YD

中华人民共和国通信行业标准

YD/T 1486-2006

承载电信级业务的IP专用网络安全框架

Security Architecture of IP Private Network for Bearing Carrier-grade Service

2006-06-08 发布　　2006-10-01 实施

中华人民共和国信息产业部　发布

目　次

前　言

本标准以 ITU-T X.805《端到端通信系统安全框架》为基础，对承载电信业务的 IP 专用网络的安全性采用 X.805 安全框架的方法作了规定。本标准的相关内容遵循了国家在信息安全方面的各项规定（包括国家商用密码管理方面）。在本标准的制定过程中还参考了 GB/T 18336 和 ITU-T X.800 系列标准。

本标准的附录 A 为资料性附录。

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：华为技术有限公司

中兴通讯股份有限公司

成都迈普产业集团有限公司

大唐电信科技产业集团

本标准主要起草人：苗福友　冯　伟　王文煜　陈建业　陈小敬

承载电信级业务的IP专用网络安全框架

1 范围

本标准规定了承载电信级业务的IP专用网络的安全框架，包括三个层面的三个平面，即基础设施层、业务层和应用层的用户、控制和管理三个平面，从访问控制和鉴别等8个安全维度对基础设施层和业务层的每个平面的安全性进行了规定。本标准没有规定应用层的安全性。

本标准适用于各种承载电信级业务的IP专用网络。

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。

ITU-T X.805　　端到端通信系统安全框架

3 缩略语

下列缩略语适用于本标准。

AH	Authentication Header	鉴别报文头协议
BGP	Border Gateway Protocol	边界网关协议
CNM	Customer Network Management	客户网络管理
CPU	Central Processing Unit	中央处理器
DIAMETER	Diameter AAA Protocol	一种验证、授权和计账协议
DHCP	Dynamic Host Configuration Protocol	动态主机配置协议
DNS	Domain Name System	域名系统
DoS	Denial of Service	拒绝服务攻击
EAP	Extensible Authentication Protocol	扩展鉴别协议
EGP	External Gateway Protocol	外部网关协议
ICV	Integrity Check Value	完整性检查值
IGP	Internal Gateway Protocol	内部网关协议
IMS	IP Multimedia Subsystem	IP多媒体子系统
IP	Internet Protocol	互联网协议
IPsec	IP Security	IP安全协议
IS-IS	Intermediary System to Intermediary System	中间系统到中间系统协议
MAC	Message Authentication Code	报文鉴别码
MLD	Multicast Listener Discovery	组播侦听者发现协议
MPLS	Multi-Protocol Label Switch	多协议标记交换

OSPF	Open Shortest Path First	开放最短路径优先协议
RIP	Route Information Protocol	路由信息协议
RADIUS	Remote Authentication Dial In User Service	拨号用户远程鉴别协议
SLA	Service Level Agreement	服务水平协议
SNMP	Simple Network Management Protocol	简单网络管理协议
SSH	Secure Shell	安全外壳程序协议

4 概述

IP 技术逐渐成为电信业务的基本承载技术。对于承载电信级业务的 IP 网络，为了保证电信业务的正常开展，网络被限定只提供一种或几种业务，为电信业务提供电信级的可靠性和可用性。但是 IP 网络承载电信业务还存在一些不足，其中 IP 网络安全性需要提高。目前 IP 网络上存在各类安全机制，分别处于不同层面和角度来考虑安全问题，并获得不同的安全特性（如完整性和保密性）。本标准采用 ITU-T X.805 “端到端通信系统安全框架”的模型方法，对电信级 IP 承载网安全性和采用的安全技术进行规定。

ITU-T X.805 定义了一个完整的端到端通信系统的安全框架，定义了三个网络层次：应用层、业务层和基础设施层，并为每个网络层次定义了控制、管理和用户三个平面。对每个层次的每个平面都分别从 8 个方面考虑其安全性：

