆ 两个或多个 VPN 的不适当合并;
- ◆ 出现点到点的 VPN 连接错误,连接了两个错误的点;
- ◆ 本应在某个 VPN 内传送的包被不适当地传送到该 VPN 之外。

VPN 之间的错误连接或交叉连接可能是由服务提供商或设备商的错误造成的，也可能是攻击者的恶意行为造成的。这种对隔离性的破坏可能是物理上的（例如 PE-CE 链路的错误连接），也可能是逻辑上的（例如设备的不当配置）。交叉连接问题是 PPVPN 用户（或潜在用户）最为关心的安全问题之一。

4.3.5 对 PPVPN 路由协议的攻击

指对服务提供商运营的以及直接支持 PPVPN 业务的路由协议的攻击。对于三层 VPN，主要指与成员发现以及每个 VPN 的路由发布有关的协议。对于二层 VPN，主要指成员和端点发现协议。对运营商骨干网络路由协议的攻击不在本标准涉及范围内。

4.3.6 对路由隔离的攻击

“路由隔离”指每个 VPN 的拓扑、可达性信息都应与其他 VPN 相分离，并且不能被任何其他 VPN 用户获得（除非 PPVPN 运营商为了某种目的做了特殊配置）。只有三层 VPN 涉及路由隔离方面的安全问题，因为服务提供商参与了 VPN 内部路由的操作（即 VR、BGP-MPLS 等）。对路由隔离性的破坏会泄漏 PPVPN 的拓扑和地址信息，也会在 PPVPN 之间引发黑洞路由或非授权的数据面交叉连接问题。

4.3.7 对地址空间隔离的攻击

不同三层 VPN 用户使用的 IP 地址空间应是完全隔离的，不同二层 VPN 用户使用的 MAC 地址和 VLAN 空间也应是完全隔离的。如果在控制面上破坏了这种地址隔离，将会导致在未经授权的情况下数据面上出现 VPN 之间的交叉连接。

4.3.8 对 PPVPN 控制面的其他攻击

除了路由和管理协议之外，还可能有一些其他控制协议也参与了 PPVPN 业务的提供（例如各种 PPVPN 的邻居发现和对等建立协议等），这些协议包括：

- ◆ MPLS 信令（LDP/RSVP-TE）；
- ◆ IPsec 信令（IKE）；
- ◆ L2TP；
- ◆ 基于 BGP 的成员发现；
- ◆ 基于数据库的成员发现（例如基于 RADIUS）；
- ◆ 其他。

攻击者可能会干扰和破坏这些协议的执行，例如采用假冒或者 DoS 方式进行攻击。

4.4 来自管理面的安全威胁

对 PPVPN 的管理和配置命令可牵涉到 P 和 PE 路由器、路由协议、VPN 拓扑、用户虚拟路由实例和虚拟交换实例、安全认证方法等各部分、各层面的业务参数。

攻击者以远程接入方式经网络接入网管系统（例如采用拨号方式接入，利用 telnet 或 http 访问网管接口），通过口令猜测等手段非法获得网管接口的访问控制权，非法访问 SP 基础设施的管理系统，对设备中的配置管理信息进行查看，非法提取信息（例如统计、拓扑信息等）甚至对设备配置进行改动，通过种植病毒、木马、开后门等恶意手段实施攻击。

5 对运营商的安全要求

5.1 隔离要求

虚拟专用网的专用性决定了一个用户的 PPVPN 应与其他用户的 PPVPN 以及 Internet 相隔离，这种隔

离包括如下几个方面:

5.1.1 地址隔离

PPVPN 用户可以使用整个 Internet 地址空间, 包括按 RFC1918 中所规定的专用地址空间, 同时一个 PPVPN 用户不会干扰同一运营商支持的另一个 PPVPN 用户。接入 Internet 时, 可能需要 NAT 功能。二层 VPN 有同样的地址隔离要求, 例如 MAC 地址的隔离。

5.1.2 路由隔离

PPVPN 核心应维护用户的信任区域之间路由的隔离性, 不允许任意一个信任区域内的路由信息被泄漏到另一个信任区域, 除非信任区域特意要配置为泄漏某些路由 (例如接入 Internet)。

对于二层 VPN, 信任区域间应保持交换信息的隔离性, 使得一个 PPVPN 中的交换信息不会影响其他 PPVPN 或 PPVPN 核心网。

5.1.3 业务流隔离

来自某个信任域的业务流在传送过程中不允许离开该信任域, 来自其他信任域的业务流不允许进入该信任域, 某些情况下进行的专门配置除外 (例如为 extranet 或访问 Internet 而进行的专门配置)。

5.2 防护

完全隔离的专用网一般定义了一些进入界面点, 只有这些进入界面点面对着外界的攻击或入侵。PPVPN 的用户共享了一个公共的核心, 对于信任域以外的网络就失去了一些明确的接口。在这种情况下, PPVPN 运营商应提供与专用网相同水平的安全防护措施。

5.2.1 对入侵的防护

入侵是指从外界渗透到信任域内, 入侵可以来自 Internet、另一个 PPVPN 或者核心网自身。对于 PPVPN 网络, 不允许添加面向信任域以外的其他部分的新的接口。此要求不涉及一些已知的接口 (例如 Internet 网关)。

5.2.2 对 DoS 攻击的防护

DoS 攻击的目的在于使合法用户不能使用业务或设备。通过 VPN 提供网络业务时遭受的 DoS 攻击在本规范涉及范围内, 通过标准接口入侵信任域的 DoS 攻击不在涉及范围内。PPVPN 做为一种虚拟专用网, 其抗 DoS 攻击的能力应不低于真正的专用网。

对于每个 VPN 能够占用的带宽资源应该能够限制, 对于超过带宽限制的用户流量, 应该进行限流, 防止一个 VPN 占用其他 VPN 的资源。

5.2.3 对哄骗的防护

要防止在业务流传送过程中, 因为攻击者改变了发送者标识 (源地址、源卷标等) 而破坏 PPVPN 的完整性。例如, 两个 CE 连接到同一个 PE, 一个 CE 对发送包进行了改造, 试图使 PE 相信这些包来自另一个 CE 时, PE 要能够识别, 不把这些包发往错误的 PPVPN。

