YD

中华人民共和国通信行业标准

YD/T 1163—2001

IP 网络安全技术要求——安全框架

IP Network Security Technical Requiremente——Security Frame

2001-10-19 发布　　2001-11-01 实施

中华人民共和国信息产业部　发布

目　　次

前　　言

本标准规定基于密码技术的网络安全技术，参考RFC ，ISO/IEC 等序列标准，对分层IP网络中在不同层上的安全性进行了框架性的描述。

本标准的附录A、附录B都是提示的附录。

本标准由信息产业部电信研究院提出并归口。

本标准起草单位：信息产业部数据科学技术研究所
深圳市中兴通讯股份有限公司
信息产业部电信传输研究所
华为技术有限公司
上海贝尔有限公司

本标准主要起草人：万兆泽　易　星　聂秀英　姚　鑫　王俊文

中华人民共和国通信行业标准

IP 网络安全技术要求——安全框架

IP Network Security Technical Requirements
——Security Frame

YD/T 1163—2001

1 范围

本标准规定 IP 网安全的总技术要求，描述 IP 网安全的一个框架性结构，可作为在 IP 网上构建安全的技术性指导文件。

2 引用标准

下列标准所包含的条文，通过在本标准中引用而成为本标准的条文。本标准出版时，所示版本均为有效。所有标准都会被修订，使用本标准的各方应探讨使用下列标准最新版本的可能性。

GB/T 9387.2-1995 信息处理系统—开放系统互连—基本参考模型—第二部分：安全体系结构

ITU-T X.800(1991) | ISO/IEC 7498-2:1989 Information processing systems – Open Systems Interconnection - Basic Reference Model - Part 2：Security Architecture.

ITU-T X.509(1997) | ISO/IEC 9594-8:1997 Information technology – Open Systems Interconnection - The Directory: Authentication framework.

IETF RFC 1352 SNMP Security Protocols

IETF RFC 1446 Security Protocols for SNMPv2

IETF RFC 1570 PPP LCP Extensions

IETF RFC 1847 Security Multiparts for MIME: Multipart/Signed and Multipart/Encrypted

IETF RFC 1962 The PPP Compression Control Protocol （CCP）

IETF RFC 1968 The PPP Encryption Control Protocol (ECP)

IETF RFC 2045 MIME Part 1: Format of Internet Message Bodies

IETF RFC 2046 MIME Part 2: Media Types

IETF RFC 2047 MIME Part 3: Message Header Extensions for Non-ASCII Text

IETF RFC 2048 MIME Part 4: Registration Procedures

IETF RFC 2049 MIME Part 5: Conformance Criteria and Examples

IETF RFC 2078 Generic Security Service Application Program Interface (V2)

IETF RFC 2084 Considerations for Web Transaction Security

IETF RFC 2228 FTP Security Extensions

IETF RFC 2246 The TLS Protocol (V1.0)

IETF RFC 2315 PKCS #7：Cryptographic Message Syntax Version1.5

IETF RFC 2401 Security Architecture for the Internet Protocol

IETF RFC 2402 IP Authentication Header

IETF RFC 2403 The Use of HMAC-MD5-96 within ESP and AH

中华人民共和国信息产业部 **2001-10-19** 批准　　**2001-11-01** 实施

IETF RFC 2404	The Use of HMAC-SHA-1-96 within ESP and AH
IETF RFC 2406	IP Encapsulating Security Payload
IETF RFC 2408	Internet Security Association and Key Management Protocol
IETF RFC 2409	The Internet Key Exchange
IETF RFC 2487	SMTP Service Extension for Secure SMTP over TLS
IETF RFC 2616	Hypertext Transfer Protocol
IETF RFC 2630	Cryptographic Message Syntax
IETF RFC 2631	Diffie-Hellman Key Agreement Method
IETF RFC 2632	S/MIME Version 3 Certificate Handling
IETF RFC 2633	S/MIME Version 3 Message Specification
IETF RFC 2634	Enchanced Security Services for S/MIME
IETF RFC 2660	The Secure HyperText Transfer Protocol
IETF RFC 2661	Layer Two Tunneling Protocol "L2TP"
IETF draft	The SSL Protocol（V3.0）

3 符号与缩略语

AES	Advanced Encryption Standard	先进加密标准
AH	Authentication Header	认证头
CCP	Compression Control Protocol	压缩控制协议
DES	Data Encryption Standard	数据加密标准
ECP	Encryption Control Protocol	加密控制协议
ESP	Encapsulating Security Payload	封装安全净荷
FTP	File Transfer Protocol	文件传送协议
HTTP	HyperText Transport Protocol	超文本传输协议
ICV	Integrity Check Value	完整性检测值
IKE	Internet Key Exchange	因特网密钥交换
IP	Internet Protocol	因特网协议
IV	Initial Vector	初始向量
MD5	Message Digital (V5)	消息摘要
MAC	Message Authentication Code	消息认证码
SA	Security Association	安全关联
SAD	Security Association Database	安全关联数据库
SDU	Service Data Unit	服务数据单元
SG	Security Gateway	安全网关
SHA	Security Hash Algorithm	安全 Hash 算法
SMIB	Security Management Information Base	安全管理信息库
SMTP	Simple Mail Transfer Protocol	简单邮件传送协议
MIME	Multipurpose Internet Mail Extension	多用途因特网邮件扩展
SNMP	Simple Network Management Protocol	简单网络管理协议
SPD	Security Policy Database	安全策略数据库
SPI	Security Parameter Index	安全参数索引
SSL	Security Socket Layer	安全套接层
TCP	Transmission Control Protocol	传输控制协议
TLS	Transport Layer Security	传输层安全

UDP　User Datagram Protocol　用户数据报协议

4 基本概念与定义

下面的概念基本上来自[ISO/IEC 7498-2]或[GB/T 9387.2]。

4.1 访问控制

防止未经授权使用资源，包括防止以未经授权的方式使用资源。

4.2 授权

授予权力，包括根据访问权进行访问的权力。

4.3 路由控制

在路由选择的过程中，应用规则来选择或绕过特定的网络、链路或转接点。

4.4 密码体制

数据变换原理、手段和方法具体化的规程，用来隐藏数据的信息内容，防止数据的未发现修改和/或未授权使用。它与下列概念密切相关：

密文 — 经过密码变换后得到的数据。

明文 — 可理解的数据。

加密 — 明文数据经过密码变换变成密文数据的操作。

解密 — 密文数据经过密码变换还原成明文数据的操作。

密钥 — 控制加密与解密操作所使用的数据。

密钥管理 — 根据安全策略产生、分发、储存、使用、更换和销毁密钥。

密码分析 — 分析密码系统及其输入与输出，以导出机密变量与敏感数据，甚至明文。

4.5 主动威胁(active threat)

蓄意擅自改变系统状态。比如：修改消息、重播消息、插入假消息、冒充有权实体以及拒绝服务。

4.6 被动威胁(passive threat)

不改变系统状态擅自透露信息。

4.7 操作检测

检测数据单元是否已被修改(偶然的或有意的)的一种机制。

4.8 通信业务(traffic)分析

从观察通信业务流(有无通信业务流，通信业务流的量、方向和频率)推断信息。

4.9 安全审计

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，并介绍控制、策略和程序中所显示的任何变化。

4.10 安全审计事件

为了便于进行安全审计而收集的数据。

4.11 数字签名

附在数据单元后面的数据，或对数据单元进行密码变换得到的数据，允许数据的接收者证明数据的来源和完整性，保护数据不被伪造。

4.12 认证信息

用来鉴定实体所声称的身份是否有效的信息。

4.13 认证

通过信息交换鉴定一个实体身份的机制。

4.14 凭证

用来证明实体所声称的身份而传送的数据。

4.15 否认

参与通信的实体否认参加了全部或部分的通信过程。

4.16 公证

委托可信任的第三方对数据进行登记注册，使他能够保证该数据特征如内容、源、时间和传递的精确性。

4.17 冒充

一个实体伪装成别的实体。

4.18 可追溯性

保证实体的行为可以追溯到唯一的实体。

4.19 可用性

根据需要，信息允许有权实体访问和使用的特性。

4.20 机密性

信息对非授权个人、实体或进程是不可知、不可用的特性。

4.21 通信业务填充

生成假通信实例、假数据单元或在数据单元中生成假数据。

4.22 密码校检值

对数据单元进行密码变换(见密码体制)导出的数据。校检值是密钥和数据单元的一个数学变换的结果，通常被用来检查数据单元的完整性。

4.23 数据完整性

数据免遭非法更改或破坏的特性。

4.24 物理安全

保护资源免遭蓄意性和偶然性威胁所使用的措施。

4.25 安全标签

挂在资源(数据单元)上的标签，指定或指出该资源的安全属性。

4.26 安全服务

由通信的系统提供的，对系统或数据传递提供充分的安全保障的一种服务。

4.27 安全策略

提供安全服务所使用的一套准则。包含两个基本概念：

基于规则的安全策略　以全局规则对所有用户均有效为基础的安全策略。规则通常依赖于被访问资源的敏感性与用户(群)或代理具有的对应属性间的比较。

基于身份的安全策略　以用户的身份为基础的安全策略。规则通常依赖于访问资源的用户身份的特权或能力，或者依赖于存取控制表。

4.28 安全级别

所选择安全服务的保护质量，本文件主要指不选择安全保护、选择认证保护、选择机密性保护、选择认证保护和机密性保护 4 种。

4.29 选择域保护

为要发送的消息的特定字段提供保护。

4.30 敏感性

资源的一种特性，表示资源的价值或重要性，可能包括资源受攻击的脆弱性。

4.31 服务拒绝

阻止授权访问资源或延迟时间敏感操作。

4.32 防重放

防止对传送数据的重放攻击。

5 IP 网基本模型

5.1 TCP/IP 协议族

TCP/IP 协议族是在 TCP(传输控制协议)和 IP(互联网协议)两个重要协议的基础上形成的协议族(详细情况请参阅对应的协议)。TCP/IP 协议族基于分层的原则，每层都明确定义功能和用途，各层功能相对独立。相邻层间都由协议准确定义边界接口，通过接口通信。

IP 网的链路层间传送帧数据，网络层间传送 IP 数据，传输层间传送 TCP/UDP 数据，应用层间传送应用数据。

TCP/IP 协议族涉及许多协议，在下面的几节中我们仅介绍一些用得较多、同时也是本标准第 7 章将要涉及的协议，它们在分层模型中的关系大致如图 1 所示。

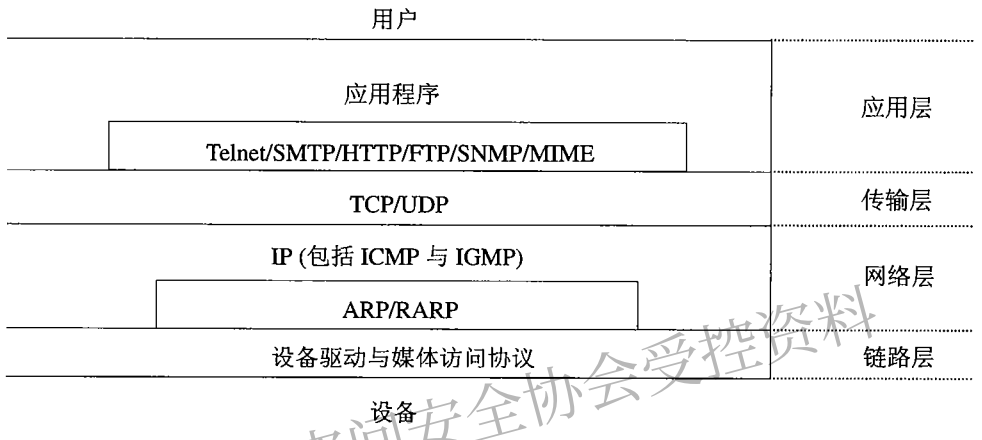

图 1 TCP/IP 协议族在分层模型中的关系

5.2 链路层

链路层负责在物理介质中传送数据，数据的传送是在两个物理连接的设备间进行，处理与本地组网相关的一些问题。链路层协议主要有以太网（IEEE 802.3）、令牌总线（IEEE 802.4）、令牌环（IEEE 802.5）、光纤分布数据接口（FDDI）以及像串行线路 IP（SLIP）和点对点协议（PPP）等。

5.3 网络层

网络层以 IP 协议为标志，提供基于 IP 地址的、不可靠的、尽最大能力的、面向无连接的数据传送服务。网络层协议还包括 ICMP(Internet Control Message Protocol)，IGMP(Internet Group Management Protocol)，ARP(Address Resolution Protocol)，RARP(Reverse Address Resolution Protocol)等。