——访问控制：只有合法的用户才被授权访问；

——鉴别：确定用户的身份是真实的；

——不可抵赖：保证有合适的证据证明事件的存在；

——数据保密性：保证数据不被泄露和或泄露后被解读；

——通信安全：保证传输的数据的安全性；

——完整性：保证数据不被篡改；

——可用性：保证业务获得适当的资源；

——隐私：不泄露身份和标识信息。

本标准将 X.805 安全框架应用到电信级 IP 承载网络的三个网络层次：

——基础设施层，由路由器等转发设备组成的网络；

——业务层，主要是传输类业务，如 VPN 和 AAA 业务，本标准只规定了 VPN 业务；

——应用层，转发设备上实现业务和传输的应用，考虑到应用的丰富性，本标准没有对这部分内容作出规定。

每个层次上都有用户、控制和管理三个平面，在每个平面上都规定了访问控制、保密性和完整性等 8 个方面的安全功能。

5 基础设施层

5.1 用户平面

5.1.1 访问控制

在用户平面，基础设施层次的访问控制分为两个方面，第一个方面是基础设施本身（如路由器）对用户数据的访问；第二个方面是用户报文访问转发基础设施，如路由器的数据转发功能。

对于第一个方面，对于电信级的承载网络，用户选择网络业务时是依赖于对运营商的信任作为基础

的，因此不要求对网络设备访问用户数据进行访问控制。但是，基础设施应该最大限度地保证自身的安全，防止其他的非授权用户或攻击者通过基础设施的安全缺陷非授权访问用户数据。

对于第二个方面，路由器、交换机和物理链路是网络提供接入和其他通信业务的基础。在 IP 承载网络的基础设施层，对用户的访问控制主要表现在对网络接入和带宽的控制。针对于不同的网络层次和接入技术存在不同的接入控制技术，如针对以太网的 802.1x 技术。目前主要的鉴别和访问控制技术基本上是依赖于二层技术，但是，IETF 目前也正在制定基于 IP 技术的网络接入鉴别和访问控制技术。

由于用户的数量很大，而网络设备本身的处理能力相对有限，为了能够实现访问控制的可规模化，通常在网络边缘第一个三层设备来实现访问控制，使用鉴别服务器来实现用户的接入鉴别，并且在网络设备和鉴别服务器之间采用 RADIUS 或 DIAMETER 等协议来实现通信。

5.1.2 鉴别

鉴别用于检查企图接入网络的用户的身份，鉴别往往同访问控制技术结合起来使用。根据上一节的内容，实际执行鉴别的设备可以是鉴别服务器。

通常，在用户（或用户设备）和网络之间可能采用各种不同的鉴别技术和鉴别算法，如：

——基于用户名/口令的鉴别；

——基于智能卡的鉴别；

——基于 X.509 证书的鉴别；

——基于公开密钥的鉴别算法；

——基于共享密钥的鉴别算法。

鉴别既可以在设备本地实现，也可以由专门的鉴别服务器完成集中鉴别。

为了能够支持各种验证算法，通常在用户（或用户设备）和网络之间采用 EAP 协议来支持各种鉴别技术，该技术也可以用于网络和鉴别服务器之间。

5.1.3 不可抵赖

不可抵赖要求网络保存用户对网络的访问记录，并且将该记录作为用户曾经访问网络的证明。

不可抵赖可以通过数字签名来实现，通过为每个报文添加一个签名来证明该报文来源于某个用户，并且使用公开密钥技术来作为用户访问网络的证明。在承载网络中，数字签名是以单个的报文来转发的，因此对每个报文都要完成一次签名检查和归档，性能难以满足网络运营的要求，一般不作为承载网的不可抵赖机制。

在 IP 网络中常通过计账技术来实现不可抵赖，该技术依赖于鉴别以及访问控制，在这两个技术的基础上，对用户的访问信息形成一个记录，包括如用户名称、访问时间段和流量等，然后通过 RADIUS/DIAMETER 协议将数据发送到计账服务器保存和处理，作为日后审计和计账的依据。

5.1.4 数据保密性

在用户平面，数据保密性要求其他用户不能获得或获得后解读用户发送的数据。

实现数据保密性可以通过加密技术来实现，如用户之间实现端到端的 IPsec 加密，对于网络设备，也存在一些技术来实现对用户数据的加密传送，如数据链路层的加密技术和隧道模式的 IPsec，因为加密需要大量的计算，对于所有或大部分数据通过加密来提供保护需要大量的计算和存储资源，大规模的应用受到限制，但是可以对关键的接入用户数据，网络可以使用加密来保证保密性。