5.3 机密性要求

某些情况下要求运营商提供加密功能, 使数据以密码形式安全地通过 PPVPN 核心网络传送, 防止被窃听。

5.4 CE 认证要求

运营商可提供 CE 认证功能, 使得 PPVPN 外部的用户不能假扮成内部用户, 用自己的 CE 设备非法接入 PPVPN。

5.5 完整性要求

在数据传送过程中，应保证数据不被更改，或者对资料的任何更改都可以被接收者发现。

5.6 反重放要求

在数据传送过程中，保证数据不被截获、保存并重新发送。为了防范重放攻击，需要提供数据流的完整性检查机制。

6 安全技术

6.1 对攻击的监测与报告

攻击者的攻击通常是从对系统进行试探、分析从系统中非法获取的数据开始的，如果系统能够监测和报告这些初级的攻击，及时地识别攻击者身份，发现他们的攻击目标和步骤，就可以及早采取防卫措施，防止遭受更加危险的攻击。

安全监视系统和入侵检测系统通常要从 PE、CE 和/或运营商的骨干网设备（P）以及主机、服务器上采集信息，应具有从这些设备上主动提取信息（例如，SNMP get）或被动接收信息（例如，SNMP notifications）的功能；PE、CE 以及运营商骨干网设备、主机、服务器也应具有相应的信息提取和传送能力。

安全监视系统与 PPVPN 设备之间的通信应得到安全保护，可以使用专用的安全通道。应当对这种通信的业务量进行合理的设计和管理，使其不干扰正常的 VPN 业务。例如，多个攻击事件可以用一个消息来报告，而不是每次攻击事件触发一个单独的消息，后者会导致消息的洪泛，本质上变成一种针对监视系统或网络的 DoS。

报告安全攻击的机制应足够灵活，以便满足 VPN 运营商、VPN 用户和代理机构的不同需要。应根据设备和安全监视系统的能力、VPN 类型、运营商与用户达成的服务等级协议来确定报告的内容。

6.2 认证

为了避免网络设备遭受攻击，对访问 PPVPN 的设备身份进行认证核实是一项关键的安全措施。认证包括 VPN 成员认证、对等体认证、管理系统认证、VPN 成员远程接入认证。

6.2.1 VPN 成员认证

为了保证 CE 设备接入它所期待的 VPN，PE 和 CE 之间要对彼此的身份进行检查核实，保证自己与期待的对等体进行通信。

6.2.2 管理系统认证

包括在使用基于目录的“自动发现”机制时，PE 设备到中心管理目录服务器的认证。还包括在使用配置服务器系统时，CE 到 PPVPN 配置服务器的认证。

6.2.3 对等体认证

主要指控制面上 PE 之间为了保证路由信息传送正确而进行的认证。除此之外，控制面上运营商为了保证骨干网络路由信息传送的正确性，可以对网络路由协议（如 BGP、OSPF、ISIS、LDP 等）进行认证，这种认证可以是基于下层传输协议的（如 TCP），也可以是基于路由协议自身的认证机制的。

6.2.4 VPN 成员远程接入认证

VPN 成员通过 IP 网络远程接入时可以使用多种认证协议，例如 RADIUS、DIAMETER 等，这类 VPN 成员通常通过安全隧道接入，例如 L2TP 和 IPsec 隧道等。

PPVPN 通过网关设备建立远程连接, 网关设备可以由 VPN 用户的某个站点管理的, 也可以是由 PPVPN 运营商管理的, 前者不在本规范涉及范围内。

PPVPN 运营商在远程接入网关上对认证进行管理时, 通常采用代理认证服务机制, 即从远程用户设备那里接收加密的认证证书, 并将其转发给 PPVPN 用户的认证系统, 接收来自该认证系统的是/否响应, 确定用户的认证是否通过。因此, PPVPN 运营商并没有真正去访问 PPVPN 用户的认证数据库, 而是起到远程认证用户代理的作用。

6.3 加密

IP/MPLS VPN 为了保证资料传送的安全性可以采用加密技术。二层 VPN 的加密技术有待研究, 三层 VPN 的 CE 与 PE 之间、PE 与 PE 之间、CE 与 CE 之间均可以支持数据包的加密传送。

三层 VPN 可以采用基于 IPsec 的加密方式, PE 与 PE 之间进行加密时, 采用 MPLS-in-IP 和 MPLS-in-GRE 两种加密封装方式 (详见附件 A); CE 之间、CE 与 PE 之间可以采用传送模式和隧道模式的 IPsec 加密封装方式。

PPVPN 用户数据包的传送路径为从 CE 到 PE、到对端 PE、再到对端 CE, 数据包传送过程中使用的加密方式可分为如下四种。

- ◆ 站点到站点的加密 (CE-to-CE): 在两个 CE 设备之间提供端到端的加密, 这种加密可以是 VPN 用户内部支持的, 也可以是 PPVPN 运营商提供的 (详见附录 B), 在这种情况下, 用户业务流以加密的形式穿过运营商网络, 实现端到端的加密。PPVPN 用户要保证数据信息对运营商网络的私密性的情况下, 可以采用这种加密措施。

- ◆ 运营商边缘到边缘加密 (PE-to-PE): 在运营网络边缘的 PE 设备之间进行加密。PE 接收 CE 发来的未加密的数据流, 加密后经 SP 网络传送到对端 PE, 对端 PE 将其解密后发给对端 CE。在接入链路安全性较高、网络内部有安全威胁的情况下, 可以采用这种加密方式。

- ◆ 接入链路加密 (CE-to-PE): 在网络两侧的 CE 和 PE 之间进行加密, 也可以只在一侧的 CE 和 PE 设备之间加密。在接入链路有安全威胁、网络内部安全性较高的情况下, 可以采用这种加密方式。

- ◆ 混合的全程加密: 将上述的第二种和第三种方式结合起来进行加密, 加密过程在 CE 到 PE、PE 到 PE、PE 到 CE 的链路上进行。在接入链路和网络内部都存在安全威胁、同时为了支持某些增值服务需要运营商完成加密功能的情况下使用这种加密方式。

加密技术可以保证设备之间传送的信息的私密性和完整性, 但加密也有可能带来一些负面的影响, 例如加密措施给完成加密解密功能的设备增加了额外的计算负担, 有可能导致设备可以支持的 VPN 用户数量减少; 在设备上配置加密业务, 增加了设备配置的复杂性, 提高了操作难度, 潜在地提高了运营商的业务成本; 加密包的长度增加, 增加了包分段的可能几率, 加重了网络业务量负担。在实际操作中要权衡加密的利弊使用适当的方法。

6.4 接入控制

接入控制是指利用过滤器或防火墙对进入 PPVPN 的数据流进行逐个包或逐个流的检查控制, 对于 PPVPN 的控制/信令/管理协议上建立会话请求进行接纳控制。这里过滤器和防火墙的主要区别在于: 过滤器是单向过滤数据流的, 防火墙可以在其两侧的会话之间进行分析和控制。