IP 协议是网络层的也是 IP 网的主要协议，它指定了通过 IP 网络传送的所有数据的格式，它执行路由功能以选择数据传送的路径，它包含一系列规则使不可靠的包传递具体化，这些规则说明主机和路由器应该怎样处理包，怎样产生、什么时候产生错误消息，在什么条件下可以丢掉包等。

5.4 传输层

传输层以 UDP/TCP 协议为标志，允许具有相同 IP 地址的不同机器独立地接收和发送数据。

UDP 通常被认为是 IP 的简单扩展，在两机器间提供基于端口以及 IP 地址的、不可靠的、尽最大能力的、面向无连接的数据传送服务。UDP 使用 IP 传送消息，但增加了在主机中区分不同源及目的端口的能力。

TCP 基于客户与服务器的方式，通过利用 IP，在两机器间提供基于端点以及 IP 地址的、可靠的、面向连接的数据传送服务。与 UDP 一样，TCP 使用 IP 传送消息，但增加了在主机中区分不同源、目的端口的能力；TCP 还为数据传送的可靠性定义了一些规则。

5.5 应用层

应用层直接为 IP 网应用提供服务，涉及许多应用协议，常用的主要有 TELNET，FTP，SMTP，HTTP，SNMP 等。

TELNET 建立在 TCP 上，支持用户远程登录。它提供三类基本服务。第一，TELNET 定义网络虚拟终端，为远端系统提供标准界面；第二，TELNET 具有允许服务器与客户端协商选项的机制，并提供可选项的标准集；第三，TELNET 对称地处理连接的两端。

FTP 建立在 TCP 上，提供对文件交互式的访问，并且能够指定文件格式和进行认证控制。

SMTP 建立在 TCP 上，后台邮件传送处理由用户代理完成。SMTP 处理首先利用域名系统把目的地机器名称映射到 IP 地址，然后与目的地机器的邮件服务器建立 TCP 连接。如果连接成功，则服务器传递邮件，否则终止连接。MIME 提供了允许使用 SMTP 传送任意数据的机制。

HTTP 即超文本传送协议，建立在 TCP 之上。HTTP 是构建 WWW 的主要协议。

SNMP 建立在 UDP 上，用于网络管理，允许从网管服务器监视和控制运行网管代理(Agent)的路由器或主机。

6 安全服务与安全机制

6.1 概述

本章介绍适合本规范的安全服务与实现这些服务的机制。下述的安全服务是基本的安全服务，这些安全服务在本规范参考模型的框架内有选择地提供。在实际应用中，它们通常与其它服务和机制相结合使用以满足安全策略和/或用户的要求。

本章介绍的安全机制是基本的安全机制。有些安全机制作为实现基本安全服务的组成部分，这里称为主要安全机制。系统可以直接调用实现基本安全服务的特殊组合。有些安全机制可适用于多种服务，它们的某一部分可以看成密钥管理的某些方面，这里称为辅助安全机制，其重要性通常直接与所要求的安全等级有关。

这些基本定义来自[ISO/IEC 7498-2]或[GB/T 9387.2]。

6.2 安全服务

6.2.1 认证

认证为通信实体和数据源提供认证服务。认证服务要求有本地存储的认证信息和为认证而传递的数据。主要有：

- 实体认证： 当选择该服务时，服务向实体保证，通信的对方与所声称的实体相符。
- 数据源认证：当选择该证服务时，服务向实体保证，某数据的来源与所声称的实体相符。

6.2.2 数据机密性

选择数据机密性服务防止数据的非授权泄露。数据机密性有以下几种情形：

- 连接机密性： 为连接的所有用户数据提供机密性；
- 无连接机密性： 为单个无连接-SDU 中的所有用户数据提供机密性；
- 选择域机密性： 为连接或单个无连接-SDU 中的所有用户数据中的选择字段提供机密性；
- 业务流机密性： 为可能从对业务流的观测结果中得到的信息提供机密性。

6.2.3 数据完整性

数据完整性服务用来对抗主动威胁，有以下几种情形：

- 有恢复连接完整性： 为连接的所有用户数据提供完整性；并检测一个完整 SDU 序列内任意数据的修改、插入、删除或重放，有恢复企图。
- 无恢复连接完整性： 为连接的所有用户数据提供完整性；并检测一个完整 SDU 序列内任意数据的修改、插入、删除或重放，无恢复企图。
- 选择域连接完整性： 为在连接上传送的-SDU 的用户数据中的选择字段提供完整性；并采用确定选择字段是否已被修改、插入、删除或重放的方式。

- 无连接完整性：当在某层提供此服务时，为上一层实体请求的完整性提供保证。本服务为单个无连接 SDU 提供完整性，并采用可确定所收到的 SDU 是否已被修改的方式。另外也可对重放提供有限的检测。
- 选择域无连接完整性：为单个无连接 SDU 中的选择字段提供完整性，并采用确定选择字段是否已被修改的方式。

若在建立连接时使用实体认证服务，并在该连接生存期间使用数据完整性服务，可共同为在该连接上传送的所有数据提供数据源认证，为这些数据的完整性提供保证；同时可以使用如序列号的方式为数据的重放提供检测。

6.2.4 抗抵赖性

抗抵赖性服务可以采用如下两种方式：

- 有源端证据的抗抵赖性：数据的源端证据被提供给数据接收者。这将防止发送者否认发送过该数据或数据内容。
- 有交付证据的抗抵赖性：数据的交付证据被提供给数据发送者。这将防止接收者否认接收到该数据或数据内容。

6.2.5 访问控制

此服务防止非授权使用资源。可用于控制对一个资源的多种访问形式(通信资源的使用，信息资源的读、写或删除，资源处理的执行)或对一个资源的所有访问。

6.3 安全机制

6.3.1 主要安全机制

6.3.1.1 加密机制

加密机制利用加密算法，为数据或通信业务流信息提供机密性。存在加密机制意味着存在密钥管理机制。

6.3.1.2 数字签名机制

数字签名机制包括两个进程：对某一个数据单元进行签名和对数据单元的签名进行验证。

签名进程使用签名者的专用信息(如私钥)，包括对数据单元进行加密或生成数据单元的密码校检值。

验证进程使用公开信息(如公钥)，来确定数据的签名是否是用签名者的专用信息产生的签名。由这些公开信息导不出签名者的专用信息。

签名机制的本质特征是签名只能由签名者的专用信息产生。因此，签名一旦经过验证，任何时候都能够向第三方(法官或仲裁者)证明。只有专用信息的唯一持有者才能产生此签名。

6.3.1.3 访问控制机制

访问控制机制通过实体的经认证的身份、信息或权限确定和实施实体的访问权。拒绝实体的非授权访问或者不正当方式访问，并且可以报告这些事件，以产生报警和/或记录作为安全审计数据的一部分。

访问控制机制可以基于下列一项或多项的使用：

- 存放实体访问权的访问控制信息库。这些信息可以由权威中心或被访问的实体保存，并且以访问控制表或分级式或分布式的形式保存。这需要预先通过实体认证。
- 认证信息，如口令，拥有并出具这样的信息以确定访问实体的授权。
- 权限，拥有并出具这样的信息以确定访问此实体或由此权限界定的资源的权力。
- 安全标签，通常根据安全策略，当安全标签与一个实体相关联时可以用来接收或拒绝访问。
- 访问的时间。
- 访问的路由。
- 访问持续时间。

访问控制机制可用于通信相关的任一端和/或任一中间点。在源端或中间点的访问控制机制用来确定发方是否被授权与接收方通信或使用所要求的资源。无连接审计传输的目的端要求的对等级访问控制机制必须先在源端给出，并录入安全管理信息库。

6.3.1.4 数据完整性机制

数据完整性包括两个方面：单个数据单元或域的完整性；数据单元或域的一个流的完整性。

确定单个数据单元的完整性包括发送实体和接收实体两个进程，发送实体给数据单元附上一个分量，这个分量是数据单元本身的函数。附加分量可以是补充信息，如分组校检码或密码校检值，并且本身可能已被加密。接收实体产生相应的附加分量，并与所收到的附加分量进行比较，以确定数据在传输中是否已被改变。此机制本身不对单个数据进行防重放保护。在适当的结构层，操作的检测可能导致该层或更高层采用恢复措施(如重发或纠错)。

对于连接数据传输，为了保护数据单元序列的完整性(如防止数据序列错乱、丢失、重发、插入或改变)，需要附加某种明排序，如序列号、时戳或密码链。

对于无连接数据传输，时戳可以用来对个别数据单元提供有限形式的防重放保护。

6.3.1.5 认证机制

认证机制可以采用如下技术：

- 使用认证信息，如由发送实体提供口令，并由接收实体验证口令；
- 密码技术；
- 使用实体的某些特性和/或控制。

为了提供对等实体认证服务，可将认证机制设在对应层。若该机制认证某实体失败，则将导致拒绝建立连接或终止连接，并且可能导致该实体数据成为安全审计数据和/或向安全管理中心报告。

当使用密码技术时，可同时使用“握手”协议，以免遭重放。

选择认证技术，可根据其应用环境与下列技术联合使用：

- 时戳和同步时钟；
- 双方和三方握手；
- 由数字签名机制和/或公证机制实现的抗抵赖服务。

6.3.1.6 通信业务填充机制

通信业务填充机制可用来提供不同级别的防通信业务分析保护。该机制仅在通信业务填充得到机密性服务保护时才有效。

6.3.1.7 路由控制机制

可以通过动态方式或预置方式安排路由，仅使用物理安全的子网、中继网或链路。当端系统检测到持续的操作攻击时，将指示网络服务提供者通过别的路由建立连接。

通过安全策略的约束，带某种安全标签的数据可能被禁止通过某些子网、中继网或链路。另外，连接的发起者(或无连接数据单元的发送者)，可以指定路由，以避免通过特定的子网、中继网或链路。

6.3.1.8 公证机制

两个或多个实体间通信数据的属性，如完整性、源端、时间和目的端，均可通过公证机制得到保证。这保证由第三方公证人提供，公证人得到实体的信任，并掌握能够以可证明的方式提供所要求的保证的所需信息。根据公证人提供的服务，每个通信实例可以使用数字签名、加密或完整性机制。当引入公证机制时，数据通过受保护的通信实例和公证人在通信实体间交流。

6.3.2 辅助安全机制

6.3.2.1 信任功能

信任功能必须用来扩充其他安全机制的范围或建立其有效性。任何直接提供安全机制的功能、或提供访问安全机制的功能应该是可信赖的。

用来保证信任的规程可用硬件或软件实现，不属于本文件的范围，并且在任何情况下均随察觉威胁的程度和被保护信息的价值而不同。这些规程通常是昂贵的，并且难实现，通过选择允许模块化实现安全功能的结构，能够减少这些困难；这种模块化的安全功能能够与非安全功能分离，并能够由非安全功能提供。

在受保护层的的上层，任何关联的保护必须由其他手段提供，如适合的信任功能。

6.3.2.2 安全标签

包括数据内容的资源可以用安全标签与其相关联，安全标签必须安全绑在与之相关联的数据上，与数据一起传送，并且易于识别，以指示资源的敏感性级别。

6.3.2.3 事件检测

安全相关的事件检测包括明显违反安全措施事件的检测，也可能包括如成功访问(或登陆)等“正常”事件的检测。事件的构成由“事件处理的管理(第 9 章)”负责说明。对不同的安全相关的事件检测可能导致一项或多项行动：

- 事件的本地报告；
- 事件的远程报告；
- 记录事件；
- 恢复行动。

这样的安全相关事件有：

- 特殊的安全违章；
- 特殊选择的事件；
- 发生事件计数的溢出。

这方面的标准将考虑事件报告和事件记录相关信息的传输，以及这种传输要规定的语法和语义。

6.3.2.4 安全审计跟踪

安全审计跟踪是一个有价值的安全机制，通过安全审计可以检测和考察安全的违章行为。安全审计是对系统记录与活动情况进行的独立回顾与检查，以检测系统控制的充分性，确保操作规程与建立的策略相一致，帮助评估损失，并在控制、策略和规程中推荐应做的改变。安全审计要求在安全审计跟踪中记录安全相关信息，分析这些信息并生成报告。对安全相关信息的记录被视为安全机制，在这里描述；而对这些信息进行分析并生成报告则被视为安全管理功能。

安全审计跟踪所收集的信息可以根据所记录的安全相关事件进行分类(如明显的安全违章或成功操作的完成)，以适应不同的要求。了解安全审计跟踪的存在可以防止某些潜在的安全攻击。