通过访问控制技术可以实现数据保密性，因为访问控制可以限制一个用户对另外一个用户数据的访

问。

在接入网，可以采用有连接的技术来保证每个用户的数据都限制在各自的连接内，避免了一个用户从另外一个连接内获得信息，间接地实现了数据的保密性。

5.1.5 通信安全

用户数据在网络中传输的时候需要保证数据不被转发到该报文目的地址和转发途径的节点之外的节点上，以及不被非法的节点拦截。通信安全主要依靠转发设备的路由/转发机制，以及转发设备本身的安全性来保证。

5.1.6 数据完整性

在用户平面，数据完整性要求其他用户不能修改用户发送的数据，即使数据被修改系统也能够发现通信流量或报文已经发生了变化。

数据完整性可以通过完整性鉴别技术来实现，如用户之间实现端到端的 IPsec 鉴别头（AH）技术，对于网络设备，也存在一些技术来实现对用户数据的加密传送，如数据链路层的完整性检查技术和隧道模式的 IPsec AH，但是因为需要大量的计算，对于所有或大部分数据通过完整性检查来提供保护需要占用大量的资源，但是可以对关键的用户数据提供完整性检查来保证完整性。

通过访问控制技术可以实现数据完整性，因为访问控制可以限制一个用户对另外一个用户数据的访问。

在接入网，可以采用有连接的技术来保证每个用户的数据都限制在各自的连接内，避免了一个用户从另外一个连接内获得信息，间接地实现了数据的完整性。

5.1.7 可用性

在用户访问网络时，网络要能够有充足的资源保证用户的访问能够实施，可以通过如下的方法来实现和改进可用性。

——对网络资源实现严格的控制，避免用户误用和过量占用大量资源；

——隔离管理和控制流量，避免用户通过针对这两个平面内发起的拒绝服务攻击（DoS）占用大量的资源，从而造成网络对用户不可用；

——在网络边缘实现严格的访问控制机制；

——使用防火墙来加强访问控制。

5.1.8 隐私

保证用户信息不被其他用户或攻击者非法获得。隐私包括的信息如下：

——用户的位置信息；

——用户设备的 IP 地址和主机名；

——用户登录网络的用户名和口令等信息；

——用户要访问的目的系统的 IP 地址或主机名。

5.2 控制平面

5.2.1 访问控制

基础设施的控制平面保证只有授权的人员和设备允许访问网络中的控制信息，如存在于路由器中的路由信息。此外，该安全功能也保证设备只接受来自授权的人员和设备的信息。

控制平面的访问控制一般依赖于鉴别技术，根据鉴别结果来决定是否允许访问系统，或者是系统根

据对报文的鉴别来决定是否将从设备和网络中获得的控制信息用于设备自身/网络的控制。目前，主要的IGP和EGP协议都实现了报文鉴别功能，如OSPFv2、RIP2、BGP4和IS-IS。

此外，访问控制可以根据设备物理上不可变更的特征来决定是否授权访问，如基于端口的访问控制。这种方法可以同路由结合起来实现比较严格的访问控制，如根据报文入端口进行反向转发检查，即单播反向路径转发。

承载电信业务的IP承载网对网络的安全性有很高的要求，并且能够对业务进行比较严格的控制，因此可以采用平面分离的方法，保证用户平面的数据不可能进入控制平面，这样就杜绝了来自于用户利用控制信息对网络和设备发起的攻击。

5.2.2 鉴别

鉴别用于检查控制平面访问者（包括设备和人员）的身份，确定访问者的身份是合法的，以及发送控制信息的设备的身份是合法的。

鉴别技术通常是访问控制技术的依据，通常采用完整性鉴别来实现，如通过检查完整性（ICV）来确定是否该报文的来源是一个合法的设备。

5.2.3 不可抵赖

不可抵赖要求对控制数据的使用和改变是可以追溯的，通常使用一个记录来保存用户和设备对网络/设备的访问信息，该记录通常称为日志。

路由器等网络设备一般都实现了日志功能，能够记录每次对控制数据的访问信息，例如：

——访问时间；

——访问者/设备；

——访问对象；

——访问类型；

——访问结果。

该数据可以作为访问和修改控制数据的证据。

路由器等网络设备对于如下控制数据的发送和访问可以记录日志来提供不可抵赖性：

——地址分配活动，如DHCP报文的接收；

——对网络和设备有比较大的影响的控制ICMP报文；

——来自于网络的路由信息/拓扑变化信息。

实现不可抵赖的另外一种技术是数字签名技术，该技术采用公开密钥技术来实现。由于采用数字签名技术需要大量的计算和处理器资源消耗，因此不推荐在网络的控制报文中使用数字签名。