6.4.1 过滤器

路由器上通常使用过滤器, 即根据数据流的转发特征、数据包的特征制定一些匹配规则, 并对匹配

这些规则的包进行特殊处理，这些特征主要包括输入输出逻辑或物理接口、IP 包头信息、TCP 或 UDP 包头信息等，IP 包头信息通常包括源地址、目的地址、协议字段、分段偏移、ToS 字段等，TCP 或 UDP 包头信息通常包括端口字段、SYN 字段等。

过滤分为无状态过滤和有状态过滤两类，无状态过滤是指完全根据匹配规则对包进行过滤，有状态过滤是指保存了特定包的状态信息，做为判定包是否符合匹配规则的辅助信息。例如，路由器对分段 IP 包的第一个包进行无状态过滤，如果符合匹配规则，则记下该包的数据单元 ID，后续其他分段的 IP 包都被认为是匹配该规则。

对于符合匹配规则的包，通常进行如下处理。

- ◆ 丢弃：通常对某些来源不明的、非预期的包进行悄悄予以丢弃，还可以同时对丢弃包进行记录或计数。
- ◆ 速率限制：将符合匹配规则的包的发送速率限制在特定带宽范围内，对包进行技术，并使包的转发速率不超过规定的限度。
- ◆ 转发和复制：在转发包的同时进行复制，并将复制包转发到另一个地址或接口。这样做可以实现包的合法截获功能，或把滤出包发送到某个入侵监测系统。

6.4.2 防火墙

防火墙在不同的 PPVPN 信任区域之间对数据流的传送提供控制机制，也可以在信任区域和非信任区域之间提供控制机制。防火墙通常可以比过滤器提供更多的功能，它可以对流而不仅仅是对单个包进行详细分析和处理，可以提供多种复杂的服务，例如门限驱动的 DoS 攻击保护、病毒扫描或者做为 TCP 连接代理等等。

对于 PPVPN，一般不允许在不同用户的 VPN 之间传送数据流。但是企业外部网（extranet）是特例，它允许从另外一个 VPN 对某个用户的 VPN 进行特定的外部访问，这种情况下，可以用防火墙来保障企业外部网的安全要求。

在 PPVPN 中，在由运营商向 VPN 用户站点提供 Internet 访问服务时，可以将防火墙设置在公众 Internet 和用户 VPN 之间。此外，在 VPN 用户站点与 PPVPN 运营商提供的任何共享的基于网络的服务之间，也可以设置防火墙。

防火墙可能有助于保护 PPVPN 核心网，使核心网免受来自 Internet 或 PPVPN 用户站点的攻击，但一般都采用其他的技术来达到这一目的。防火墙还可以保护用户站点免受来自 Internet 的攻击、保护不同的 VPN 用户网络甚至保护一个 VPN 用户网络中的不同站点。

6.4.3 对管理接口的接入控制

对管理接口的安全管理措施大多要使用到前文提到的认证技术，除此之外管理接口还应采取其他一些措施。

应该对管理接口（特别是 PPVPN 设备上的控制口）进行配置，使得对管理接口的访问只能以带外方式进行，即应通过物理上或逻辑上与 PPVPN 基础设施相隔离的系统来访问管理接口。

如果要在 PPVPN 域内以带内方式访问管理接口，则可以使用过滤器或防火墙技术，以便限制未经授权的数据流进入管理接口。可以将过滤器或防火墙配置在数据流可能经过的其他设备上，也可以直接配置在 PPVPN 设备上，选择哪种方式可以根据设备能力来考虑。

6.5 使用隔离的网络基础设施

为了保护支持 VPN 业务的网络基础设施，可以将支持 VPN 业务的资源与用于其他用途的资源（例如用于支持 Internet 业务的资源）隔离开。在某些情况下，可能需要为 VPN 业务使用物理上隔离的设备，甚至使用物理上隔离的网络。

例如，基于 PE 的 L3 VPN 可以运行在不连接 Internet 的隔离的骨干网上，或者使用不支持 Internet 业务、只支援 VPN 业务隔离的边缘路由器。专网 IP 地址（运营商在局部范围内使用并且不能在 Internet 上寻路）有时也用于提供附加的隔离措施。

基于 CE 的 L3 VPN 通常使用专属于某个特定 VPN 的 CE 设备。多数情况下，基于 CE 的 VPN 会使用普通的 Internet 业务来互连 CE 设备。

6.6 合并网络基础设施下的隔离措施

通常情况下，为了支援每个 VPN 而使用完全隔离的网络资源是不现实的。推出 VPN 业务的一个主要原因就是允许在多个不同的用户之间实现资源共享。因此，即使 VPN 业务使用了与 Internet 业务相隔离的网络，仍然会有多个 VPN 用户共享同样的网络资源。在某些情况下，VPN 业务会与 Internet 业务或其他业务共同使用网络资源。

因此，对于 VPN 业务，在不同的 VPN 使用的资源之间提供保护机制是很重要的。应该保护行为端正的 VPN 用户的资源，使其不受其他 VPN 用户的错误行为侵害。这就要求对任何一个 VPN 可以使用的资源量进行限制。例如，对控制流和用户数据流可以进行速率限制。在某些情况下或在网络的某些局部，如果可以提供数量足够充足的队列，则可以让每个 VPN（也可以是每个 VPN 及 VPN 内的 CoS）使用一个单独的队列。控制面的资源（例如链路带宽、CPU 和存储资源等）也可以为每个 VPN 保留。

在共享相同的网络基础设施条件下，用于在多个 VPN 之间提供资源保护的技术措施也可以用于保护 VPN 业务不受 Internet 业务的侵扰。

在共享网络基础设施的做法可以使多个突发流随机复用起来，从而使运营商在资源的高效利用上获益，在某些情况下，由于来自多个 VPN 的数据流相互交织传送，也阻碍了攻击者对数据流类型进行分析，提供了一定程度的安全保护。

6.7 PPVPN 运营商对业务实施的保障

PPVPN 业务的实施要求运营商完成数量相当庞大的设备配置工作，例如，应将每个 VPN 站点配置到相应的 VPN 上，还要对 QoS 和 SLA 协议进行相应配置。进行数量众多配置时，有可能出现一些错误配置。

对于 PPVPN 运营商，采取一些操作措施来降低错误配置出现的几率、减小其影响是很重要的，还可以使用 CE 到 CE 的认证技术来检查是否出现了错误配置。

6.8 部署可测试的 PPVPN 业务

在 PPVPN 业务的部署中应提供一些测试方面的解决方案，以便对设备是否配置正确进行测试检查。例如，对于点到点 VPN，应对目标连接是否工作良好进行检查，以便保证连接没有建立到某些非目标站点上。

