ICS 33 040 40
L 78

YD

中华人民共和国通信行业标准

YD/T 1613-2007

公众IP网络安全要求
——安全框架

Security Requirements for Public IP Network

——Security Architecture

2007-04-16 发布　　2007-10-01 实施

中华人民共和国信息产业部　发布

目　次

前　言

本标准是“公众IP网络安全”系列标准之一。该系列标准预计的结构及名称如下：

1. 公众IP网络安全要求——安全框架；
2. 公众IP网络安全要求——基于数字证书的访问控制；
3. 公众IP网络安全要求——基于远端接入用户验证服务协议（RADIUS）的访问控制；
4. 公众IP网络安全要求——基于Diameter的访问控制。

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：信息产业部电信研究院
中国电信集团公司

本标准主要起草人：马军锋　魏　亮　唐永丽　彭　俊　余英泽

公众IP网络安全要求——安全框架

1 范围

本标准规定了公众IP网络的基本安全框架；提出了基于网络自身安全、业务提供安全、信息传递安全和信息内容安全的4层安全分层模型；阐述了在控制平面、管理平面以及数据平面适用的不同安全机制。

本标准适用于公众IP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。

GB 4943-2001	信息技术设备的安全
GB/T 18336-2001	信息技术安全评估准则
YD/T 1163-2001	IP网络安全技术要求——安全框架
ITU-T X.805（2003）	端到端通信的安全体系架构
IETF RFC2401（1998）	互联网协议的安全框架

3 定义与缩略语

3.1 定义

下列定义适用于本标准。

· 访问控制 access control

防止对资源的未授权使用，包括防止以未授权方式使用某一资源。

· 可确认性 accountability

确保一个实体的行为能够被独一无二地跟踪。

· 主动威胁 active threat

这种威胁是对系统的状态进行故意的非授权的改变。

注：与安全有关的主动威胁的例子可能是：篡改消息、重发消息、插入伪消息、冒充已授权实体等。

· 鉴别 authentication

见“数据原发鉴别”与“对等实体鉴别”。

注：在本标准中，当涉及数据完整性时不使用术语“鉴别”，而另用术语“数据完整性”。

· 鉴别信息 authentication information

用以建立身份有效性的信息。

· 授权 authorization

授予权限，包括允许基于访问权的访问。

· 可用性 availability

根据授权实体的请求可被访问与使用。

· 密文 ciphertext

经加密处理而产生的数据，其语义内容是不可用的。

注：密文本身可以是加密算法的输入，这时候产生超加密输出。

· 明文 cleartext

可理解的数据，其语义内容是可用的。

· 保密性 confidentiality

这一性质使信息不泄露给非授权的个人、实体或进程，不为其所用。

· 数据完整性 data integrity

这一性质表明数据没有遭受以非授权方式所作的篡改或破坏。

· 数据原发鉴别 data origin authentication

确认接收到的数据来源是所要求的。

· 解密 decipherment

与一个可逆的加密过程相对应的反过程。

· 服务拒绝 denial of service

阻止对资源的授权访问或拖延时限操作。

· 密码学

是研究秘密通信的原理和破译密码方法的一门科学，包含密码编制学和密码分析学两方面内容。

· 数字签名 digital signature

附加在数据单元上的一些数据，或是对数据单元所作的密码变换（见“密码学”）。这种数据或变换允许数据单元的接收者用以确认数据单元来源和数据单元的完整性，并保护数据，防止被人（例如接收者）进行伪造。