5.2.4 数据保密性

控制平面的控制数据要避免非授权用户和攻击者获得或获得后解读，需要提供保密性保护的数据包括：存在于网络设备上的控制数据，如路由信息，以及在网络上传输的控制信息。

对于设备上存储的控制信息，访问控制技术能够避免非授权用户和攻击者获得该信息，这样就间接地提供了保密性。此外，还可以采用加密的方法对本地存储的数据进行加密，因为路由器等网络设备的计算能力有限，需要考虑性能和安全之间的平衡。

对于网络中传输的控制数据，一般可以采用加密技术来提供保密性，如3DES加密算法。目前大多数的路由协议本身都没有实现加密，如RIP2和BGP4，但是可以在该协议的下层协议来实现，如IPsec

来保护 BGP4 协议。此外，也可以使用数据链路层的加密技术来实现保密性，相对于端到端的加密方法（如传输模式的 IPsec），它更适合控制信息的传递路径上的一些设备需要根据报文内容改变自身的状态。

实现保密性另外一种方式是实现平面隔离，参见 5.2.1 小节。

5.2.5 通信安全

控制数据在网络中传输的时候，需要保证数据不被转发到该报文目的地址和转发路径上的节点之外的节点上，主要依靠转发设备的路由/转发机制以及转发设备本身的安全性来保证。

此外，对于一些组网情况和特定的控制数据，可以采用带外控制的方式，用专用的逻辑或物理传输资源将控制数据的传输同用户数据的传输分离开，以保证通信安全。

5.2.6 数据完整性

控制数据要避免非授权用户和攻击者的篡改，需要提供完整性保护的数据包括存在于网络设备上的控制信息，如路由表，以及在网络上传输的控制信息。

对于设备上存储的控制信息，访问控制技术能够避免非授权用户和攻击者获得该信息，这样就间接地提供了完整性。此外，还可以采用完整性鉴别的方法，如有密钥的哈希技术，对本地存储的数据进行处理，产生一个完整性检查值作为是否被非法篡改的依据，但是路由器等网络设备的计算能力有限，因此要考虑性能和安全之间的平衡。

对于网络中传输的控制数据，一般可以采用完整性鉴别来提供完整性。目前大多数的路由协议本身都实现了完整性保护，如 OSPFv2 和 BGP4。

5.2.7 可用性

控制平面的可用性对于网络是非常重要的，保证可用性的措施如下：

——保证控制协议，如路由协议，不存在可以被用来发起拒绝服务攻击的缺陷，数据完整性机制一定程度上能够避免发起拒绝服务攻击；

——访问控制，对于来自于网络的控制报文实现数据源鉴别；

——将控制信息隔离到专用的通道中，并且为控制信息的传输和处理分配充足的资源，如 CPU 处理周期、存储和带宽。

5.2.8 隐私

保证控制平面内标识网络设备或人员的信息不被非授权访问者获得和使用，例如：

——IP 地址；

——MAC 地址；

——DNS 名。

5.3 管理平面

5.3.1 访问控制

在基础设施的管理平面，访问控制安全维度只允许授权的人员和设备对网络设备和通信链路实施管理活动。对于设备和通信链路的管理一般包含的方式如下：

——通过 SNMP 或其他的网络管理协议实现的网络管理活动；

——通过本地端口实现的管理活动，如控制台接口；

——通过远程网络连接登录到设备来实施的管理活动。

访问控制安全维度要求能够在以上的管理活动中对用户/管理员进行标识，并根据标识和鉴别的结果

确定用户的访问权限，访问权限包括：

——允许的操作类型，如读操作或写操作/完全控制等；

——允许的操作对象。

访问控制安全功能根据本地或远程存储的对象标识和访问权限，决定对具体被管理对象的访问授权和授权类型。

此外，一些网络管理活动是通过中间设备来实现对某个设备的管理，对于这种类型管理活动，访问控制根据中间设备或原始用户（通过中间设备实施管理的人员）的标识信息实施访问控制。