7 运营安全防护

PPVPN 的安全防护措施应基于综合安全防范理念，从多层次和多方面来增强系统的安全可靠性。一般的安全措施包括以下几点。

- ◆ 对网络实体（包括网络设备和用户）进行认证和授权。
- ◆ 对网络资源设置分级管理权限，合理划分运营商和用户的管理范围。
- ◆ 在接入网通过电路或虚电路对不同用户的数据流量进行隔离，并把接入电路或虚电路分别与用户 VPN 进行绑定。

- ◆ 为网络的管理平面和控制平面设置安全的传输通道，包括用物理专网或逻辑专网（VPN）来传输网管和控制数据，并启用安全的加密认证机制。管理数据和控制数据应得到优先处理。在数据平面过滤恶意的、非法的和畸形的流量，防止拒绝服务攻击。

- ◆ 通过静态配置或策略服务器动态调整的方式来控制用户接入带宽。当入侵检测设备监控到用户的（主动或受控的）攻击行为后，可动态降低或关闭该用户的有害数据流程的带宽，并进行告警。

- ◆ 对关键设备采用热备份，提高 PPVPN 业务在攻击下的恢复能力和可用性。

- ◆ 日常执行严格的安全维护措施，包括及时安装软件补丁，定期进行病毒扫描和系统安全漏洞扫描，定期做入侵检测，定期对路由器和防火墙的过滤规则进行更新，详细记录安全日志，定期作安全审计，定期更改密码等。

更具体一些，对 PPVPN 的攻击来自数据面和控制面，运营的防护措施也主要针对这两个层面。下文分别对三层 VPN、二层 VPN 的安全防护方式进行规定。

7.1 三层 VPN 的安全防护

MPLS VPN 系统的构成如图 1 所示。

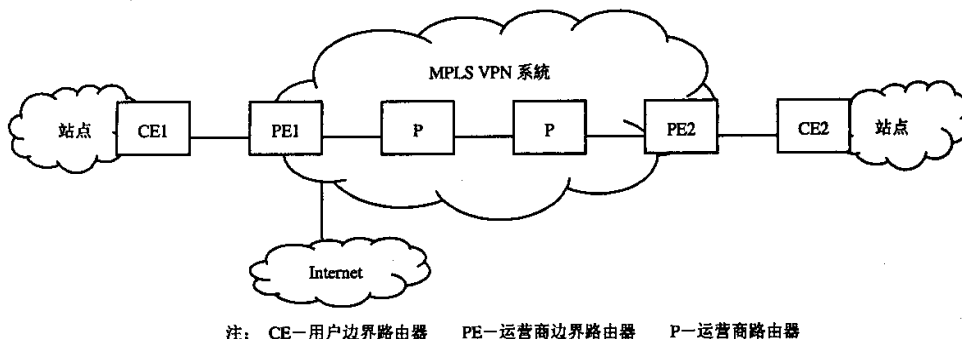


图 1 三层 IP/MPLS VPN 系统结构示意图

三层 IP/MPLS VPN 网络系统应保证控制面路由信息传送准确可靠，保证数据面用户数据传送的私密性、准确性和完整性，保证管理面上配置信息的安全性。为了支持这些功能，网络设备本身应具备一定的抗攻击能力，安全上应考虑如下问题：

- ◆ 控制面上 CE-PE、PE-PE 之间 VPN 路由信息传送的安全性；
- ◆ 资料面上 CE-PE、PE-PE、CE-CE 之间 VPN 用户数据传送的安全性。

7.1.1 三层 VPN 控制面的安全性

7.1.1.1 PE-CE 间 VPN 路由信息传送的安全性

CE 通过 BGP、OSPF、RIP 或 ISIS 等路由协议将本地站点的路由传送给 PE（也可以通过静态设置方式使 PE 获取路由），控制面上首先要保证这些路由信息传送的安全性。

VPN 用户的 CE 设备如果是通过专线接入 PE 设备，或者通过以太网交换机以 VLAN 方式接入，CE 到 PE 之间的数据链路通常是由网络管理员建立的，非法 CE 设备很难以冒名顶替的方式介入，与 PE 设

备建立连接并交换路由信息，CE 与 PE 之间路由信息的传送路径本身可保证一定的安全性。在这种情况下，运营商如果考虑业务开放的成本和配置的简单化，可以允许 CE 接入时不经过认证。

VPN 用户的 CE 设备如果以无线方式接入，或者通过 IP 网络远程接入，则要求对 CE 设备进行认证，在经过认证之后才允许进行路由信息的交换。对于基于 TCP 的路由协定（如 BGP），通常使用 TCP 认证来保证路由信息的可靠性和完整性，其他路由协议（如 OSPF、ISIS 等）可以采用自身的认证机制。

7.1.1.2 PE 之间 VPN 路由信息传送的安全性

PE 路由器之间通过 MP-BGP 协议交换路由信息，PE 之间路由信息的传送要经过一个或多个 P 路由器，非法用户有可能采用源地址欺骗等手段要求与 PE 建立连接并交换 VPN 路由信息。因此，PE 不应该在控制连接上任意与另外一个对等体通信，除非它确信这个对等体确实是合法的。否则，可能会导致 VPN 路由的泄漏，招致用户数据信息被传往错误的方向、服务拒绝攻击或者用户期望的 QOS 发生了变化等不良后果。

运营商对 PE 之间 MP-BGP 路由信息的交换应强制执行认证功能，每个 PE 都应在认证的基础上接受来自其他实体的连接请求，防止非法用户对路由信息的窃取和攻击。PE 之间的 VPN 路由信息是通过 MP-BGP 传送的，可以使用 TCP 认证算法对 MP-BGP 消息的完整性进行保护，保证路由信息的来源可靠，而且在传送过程中未被修改。

此外，MP-BGP 协议在连接建立阶段也可以支持认证功能，可以防止攻击者与运营商的路由器非法建立 MP-BGP 连接并交换路由信息。为了进一步加强 PE 路由器之间路由信息传送的安全性，实现 TCP 和 BGP 协议的双重认证保护，运营商可以要求厂家设备支持该项功能。

7.1.1.3 网络基础设施的安全性

MPLS VPN 系统是由运营商边界路由器（PE）和运营商 IP 网络内部的路由器（P）相互连接构成的，这设备自身的安全性是保证整个系统安全性的关键。

PE 路由器承担着为用户建立虚拟路由表、转发 VPN 用户数据包的任务，如果受到过大业务量的冲击而不能正常工作甚至瘫痪，必然会影响 VPN 业务的正常运作。因此，PE 路由器上应采取流量控制措施，PE 路由器上应对每个接入用户的流量进行限制，还可以采取 URPF 检查、设置过滤器、关闭 ICMP 功能等流控措施来防范 DOS 攻击。