系统的安全审计跟踪将考虑什么信息应该被可选地记录，在什么条件下信息应该被记录，以及用来交换安全审计跟踪信息的语法和语义定义。

6.3.2.5 安全恢复

安全恢复机制用来处理诸如来自事件处理和管理功能方面的机制的请求，并采用一套规则来完成恢复行为。恢复行为有：

- 立即恢复行为：立即终止操作，如拆线；
- 临时恢复行为：会导致某一实体的暂时失效；
- 长期恢复行为：可能把某一实体列入“黑名单”或改变密钥。

恢复行为和安全恢复管理的细节将在相应的文件中描述。

6.3.2.6 安全服务与主要安全机制的关系

哪些机制在单独或与其他机制组合使用时，适合提供哪一个服务，表 1 中列出了它们之间的关系，但这些关系并不是限定性的。

表 1　安全服务与主要安全机制的关系

机制 / 服务	加密	数字签名	访问控制	完整性	认证	业务填充	路由控制	公证
对等实体认证	Y	Y	•	•	Y	•	•	•
数据源认证	Y	Y	•	•	•	•	•	•
访问控制	•	•	Y	•	•	•	•	•
连接机密性	Y	•	•	•	•	•	Y	•
无连接机密性	Y	•	•	•	•	•	Y	•
选择域机密性	Y	•	•	•	•	•	•	•
业务流机密性	Y	•	•	•	•	Y	Y	•
有恢复连接完整性	Y	•	•	Y	•	•	•	•
无恢复连接完整性	Y	•	•	Y	•	•	•	•
选择域连接完整性	Y	•	•	Y	•	•	•	•
无连接完整性	Y	Y	•	Y	•	•	•	•
选择域无连接完整性	Y	Y	•	Y	•	•	•	•
有源端证据抗否认性	•	Y	•	Y	•	•	•	Y
有交付证据抗否认性	•	Y	•	Y	•	•	•	Y

说明：

• 表示对该安全服务使用该安全机制是不适合的；

Y　表示无论对该安全服务单独使用或与其他安全机制组合使用该安全机制是适合的。

7　IP 网安全体系结构

7.1　安全服务、安全机制与模型分层的关系

7.1.1　分层安全原则

在各层提供安全服务并配置相应的安全机制，遵循如下原则：

- 应极小化达到安全服务目标可供选择的方法和数目；
- 通过在多于一层上提供安全服务来建立安全系统是可接受的；
- 安全所需的附加功能不应当不必要地重复现有的系统互连功能；
- 避免破坏各层的独立性；
- 应极小化信任功能的数目；
- 如实体与下层实体提供的安全机制有关，则中间层的构建应使破坏安全是不可行的；
- 只要有可能，为某层定义的附加安全功能不应排除作为自含模块实现；
- 应适用于包含所有层功能的系统。

为了满足某层对安全服务的请求，无论安全服务是由该层还是下层提供，必要时可对该层安全服务的定义进行修正。

7.1.2　分层安全服务的使用

在连接通信的情形，保护服务通常是在建立连接时申请/批准的。在调用无连接通信的情形，保护服务是申请无连接服务时申请/批准的。

本安全体系结构能够容纳各种不同的安全策略，包括基于规则的安全策略和基于身份的安全策略或基于两者的混合策略，以及主管部门强制的保护策略。保护服务必须遵守并优先实施主管部门强制的

保护策略。

7.1.3 安全服务、安全机制与模型分层关系

表 2 给出了安全服务与适合提供此服务的参考模型的层之间的关系(其中“ Y” 表示应将该服务列入相应层作为提供服务的可选项，“ • ” 表示在相应层不提供该服务)。

表 2 安全服务与参考模型的层之间的关系

服　　务	链路层	网络层	传输层	应用层
对等实体认证	•	Y	Y	Y
数据源认证	•	Y	Y	Y
访问控制服务	•	Y	Y	Y
连接机密性	Y	Y	Y	Y
无连接机密性	•	Y	Y	Y
选择域机密性	•	•	•	Y
业务流机密性	Y	Y	•	Y
有恢复连接完整性	•	•	Y	Y
无恢复连接完整性	•	Y	Y	Y
选择域连接完整性	•	•	•	Y
无连接完整性	•	Y	Y	Y
选择域无连接完整性	•	•	•	Y
有源端证据抗否认性	•	•	•	Y
有交付证据抗否认性	•	•	•	Y

安全服务均由相应的安全机制提供：

- 对等实体认证：　通过适当的组合由密码导出的或受保护的认证交换，受保护的口令交换与签名机制提供；
- 数据源认证：　通过加密机制或签名机制提供；
- 访问控制服务：　通过适当的使用特殊的访问控制机制提供；
- 机密性：　通过通信业务填充机制，和/或加密机制，和/或路由控制机制提供；
- 完整性：　通过数据完整性机制，有时也与加密机制协同提供；
- 抗否认性：　通过适当的组合数据完整性机制，签名机制和公证机制提供；

7.2 链路层安全技术要求

链路层安全的设计基于密码技术，提供点到点的安全性，提供的安全服务主要为机密性。链路层协议根据连接的方式可以分为两类：点到点连接与端到端连接。采用端到端方式的链路层协议均采用虚电路的方式来实现，虚电路具有与点到点链路相同的安全性。

链路层协议不应对物理层的安全性做任何假设，二层隧道协议如 L2TP(Layer Two Tunneling Protocol)等也提供有关的安全性，但对于链路层来说是作为物理层而存在的。

链路层安全技术将由相应的文件详细规范，这里主要简单描述 PPP 协议的安全性与 L2TP 的安全性(尽管严格来说 L2TP 是隧道协议)。

7.2.1 PPP 安全技术

PPP(The Point-to-Point Protocol)协议是目前唯一一个能提供身份认证、加密、压缩等安全服务的链路层协议，也是使用最广泛的链路层协议。

7.2.1.1 身份认证

PPP 安全所涉及的身份认证协议主要有 PAP(PPP Authentication Protocol)、CHAP(PPP Challenge Handshake Authentication Protocol)协议：

使用 PAP 作为认证协议时，所传送的用户名、口令为明文的；而 CHAP 基于“挑战-响应”（Chanllenge-Response）机制，每次传送的验证数据均不一样，减少了由于窃听而导致的口令失密的可能。

PPP 可以采用本地数据库对用户进行认证，也可以通过 AAA(Authentication Authorization Accounting protocols)协议（如 RADIUS(Remote Authentication Dial In User Service)），采用 AAA 数据库对用户进行验证。AAA 不直接与用户交互，PPP 负责将 PAP 或 CHAP 等协议所获得的用户名及口令等信息交给 AAA 协议进行验证。AAA 协议的实现也需要考虑安全性，保证用户名、口令的安全传输。

安全的链路层协议必须保证用户名、口令不明文传输，推荐采用 CHAP 机制实现。

7.2.1.2 PPP 加密控制协议

链路层提供提供的机密性服务由 ECP(The PPP Encryption Control Protocol)协议来完成。

通过 ECP 协议，PPP 在链路建立完成时，可以在通信的两点之间协商合适的加密算法，对数据进行加密。有关处理细节的规范，参考[RFC 1968]。

这里，ECP 本身的协商是不受保护的，ECP 协议也没有关于密钥管理的描述，这使得 ECP 协议的安全性存在漏洞。

安全的链路层协议在数据加密上必须提供安全的协商机制以及安全的密钥管理机制，比如可以与 CA 相结合等。具体的协议实现超出了本标准的范围。

7.2.1.3 PPP 压缩控制协议

数据压缩一方面可以减小报文的长度，使得在加密时所耗费的时间减少；另一方面通过压缩减少了报文中的冗余信息，压缩后的报文再加密更难被破解。数据压缩由 CCP(The PPP Compression Control Protocol)协议来完成。

通过 CCP 协议，PPP 在链路建立完成时，可以在通信的两点之间协商合适的压缩算法，对数据进行压缩。有关处理细节的规范，参考[RFC 1962]。

数据压缩对于的链路层安全是可选的。如果选择数据压缩和机密性服务，则必须先进行数据压缩，然后再进行加密。

7.2.1.4 回呼技术

回呼（CallBack）技术，最初由客户端发起呼叫，要求服务器端向本端回呼；而服务器端接受呼叫，并决定是否向客户端发起回呼。

利用回呼技术可增强安全性。回呼处理中，服务器端根据本端配置的呼叫号码呼叫客户端，从而可避免因用户名、口令失密而导致的不安全性。另外，服务器端还可根据本端的配置，对呼入请求进行分类，即拒绝呼叫、接收呼叫（不回呼）或接收回呼，从而可以对不同的客户端实施不同的限制，并且服务器端在外部呼入时可以实现资源访问的主动性。具体的规定参考[RFC 1570]。

建议安全的链路层协议支持回呼技术。

7.2.2 二层隧道协议 L2TP

二层隧道协议 L2TP[RFC 2661]将网络层数据包封装在 PPP 帧中，可以通过 IP、X.25、FR 和 ATM 网络中任一类具有二层点到点串行链路的网络进行传送。

L2TP 有两类信道：控制信道和数据信道。通过控制信道中可靠传送的一系列控制消息，完成隧道及呼叫的建立、维护与拆除。通过数据信道中不可靠传送的一系列数据消息，完成传送隧道中的 PPP 封装的数据信息。

L2TP 协议具有以下功能：

- 同时适用于客户到网关和网关到网关两类应用；
- 支持多种网络层协议；

- 支持多种用户认证协议；
- 支持 IP 地址动态分配；
- 支持对隧道的认证。

7.2.2.1 L2TP 协议结构

L2TP 消息有控制消息与数据消息两种类型。控制消息用来建立、保持、清除隧道与调用，数据消息用来封装在隧道中传送的 PPP 帧。控制消息利用 L2TP 中的可靠控制信道确保传递。L2TP 协议结构见表 3(详细描述见[RFC 2661])。

表 3 L2TP 协议结构

PPP 帧	
L2TP 数据消息	L2TP 控制消息
L2TP 数据信道(不可靠)	L2TP 控制信道(可靠)
包传输 (UDP, FR, ATM, 等)	

7.2.2.2 L2TP 头格式

L2TP 控制信道与数据信道的包具有共同的头格式，需要注意的是长度、Ns、Nr 对数据消息是可选的，但对控制消息是必须的。包头组成如表 4 所示。

表 4 包头组成

T|L|x|x|S|x|O|P|x|x|x|x| Ver	长度 (可选)
隧道 ID	会话 ID
Ns (可选)	Nr (可选)
偏移量 (可选)	偏移填充... (可选)

其中

T：指示消息类型，0 为数据消息，1 为控制消息；

L：指示长度域的存在，0 表示不存在，1 表示存在；

x：保留值；

S：指示 Ns 与 Nr 域的存在，0 表示不存在，1 表示存在；

O：指示偏移量域的存在，0 表示不存在，1 表示存在；

P：指示数据的处理方式；

Ver：为 2，指示 L2TP。

有关 T、L、S、O、P 以及其他域的作用与详细描述参考[RFC 2661]。

7.2.2.3 控制消息类型

L2TP 定义了如下 4 类控制消息，详细的描述参考[RFC 2661]。

控制连接管理消息

0 (保留值)

1 (SCCRQ) Start-Control-Connection-Request

2 (SCCRP) Start-Control-Connection-Reply

3 (SCCCN) Start-Control-Connection-Connected

4 (StopCCN) Stop-Control-Connection-Notification

5 (保留值)

6 (HELLO) Hello

调用管理消息

7 (OCRQ) Outgoing-Call-Request
8 (OCRP) Outgoing-Call-Reply
9 (OCCN) Outgoing-Call-Connected
10 (ICRQ) Incoming-Call-Request
11 (ICRP) Incoming-Call-Reply
12 (ICCN) Incoming-Call-Connected
13 (保留值)
14 (CDN) Call-Disconnect-Notify
错误报告消息
15 (WEN) WAN-Error-Notify
PPP 会话控制消息
16 (SLI) Set-Link-Info

7.2.2.4 控制连接协议

控制连接消息用来建立、保持、清除 L2TP 隧道。用 L2TP 为 PPP 会话建立隧道有两部分组成：为隧道建立控制连接，为激活入调用与出调用请求建立会话。隧道与相应的控制连接必须在发起入调用与出调用前建立，L2TP 会话必须在 L2TP 能够开始用隧道传送 PPP 帧之前建立。

L2TP 的控制连接协议对隧道的建立、保持、认证与清除进行了详细规定[RFC 1661]。

7.3 互联网络层安全技术要求

互联网络层安全体系结构(后面将称为 IPsec)的设计是为 IP 层环境提供可互操作的、高效的和基于密码技术的安全性。提供的安全服务包括访问控制、无连接完整性、数据来源认证、防重放保护(部分序列完整性的一种形式)、机密性(加密)和有限的业务流机密性。这些服务在 IP 层提供时，为 IP 层或者更高层协议提供保护。这些目标是通过使用两个业务安全协议—IP 认证头(AH)和 IP 封装安全净荷(ESP)，以及通过使用加密的密钥管理程序与协议来达到。当这些安全机制得到正确的执行和配置时，对那些不采用这种安全机制保护他们的业务的用户、主机和其他的因特网组机组件不会产生负面的影响。这些安全机制的设计与算法是独立的，这种模块性设计允许选择不同的算法集而不影响其他方面的实现。指定作为缺省值的算法集是为了全球因特网容易互通。