5.3.2 鉴别

鉴别用于检查对网络设备和链路实施网络管理活动的人员的身份，鉴别技术通常是访问控制技术实施的一个环节。

鉴别首先要标识访问者的身份，该身份可以采用用户名、证书、智能卡等方式来实现。此外，在采用共享密钥的对称密钥加密技术的情况下，还需要对方拥有共享密钥，该共享密钥用于身份鉴别。在公开密钥加密技术中，鉴别的依据是使用访问者私有密钥加密的数据和公开密钥。

EAP 在当前 IP 网络的数据平面鉴别中得到广泛采用，其统一的用户和协议接口，在管理平面的鉴别中也逐渐得到采用。

SNMP 和 Telnet/SSH 等协议都实现了身份鉴别。

5.3.3 不可抵赖

不可抵赖要求系统提供记录来证明用户对通信设备的访问活动确实发生，该记录可以作为管理活动发生的证据。

在 IP 网络中，日志是主要的提供不可抵赖的工具，通过对用户的管理活动进行记录来证明用户确实访问了系统，记录的信息如下：

——访问者身份；

——访问时间；

——操作对象；

——操作类型；

——操作结果。

5.3.4 数据保密性

网络管理数据不应被非授权的用户或攻击者获得或获得后解读。

网络管理数据如下：

——被管理的路由器上存在的配置、故障、安全、性能和计账数据；

——备份在服务器或其他存储介质上的管理数据；

——在网络中传输的管理数据。

对于路由器上的管理数据，需要加强访问控制和鉴别管理来保证数据的保密性，此外可以结合加密技术来实现保密。对于备份数据，应该严格管理这些数据，确保数据的安全，如果必要，可以采用加密技术来实现这些数据的安全。

对于网络中传输的管理数据，可以有以下几种方式避免数据保密性被破坏：

——避免非授权用户或攻击者从物理/逻辑上获得该数据，如采用物理隔离的方式；

——采用加密技术，如 3DES 加密算法，即使攻击者获得该管理信息，仍不能够解读该数据。

5.3.5 通信安全

当采用远程访问的方式来管理路由器、交换机等设备和通信链路时，需要保证数据不被转发到被管理对象之外的设备，并且管理数据不被非法的设备拦截。可以采用带外管理和专用管理接口的方式将管理数据同普通数据隔离，并且使用专门的传输路径来保证数据不被非法拦截。

5.3.6 数据完整性

网络管理数据不应该被非授权的用户或攻击者破坏和篡改。

网络管理数据如下：

——被管理设备上存在的配置、故障、安全、性能和计账数据；

——备份在服务器或其他存储介质上的管理数据；

——在网络中传输的管理数据。

对于设备上的管理数据，需要加强访问控制和鉴别管理来保证数据的完整性，此外可以结合加密技术来实现保密。对于备份数据，应该严格管理这些数据，确保数据的安全，如果必要，可以采用加密技术来实现这些数据的安全。

对于网络中传输的管理数据，可以有以下几种方式避免数据完整性被破坏：

——避免非授权用户或攻击者获得并篡改该数据，如采用物理/逻辑隔离的方式；

——采用完整性鉴别，如 MAC 算法，即使攻击者篡改了该管理信息，系统能够检测出报文已经被非授权改变，避免被欺骗。

数据完整性保护通常同访问控制和鉴别机制等一起来保证系统的安全。

5.3.7 可用性

可用性确保授权用户能够对路由器、交换机和链路实现管理。目前对网络管理数据可用性影响比较大的攻击主要是拒绝服务攻击，通过大量的非授权活动致使系统的资源被大量占用，从而授权用户无法访问或不能顺利访问系统。