7.1.2 三层 VPN 数据面的安全性

在数据面上，用户 IP 包从 CE 传送到 PE，在 PE 上被打上标记，形成标记包经 MPLS 网络内的一个或多个 P 路由器传送，送达对端 PE 之后，包的外层标记被去掉，内层封装的 IP 包被传送给对端 CE。数据面的安全性主要考虑防止用户数据包被非法截获和篡改，采取的主要安全措施是加密，通常采用 IPsec 加密方式。

7.1.2.1 CE-PE 的数据加密传送

如果用户以专线方式接入，或通过以太网交换机 VLAN 方式接入，传输路径是由网络管理员配置调度的，CE 与 PE 之间的传输路径相对来说是比较安全的，如果考虑业务开放的成本和配置的简单化，可以允许用户信息以非加密方式接入。

如果用户以无线方式接入，或者通过 IP 网络远程接入，则通常采用加密接入方式。在这种情况下，如果网络运营部门需要支持国家信息网络的安全监测功能，就应要求 CE-PE 之间的加密通道在 PE 设备上终结，即 PE 设备可将密文解码为明文，便于设置监测点。

7.1.2.2 PE-PE 数据信息的加密传送

PE-PE 数据信息的加密传送功能是由运营商的网络边缘设备完成的，用户设备无需进行特别的配置，由运营商的 PE 设备完成基于 IPsec 的加密功能，是基于网络的加密模式。

运营商为用户提供 BGP MPLS VPN 业务时，PE 之间通过 MPLS 网络传送的用户数据包通常被打上至少两层标记，最内层为 VPN 内部标号，外层为 MPLS 网络的路由标记，对应于 PE 之间建立的 LSP。

为了保证数据传送的安全性，可以用基于 IPsec 的安全 IP 隧道传送 MPLS 包，即将 MPLS 包封装到 IPsec 的载荷部分传送。PE 之间数据的安全封装传送存在两种方式：MPLS-in-IP 和 MPLS-in-GRE，这两种封装方式实际上是在 PE 之间建立了一条基于 IPsec 的安全 IP 隧道，加密方式详见附录 A。

对于一般的企业用户，要求 PE 之间信息的传送不采用加密方式，原因如下：

- VPN 用户使用 MPLS 标记隧道传送信息，本身已经具备了一定的安全性；
- PE 之间的加密方式实现上比较复杂，信息传送的开销比较大，如果用户没有特殊的安全性要求，运营商可以不考虑采用这种加密方式，以免给网络设备带来过重的处理负担；
- 如果需要支持国家网络的信息安全功能，在 PE 和 P 路由器上设置信息检测点，就需要要求 PE 间信息的传送不加密。

7.1.2.3 CE-CE 数据信息的加密传送

(1) VPN 用户支持的 CE-CE 加密

用户数据的加密和解密功能完全在 VPN 用户的 CE 设备上完成，运营商网络只是提供了加密数据包的透明承载通道，不参与加密过程中的任何操作。一般企业用户可以不使用这类加密传送方式，仅利用 VPN 自身的安全机制保证信息传送的安全性。

网络运营部门如果需要支持国家信息安全的监测功能，就需要采取管理上的措施对用户进行资格审批，只允许确有需要的用户采用 CE-CE 的信息加密传送方式，同时采用必要的技术措施进行监管，要求其他用户不采用 CE-CE 加密传送方式。技术措施在实施上有一定难度，管理部门需要得到设备制造商和运营商的配合。

(2) 运营商提供的 CE-CE 信息加密传送

CE-CE 数据信息的加密传送可以由业务提供商 (SP) 来支援。为了支持这一功能，运营商要维护一个安全 VPN 数据库，CE 设备要从数据库中提取信息，完成安全配置并建立基于 IPsec 的安全隧道，通过安全隧道传送 VPN 用户的数据包。

本标准为运营商支持的 CE-CE 数据信息加密传送提供了一种参考实现方案，在这个方案中，SP 要提供安全服务器，服务器上维护管理一个安全数据库，这个数据库可以为多个 VPN 提供服务，参见附录 B。

在这种实现方案下，CE 为了与属于同一 VPN 的其他 CE 建立基于 IPsec 的安全隧道，首先要从 SP 的 VPN 数据库中提取相应的安全信息，CE 可以利用这些信息通过 IKE 与对端 CE 建立 SA，SA 建立成功后在 CE 之间自动形成了一个新的安全隧道，这个隧道可以是 IPsec 传送模式 SA 保护下的 IP-in-IP 隧道，也可以是隧道模式的 IPsec SA。

目前这项技术还不成熟，运营商如果考虑这类安全性需求，可随时跟踪技术的发展，在相应的标准成熟且有多家厂商支持的情况下，运营商才有可能将这种加密传送作为一种 VPN 上的增值服务项目对用户提供。

7.2 VPWS 的安全防护

VPWS 的系统模型如图 2 所示：

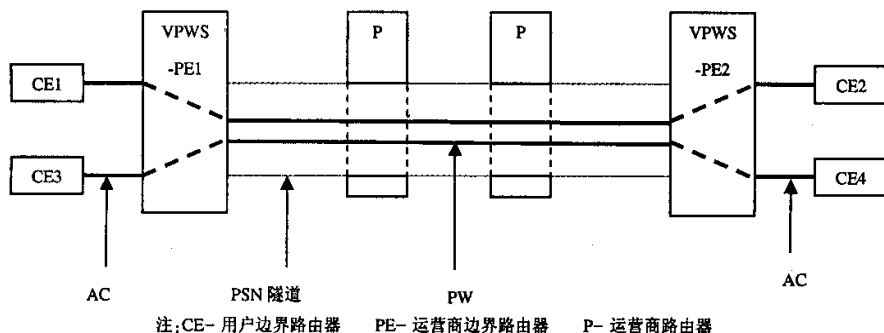


图 2 VPWS 系统结构示意图

VPWS 为用户提供的伪线路是在 PE 之间通过信令建立的，用户数据通过建立好的伪线路进行端到端传送，系统的安全性决定于如下两个方面：

- ◆ 控制面 PE-PE 信令传送的安全性；
- ◆ 资料面 CE-CE、PE-PE 用户数据传送的安全性。

7.2.1 VPWS 控制面的安全性

在控制面上，VPWS 通过 BGP 或 LDP 建立伪线路（PW）。

一个 PE 只有在确信另一个 PE 是目标 PE 的情况下，才可以与该 PE 建立控制连接并传送数据；否则，可能会把 L2VPN 流量发送到错误的地方。

因此，对于 PE 之间的控制连接，也建议运营商采用某种认证机制。对于采用 TCP 方式传送的信令，可以利用 TCP MD5 选项来作为 PE-PE 之间的认证方式，这要求 PE 之间使用一个共享的密钥。如果控制协议利用 UDP 消息，也应采用某些认证保护机制，有关技术正处于研究之中。