这部分仅从整体上描述 IPsec 的组成部分以及在 IP 环境下这些部分怎样相互适应，描述 IP 安全协议所提供的安全服务和在 IP 环境下怎样完成这些安全服务。IPsec 的详细结构将会由相应的文件说明，因而在此节不涉及。在相应的文件未出前可参考[RFC 2401]，[RFC 2402]，[RFC 2406]，[RFC 2408]，[RFC 2409]等。

下面将对 IPsec 基本组成部分分别进行描述。

7.3.1 安全协议

7.3.1.1 认证头(AH)

AH 被用来为 IP 数据报提供无连接完整性和数据来源认证(以后简称“认证”)，并提供防重放保护。AH 可以单独使用，也可以与 ESP 组合使用，或利用隧道模式的嵌套方式(见下节“安全关联”)。安全服务可以在正在通信的主机之间提供，可以在正在通信的安全网关之间提供，或者可以在主机与安全网关之间提供。有关 AH 及其组成的详细描述以及在不同的网络环境怎样使用 AH，参考[RFC 2402]。

7.3.1.1.1 认证头格式

认证头(AH)由下一头，净荷长度，保留值，安全参数索引(SPI)，序列号域，认证数据(可变)6 个域组成，格式见表 5。

这些域都是强制性的，总是在 AH 格式里出现，并且包括在完整性检测值(ICV)的计算中。

7.3.1.1.2 认证头(AH)处理

AH 可以用传输模式或隧道模式两种方法引入。在传输模式，AH 被插入在 IP 头之后，在上层协议(如 TCP, UDP, ICMP 等)之前，或在任意已经插入的 IPsec 头之前。在隧道模式，AH 保护整个内 IP 包，

包括整个内 IP 头。隧道模式中 AH 的位置，相对于外 IP 头，与在传输模式中 AH 的位置一样。

表 5　认证头格式

下一头	净荷长度	保留值
安全参数索引(SPI)		
序列号域		
认证数据(可变)		

引入 ICV 计算的认证算法由安全关联 SA 指定，适合的认证算法包括基于对称算法或单向 HASH 函数(如 MD5 或 SHA-1)的带密钥的消息认证码(MACs)。

出界包处理将依次经过查找安全关联、产生序列号、计算 ICV 和分段 4 个相继的过程。对应地，入界包处理将依次经过重组、查找安全关联、验证序列号和验证 ICV4 个相继的过程。

如果不存在有效的安全关联，接收方必须丢弃此包，这是可审计事件。如果计算的 ICV 与收到的 ICV 匹配，则数据报有效并接受；如果检测失败，则接收方必须视收到的 IP 数据报为无效而丢弃，检测失败是可审计事件。

适合的 AH 实现必须支持下面强制实现算法：

- 用 MD5 的 HMAC，参阅[RFC 2403]；
- 用 SHA-1 的 HMAC，参阅[RFC 2404]。

7.3.1.2　封装安全净荷(ESP)

在 IP 环境里，封装安全净荷 ESP 是设计来提供混合安全服务的，ESP 为 IP 数据报提供安全服务有机密性，数据来源认证，无连接完整性，防重放保护(部分序列完整性的一种形式)，和有限的通信业务流机密性。ESP 可以单独使用，也可以与 IP 认证头(AH)组合使用，或者通过使用隧道模式以嵌套方式使用(见下节“安全关联”)。安全服务可以在一对正在通信的主机之间提供，可以在正在通信的安全网关之间提供，或者可以在主机与安全网关之间提供。有关 ESP 及其组成的详细描述以及在不同的网络环境怎样使用 ESP，参考[RFC 2406]。

ESP 头是插在 IP 头后，在高层协议头(传输模式)或封装的 IP 头(隧道模式)前。

7.3.1.2.1　封装安全净荷包格式

封装安全净荷 ESP 包由安全参数索引、序列号、净荷数据(可变)、填充(0-255 字节)、填充长度、下一头和认证数据(可变)共 7 个域组成。格式见表 6。

表 6　封装安全净荷包格式

安全参数索引		
序列号		
净荷数据(可变)		
填充(0-255 字节)	填充长度	下一头
认证数据(可变)		

这些域中填充域和认证数据域是“可选性的”域，其它的域都是“强制性的” 域。“可选性的”表示此域如果没有被选，则没有此域出现，是否选取是作为安全关联(SA)定义的一部分；“强制性的”表示此域总是在 ESP 格式里出现。

7.3.1.2.2　封装安全协议处理

ESP 可以用传输模式或隧道模式两种方法引入。在传输模式，ESP 被插入在 IP 头之后，在上层协议(如 TCP, UDP, ICMP 等)之前，或在任意已经插入的 IPsec 头之前。隧道模式 ESP 可以用在主机或安

全网关。在隧道模式，ESP 保护整个内 IP 包，包括整个内 IP 头。隧道模式中 ESP 的位置，相对于外 IP 头，与在传输模式中 ESP 的位置一样。

引入的加密算法由 SA 指定，ESP 是为使用对称加密算法设计的，由于加密(机密性)是可选的，此算法可以是“NULL”。引人 ICV 计算的认证算法由 SA 指定，适合的认证算法包括基于对称算法(如 AES)或单向 HASH 函数(如 MD5 或 SHA-1)的带密钥的消息认证码(MACs)。由于认证是可选的，此算法可以是 “NULL”。但是加密算法与认证算法不能同时都为 “NULL”。

出界包处理将依次经过查找 SA、包加密、产生序列号、计算完整性检测值和分段 5 个过程。相应地，入界包处理将依次经过重组、查找 SA、验证序列号、验证完整性检测值和包解密 5 个过程。

如果不存在有效的 SA，接收方必须丢弃此包，这是可审计事件。如果计算的 ICV 与收到的 ICV 匹配，则数据报有效并接受。如果检测失败，则接收方必须视收到的 IP 数据报为无效而丢弃。检测失败是可审计事件。

适合的 ESP 实现必须支持下面强制实现算法：

- CBC 模式的 AES(即 Rijndael)；
- 用 MD5 的 HMAC，参阅[RFC 2403]；
- 用 SHA-1 的 HMAC，参阅[RFC 2404]；
- NULL 认证算法(即不使用认证算法)；
- NULL 加密算法(即不使用加密算法)。

7.3.2 安全关联

安全关联(SA)是两个或多个实体间的关系，描述实体怎样利用安全服务安全地通信。这关系通过一个信息集表现出来，能够当作实体间的一种约定。信息必须得到所有实体的认同和分享，安全通信才有可能。SA 是 IPsec 中的基本概念，AH 和 ESP 都利用 SA，因特网密钥交换协议 IKE 中的大多数功能函数是建立和保持 SA。为 IP 安全指定的 SA 属性包括(但不限于)认证机制、密码算法、算法模式、密钥长度和初始向量(IV)。提供算法和机制独立安全性的其它协议必须定义它们对 SA 属性的要求。

这部分描述 IP 环境下 SA 的概念。有关 SA 的协商、建立、改变与删除以及使用的详细规范将由相应的文件描述。

7.3.2.1 定义与范围

SA 由安全参数索引(SPI)、IP 目的地址和安全协议(AH 或 ESP)标识符三元组唯一确定，通过单独使用 AH 或 ESP(两者不能同时使用)，为由它传送的业务提供安全服务。如果 AH 和 ESP 保护都用在一个业务流中，则会产生两个或多个 SA 对此业务流提供保护。两主机之间或两安全网关之间典型的双向通信要求两个 SA(每个方向一个)。

为 IP 环境定义了传输模式 SA 和隧道模式 SA 两种类型。传输模式 SA 是两主机间的一个安全关联。在 IPv4 环境下，传输模式安全协议头立即出现在基 IP 头和任何选项的后面，并且在任意高层协议(如 TCP 和 UDP)的前面。在 Ipv6 环境下，安全协议头立即出现在基 IP 头和扩展后面，但可在目的地选项的前面或后面，并且在任意高层协议的前面。对于 ESP 的情形，传输模式 SA 仅为这些高层协议提供安全服务，并不为在 ESP 头前的 IP 头或任意扩展头提供安全保护。对于 AH 的情形，这种保护延伸到了 IP 头的选择部分、扩展头的选择部分和选择的选项。详细情形在相应的文件中规范 [RFC 2402]。

在 IP 隧道中应用 SA 时必须用隧道模式 SA。任何时候安全关联只要有一端是安全网关则 SA 必须是隧道模式。对于隧道模式 SA，存在一个“外部的” IP 头，说明 IPsec 处理目的地址。“内部的” IP 头说明包的最终目的地址。安全协议头出现在外部 IP 头后、内部 IP 头前。如果在隧道模式中引入 AH，则外部 IP 的一些部分会得到象隧道的 IP 包一样的保护(即所有内部 IP 头和高层协议都得到保护)。如果在隧道模式中引入 ESP，则只对隧道包提供保护，并不对外部的 IP 头提供保护。

7.3.2.2 安全关联功能

由 SA 提供的安全服务取决于所选的安全协议、SA 的模式、SA 的端点和在协议内可选服务的选择。AH 在接收方判断时也提供防重放(部分序列完整性)服务，帮助防止拒绝服务攻击。当不要求机密性时(或

不允许，如官方在加密方面的限制)，引用 AH 协议时适当的。AH 也为 IP 头的所选部分提供认证，在某些情形下这可能是必需的。

ESP 随意地对业务提供机密性，ESP 也可随意地提供认证。如果为 ESP_SA 协商认证，接收器也可选择强制防重放服务(与 AH 的防重放服务具有相同的特征)。由 ESP 提供的认证范围比 AH 提供的小，即并不对 ESP 头“外面的”IP 头提供保护。若仅上层协议需要认证，则 ESP 认证是恰当的选择，且空间比用 AH 封装 ESP 更有效。需要注意的是，这里机密性与认证尽管都是选项，但不能同时都省略，至少必选其一。

如果选择机密性服务，则两安全网关间隧道模式的 ESP SA 能提供部分的业务流机密性。用隧道模式允许加密内部 IP 头，隐藏最终的业务源地址与目的地址身份。此外，ESP 净荷填充也能用来掩饰包的大小，进一步隐藏业务的表面特征。 当移动用户在拨号环境下被分配一个动态 IP 地址，并与公司的防火墙(起安全网关作用)建立一个隧道模式的 ESP SA 时，可以提供类似的业务流机密性服务。需要注意的是，对于业务分析，分段精细的 SA 比分段粗糙的 SA 更脆弱。

7.3.2.3 组合安全关联

在单个 SA 之上传送的 IP 数据报，仅能由一个安全协议提供保护，或者 AH，或者 ESP ，不能两个都用。有时安全策略会为用单个 SA 不能完成的特殊业务流要求 SA 组合服务，因而必须为所要求的安全策略的实现引入多重 SA。术语“安全关联捆绑”或“SA 捆绑”是指一个 SA 序列，必须通过这些 SA 对业务进行满足安全策略的处理。 序列的顺序由策略定义。

安全关联可用传输邻接和迭代隧道两种方法组合成捆绑(这两种方法也能组合，如一个 SA 捆绑可以由一个隧道模式 SA 与一个或两个传输模式 SA 构成，呈序列使用)。

传输邻接是指不调用隧道，对同一个数据报使用多个安全协议。这方法组合 AH 和 ESP 允许仅一级的组合，这种情形，AH 出现在 ESP 前，用于 ESP 输出的密文。

迭代隧道是指多层安全协议的应用是通过 IP 隧道来实现的。由于每个隧道在 IPsec 路径上可以起始于或终止于不同的站点，这种方法允许多重级别的嵌套，并且允许 AH 与 ESP 的任意使用顺序。迭代隧道有 3 种基本情形：

- SA 的两个端点都相同——内部和外部隧道都可以或者是 AH 或者是 ESP;
- SA 的一个端点相同——内部和外部隧道都可以或者是 AH 或者是 ESP;
- SA 的两个端点都不相同——内部和外部隧道都可以或者是 AH 或者是 ESP。