· 加密 encipherment

对数据进行密码变换（见“密码学”）以产生密文。

注：加密可以是不可逆的，在这种情况下，相应的解密过程便不能实际实现了。

· 基于身份的安全策略 identity-based security policy

这种安全策略的基础是用户或用户群的身份或属性，或者是代表用户进行活动的实体以及被访问的资源或客体的身份或属性。

· 密钥 key

控制加密与解密操作的一序列符号。

· 密钥管理 key management

在一种安全策略指导下密钥的产生、存储、分配、删除、归档及应用。

· 冒充 masquerade

一个实体伪装为另一个不同的实体。

· 公证 notarization

由可信赖的第三方对数据进行登记，以便保证数据的特征如内容、原发、时间、交付等的准确性不致改变。

· 被动威胁 passive threat

这种威胁是对信息的非授权泄露，但并未改变系统状态。

· 口令 password

保密的鉴别信息，通常由一串字符组成。

· 对等实体鉴别 peer-entity authentication

确认有关的对等实体是所需的实体。

· 物理安全 physical security

为防范蓄意的和意外的威胁而对资源提供物理保护所采取的措施。

· 私密 privacy

一种个人权限，它控制和影响与这些个体有关的哪些信息可以被收集、存储以及这些信息可以被谁泄露和泄露给谁。

注：由于这一术语涉及到私人权限，不可能精确地予以限定，因此，除了作为要求安全保护的一种动机外，应避免使用。

· 抵赖 repudiation

在一次通信中涉及到的实体之一不承认参加了该通信的全部或一部分。

· 无连接完整性 Connectionless Integrity

对单份数据包是否被修改进行检查，而对数据包的到达顺序不作要求。

· 连接完整性 Connection Integrity

为连接用户提供数据完整性，检测一个完整数据包序列内任意数据的修改、插入、删除或重放。

· 基于规则的安全策略 rule-based security policy

这种安全策略的基础是强加于全体用户的总体规则。这些规则往往依赖于把被访问资源的敏感性与用户、用户群或代表用户活动的实体的相应属性进行比较。

· 安全审计 security audit

对系统的记录及活动独立的复查与检查，以便检测系统控制是否充分，确保系统控制与现行策略和操作程序保持一致、探测违背安全性的行为，并通告控制、策略和程序中所显示的任何变化。

· 安全策略 security policy

提供安全服务的一套准则（见“基于身份的安全策略”与“基于规则的安全策略”）。

注：一种完备的安全策略势必涉及超出OSI范围之外的许多事项。

· 安全服务 security service

由参与通信的开放系统的层所提供的服务，它确保该系统或数据传送具有足够的安全性。

3.2 缩略语

下列缩略语适用于本标准。

AAA	Authentication Authorization Accounting	鉴别、授权、计费
BBS	Bulletin Boards System	电子公告系统
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
CHAP	Challenge Authentication Protocol	质询认证协议
EAP	Extensible Authentication Protocol	扩展认证协议
FTP	File Transfer Protocol	文件传输协议
IKE	Internet Key Exchange	密钥交互
IP	Internet Protocol	互联网协议
MAC	Media Access Control	媒质访问控制
PAP	Password Authentication Protocol	密码认证协议
SNMP	Simple Network Management Protocol	简单网管协议

VPN	Virtual Private Network	虚拟专用网
WWW	World Wide Web	万维网

4 公众 IP 网络安全分层模型

4.1 网络安全分层模型

根据公众 IP 网络的特点，安全研究可以分成网络自身安全、业务提供安全、信息传递安全以及信息内容安全 4 个层面，如图 1 所示。图中，网络层包括各类数据转发设备，如路由器、交换机及其连接链路等，它为传送用户信息提供一个传输平台；业务提供层包括提供相关业务的网络设备，如接入认证系统、计费系统等，它为用户提供业务平台；信息传递安全则是要通过使用安全机制来保障用户有效信息在网络上的传输是安全的，主要考虑用户数据的完整性、不可否认性、机密性、可用性等特性；信息内容安全则是要从数据源来控制用户传递的信息内容，过滤不符合国家相关电信法律条文约束以及垃圾邮件、垃圾短信、病毒等内容。从该模型可以看出，网络自身安全和业务提供安全是上层用户信息传递安全的基石，只有基础传输网络是安全的，才能够保障业务层面为用户提供业务安全。