VPWS 系统由 PE 和 P 路由器相互连接构成，PE 和 P 路由器的安全性同样关系到整个系统的安全性，应采取一些措施防范恶意攻击，主要是 DOS 攻击。PE 路由器上，应对用户的接入速率进行限制；P 路由器上应采取 URPF 检查、设置过滤器、关闭 ICMP 等措施对流量进行控制。

7.2.2 VPWS 数据面的安全性

目前 VPWS 用户 CE 设备通常采用 Ethernet、ATM 等二层链路接入运营商的 PE 设备，这种接入电路是通过网管人员调配的，本身具有较强的安全性。但 PE 设备之间的连接经过了 IP 网络，有可能遭受攻击。

二层 VPN 的加密技术具有一定的复杂性，因为，IPsec 等常用的加密方式是在 IP 层上进行的，如果要对通过 IP 网传送的二层链路帧进行加密，则要进行一系列复杂的封装转换处理，信息传送的开销比较大。此外，运营商通过隧道机制实现了二层链路帧的端到端传送，本身具有一定的安全性。虽然运营商有可能利用某种方式实现二层链路帧的加密传送，但这种做法的必要性仍不明确，是否需要加密以及如何加密仍有待研究。

总之，VPWS 业务传送的是二层链路帧，加密的必要性有待研究，加密技术目前也还没有切实可行的方案，运营商可暂不考虑对此项加密功能的支持。

7.3 VPLS/IPLS 的安全防护

VPLS/IPLS 的系统模型如图 3 所示。

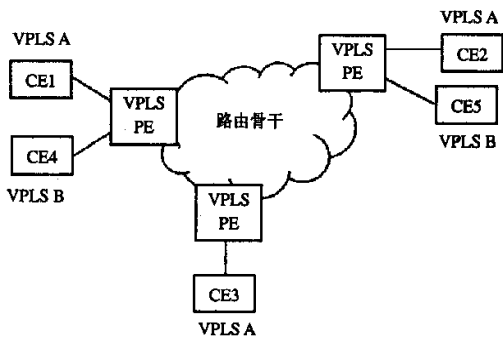


图3 VPLS/IPLS 系统结构示意图

VPLS 的解决方案实际上是对 VPWS 解决方案概念的扩展，通过在 PE 之间建立一个全网状的伪线路连接来仿真多点到多点的连接。除此之外，VPLS 系统可以向用户提供基于以太网的桥接接入方式，具备 MAC 路由学习和二层交换功能，使得整个 VPLS 系统的外在表现类似于一个功能强大的二层交换机。

VPLS 系统首先要为用户提供伪线路，同时在通信过程中完成 MAC 地址的学习功能，以及 MAC 单播和广播包的转发功能，系统的安全性决定于如下两个方面：

- 控制面 PE-PE 信令传送的安全性；
- 资料面 CE-CE、PE-PE 用户数据传送的安全性。

IPLS 是 VPLS 的一个特例，是 VPLS 功能上的一个子集，它只支持用户的 IP 业务，可以在一个可能不能支持所有 VPLS 功能的硬件平台上运行。

7.3.1 VPLS/IPLS 控制面的安全性

控制面上，VPLS/IPLS 使用与 VPWS 相同的机制建立伪线路，PE 之间建立伪线路时也应采用同样的安全认证机制。

对于 PE 之间的控制连接，同样建议运营商采用某种认证机制。对于采用 TCP 方式传送的信令，可以利用 TCPMD5 选项来作为 PE-PE 之间的认证方式，这要求 PE 之间使用一个共享的密钥。如果控制协议利用 UDP 消息，也应采用某些认证保护机制，有关技术正处于研究之中。

VPLS/IPLS 系统对网络基础设施采取的安全措施类似于 VPWS，PE 路由器上，应对用户的接入速率进行限制；P 路由器上应采取 URPF 检查、设置过滤器、关闭 ICMP 等措施对流量进行控制。

7.3.2 VPLS/IPLS 数据面的安全性

与 VPWS 业务类似，VPLS/IPLS 传送的是二层链路帧，加密的必要性有待研究，加密技术目前也还没有切实可行的方案，运营商可暂不考虑对加密功能的支持。

此外，VPLS 系统具有 MAC 地址学习和广播包/组播包的发送功能，如果某个 CE 设备发送大量的广播包/组播包，就会给很多接收广播包/组播包的 PE 设备和网络上的 P 设备带来较重的处理负担，如果这种发送是恶意的，就可能产生类似于 DOS 攻击的效果，使 PE 或 P 设备不能正常工作。

为了保证系统的安全性，运营商应在 PE 上对广播信息的传送进行限制，例如采用对广播包/组播包的带宽限制等措施。

附录 A
(规范性附录)

三层 VPN 的 PE-PE 数据信息的加密传送

PE-PE 数据信息的加密传送功能是由运营商的网络边缘设备完成的，用户设备无需进行特别的配置，由运营商的 PE 设备完成基于 IPsec 的加密功能，是基于网络的加密模式。

运营商为用户提供 BGP MPLS VPN 业务时，PE 之间通过 MPLS 网络传送的用户数据包通常被打上至少两层标记，最内层为 VPN 内部标号，外层为 MPLS 网络的路由标记，对应于 PE 之间建立的 LSP。为了保证数据传送的安全性，可以用基于 IPsec 的安全 IP 隧道传送 MPLS 包，即将 MPLS 包被封装到 IPsec 的载荷部分传送。

A.1 设备的配置

PE 之间数据的安全封装传送存在两种方式：MPLS-in-IP 和 MPLS-in-GRE，这两种封装方式实际上是在 PE 之间建立了一条基于 IPsec 的安全 IP 隧道，为了支持这两种封装格式，加 IPsec 封装的 LSR 应了解如下两点：

- ◆ 去封装的 LSR 的 IP 地址；
- ◆ 去封装的 LSR 能够支持这种 IPsec 封装格式。

这些信息可以手工配置到处理 IPsec 封装的路由器上，也可以通过某些自动发现协议进行传送。例如，如果 IPsec 隧道支持某些应用，而该应用具有建立连接或自动发现协议，则可以利用该应用层协议传送有关 IPsec 封装方式的信息。

此外，IETF 正在考虑是否用 BGP 协议完成自动配置功能，在 BGP 消息中增加一个“IPsec 扩展团体”属性，将安全配置要求由出口 PE 传送给入口 PE，配置完成后，入口 PE 可根据安全配置要求对从 CE 收到的 IP 包进行基于 IPsec 的 MPLS 封装，并将其通过 MPLS 网络发送给出口 PE。