7.3.2.4 安全关联数据库

这部分描述与安全关联相关的处理 IP 通信业务的一般模型，支持互通性和功能性。IPsec 实现的外部行为必需与此模式可见的外部特征可对应。

此模型有两个极小的数据库：安全策略数据库(SPD)和安全关联数据库(SAD)。前者详细说明确定所有主机，安全网关，BITS 或 BITW IPsec 实现的出界、入界的部署策略。后者包含与每个(激活)安全关联相关的参数。这部分也定义选择器，一些 IP 层和更高层协议的域值，安全策略数据库把业务映射到策略时要使用它们。

有关数据库与选择器的详细规范将由相应的文件提供，参考[RFC 2401]。

7.3.2.4.1 选择器

为了 SA 管理容易控制 SA 分段，必需支持下面的选择器参数：IP 目的地址 ，IP 源地址，名称(有用户 ID 与 系统名称)，数据敏感性级别，传输层协议，源和目的(如 TCP/UDP)端口。怎样使用选择器由 IPsec 实现环境确定。

7.3.2.4.2 安全策略数据库(SPD)

安全关联是 IPsec 环境下用来执行安全策略的一个管理构想。SA 处理本质元素是所依赖的 SPD，这个 SPD 详细说明以何种方式对 IPsec 数据提供何种服务。这部分指定了所有的 IPsec 实现都必须支持的 SPD 元素的一个标准集，允许用户或系统管理员管理 SPD。

SPD 必需在处理所有通信业务(入界和出界)时协商，包括非 IPsec 通信业务。发送方使用这种 IPsec

保护则此 IPsec 保护必需在接收方出现。对于任意的出界或入界数据包，可选择 3 种处理方式：丢弃、绕过 Ipsec 和使用 IPsec。第一种选择是指通信业务不允许离开主机、通过安全网关或传送给某个应用。第二种选择是指通信业务允许不采取 IPsec 保护通过。第三种选择是指对通信业务提供 IPsec 保护，对这种通信业务，SPD 必须详细说明所提供的安全服务、引用的协议和使用的算法等。

SPD 包含一个有序的策略条目表，每个条目包含这样的指示：与此策略匹配的通信业务是否绕过 IPsec 处理、丢弃或进行 IPsec 处理，如果进行 IPsec 处理，则条目包括一个 SA(或 SA 捆绑)的详细说明，IPsec 协议表列，模式和所引入的算法，包括任意的嵌套要求。每个策略条目由一个或多个选择器控制，选择器定义由这个策略条目包含的 IP 通信业务集合。

安全策略可能要求对某特定的通信业务集合——有固有的顺序，使用多个 SA，出现这种情形时，SPD 中的策略条目必须保持这些顺序要求。SPD 被用来控制所有通过 IPsec 系统的通信业务流，在 SPD 中必须明确说明安全关联与密钥管理通信业务，否则它将被丢弃。相关的详细描述与实现过程参考[RFC 2401]、[RFC 2408]。

7.3.2.4.3 安全关联数据库(SAD)

每个 IPsec 实现都有一个名义上的安全关联数据库，在此库里，每个条目定义与一个 SA 相关联的参数。每个 SA 在 SAD 中有一个条目。对于出界处理，SPD 中的条目指向这些条目；如果一个 SPD 当前并不指向适合此包的 SA，则实现产生一个适合的 SA(或 SA 捆绑)，并把 SPD 条目连接到 SAD 条目。对于入界处理，SAD 中的每个条目由 IP 目的地址、IP 协议类型和 SPI 索引；这三元组在入界处理时被用来查找 SAD 中的 SA，这些域对所有的应用都要求。

上面定义的每个选择器，SAD 中的 SA 条目必须包含在 SA 产生时所协商的值。对于发送方，这些值用来决定给定的 SA 是否适合于一个出界包。对于接收方，这些值用来检查一个入界包中选择器值与 SA 中的选择器值的匹配。对于同一个 ESP SA，加密算法或认证算法可能是“NULL”，但不能同时为“NULL”。

在进行 IPsec 处理时要用下面的 SAD 域：

- 序列号计数器 — 所有实现都要求，但仅在出界通信业务使用；
- 序列计数器溢出 — 所有实现都要求，但仅在出界通信业务使用；
- 防重放窗口 — 所有实现都要求，但仅在出界通信业务使用；
- AH 认证算法、密钥等 — AH 实现要求；
- ESP 加密算法、密钥、IV 模式、IV 等 — ESP 实现要求；
- ESP 认证算法、密钥等 — ESP 实现要求；
- 安全关联的寿命 — 所有实现都要求；
- IPsec 协议模式 — 主机实现必须支持所有模式，网关实现必须支持隧道模式；
- 路径 MTU (Maximum Transfer Unit) — 所有实现都要求，但仅在出界通信业务使用。

7.3.2.5 安全关联的基本组合

这部分描述适应的 IPsec 主机和安全网关必须支持的 4 种安全关联的组合情形：

- 情形 1：提供两主机间端对端的安全性；
- 情形 2：支持简单专用虚拟网；
- 情形 3：情形 1 与情形 2 的组合，在发送主机和接收主机间加了端对端的安全性；
- 情形 4：远端主机利用因特网到达某机构的防火墙，然后获准访问一些服务器或其它机器。

适应的实现必须能够产生这 4 种组合，并且收到处理它们，但应该能够接收和处理任意的组合。其详细规范将由相应的文件给出，也可参考[RFC 2401]。

7.3.3 密钥管理

密钥管理技术包括密钥的产生、认证、交换、存储、使用、销毁等方面，Ipsec 实现要求支持人工的与自动的 SA 和秘密密钥管理。 这部分描述对两种 SA 管理类型的极小要求，有关密钥管理的详细规范由相关文件描述。

7.3.3.1 人工技术

管理最简单的形式是人工管理，由人用密钥材料和与其它系统安全通信相关的安全关联管理数据手工地配置每个系统。人工管理技术在静态小环境适用，通常使用静态配置对称密钥。

7.3.3.2 自动技术

大范围的 Ipsec 应用要求自动的 SA/密钥管理协议，为了互通，使用 IPsec 选择的自动的密钥管理协议必须支持缺省值 — 因特网密钥管理协议(IKE)[RFC 2409]，同时可以引用自动的 SA/密钥管理协议。

自动的 SA/密钥管理协议的输出应该可以用来产生多重密钥，以满足加密算法使用多重密钥、认证算法使用多重密钥或同时引用加密算法和认证算法使用多重密钥的需要。

密钥管理系统可以为每个密钥提供不同的比特串，或者产生一个比特串，所需的串从这里摘录。如果提供单个比特串，则必须小心，保证系统的部分在 SA 的两端以相同的方式把摘录的串映射到所要求的密钥。为了保证在 SA 的每端 IPsec 实现对相同的密钥使用相同的比特串，并且与把比特串分成单个的密钥的系统部分无关，加密密钥必须来自第一个(最左边的，高阶的)比特串，认证密钥必须来自剩下的比特串。每个密钥的比特数在相关算法中定义。在多重加密密钥或多重认证密钥情形下，算法的详细说明必须指定从提供给算法的单个比特串中选取密钥的顺序。

7.4 传输层安全技术要求

传输层安全技术的设计是为 TCP/UDP 环境提供可互操作的、高效的和基于密码技术的安全性。提供的安全服务包括访问控制、完整性、数据来源认证、防重放保护(部分序列完整性的一种形式)、机密性(加密)和有限的通信业务流机密性。这些服务都是在传输层提供，为传输层或者更高层协议提供保护。这些目标是通过使用两个安全协议—TLS 与 SSL 来达到。当这些安全机制得到正确的执行和配置时，对那些不采用这种安全机制保护他们的通信业务的用户、主机和其他的因特网组机组件不会产生负面的影响。这些安全机制的设计与算法是独立的，这种模块性设计允许选择不同的算法集合而不影响其他方面的实现。指定作为缺省值的算法集是为了全球因特网容易互通。

这部分仅从整体上描述传输层安全技术的组成部分以及在 TCP/UDP 环境下这些部分怎样相互适应，描述 TCP/UDP 安全协议所提供的安全服务和在 TCP/UDP 环境下怎样完成这些安全服务。传输层安全技术的详细结构将会由相应的文件规定，因而在此节不涉及。在相应的文件未出前可参考[RFC 2246]，[SSL]等。

下面将对传输层安全技术：UDP 安全、TCP 安全以及安全套接层分别进行描述。

7.4.1 UDP 安全技术

UDP 是面向无连接的传输协议，通常作为 IP 的一个简单扩展。UDP 安全技术将考虑端口到端口间的基于密码技术的安全性，提供的安全服务包括访问控制、完整性、机密性、数据来源认证和防重放保护，设计目标应考虑密码安全性、互操作性、可扩展性和有效性，这些将在下一版本中讨论，这里由调用 IPsec 提供。

7.4.2 TCP 安全技术(TLS)

TLS 为两实体间的通信应用提供面向连接的安全性，其设计对应用层透明，以基于客户/服务器的方式，利用密码技术，为应用通信提供防窃听、防篡改和防消息伪造服务。通信双方对发送的消息数据进行分组、压缩、使用 MAC 和加密，对接收到的消息数据进行解密、验证、解压和重组。TLS 的设计目标，按照它们的优先级为：

1. 密码安全性： 两用户间可用 TLS 建立安全连接。
2. 互操作性： 独立的程序员在相互不知道对方编码的情况下，能够利用 TLS 开发能够成功地交换密码参数的应用。
3. 可扩展性： TLS 提供的框架支持新的公钥密码算法和新的对称密码算法。
4. 相对有效性： TLS 充分考虑了降低密码算法计算方面的花消和减少网络活动。

TLS 由两层结构——处于相对低层的 TLS 记录协议与处于相对高层的 TLS 握手协议组成。TLS 记

录协议用于封装不同的高层协议，TLS 协议允许客户与服务器在应用协议处理数据之前进行相互认证，协商加密算法和密钥。

7.4.2.1 TLS 记录协议

TLS 记录协议位于可靠的传输协议(如 TCP)之上，用来封装不同的高层协议(如 TLS 握手协议)，它提供的面向连接的安全性具有两个基本性质：

- 连接是秘密的：对称密码用于数据加密，基于别的协议(如 TLS 握手协议) 为每一连接秘密协商唯一的密钥。
- 连接是可靠的：消息传输包括利用安全 Hash 函数产生的带密钥的 MAC。

7.4.2.1.1 连接状态

TLS 连接状态是 TLS 记录协议的操作环境，它指出所引用的压缩算法、加密算法和 MAC 算法，以及这些算法所需的参数。逻辑上，存在四种显著的连接状态：当前读、写状态和即将读、写状态。所有的记录都是当前在读、写状态进行处理，即将读、写状态的安全参数由 TLS 握手协议设置。握手协议能够选择地使即将读或写状态成为当前状态，同时使对应的当前状态成为即将状态并被初始化为空状态。

使没有进行安全参数初始化的即将状态成为当前状态是非法的，初始当前状态总被设置为不使用加密、压缩与 MAC 算法。

TLS 连接状态的安全参数由下列值设置：

- 连接端：　　说明实体是“客户”还是“服务器”。
- 加密算法：　　说明加密所用的算法，包括算法的密钥长度，分组算法包括分组大小。
- MAC 算法：　　说明用于消息认证的算法，包括 HASH 输出的大小。
- 压缩算法：　　说明用于数据压缩的算法，包括必须的所有信息。
- 主秘密：　　连接实体间的共享秘密。
- 客户随机数：　　客户方提供的随机数。
- 服务器随机数：　　服务器方提供的随机数。

记录层将用这些安全参数产生下列值：

- 客户写 MAC 秘密
- 服务器写 MAC 秘密
- 客户写密钥
- 服务器写密钥
- 客户写 IV (分组密码)
- 服务器写 IV (分组密码)

客户写参数用于服务器接收和处理记录，服务器写参数用于客户接收和处理记录，计算这些参数的算法将在 7.4.2.1.3 描述。

一旦生产了密钥和设置了安全参数，连接状态即可被初始化成为当前状态。对每个记录处理，连接状态必须更新。连接状态包括下列元素：

- 压缩状态：　压缩算法的当前状态。
- 密码状态：　加密算法的当前状态，包括所有必须的信息。
- MAC 秘密：　上面为此连接产生的 MAC 秘密。
- 序列号：　　每个连接状态都包含一个序列号，并且是读、写分离的。

7.4.2.1.2 记录层

记录层从高层接收未解释的任意长度的非空数据块，对其进行分块、压缩与解压、净荷保护处理。具体的计算与处理过程将在后续的相应标准文件中描述，也可参考[RFC 2246]。