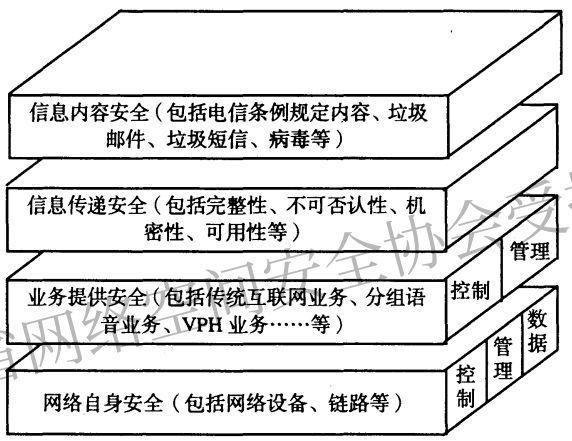

图1 公众 IP 网安全分层模型

4.2 网络自身安全

网络自身安全包括网络可靠性与生存性。网络可靠性与生存性依靠环境安全、物理安全、节点安全、链路安全、拓扑安全、系统安全等方面来保障。这里承载与业务网是拥有自己节点、链路、拓扑和控制的网络。

网络自身安全应在控制、管理和数据层面保障。在控制层面，应在控制信息访问控制、控制信息鉴别、控制信息可用性、控制信息不可抵赖、控制信息通信安全和控制信息完整性、私密性等方面保障安全。在管理层面，应在管理信息访问控制、管理信息鉴别、管理信息可用性、管理信息不可抵赖、管理信息通信安全和管理信息完整性、私密性等方面保障安全。在数据平面，应在资源可用性方面保障安全，确保授权用户不会因为网络遭受流量冲击而造成网络不可用。

4.3 业务提供安全

网络服务安全包括服务可控性与服务可用性，此外还应符合电信监管部门对电信业务的监管要求。服务可控性依靠服务接入安全、服务防否认、服务防攻击等方面来保障。服务可用性与承载业务网络的可靠性以及维护能力等相关。服务可以是网络提供的虚拟专线、话音业务、VPN业务、Internet业务等。

业务提供安全应在控制层面和管理层面保障。在控制层面，应在控制信息访问控制、控制信息鉴别、控制信息可用性、控制信息不可抵赖、控制信息通信安全和控制信息完整性、私密性等方面保障安全。在管理层面应在管理信息访问控制、管理信息鉴别、管理信息可用性、管理信息不可抵赖、管理信息通

信安全和管理信息完整性、私密性等方面保障安全。

4.4 信息传递安全

信息传递安全包括信息完整性、保密性、不可否认性和可用性。信息完整性可以依靠报文鉴别机制例如哈希算法等来保障；信息保密性可以依靠加密机制以及密钥分发等来保障；信息不可否认性可以依靠数字签名等技术来保障。

4.5 信息内容安全

信息内容安全在本标准中主要是针对有害信息的控制。有害信息主要是指传递的信息中包含中华人民共和国电信条例第五十七条所规定的内容。第五十七条规定不得利用电信网制作、复制、发布、传播含有违反国家宪法、危害国家安全，泄露国家保密，颠覆国家政权，破坏国家统一，损害国家荣誉和利益，煽动民族仇恨、民族歧视，破坏安定团结等内容。

有害信息控制是指网络应采用一定技术和管理手段防止有害信息在网络上泛滥和扩散，如垃圾邮件、BBS 不良信息、病毒、非法 IP 电话等。

5 公众 IP 网络安全

5.1 公众 IP 网络自身安全

公众 IP 网络的自身安全可以从控制、管理和数据三个层面来保障，包括网络的可靠性与生存性两个方面，依赖于公众 IP 网络的物理安全，并在此基础上应用访问控制、鉴别、信息不可抵赖、信息保密、通信安全和通信完整性等机制。