对基础设施平面的网络管理方面的进攻方式如下：

——占用网络管理通信通道大量带宽，造成管理通信不能建立；

——对被管设备进行资源耗尽攻击，如路由器的 CPU 和内存。

拒绝服务攻击的主要抵制方式是对用户的资源使用进行准确控制，此外也可以结合密码技术。

5.3.8 隐私

隐私保证被管设备和管理系统的标识信息不被非法获得，例如：

——IP 地址；

——主机名；

——硬件地址；

——管理员用户名和口令。

隐私保护通常采用加密的方法来实现，物理隔离和逻辑隔离也可以实现隐私保护。

6 业务层

6.1 概述

在电信级的 IP 承载网络中存在丰富的业务，主要分为两类：

——对 IP 网络的承载功能进行扩展产生的业务，如 VPN 业务和组播业务；

——用来支持 IP 网络正常运转的业务，如 DHCP 和 DNS 等。

考虑到每种业务的特殊性和业务的丰富性，不能对各种业务的安全性做全部规定，本章只规定 VPN 业务的安全。对于位于 IP 层以上或同 IP 承载功能本身无关的业务，如 IMS 服务，不在本标准的讨论范围之内。

6.2 用户平面

在用户平面，有两个层次的安全问题。一方面，VPN 每个站点（Site）内的终端用户在 8 个安全维度上的安全，对于 VPN 内部而言，同第 5 章的规定基本上没有差别，这里不做规定。另一方面是 VPN 对来自 VPN 外部的威胁所产生的安全问题和相应的安全技术，本节主要分析后一种情况。

6.2.1 访问控制

在用户平面，访问控制要求只有授权的用户才允许访问 VPN 服务，一般 VPN 内部的用户管理由申请 VPN 服务的组织来负责，该组织可以决定采用哪种方式来实现访问控制，对于大部分的企业用户，一般都是通过管理手段结合技术手段来管理访问控制。

也有很多情况，VPN 向外部客户提供服务，这种情况下可以参见 5.1.1 节。

VPN 访问控制的另外一个重要的方面是一个场所如何安全地加入一个 VPN。对于一些 VPN 来说，场所加入是一个配置的过程，配置中涉及到对场所/链路的鉴别和检查，然后决定其是否可以连接到网络中，在这里访问控制基本上是一个手工配置的过程，如 MPLS/BGP VPN。

也有一些 VPN 是动态地加入成员，如 VPDN，对于此类 VPN 应该实现对用户/设备的鉴别和访问控制，可以参见 5.1.1 和 5.1.2 节。

6.2.2 鉴别

鉴别用于检查访问 VPN 客户的身份，包括设备和人员。通常鉴别技术是访问控制技术的依据，参见 6.2.1 节。

6.2.3 不可抵赖

VPN 管理者需要提供记录来标识用户完成的 VPN 访问活动，该记录可以用来证明用户访问 VPN 的活动。

6.2.4 数据保密性

隧道是实现 VPN 的重要技术，一些 VPN 技术的隧道本身采用加密隧道，如 IPsec VPN，通过加密技术能够实现比较严格的数据在公网上传播的保密性。对于非加密的隧道技术，只要攻击者和其他用户不能对隧道路径上的节点和链路实现控制，也能够保证不同 VPN 之间以及 VPN 数据同非 VPN 数据的隔离，从而提供比较强的保密性，如 MPLS/BGP VPN。

接入链路是另外一个在 VPN 中需要考虑保密性的部分，通常也可以采用加密的方式实现保密性。

6.2.5 通信安全

必须保证 VPN 内的用户数据不被转发到 VPN 之外，同时避免非法的设备和用户拦截 VPN 的用户数据。

6.2.6 数据完整性

采用加密的隧道和接入连接本身可以实现数据的完整性或完整性检查，也可以在隧道和接入连接中实现报文的完整性检查机制。此外，专用的隧道和连接使攻击无法从外部发起，也能够提供较强的数据完整性。