7.4.2.1.3 密钥计算

记录层需要从握手协议提供的安全参数产生密钥、IV 和 MAC 秘密。主秘密被 Hash 成足够长的、

安全的字节序列——密钥块，然后密钥块被指派给当前连接状态的 MAC 秘密、密钥和非输出的 IV。密码说明(CipherSpecs)需要客户写 MAC 秘密、服务器写 MAC 秘密、客户写密钥、服务器写密钥、客户写 IV 和服务器写 IV，这些都是由主秘密产生的密钥块按照固定的顺序产生。当产生密钥和 MAC 秘密时，主秘密是作为熵源，随机数为可输出密码提供不加密的材料与 IV。其中 IV 仅在分组密码的情形产生，可输出 IV 与不可输出 IV 的产生也不相同。密钥块中不用的部分将被丢掉。具体的计算与产生过程将在后续的相应标准文件中描述，也可参考[RFC 2246]。

7.4.2.2 TLS 握手协议

TLS 握手协议允许服务器与客户相互认证，并在应用协议发送或接收数据前协商加密算法和密钥，它提供的面向连接的安全性具有 3 个基本性质：

— 实体的身份可以通过公钥(或非对称)密码认证。

— 共享秘密的协商是安全的：窃听者得不到协商的秘密，并且对任意认证的连接，即使是能把自己置于连接中间的攻击者也得不到秘密。

— 协商是可靠的：通信双方能够检测到任何试图改变协商通信的攻击者。

TLS 握手协议由下面的改变密码说明协议、报警协议和握手协议组协议族成，它允许实体为记录层取得一致的安全参数，进行相互认证、协商安全参数和报告错误条件。握手协议负责协商由下列项组成的会话：

— 会话标识符：由服务器选取的标识会话状态的字节序列。

— 实体证书：实体的(X509v3 [X509])证书，可以为 NULL。

— 压缩方法：加密前压缩数据的算法。

— 密码说明：指定加密算法和 MAC 算法，也定义密码属性，如 Hash 值的输出长度。

— 主秘密：客户与服务器之间的 48 字节共享秘密。

— 可恢复标志：一个会话是否能够用来发起新的连接的标志。

7.4.2.2.1 改变密码说明协议

此协议由一条消息组成，这条消息由一个值为 1 的字节构成，在当前状态下被加密和压缩。改变密码说明消息可由客户或服务器发送，通告接收方后面的记录将被新协商的密码说明和密钥保护。接收方受到此消息后，立即指示记录层把即将读状态变成当前读状态，发送方发送此消息后，应立即指示记录层把即将写状态变成当前写状态。

7.4.2.2.2 警报协议

警报消息传达消息的严重性并描述警报。致命级的警报信息导致立即终止连接。与其它消息一样，警报消息在当前状态下被加密和压缩。警报消息有：

— 结束通告消息
— 意外消息
— 坏记录 MAC 消息
— 解密失败消息
— 记录液出消息
— 解压失败消息
— 握手失败消息
— 坏证书消息
— 不支持的证书消息
— 证书撤回消息
— 证书期满消息
— 证书未知消息
— 非法参数消息
— 未知 CA 消息
— 访问拒绝消息
— 解码错误消息
— 解密错误消息
— 输出限制消息
— 协议版本消息
— 不够安全消息
— 内部错误消息
— 用户取消消息
— 不重新协商消息

警报消息的详细描述与处理，参考[RFC 2246]。

7.4.2.2.3 握手协议

TLS 握手协议在 TLS 记录协议上面执行操作，产生会话状态所需的密码参数。当 TLS 客户和服务器要开始通信时，它们确认协议版本，选择密码算法，可选地相互认证，并利用公钥加密技术产生共享秘密。

TLS 握手协议包括下列步骤：

— 交换 HELLO 消息，以确认算法、交换随机值并为重开会话进行检测。
— 交换必要的密码参数，使客户与服务器确认预主秘密。
— 交换证书和密码信息，使客户和服务器相互认证。
— 从预主秘密和交换的随机值计算主秘密。
— 向记录层提供安全参数。
— 允许客户和服务器验证它们的对等实体已经计算出相同的安全参数，确认握手是在没有攻击者篡改的情况下发生。

完全握手的消息流交换过程如下：

```
客户                                              服务器

客户 HELLO              ---------->
                                                  服务器 HELLO
                                                  证书*
                                                  服务器密钥交换*
                                                  证书请求*
                        <----------               服务器 HELLO 完成
证书*
客户密钥交换*
证书验证*
[改变密码说明]
结束                    ---------->
                                                  [改变密码说明]
                        <----------               结束
应用数据                <---------->              应用数据
```

注： * 表示本条消息并不总是被发送，[]表示本条消息实际上不是握手消息。

如果客户和服务器决定恢复前一个会话或者重复一个已经存在的会话，则可省掉不必要的握手消息，采取如下的握手过程：

```
客户                                              服务器

客户 HELLO              -------->
                                                  服务器 HELLO
                                                  [改变密码说明]
                        <--------                 结束
[改变密码说明]
结束                    -------->
应用数据                <------->                 应用数据
```

握手过程与交换消息的详细描述，以及具体的、密码相关的操作处理过程的详细描述，将在后续的相应标准文件中介绍，也可参阅[RFC 2246]。

7.4.2.3 密钥管理

TLS 通信双方所需的密钥由主秘密按照一定方法计算，主秘密是通过共享预主秘密和通信双方交

换的随机值计算。共享预主秘密采用公钥技术获得。

7.4.3 安全套接层(SSL)

SSL 位于 TCP 之上，为两实体间的通信应用提供面向连接的安全性，其设计对应用层透明，以基于客户/服务器的方式，利用密码技术，为应用通信提供防窃听、防篡改和防消息伪造服务。通信双方对发送的消息数据进行分组、压缩、使用 MAC 和加密，对接收到的消息数据进行解密、验证、解压和重组。SSL 的设计目标，按照它们的优先级为：

1．密码安全性：　两用户间可用 SSL 建立安全连接。

2．互操作性：　独立的程序员在相互不知道对方编码的情况下，能够利用 SSL 开发能够成功地交换密码参数的应用。

3．可扩展性：　SSL 提供的框架支持新的公钥密码算法和新的对称密码算法。

4．相对有效性：　SSL 充分考虑了降低密码算法计算方面的花消和减少网络活动。

SSL 由两层结构——处于相对低层的 SSL 记录协议与处于相对高层的 SSL 握手协议组成。SSL 记录协议用于封装不同的高层协议，SSL 协议允许客户与服务器在应用协议处理数据之前进行相互认证，协商加密算法和密钥。SSL 它提供的面向连接的安全性具有 3 个基本性质：

— 连接是秘密的：在初始握手定义秘密密钥后，用对称密码加密数据。

— 实体的身份能够用公钥密码进行认证。

— 连接是可靠的：消息传输包括利用安全 Hash 函数产生的带密钥的 MAC。。

7.4.3.1 会话与连接状态

SSL 会话是状态化的，SSL 握手协议负责协调这些状态。逻辑上，存在当前操作状态和即将操作状态，又分别划分为读与写状态。所有的记录都是当前在读、写状态进行处理，即将读、写状态的安全参数由 SSL 握手协议设置。握手协议能够选择地使即将读或写状态成为当前状态，同时使对应的当前状态成为即将状态并被初始化为空状态。

SSL 会话状态包括下列元素：

— 会话标识符：　由服务器选取的标识会话状态的字节序列。

— 实体证书：　实体的(X509v3 [X509])证书，可以为 NULL。

— 压缩方法：　加密前压缩数据的算法。

— 密码说明：　指定加密算法和 MAC 算法，也定义密码属性，如 Hash 值的输出长度。

— 主秘密：　客户与服务器之间的 48 字节共享秘密。

— 可恢复标志：　一个会话是否能够用来发起新的连接的标志。

SSL 连接状态包括下列元素：

— 服务器与客户随机数：　客户方与服务器方提供的随机数。

— 服务器写 MAC 秘密：　服务器写数据时用于对数据进行 MAC 操作的秘密。

— 客户写 MAC 秘密：　客户写数据时用于对数据进行 MAC 操作的秘密。

— 服务器写密钥：　服务器加密数据、客户解密数据的密钥。

— 客户写密钥：　客户加密数据、服务器解密数据的密钥。

— 初始向量：　进行 CBC 模式加密时使用的数据。

— 序列号：　每个连接状态都包含一个序列号，并且是读、写分离的。

这些元素的详细说明与处理，参阅[IETF SSL]。

7.4.3.2 记录层

记录层从高层接收未解释的任意长度的非空数据块，对其进行分块、压缩与解压、净荷保护处理。具体的计算与处理过程将在后续的相应标准文件中描述，也可参考[ITEF SSL]。

7.4.3.3 改变密码说明协议

此协议由一条消息组成，这条消息由一个值为 1 的字节构成，在当前状态下被加密和压缩。改变密码说明消息可由客户或服务器发送，通告接收方后面的记录将被新协商的密码说明和密钥保护。接收

方受到此消息后，立即指示记录层把即将读状态变成当前读状态，发送方发送此消息后，应立即指示记录层把即将写状态变成当前写状态。

7.4.3.4 警报协议

警报消息传达消息的严重性并描述警报。致命级的警报信息导致立即终止连接。与其它消息一样，警报消息在当前状态下被加密和压缩。警报消息有：

- 关闭通告消息
- 意外消息
- 坏记录 MAC 消息
- 解压失败消息
- 握手失败消息
- 无证书消息
- 坏证书消息
- 不支持的证书消息
- 证书撤回消息
- 证书期满消息
- 证书未知消息
- 非法参数消息

警报消息的详细描述与处理，参考[IETF SSL]。

7.4.3.5 SSL 握手协议

SSL 握手协议允许实体为记录层取得一致的安全参数，进行相互认证、协商安全参数和报告错误条件。SSL 握手协议在 SSL 记录层上面执行操作，产生会话状态所需的密码参数。当 SSL 客户和服务器要开始通信时，它们确认协议版本，选择密码算法，可选地相互认证，并利用公钥加密技术产生共享秘密。

SSL 握手协议包括下列步骤：

- 交换 HELLO 消息，以确认算法、交换随机值并为重开会话进行检测。
- 交换必要的密码参数，使客户与服务器确认预主秘密。
- 交换证书和密码信息，使客户和服务器相互认证。
- 从预主秘密和交换的随机值计算主秘密。
- 向记录层提供安全参数。
- 允许客户和服务器验证它们的对等实体已经计算出相同的安全参数，确认握手是在没有攻击者篡改的情况下发生。

完全握手的消息流交换过程如下：

```
客户                                              服务器

客户 HELLO              ---------->
                                                  服务器 HELLO
                                                  证书*
                                                  服务器密钥交换*
                        <----------               证书请求*
证书*
客户密钥交换*
证书验证*
[改变密码说明]
结束                    ---------->
                                                  [改变密码说明]
                        <----------               结束
  应用数据              <---------->              应用数据
```

注： * 表示本条消息并不总是被发送，[]表示本条消息实际上不是握手消息。

如果客户和服务器决定恢复前一个会话或者重复一个已经存在的会话，则可省掉不必要的握手消息，采取如下的握手过程：

客户		服务器
客户 HELLO	-------->	
		服务器 HELLO
		[改变密码说明]
	<--------	结束
[改变密码说明]		
结束	-------->	
应用数据	<------->	应用数据

握手过程与交换消息的详细描述，以及具体的、密码相关的操作处理过程的详细描述，将在后续的相应标准文件中介绍，也可参阅[ITEF SSL]。

7.4.3.6 密钥管理

SSL 通信双方所需的密钥由主秘密按照一定方法计算，主秘密是通过共享预主秘密和通信双方交换的随机值计算。共享预主秘密采用公钥技术获得。

7.5 应用层安全技术要求

应用层安全技术的设计是为不同的应用环境提供可互操作的、高效的和基于密码技术的安全性。提供的安全服务包括访问控制、完整性、实体与数据源认证、机密性和抗抵赖性。这些服务都是在应用层提供，为应用层协议提供保护。这些不同目标是通过使用不同安全协议来达到。当这些安全机制得到正确的执行和配置时，对那些不采用这种安全机制保护的用户、主机和其他的因特网组机组件不会产生负面的影响。这些安全机制的设计与算法是独立的，这种模块性设计允许选择不同的算法集合而不影响其他方面的实现。

这部分仅从整体上描述应用层安全技术的组成部分以及在相应的环境下这些部分怎样相互适应，描述相应的安全协议所提供的安全服务和在相应的环境下怎样完成这些安全服务。应用层安全技术的详细结构将会由相应的文件规定，因而在此节不涉及。

7.5.1 HTTP 安全技术(SHTTP)

这一节描述超文本传输协议的安全要求，在 HTTP[RFC 2616]上提供机密性、完整性、认证、抗抵赖性等安全服务，这些安全服务都是可选的[RFC 2660]。

SHTTP 在 HTTP 客户与服务器之间提供安全的通信机制，支持可选的不同操作模式、密钥管理机制、信任模型、密码算法与封装格式，允许交易双方进行选项协商，以满足不同的应用需求。SHTTP 具有如下特征：