5.1.1 公众 IP 网络物理安全

公众 IP 网络的物理安全是整个通信网络系统安全的前提，它通常包括环境安全和设备安全等方面，涵盖以下内容：

——公众IP网络物理环境安全；

——公众IP网络节点设备安全；

——确公众IP网络缆线及布放安全。

5.1.1.1 公众 IP 网络物理环境安全

公众IP网络环境安全要求规范设备设施对所属环境温度、湿度、电磁、防盗、防毁等环境的要求。

公众IP网络应规范物理环境安全要求。

5.1.1.2 公众 IP 网络节点设备安全

公众IP网络节点设备安全要求规范公众IP网络上运行的局端设备的安全，如路由器、交换机、服务器等。

注释：公众IP网络节点设备的安全要求可以参考相应的设备安全标准。

5.1.1.3 公众 IP 网络缆线及布放安全

网络线缆特性是指线缆传输距离，传输质量等特性。网络线缆布放是指物理路由要求、埋放深度、管道要求等。

公众IP网络应对缆线特性以及布放原则提出要求，防止物理通路的损坏、物理通路的窃听、对物理通路的攻击（干扰等）。

5.1.2 控制平面

5.1.2.1 访问控制

访问控制是防止对资源的未授权使用，包括防止以未授权方式使用某一资源。公众IP网访问控制通常与认证一起由AAA功能实现。

公众IP网络控制平面的访问控制一般依赖于验证技术，根据验证结果来决定是否允许访问系统或者是系统根据对报文的验证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。在控制平面要确保只有授权的用户和网络设备才能够访问网络的控制信息，如路由信息。

5.1.2.2 鉴别

鉴别是保证使用服务的用户是经过授权的，未经授权的用户不能使用服务。

公众IP网络上可以采用基于端口的802.1X认证，基于端口链路层地址绑定的认证，基于用户名和口令的PAP、CHAP、EAP等网络层接入认证，基于用户名和口令的高层协议认证等方式。

认证系统服务器端可以采用RADIUS、DIAMETER等AAA协议实现。

公众IP网络控制平面的认证检查控制平面访问者（包括设备和人员）的身份，确定访问者身份的合法性，以及发送控制信息设备的身份合法性。

5.1.2.3 可用性

公众IP网络的可用性是指网络有足够的资源保证用户访问能够实施。目前对网络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。

公众IP网络可用性要求在控制平面确保网络设备能够从信任的网络实体接收控制信息，需要采取相应的措施抵御来自外部的拒绝服务攻击和路由抖动。

5.1.2.4 信息不可抵赖

信息不可抵赖性，是指使得信息发送者不可否认对信息的发送、信息接收者不可否认对信息的接收的特性。公众IP网络可以使用数字签名来提供不可抵赖性服务。

公众 IP 网络在控制平面不可抵赖要求对控制信息的使用和改变是可以追溯的，通常使用日志来保存用户和设备对网络/设备的访问信息。

5.1.2.5 信息保密

公众IP网络信息保密是指通信实体的通信内容不应当被非授权用户获得和解读。在控制平面，控制数据要避免非授权用户和攻击者获得和解读，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信息以及在网络上传输的控制信息，可以通过加密技术实现。

5.1.2.6 通信安全

确保控制数据只在两个授权的实体之间交互，不会被转移到非授权的第三方实体或者是中途截取。

5.1.2.7 数据完整性

控制平面的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以及在网络上传输的控制信息，如路由信息、DNS信息等。

5.1.2.8 私密性

保证控制平面内标识网络设备或通信链路的信息不被非授权访问者或设备获得和使用，包括 IP 地址、MAC 地址、DNS 域名等。

5.1.3 管理平面

5.1.3.1 访问控制

IP 网络管理平面的访问控制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下列方式：

——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。

访问控制要求在以上实现的管理活动中对用户和管理员进行标识，并且根据标识和验证的结果来确定用户的访问权限。访问权限包括管理员可以执行的操作，如读操作、写操作或者是读写操作，以及可以访问的对象。