6.2.7 可用性

可用性主要的威胁是拒绝服务攻击和网络的配置错误造成的服务不可用。对于拒绝服务攻击可以从两个方面考虑：

——对于来自 VPN 内部的拒绝服务攻击，可以同普通 IP 网络相同的方式来处理，参见 5.1.7 节；

——来自 VPN 外部的拒绝服务攻击往往是通过侵占 VPN 的带宽来实现，可以采用分配给 VPN 固定带宽的方法来避免带宽被侵占。

6.2.8 隐私

VPN 将 VPN 外部和内部的流量隔离开来，本身有比较强的隐私保护能力。

6.3 控制平面

VPN 控制平面控制 VPN 隧道的建立、接入连接、场所的增加和删除以及 VPN 内的路由交换等。

6.3.1 访问控制

VPN 内访问控制信息同 IP 承载网的访问控制类似，参见 5.2.1 节。

6.3.2 鉴别

对于 VPN 的控制协议，鉴别机制能够保证只有合法用户才能够对 VPN 的控制信息有访问权限，参见 5.2.2 节。

6.3.3 不可抵赖

对于 VPN 的控制数据，不可抵赖机制记录对 VPN 控制数据访问和控制数据的通信的活动，作为访问发生的证明，参见 5.2.3 节。

6.3.4 数据保密性

在 VPN 内部，控制数据的保密性同 IP 承载网上的控制数据的保密性有共同的需求和特性，参见 5.2.4 节。

对于来自 VPN 外部的威胁，VPN 内控制数据保密性同用户数据保密性有共同的需求和特性，参见 5.1.4 节。

6.3.5 通信安全

VPN 的控制数据必须只能在组成 VPN 的节点之间转发，不能被非参与 VPN 的节点获得控制数据。

6.3.6 数据完整性

在 VPN 内部，控制数据的完整性同 IP 承载网上的控制数据的完整性有共同的需求和特性，参见 5.2.6 节。

对于来自 VPN 外部的威胁，VPN 内控制数据完整性同用户数据完整性有共同的需求和特性，参见 5.1.6 节。

6.3.7 可用性

提高控制平面的可用性可以从两个方面来考虑：一方面是在公网上传输的 VPN 控制数据的可用性，另一方面是 VPN 内部的控制数据的可用性。具体到威胁和安全技术，两个方面都同 IP 承载网的安全问

题类似，可以参见 5.2.7 节。

6.3.8 隐私

公网上 VPN 外部的用户是不能够访问 VPN 内的控制数据，所以不能够获得内部用户的用户信息、位置信息、节点标识等，能够提供很强的隐私保护能力。

6.4 管理平面

本节讨论 VPN 的管理平面，考虑一般的 VPN 管理系统的安全要求同 IP 承载网的管理系统的安全需求有很大的相似性，这里主要侧重客户网络管理系统（CNM）。在运营商管理的 VPN 中，用户需要对 VPN 能够实施有限的管理活动，该管理活动有更大的安全威胁，并需要更明确的安全手段来保护网络管理系统。

6.4.1 访问控制

CNM 需要实现严格的访问控制，否则一个 VPN 用户或攻击者就可能非授权访问其他的 VPN 的 CNM，并且实施攻击和破坏活动。

CNM 的访问控制可以基于各种鉴别技术，见 6.4.2 节，根据鉴别过的身份来决定 CNM 用户能够访问的 VPN 管理信息，如配置、故障、性能、安全和计账信息。

6.4.2 鉴别

CNM 要求对访问 CNM 和 VPN 管理数据的用户实现鉴别，并将该鉴别作为访问控制的依据。鉴别技术参见 5.3.2 节。

6.4.3 不可抵赖

对于 CNM 用户的操作和管理活动，系统要能够对用户的操作进行记录，记录的内容如下：

——VPN 名称和其他标识信息；

——访问的用户；

——访问时间；

——访问对象；

——访问操作类型；

——访问结果。

该日志数据可以用于安全管理用途。

6.4.4 数据保密性

用户通常是通过未受保护的网络访问 CNM，因此对 CNM 通信要提供数据保密性保护，可以采用加密的办法来实现数据保密性。此外，也可以将 CNM 的访问通过用户自己的 VPN 来完成，这样就将来自外部的攻击隔离在 VPN 外。

6.4.5 通信安全

参见 5.3.5 节。

6.4.6 数据完整性

用户通常是通过未受保护的网络访问 CNM，因此对 CNM 通信要提供数据完整性保护，可以采用完整性鉴别来实现数据完整性。此外，也可以将 CNM 的访问通过用户自己的 VPN 来完成，这样就将来自外部的攻击隔离在 VPN 外。

6.4.7 可用性

网络管理的可用性参见 5.3.7 节。

6.4.8 隐私

用户访问 CNM 的标识信息，如访问的系统主机名和用户名，都应该被保护，防止非法用户获得用来实现对 CNM 的非法访问。

附 录 A
（资料性附录）
ITU-T X.805《端到端通信系统安全框架》介绍

ITU-T X.805 定义了一个完整的端到端通信系统的安全框架，该标准定义了三个安全层：应用层、业务层和基础设施层，并为每个网络层定义了控制、管理和用户三个平面。应用层关注为客户提供服务的基于网络的应用程序的安全性；业务层关注供应商为客户提供的各种通信服务的安全；而基础设施层由网络传输设施以及个人设备等组成，如路由器和物理链路。