A.2 PE 间传送的用 IPsec 封装 IP/MPLS VPN 包的格式

对 MPLS VPN 包的封装方式包括两种：MPLS-in-IP 和 MPLS-in-GRE。

基于 IPsec 的 MPLS-in-IP 封装格式如图 A.1 所示。

IP 头	IPsec 头	MPLS 标记栈	MPLS 载荷
------	---------	----------	---------

图 A.1 MPLS-in-IP 封装格式

这种封装格式下，IP 头可以是 IPv4 或 IPv6 包头，其中源地址和目的地址分别是加封装的 LSR (PE) 和去封装的 LSR (PE) 的 IP 地址。

这种封装方式使得 MPLS 标记包被封装到一条基于 IPsec 的 IP 隧道中传送，这种包可以直接通过 IP 网络传送，如果通过 MPLS 网络传送，还要在 IP 头之前打上 MPLS 路由标记，隧道接收端的设备去掉 IP 头和 IPsec 封装，然后将标记栈最顶层的标记作为“输入标记”进行处理。

基于 IPsec 的 MPLS-in-GRE 封装格式如图 A.2 所示。

IP 头	IPsec 头	GRE 头	MPLS 标记栈	MPLS 载荷
------	---------	-------	----------	---------

图 A.2 MPLS-in-GRE 封装格式

这种封装格式下，IP 头可以是 IPv4 或 IPv6 包头，其中源地址和目的地址分别是加封装的 LSR (PE)

和去封装的 LSR (PE) 的 IP 地址; GRE 头中的协议类型 (PT) 字段值应为 “0x8847” 或 “0x8848”, 分别表示 MPLS 单播和组播。

这种封装方式使得 MPLS 标记包可以与其他协议包共享一条 IP 隧道传送, 同时使用 IPsec 进行加密, 使数据传送的安全性得到保证。这种 MPLS-in-GRE 包可以直接通过 IP 网络传送, 如果通过 MPLS 网络传送, 还要在 IP 头之前打上 MPLS 路由标记, 隧道接收端的设备去掉 IP 头、IPsec 头和 GRE 封装, 然后将标记栈最顶层的标记作为“输入标记”进行处理。

附录 B

(资料性附录)

三层 VPN 的 CE-CE 数据信息的加密传送

CE-CE 数据信息的加密传送可以由业务提供商 (SP) 来支援。为了支持这一功能, 运营商要维护一个安全 VPN 数据库, CE 设备要从数据库中提取信息, 完成安全配置并建立基于 IPsec 的安全隧道, 通过安全隧道传送 VPN 用户的数据包。

B.1 设备配置

设备配置包括两个方面: SP 设备配置和 CE 设备配置

(1) SP 设备配置

SP 要在服务器上维护一个安全 VPN 数据库, 这个数据库可以为多个 VPN 提供服务。随着 VPN 数量的增加, 可以部署多个服务器。为了保证可靠性, 可以在主用服务器之外部署备份的 VPN 数据库服务器。

SP 的 VPN 管理基础设施要为每个附着的 CE 提供安全的配置信道, 以便在 SP 的 VPN 数据库和 CE 之间交换 VPN 特定配置信息。

SP 要在 VPN 数据库中建立 VPN 条目, 同时登录属于该 VPN 的 CE, 对每个 CE 设备要配置和维护下列信息:

- ◆ 安全远程管理协议需要的安全信息, 这些信息用于 CE 和 SP 的 VPN 服务器的双向认证以及管理数据的加密。具体的信息内容决定于用于远程管理的特定协议 (栈);
- ◆ 统一 VPN 内对等 CE 之间建立和维护安全连接 (SA) 所需的安全信息。

(2) CE 设备配置

CE 要与 SP 的 VPN 服务器建立安全的通信路径, 为此需要配置下列信息:

- ◆ SP 的 VPN 服务器的 IP 地址, 或者到达 SP 的 VPN 数据库中特定 CE 的 VPN 信息的 URL;
- ◆ SP 的安全远程管理协议 (栈) 需要的安全信息;
- ◆ SP 路由空间中的一个 IP 地址, 可以静态配置, 也可以动态获得 (例如通过 DHCP)。

B.2 CE 之间基于 IPsec 的安全隧道的建立方式

CE 为了与属于同一 VPN 的其他 CE 建立基于 IPsec 的安全隧道, 首先要从 SP 的 VPN 数据库中提取信息。CE 可以选择在 IKE 协商认证中使用何种方式 (预先共享密钥方式、数字签名和证书方式), SP 服务其应提供相应的信息。

使用预先共享密钥方式时 SP 的 VPN 服务器应提供下列信息:

- ◆ 对等 CE 的 IP 地址;
- ◆ 预先共享密钥;
- ◆ SA 信息 (即与对端 CE 协商建立 SA 所需的信息);
- ◆ 隧道信息 (如在 IP-in-IP 封装上使用隧道方式的 IPsec 还是传送模式的 IPsec 等信息)。

使用数字签名认证方式时 SP 的 VPN 服务器应提供下列信息:

- ◆ 私钥、公钥对;

- ◆ 公钥的证书;
- ◆ 来自证书授权机构的公钥;
- ◆ 有关对端 CE IP 地址、SA 信息、隧道信息的表。

从 SP 的 VPN 服务器提取上述信息后, CE 可以利用这些信息通过 IKE 与对端 CE 建立 SA, SA 建立成功后在 CE 之间自动形成了一个新的安全隧道, 这个隧道可以是 IPsec 传送模式 SA 保护下的 IP-in-IP 隧道, 也可以是隧道模式的 IPsec SA。

B.3 CE 间传送的用 IPsec 封装的数据包格式

IPsec 封装存在两种模式: 传送模式和隧道模式, CE 间资料包 IPsec 封装对应于这两种模式。

(1) 传送模式的 IPsec 封装

传送模式的 IPsec 封装是将 IPsec 头加到 VPN 内部的 IP 包头和载荷之间。进行传送时, CE 要构建一个 IP-in-IP 隧道, 封装格式为外层 IP 为隧道资料包, 源地址为源端 CE 的公网地址, 目的地址为对端 CE 的公网 IP 地址, 内层 IP 包为 VPN 内部数据包, 用 IPsec 封装该内层数据包, 如图 B.1 所示。