5.1.3.2 鉴别

鉴别就是检查对网络设备和链路实施网络管理活动的人员或者设备的身份。鉴别可以作为访问控制的依据，通过简单的用户名、口令进行验证。

5.1.3.3 可用性

可用性就是要确保授权的用户/管理员具有对路由器、交换机和链路实现随时管理的能力，能够抵御被动攻击（如拒绝服务攻击）和主动攻击（如更改或删除管理认证信息，管理员标识和密码）。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。

5.1.3.4 信息不可抵赖

不可抵赖要求系统能够提供日志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的凭证。在公众 IP 网络中可以通过日志对用户的管理活动进行记录从而证明用户的访问行为。

5.1.3.5 信息保密

网络管理数据不应该被非授权的用户或攻击者获得和解读，这对于保持网络的安全是非常重要的一个方面。网络管理数据包括：

——被管理的路由器上存在的配置、故障、安全、性能和记账数据；

——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。

对于保存在网络设备和在网络中传输的管理数据，需要加强访问控制和验证管理来保证数据的保密性，可以结合加密技术来实现。

5.1.3.6 通信安全

在通过远程方式对网络设备和通信链路进行管理时，需要避免非授权用户和攻击者篡改管理数据。要确保管理数据流只在管理者和被管理者之间交互，不会被转移到第三方实体或者是被中途截取。

5.1.3.7 数据完整性

确保网络设备中的配置信息以及在网络中传输的管理信息不被非授权的用户或攻击者破坏和篡改。可以通过加强访问控制和验证管理，并且结合加密技术来保证数据的完整性。

5.1.3.8 私密性

私密性保证被管设备和管理系统的标识信息不被非法获得，包括 IP 地址、DNS 域名、MAC 层地址、管理员用户名和口令等。

私密性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。

5.1.4 数据平面

公众IP网络数据平面的安全特性重点在于资源的可用性方面，要确保授权用户对网络的访问不会因为网络受到攻击而中断。此外也要应用相应的访问控制策略限制用户数据访问网络，从而抑制用户的攻击数据进入网络。

5.2 公众 IP 网络业务提供安全

目前公众 IP 网络提供两类基本服务，即提供 Internet 接入所必须的基础服务（如 AAA、DHCP 和 DNS 等）和附加增值服务（如 VPN 服务）。运营商也可以依托公众 IP 网络为用户提供例如 Internet 传统业务（WWW、E-mail、FTP 等）、分组语音业务、流媒体业务等。

公众 IP 网络业务提供安全可以从控制和管理两个层面保障，包括公众 IP 网络服务可控性与服务可用性。

5.2.1 控制平面

5.2.1.1 访问控制

业务层面的访问控制要确保网络设备接收的与业务相关的控制信息来自授权的用户和设备，要避免非授权的用户监听业务控制信息。通过用户标识、口令等认证信息保证只有授权的用户能够使用该项业务。参考见5.1.2.1。