ITU-T X.805 对每个层次的每个平面都分别从 8 个方面考虑其安全性：

——访问控制，保证只有授权的人员和设备才允许访问网络元素、存储的信息、信息流、业务和应用；

——鉴别，保证参与通信的实体声称的身份的有效性，并保证实体不企图伪造或以非授权的方式回放前面的通信流；

——不可抵赖，保证可提交给第三方用于证明某些事件或行为发生的证据的可用性；

——数据保密性，保证数据内容不被非授权的实体理解；

——通信安全，保证信息只在授权的端点之间流动，而不被拦截或转移；

——完整性，保证数据的正确性或精确性，非授权活动能够被检测；

——可用性，保证对网络元素、存储的信息、信息流、业务和应用的授权访问不被否决；

——隐私，保证即使通过对网络活动进行观察也不能获得有用的信息，这些信息包括地址位置、IP 地址等。

参考文献

GB 4943-2001　信息技术设备的安全

GB/T 18336.1-2001　信息技术　安全技术　信息技术安全性评估准则 第1部分：简介和一般模型

GB/T 18336.2-2001　信息技术　安全技术　信息技术安全性评估准则 第 2 部分:安全功能要求

GB/T 18336.2-2001　信息技术　安全技术　信息技术安全性评估准则 第3部分:安全保证要求

YD/T 1162.1-2001　多协议标记交换（MPLS）总体技术要求

YD/T 1162.2-2001　在 ATM 上实现 MPLS 的技术要求

YD/T 1162.3-2001　在帧中继上实现 MPLS 的技术要求

YD/T 1163-2001　IP网络安全技术要求--安全框架

YD/T 1190-2002　基于网络的虚拟IP专用网（IP-VPN）框架

YD/T 1260-2003　基于端口的虚拟局域网（VLAN）技术要求和测试方法

ITU-T X.509　信息处理系统—开放系统互连—目录：鉴别框架

ITU-T X.800　信息处理系统—开放系统互连—基本参考模型—第二部分：安全框架

IETF RFC 1352　SNMP安全协议

IETF RFC 1446　SNMPv2 安全协议

IETF RFC 1570　PPP LCP 扩展

IETF RFC 1631　IP网络地址翻译

IETF RFC 1962　PPP压缩控制协议

IETF RFC 2078　通用安全服务应用编程接口

IETF RFC 2084　Web交易安全考虑

IETF RFC 2228　FTP安全扩展

IETF RFC 2246　TLS 协议（V1.0）

IETF RFC 2401　IP 协议安全框架

IETF RFC 2402　IP 鉴别报文头

IETF RFC 2403　在 ESP 和 AH 中使用 HMAC-MD5-96

IETF RFC 2404　在 ESP 和 AH 中使用 HMAC-SHA-1-96

IETF RFC 2406　IP 封装安全载荷

IETF RFC 2408　互联网安全联盟和密钥协商协议

IETF RFC 2409　互联网密钥交换

IETF RFC 2547　BGP/MPLS VPN

IETF RFC 2616　超文本传输协议

IETF RFC 2631　Diffie-Hellman 密钥协商方法

IETF RFC 2661　二层隧道协议

IETF RFC 2663　NAT 术语和考虑

IETF RFC 2827　网络入过滤：防御地址仿冒造成的拒绝服务攻击

IETF RFC 3411　SNMP 管理框架描述

IETF RFC 3414	SNMPv3 基于用户的安全模型
IETF RFC 3415	SNMPv3 基于视图的访问控制模型

中华人民共和国
通信行业标准
承载电信级业务的IP专用网络安全框架
YD/T 1486-2006

*

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

*

开本：880×1230　1/16　　2006年8月第1版
印张：1.5　　2006年8月北京第1次印刷
字数：34千字

ISBN 7-115-1260/06-81
定价：10元
本书如有印装质量问题，请与本社联系　电话：(010)67114922