- SHTTP 是面向消息的安全通信协议，其设计基于 HTTP 的消息模式，很容易与 HTTP 应用集成；
- SHTTP 提供多种安全机制，为大量、可能的应用提供了适合的安全服务选项；
- SHTTP 支持唯对称密钥操作模式；
- SHTTP 支持端到端的安全交易；
- SHTTP 支持协商密码算法、模式与参数。

7.5.1.1 消息处理模型与操作模式

SHTTP 消息处理模型包括消息产生与消息恢复。消息产生是通过明文消息、收方的密码选项与密钥材料、发方的密码选项与密钥材料产生 SHTTP 消息；消息恢复是通过 SHTTP 消息、收方说明的密码选项与密钥材料、收方当前的密码选项与密钥材料、发方预先说明的密码选项产生明文消息。

SHTTP 对消息提供的保护操作模式为签名、认证、加密以及它们的任意组合，并提供了基于公钥密码的密钥交换机制与基于对称密码的密钥交换机制。

消息的详细处理请看[RFC 2660]。

7.5.1.2 消息格式

SHTTP 消息格式的构成与 HTTP 的消息格式相同，由请求行、状态行、消息头与消息内容组成，不过 SHTTP 消息格式使用了安全标志，对内容进行了密码处理，并且提供了不同的封装格式选项。有关 SHTTP 消息头的详细组成与处理细节，以及 SHTTP 消息的处理细节请看[RFC 2660]。

7.5.1.3 密码参数

进行 SHTTP 消息的安全处理需要双方确认所用的密码参数，这些密码参数包括加密算法、认证算法、MAC 算法、密钥材料、工作模式等，SHTTP 提供有效的协商机制，对密码参数的协商语法和格式进行了明确规定[RFC 2660]。

7.5.2 SMTP 安全技术

这一节描述 SMTP 服务的扩展，允许 SMTP 服务器与客户利用 TLS 在互联网上提供秘密、认证的通信。这使 SMTP 客户有能力保护某些或所有的通信不被窃听和攻击。这些安全服务通过 STARTTLS 关键字和 TLS 来实现[RFC 2487]。

7.5.2.1 STARTTLS 关键字

STARTTLS 关键字是用来告诉 SMTP 客户，SMTP 服务器允许使用 TLS，它没有参数。

7.5.2.2 STARTTLS 扩展

STARTTLS 扩展到 SMTP，展示如下:

(1) SMTP 服务的名称在这里定义为 STARTTLS;

(2) 与扩展相关的 EHLO 关键字值是 STARTTLS;

(3) STARTTLS 关键字没有参数;

(4) 定义一个新的 SMTP 动词，“STARTTLS”;

(5) 对任意 SMTP 命令不增加新的参数。

7.5.2.3 STARTTLS 命令

STARTTLS 命令的格式为:

STARTTLS

在客户给出 STARTTLS 命令后，服务器响应码为下列之一：

220 已准备好开始 TLS

501 语法错误 (不允许有参数)

454 临时原因不可用 TLS

为了在本地传递邮件，为了防止 STARTTLS 扩展损坏互联网的 SMTP 基础设施的可互操作性，公开引用的 SMTP 服务器必须不要求使用 STARTTLS 扩展。有关 STARTTLS 命令对 SMTP 服务器的影响，给出 STARTTLS 命令后的具体响应和处理细节，进行 TLS 协商，以及实现安全性等方面的详细描述，参阅[RFC 2487]。

7.5.3 MIME 安全技术(S/MIME)

S/MIME (Secure/Multipurpose Internet Mail Extensions) 通过流行的互联网 MIME 标准，为电子消息应用提供认证、消息完整性、源不可否认性以及数据机密性等基于密码技术的安全服务。S/MIME 并不局限于电子邮件的安全，它适合传输 MIME 数据的任何传输机制，还可用于不需人工干预的使用基于密码技术的安全服务的自动消息传输代理。S/MIME 集成了 PKI 技术，通过证书中心建立信任。

S/MIME V3 由下列协议组成（参考[RFC 2630，RFC 2633，RFC 2632，RFC 2631，RFC 2634]）：

- Crptographic Message Syntax;
- S/MIME Version 3 Message Specification;
- S/MIME Version 3 Certificate Handling;
- Diffie-Hellman Key Agreement Method;
- Enchanced Security Services for S/MIME.

7.5.3.1 密码消息语法(CMS)

CMS[RFC 2630] 描述数据保护的一种封装语法，支持数字签名、消息认证码和加密，允许多重封装，CMS 能够支持多种基于证书的密钥协商结构。

CMS 定义了一种保护内容---ContentInfo，ContentInfo 封装单个明确的内容类型，CMS 定义了六种内容类型：数据、签名数据、封装数据、摘要数据、加密数据和认证数据，适合此规范的实现必须实现保护内容--- ContentInfo，并实现数据、签名数据和封装数据内容类型，其他的内容类型可根据需要实现。CMS 对内容类型的编码处理也进行了规定。

7.5.3.2 S/MIME 消息规范

MIME 标准[RFC 2045，RFC 2046，RFC 2047，RFC 2048，RFC 2049]为互联网消息的内容类型提供了一个同一结构，允许应用新的内容类型。S/MIME 消息规范[RFC 2633]描述怎样对 MIME 数据增加密码签名和加密服务，为了产生 S/MIME 消息，S/MIME 代理必须遵守此规范。

S/MIME 消息规范对下列情形进行了明确规定：

- 定义了怎样产生一个由 PKCS #7[RFC 2315]导出的密码增强的 MIME 体部分，同时也定义了能够用来传输那些体部分的申请(application)/PKCS #7MIME 类型。
- 讨论了怎样用[RFC 1847]中定义的多用途/签名 MIME 类型来传输 S/MIME 签名消息，也定义了用来传输 S/MIME 消息的申请(application)/PKCS #7 签名 MIME 类型。

7.5.3.3 S/MIME 证书处理

在利用公钥为发送和接收 MIME 消息提供安全服务前，S/MIME 代理必须证明公钥是有效的，必须用[RFC 2459]中描述的 X.509 证书来证明公钥的有效性，因而 S/MIME 代理必须按照 S/MIME 证书处理[RFC 2632]的要求进行证书处理。

S/MIME 证书处理描述了证书撤消、证书确认、证书与证书撤消签名与签名算法、以及证书扩展的详细处理过程。

7.5.3.4 D-H 密钥协商

D-H 密钥协商[RFC 2631]描述了收发双方怎样利用公钥技术成功协商仅他们双方知道的共享秘密，同时也对双方由共享秘密产生密钥材料，进而产生密钥加密密钥和消息加密密钥作了明确的规定。

7.5.3.5 S/MIME 增强安全服务

S/MIME 增强安全服务[RFC 2634]描述了 S/MIME 下列四种可选的安全服务：

— 签名的收条，
— 安全标签，
— 安全邮件表，
— 进行证书签名。

S/MIME 增强安全服务描述了这 4 种服务所需程序和属性。

7.5.4 FTP 安全技术

这一节定义 FTP 规范 STD 9，RFC 959 的安全扩展。基于 FTP 规范，通过引入新的可选命令，响应码和文件传输编码，利用密码技术，在控制与数据信道方面提供强的认证，完整性和机密性。

此规范将用到下列新的可选命令:

- AUTH (Authentication/Security Mechanism) 认证/安全机制
- ADAT (Authentication/Security Data) 认证/安全数据
- PROT (Data Channel Protection Level) 数据信道保护级别
- PBSZ (Protection Buffer Size) 保护缓冲器容量
- CCC (Clear Command Channel) 清除命令信道
- MIC (Integrity Protected Command) 完整性保护命令
- CONF (Confidentiality Protected Command) 机密性保护命令
- ENC (Privacy Protected Command) 保密保护命令

此规范还引入一新的响应类型：6yz 。

后续部分将对 FTP 安全扩展及其新的可选命令与响应码进行概述，相关的详细描述与实现细节，以及注册授权等，参阅[RFC 2228]。

7.5.4.1 FTP 安全概述

在最高层，FTP 安全扩展寻求为认证和/或授权连接，为命令、回答、时间传输完整性和/或机密性保护提供一个抽象的机制。

在 FTP 安全扩展，认证通常用密码技术，以安全的方式建立客户的身份和/或服务器的身份。

授权是对注册确认用户的过程，在 FTP 安全扩展，用来认证的安全机制也可用来决定授权。

FTP 安全扩展的交互由客户在 AUTH 命令中告诉服务器用什么安全机制开始。服务器接受或拒绝此安全机制，或者在服务器没有实现安全扩展时完全拒绝此命令。客户可提供多种安全机制直到接受一种安全机制，这允许进行简单的协商。服务器的回答将指示客户是否需要为解释安全机制提供附加的数据。

如果服务器需要额外的安全信息，则客户与服务器将进行安全数据交换，直到交换完成，在服务器与客户间就建立了一个安全关联。这种安全关联可以包括认证和为完整性或机密性提供密钥信息。

一旦建立了安全关联，作为安全关联一部分的认证可用来代替用户名/口令交换，附加在用户名/口令交换上，以授权用户连接到服务器。

为了防止攻击者在控制流中插入或删除命令，如果安全关联支持完整性，则服务器与客户必须使用完整性保护控制流。

一旦客户与服务器协商了 PBSZ 命令——在数据信道上封装受保护数据可接受的缓冲器容量，安全机制也可以用来保护数据信道传输。

FTP 安全扩展实现的认证、完整性、或机密性都是可选的，因而可接受这样的机制：仅实现完整性保护，单向认证与/或加密，没有认证或完整性保护的加密，或任意别的功能子集。一实体也可以要求比另一方能够提供的更强的策略保护，防止完全可互操作性。

7.5.4.2 FTP 安全中的新命令

下列命令是可选的，它们是 FTP 访问控制命令的扩充。服务器对这些命令进行处理的详细描述以及响应码的具体规定，参考[RFC 2228]。

(1) 认证/安全机制 (AUTH)

参数域是识别所支持的机制的 Telnet 串，这串不区分大小写。

(2) 认证/安全数据 (ADAT)

参数域是表示基 64 编码的安全数据的 Telnet 串(“基 64 编码”参阅[RFC 2228])。

ADAT 必须在一个成功的 AUTH 命令后面，或在一个重置安全状态的 AUTH 命令后面。

(3) 保护缓冲器容量 (PBSZ)

参数为十进制整数，单位为字节，表示在文件传送过程中发送或接收编码数据块的最大容量。此数需 32 比特无符号整数能够表示。

此命令允许 FTP 客户与服务器为连接协商受保护缓冲器的最大容量，没有缺省值，客户必须在它能够发布第一个 PROT 命令前发布 PBSZ 命令，且 PBSZ 必须在成功的安全数据交换后面。

(4) 数据信道保护级别 (PROT)

参数是单个 Telnet 字符码，指定数据信道保护级别。

此命令向服务器指明客户与服务器将用什么类型的数据信道保护。指定了下列码字：

C – Clear　　缺省保护级别，表示不采用安全保护；

S – Safe　　指示对数据采用完整性保护；

E – Confidential　　指示对数据采用机密性保护；

P – Private　　指示对数据采用完整性和机密性保护。

PROT 命令必须在一个成功的保护缓冲器容量协商后面。

(5) 清除命令信道 (CCC)

此命令没有参数。

CCC 命令激活非完整性保护的控制信道消息，CCC 本身必须是受完整性保护的。CCC 命令必须在成功的安全数据交换后面。

(6) 完整性保护命令(MIC)、机密性保护命令(CONF)与秘密保护命令(ENC)

MIC 域的参数是一个 Telnet 串，由一个基 64 编码的“可靠(safe)”消息构成，此消息由安全机制特殊的消息完整性程序产生。CONF 域的参数是一个 Telnet 串，由一个基 64 编码的“机密性(confidentiality)”消息构成，此消息由安全机制特殊的消息机密性程序产生。ENC 域的参数是一个 Telnet 串，由一个基 64 编码的“秘密(privacy)”消息构成，此消息由安全机制特殊的消息完整性和机密性程序产生。

服务器将解码和/或验证编码的消息。

这些命令必须在成功的安全数据交换后面。

7.5.4.3 FTP 安全扩展中的新响应

新的响应码分为两类，第一类是 FTP 安全命令必须的新的响应，第二类是一种新的响应类型——指示受保护的响应。下面列出这些响应码，有关的说明参考[RFC 2228]。