5.2.1.2 鉴别

公众IP网络业务控制平面的鉴别检查控制平面访问者（包括设备和人员）的身份，确定访问者身份的合法性，以及发送控制信息设备的身份合法性。参考见5.1.2.2。

5.2.1.3 信息不可抵赖性

公众IP网络业务开放和使用必须有一定的日志要求，即在一段时间内用户对业务的使用必须是有记录并可追查。此外也可根据此数据进行计费。参考见5.1.2.4。

5.2.1.4 信息保密

公众IP网络业务控制信息要避免非授权用户和攻击者获得和解读，特别是要避免用户业务认证信息（如用户名和口令）不被非授权用户盗取。参考见5.1.2.5。

5.2.1.5 通信安全

确保业务控制数据只在两个授权的实体之间交互，不会被转移到非授权的第三方实体或者被中途截取。

5.2.1.6 数据完整性

避免与业务相关的控制信息被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以及在网络上传输的控制信息。

5.2.2 管理平面

5.2.2.1 访问控制

业务管理平面需要实现严格的访问控制，否则一个用户或攻击者就可能非授权访问其他的业务网管，并且实施攻击和破坏活动。

5.2.2.2 鉴别

业务网管平面要求对访问业务管理数据的用户实现认证，并将该认证作为访问控制的一部分。认证技术参考5.1.2.2。

5.2.2.3 信息不可抵赖性

对于网管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，提供日志文件。

5.2.2.4 信息保密

用户通常是通过未受保护的网络访问网管系统，因此对网管系统的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。

5.2.2.5 通信安全

确保管理数据只在两个授权的实体之间交互，不会被转移到非授权的第三方实体或者被中途截取。

5.2.2.6 数据完整性

避免与业务相关的管理信息被非授权用户和攻击者篡改或者被中途截取。需要提供完整性保护的数据包括存在于网络设备上的管理信息以及在网络上传输的控制信息，如管理员标识、口令等。

5.3 公众 IP 网络信息传递安全

在公众IP网络中传递信息（主要指用户数据信息）要保证信息的完整性、保密性、不可否认性和可用性。在技术层面涵盖以下内容：加密技术、密钥管理技术、数字签名技术、完整性检查、数字证书和信息流审计等。

5.3.1 公众 IP 网络数据保密性要求

数据保密性是指信息对于未授权的个人、实体或进程是不可知、不可用的特性。公众IP网络数据保密性要求可以通过加密的手段来实现。

公众IP网络可以提供ESP等协议以及加密算法提供数据保密性服务。

公众IP网络保密性要求还与密钥管理技术相关。密钥管理分对称加密技术密钥管理机制与非对称加密技术密钥管理机制。

在公众IP网络上可以使用互联网密钥交换协议（IKE）以及证书机制等方式作密钥管理。

5.3.2 公众 IP 网络数据不可否认性要求

数据不可否认性是指使得信息发送者不可否认对信息的发送、信息接收者不可否认对信息的接收的特性。

公众IP网络可以使用数字签名、日志等来提供不可否认性服务。

5.3.3 公众 IP 网络数据完整性要求

数据完整性指接收方收到的数据与原始定义的数据严格相同，即数据不能被非授权地修改或删除，包括数据正确性、一致性和有效性。公众IP网络数据完整性包括无连接完整性与防重放攻击（部分序列完整性）。

公众IP网络可以使用AH等协议提供数据完整性服务。

5.4 公众 IP 网络信息内容安全

5.4.1 过滤要求

过滤是指通过读取源地址、目的地址、源端口、目的端口、协议、数据内容等信息来判定记录、拦截、转发等动作。

公众IP网络可以通过设置过滤系统例如防火墙等设备来实现过滤。

5.4.2 公众 IP 网信息过滤系统接入要求

公众IP网络通常需要接入信息安全主管部门的信息过滤系统。

公众IP网络应规范对外接口来接入信息过滤系统。

参 考 文 献

[1] X.800（1991） CCITT应用开放系统互连安全体系架构

[2] X.810（1996） 信息技术：开放系统互连——开放系统安全框架：概述

[3] ITU-T X.509（1997） 信息技术：开放系统互连——目录：认证框架

[4] RFC2402（1998） IP认证头协议

[5] RFC2408（1998） 互联网安全联盟和密钥管理协议

[6] RFC2409（1998） 密钥交换协议

中华人民共和国
通信行业标准

公众IP网络安全要求
——安全框架

YD/T 1613-2007

*

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　　2007年6月第1版
印张：1　　2007年6月北京第1次印刷
字数：26千字
ISBN 978-7-115-1411/07-74
定价：10元
本书如有印装质量问题，请与本社联系　电话：(010)67114922