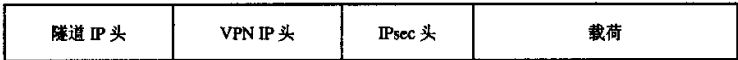


图 B.1 CE 间传送模式 IPsec 封装格式

(2) 隧道模式的 IPsec 封装

隧道模式的 IPsec 封装是将 IPsec 头加到 VPN 内部 IP 包的包头之前。CE 之间通过 IP 隧道传送加了 IPsec 封装的数据包, 也就是再 IPsec 头之前再加上一个 IP 头, 外层 IP 头的源地址为源端 CE 的公网地址, 目的地址为对端 CE 的公网 IP 地址, 内层 IP 包为 VPN 内部数据包。封装格式如图 B.2 所示。

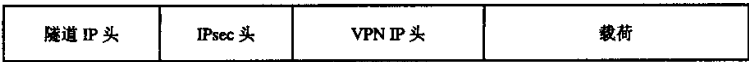


图 B.2 CE 间隧道模式 IPsec 封装格式

附录 C

(资料性附录)

三层 VPN 几种加密方式的比较

三层 VPM 的加密方式通常分为四种：CE-PE 方式、PE-PE 方式、CE-CE 方式、CE-PE 与 PE-PE 相结合的数据加密方式。加密方法见 6.3，加密信息的封装格式参见附录 A 和附录 B。选择使用上述四种加密措施时应考虑如下几种因素：

- 抗窃听能力：数据在设备间传送并受到攻击者窃听时，能否得到加密保护；
- 设备安全性：假定攻击者可访问某种设备（或改变设备的配置），这种情况下数据是否被保护；
- 设备配置和管理的复杂性：假定每个 VPN 有 N 个 CE 分别连接着 N 个 PE 设备，需要建立和维护多少设备配置；
- 设备的处理负担：假定要传送 n 个包，需要做多少次加密和解密处理；
- SP 提供增值服务（QoS、防火墙、入侵检测等）的可能性：SP 是否可以查看资料，以便提供增值服务。

下面从这几个角度出发分析上述四种加密方式的特点以及使用条件：

(1) CE-CE 方式

其特点如下：

- 抗窃听能力：具有端到端的抗窃听能力；
- 设备安全性：CE 设备遭受攻击时数据安全受威胁；
- 设备配置和管理的复杂性：加密是在 CE 之间进行的，存在基于 CE 数目的 n^2 问题。
- 设备的处理负担：传送 n 个包时，分别在两侧的 CE 上进行加密/解密操作，总的操作次数为 $2n$ ；
- SP 提供增值服务的可能性：受到严重限制，一般只有 DiffServ 标记对 SP 是课件的，可以提供一些 QoS 服务。

如果用户对自己管理的站点之外的网络链路不信任，需要端到端或 CE-CE 的加密传送时可以采用这种方式，这种方式下使用的 CE 设备可以由 SP 提供。

(2) PE-PE 方式

其特点如下：

- 抗窃听能力：在 SP 骨干网络上具有抗窃听能力；
- 设备安全性：CE 或 PE 设备遭受攻击时数据安全受威胁；
- 设备配置和管理的复杂性：配置的复杂性取决于加密的方式，如果加密是基于 VPN 站点间的，则存在基于站点数目的 n^2 问题；如果加密是基于 PE 之间的，则存在基于 PE 数目的 n^2 问题。
- 设备的处理负担：传送 n 个包时，分别在两侧的 PE 上进行加密/解密操作，总的操作次数为 $2n$ ；
- SP 提供增值服务的可能性：完全具备支持增值服务的能力，SP 可查看用户数据流的细节信息，并据此提供任何增值服务。

如果认为接入链路比较安全，安全隐患主要存在于 SP 网络上，可以使用这种方式。

(3) CE-PE 方式

其特点如下：

- ◆ 抗窃听能力：在 CE-PE 的链路上具有抗窃听能力；
- ◆ 设备安全性：CE 或 PE 遭受攻击时数据安全受威胁；
- ◆ 设备配置和管理的复杂性：用户的 CE 设备和 SP 的 PE 设备分别进行配置，由于不存在网状连接问题，增加 n 个 CE 会相应增加 n 个配置；
- ◆ 设备的处理负担：传送 n 个包时，分别在两侧的 PE 和 CE 上进行加密/解密操作，总的操作次数为 $4n$ ；
- ◆ SP 提供增值服务的可能性：完全具备支持增值服务的能力，SP 可查看用户数据流的细节信息，并据此提供任何增值服务。

如果认为 SP 骨干网络的安全性很强，只是在接入链路上存在安全隐患的情况下可以使用这种方式。

(4) CE-PE 与 PE-PE 相结合的方式

其特点如下：

- ◆ 抗窃听能力：具有端到端的抗窃听能力；
- ◆ 设备安全性：CE 或 PE 设备遭受攻击时数据安全受威胁；
- ◆ 设备配置和管理的复杂性：在接入链路上，用户的 CE 设备和 SP 的 PE 设备分别进行配置，由于不存在网状连接问题，增加 n 个 CE 会相应增加 n 个配置。在 SP 骨干网上，PE 配置的复杂性取决于加密的方式，如果加密是基于 VPN 站点间的，则存在基于站点数目的 n^2 问题；如果加密是基于 PE 之间的，则存在基于 PE 数目的 n^2 问题。
- ◆ 设备的处理负担：传送 n 个包时，分别在 CE-PE、PE-PE、PE-CE 的链路上进行加密/解密操作，总的操作次数为 $6n$ ；
- ◆ SP 提供增值服务的可能性：完全具备支持增值服务的能力，SP 可查看用户数据流的细节信息，并据此提供任何增值服务。

SP 管理 PE 设备，CE 设备由用户管理，SP 为用户提供端到端的加密信息传送时可以采用这种方式。

上述四种加密方式的不同特点对网络和业务带来不同的影响：抗窃听能力关系到数据的安全性，设备的安全性关系到设备中存储数据的安全性，设备的配置复杂性关系到系统的扩展能力，设备的处理负担关系到每个设备支持 VPN 业务的容量以及业务的 QoS，提供增值服务的可能性关系到业务的发展和用户市场的进一步开发，SP 应综合考虑上述因素决定采用何种加密方式。

中 华 人 民 共 和 国
通 信 行 业 标 准
运营商提供的虚拟专用网安全技术要求
YD/T 1909-2009

*

人民邮电出版社出版发行
北京市崇文区夕照寺街 14 号 A 座
邮政编码: 100061
北京新瑞铭印刷有限公司印刷
版权所有 不得翻印

*

开本: 880×1230 1/16 2009 年 8 月第 1 版
印张: 1.75 2009 年 8 月北京第 1 次印刷
字数: 45 千字

ISBN 978 - 7 - 115 - 1876/09 - 118

定价: 15 元

本书如有印装质量问题, 请与本社联系 电话: (010)67114922