(1) 新的专用响应码

232 用户通过安全数据交换注册，授权；

234 安全数据交换完成；

235 [ADAT=base64data]；

334 [ADAT=base64data]；

335 [ADAT=base64data]；

336 用户名通过，需要口令，挑战是“……”；

431 需要一些难以获取的资源来处理安全；

533 由于策略原因否决命令保护级别；

534 由于策略原因否决请求；

535 安全检测失败(Hash 值，序列号等)；

536 机制不支持所要求的 PROT 级别；

537 安全机制不支持命令保护级别。

(2) 受保护的响应

引入一新的响应类型，此类响应仅在安全数据交换成功后发送：

6yz 受保护的响应

这种类型有 3 个响应码:

631 指示完整性受保护的响应。

632 指示机密性和完整性受保护的响应。

633 指示机密性受保护的响应。

631 响应的文字部分是 Telnet 串，由一个基 64 编码的“可靠”消息构成，此消息由安全机制特殊的消息完整性程序产生。632 响应的文字部分是 Telnet 串，由一个基 64 编码的“保密”消息构成，此消息由安全机制特殊的消息完整性与机密性程序产生。632 响应的文字部分是一个 Telnet 串，由一个基 64 编码的“机密性”消息构成，此消息由安全机制特殊的消息机密性程序产生。

7.5.4.4 FTP 安全扩展中的数据信道封装

当数据传输在客户与服务器间受保护时，必须执行确定的变换与封装，以确保接收方能够正确地对传输的文件解码。其实现细节请参阅[RFC 2228]。

7.5.4.5 FTP 安全扩展的实现策略

当客户与服务器策略没有限制时，推荐下列应该实现：

- 一旦安全数据交换发生，服务器应该要求所有的命令受保护(用完整性和/或机密性)，并且应该

用与保护命令相同的保护级别保护所有的响应。不推荐使用 CCC。

- 只要可能，客户应该加密 PASS 命令。
- 虽然实现没有强制的安全命令，但推荐实际实现提供能够实现的所有命令，给出支持的机制与站点的策略考虑（如输出控制）。

7.5.5 SNMP 安全技术

简单网络管理协议 (SNMP)规范允许使用多种安全协议保护网络管理操作。这一节针网络管理的两个主要威胁——修改信息与假冒伪装，两个次要威胁——修改消息流与泄露，描述 SNMP 安全的目标，利用密码技术及相关机制，对网络管理提供数据完整性、数据源认证、数据机密性保护，这些安全服务是通过摘要认证协议和对称加密协议来实现[RFC 1446]、[RFC 1352]。

7.5.5.1 SNMP 安全的目标

SNMP 安全的目标为：

- 协议应该为每个收到的 SNMP 消息在在通过网络期间没有被非授权管理操作引起改变提供验证；
- 协议应该为每个收到的 SNMP 消息的发端身份提供验证；
- 协议应该为每个最近收到的 SNMP 消息提供明确的产生时间；
- 协议应该为所有先传递的来自类似源的消息的每个后续收到的 SNMP 消息提供明确的产生时间；
- 必要时，协议应该提供保护，使每个收到的 SNMP 消息的内容不被泄露。

SNMP 安全的制约因素：

- 当管理的有效性要求与安全性要求不能兼顾时，选择有效性；
- 安全协议与下层的安全机制都不应依赖别的网络服务的可用性；
- 安全机制应该不改变基本的 SNMP 网络管理原则。

7.5.5.2 摘要认证协议

摘要认证协议为消息的接收提供完整性验证和消息源认证。完整性保护通过在消息的适合部位计算摘要来提供。摘要在消息发端计算，与消息一起传送，在消息收端验证。

摘要认证协议使用消息摘要算法为国家有关部门指定的算法或 MD5(这是一个输出为 128 比特的 Hash 算法，此算法的安全性目前是有效的)。在计算摘要前，为消息前缀一条只有发端和收端知道的秘密值，这样，在验证摘要时隐含了消息源的认证。

摘要认证协议包括产生消息与接收消息两个处理过程。产生消息处理和接收消息处理的具体执行程序及有关的规定细节，参阅[RFC 1446]、[RFC 1352]。

7.5.5.3 对称保密协议

对称保密协议对收到消息提供防泄露保护，即机密性保护。消息的适合部分用仅发端与收端知道的密钥加密。

此协议基于对称加密算法机制。此外，被加密的消息必须按照摘要认证协议的约定进行保护。对称加密算法为国家有关部门指定的算法或 AES，即 Rijndael，这是一个分组长度为 128 比特，支持密钥长度大于或等于 128 比特的分组密码算法(也支持其它长度的分组与密钥)，其安全性目前有效。

对称保密协议包括产生消息与接收消息两个处理过程。产生消息处理和接收消息处理的具体执行程序及有关的规定细节，参阅[RFC 1446]、[RFC 1352]。

7.5.5.4 时钟与秘密分配

摘要认证协议和对称保密协议都假定存在松散同步的时钟与共享的秘密值，这通过时钟与秘密分配来完成。时钟与秘密分配包括初始化配置、时钟分配、时钟同步、秘密分配与事故恢复五个处理过程，初始化配置第一次必须人工完成。有关时钟与秘密分配的详细处理程序请参阅[RFC 1446]、[RFC 1352]。

有 3 个要求限制分配时钟值和秘密值的策略：

- 如果认证时钟的值减少，最终时戳与私有认证密钥必须及时改变；

- 私有认证密钥与私有加密密钥必须仅需要它们的用户知道；
- 必须存在至少一个 SNMP 协议实体起作负责管理站的作用。

7.5.5.5 安全性与一致性

SNMP 安全有效的推荐实现以及一致性方面的描述参阅[RFC 1446]、[RFC 1352]。

7.5.6 Telnet 安全技术

Telnet 协议的安全要求包括机密性，完整性，认证。这些服务基于密码技术，可作为 Telnet 的安全扩展提供，或者作为一个封装的安全协议，这里将其称为 Telnet 的安全版本。

Telnet 的安全版本，应提供数据的保密和认证服务，独立于底层所提供的安全服务，这将在本标准下一版本要研究与描述。

Telnet 安全版本必需定义下列的服务：

- Telnet 请求和/或响应的机密性；
- Telnet 请求和/或响应的数据源的验证和数据完整性；
- 请求和/或响应的数据源的不可抵赖性；
- 请求和/或响应的传输及时性（freshness）；
- 与 Telnet 其它特征的易集成性；
- 对以上服务多机制的支持。

这些服务必需彼此独立地提供，并且支持中介与代理的需要。

7.5.7 通用安全服务应用程序接口(GSS-API)

通用安全服务应用程序接口 GSS-API(Generic Security Service Application Program Interface) [RFC 2078]为调用者提供通用安全服务，可支持不同的下层机制与技术，从而允许应用程序对不同环境源码级的可移植性。

GSS-API 提供的安全服务有认证、完整性、和/或机密性。GSS-API 在对等实体间分离初始化安全文字(security context)的操作，从相关的提供预消息(per-message)数据源认证和数据完整性保护的操作中，达到对等实体认证，这里机密性是可选的。GSS-API 具有如下特点：

- GSS-API 是机制独立的——GSS-API 定义一个接口，利用密码技术实现强的认证和其它安全服务，这些服务与特定的下层机制独立。如它提供的服务可用对称密码技术实现，也可用公开密码技术实现。
- GSS-API 是协议环境独立的——GSS-API 与引用它的通信协议独立，允许用于大量不同的协议环境。
- GSS-API 是协议关联独立的——GSS-API 的安全文字结构与通信协议关联结构独立。这种特征允许 GSS-API 实现于不同的调用协议模块，GSS-API 服务也能够被应用直接调用。
- GSS-API 适合于不同的实现布局——调用 GSS-API 的客户不必位于实现此 GSS-API 的可信系统内。

7.5.7.1 GSS-API 结构

GSS-API 结构的基本组成单元是信任凭证，令牌，安全文字，机制类型，名称和信道捆绑。

- 信任凭证提供使对等实体相互建立安全文字的先决条件。
- 令牌交换是为了在对等实体间建立和管理安全文字，以及与已建立的安全文字一起为相应是数据消息提供保护性的安全服务。
- 安全文字是在对等实体间建立，它的建立使用与每个对等实体局部地关联建立的或对等实体通过委托接收到的信任凭证。
- 机制类型不仅规定使用的特定密码技术，而且规定使用此机制保护的数据单元的语法和语意，必须同时被发起方和目的方对等实体支持。
- 名称在 GSS-API 中是明的，是为了支持发起与接受安全文字。

- 信道捆绑是指把建立的安全文字与下层通信信道和应用于通信信道的保护机制的有关特征捆绑在一起。

详细描述及相关作用，参阅[RFC 2078]。

7.5.7.2 GSS-API 界面

GSS-API 的服务界面划分为 4 个集合：信任凭证管理调用、文字级调用、预消息调用和支持调用。

信任凭证调用　用于获取和释放信任凭证，包括：

- GSS_Acquire_cred　　为使用获取信任凭证；
- GSS_Release_cred　　使用后释放信任凭证；
- GSS_Inquire_cred　　显示信任凭证信息。

文字级调用　用于安全文字的管理，包括：

- GSS_Init_sec_context　　发起出界安全文字；
- GSS_Accept_sec_context　　接受入界安全文字；
- GSS_Delete_sec_context　　冲洗不再需要的安全文字；
- GSS_Process_sec_context　　处理在安全文字上收到的控制令牌；
- GSS_Context_time　　指示安全文字上保持的有效时间。

预消息调用　用于建立安全文字上私有消息的保护，包括：

- GSS_Sign　　应用签名，接收作为令牌，与消息分开；
- GSS_Verify　　连同消息的有效令牌；
- GSS_Seal　　签名，可选加密，封装；
- GSS_Unseal　　解封，若需要解密，签名有效。

支持调用　提供对 GSS-API 调用者有用的辅助功能，包括：

- GSS_Display_status　　把状态翻译成可打印的类型；
- GSS_Indicate_mechs　　指示本地系统支持的机制类型(mech_types)；
- GSS_Compare_name　　比较两个名称是否相同；
- GSS_Display_name　　把名称翻译成可打印的类型；
- GSS_Import_name　　把可打印名称转换成正规化类型；
- GSS_Release_name　　释放正规化类型名称的内存；
- GSS_Release_buffer　　释放可打印类型名称的内存；
- GSS_Release_oid_set　　释放 OID(Object Identifier)集对象的内存。

有关 GSS-API 调用的详细描述与实现细节，参阅[RFC 2078]。附录 A1 为一个 GSS-API 实现示范。

8 加密算法与认证算法

加密算法与认证算法的引用在具体的实现中是独立的，用户可以选择喜欢的算法或自己设计算法，但是，所有的算法及应用都必须首先遵守国家密码管理委员会的有关规定。为了保证互通，适合的实现必须支持相关安全协议中规定的强制实现的算法。有关算法的详细规范由相应的文件描述。

8.1 加密算法

- 国家有关主管部门指定的算法；
- 国际通用标准算法，如 AES(此算法完全公开，没有任何专利)；
- NULL 加密算法。

8.2 认证算法

- 国家有关主管部门指定的算法；
- 国际通用标准算法，如 MD5，SHA-1 等；
- NULL 认证算法。

9 安全管理

9.1 概述

IP 网安全的管理方面所涉及的是不属于正常通信实例但需要用来支持和控制该通信的安全方面的操作。

IP 网系统的主管部门有可能推行许多安全策略，有关 IP 网安全管理的标准应当支持这些策略。由同一个主管部门管辖并遵守同一个安全策略的实体，有时会被集中到所谓的“安全域”里。

IP 网安全管理涉及 IP 安全服务和安全机制的管理，这要求将管理信息分配于这些服务和机制内，并收集有关这些服务和机制的操作信息。例如，密钥的分配、主管部门强制的安全选择参数的设置、有关正常和不正常的安全事件(审计数据)以及服务激活与解除激活。安全管理不涉及需要调用特定安全服务的协议中有关安全信息的传递。

安全管理信息库(SMIB)是 IP 网系统所需的全部安全信息的假想贮藏室。此概念不包含上述信息的储存格式或实现方法，但是，为了能够履行适当的安全策略，每个端系统必须包含必要的局部信息。当需要在一个(以逻辑形式或物理形式组合的)端系统群中履行一致的安全策略时，SMIB 是一个分布式信息库。

管理协议，特别是安全管理协议，以及传递管理信息的通信信道，都有潜在的危险。因此，务必注意为管理协议和信息提供保护，以保证一般通信实例的安全保护不被削弱。

为了建立或扩建 SMIB，安全管理可要求在不同的系统主管部门之间交换安全的相关信息。在某些情形，与安全相关的信息需要通过非 IP 通信路径，因此，本地的系统主管部门将通过非 IP 标准的方法去更新 SMIB；在其他的情形，有可能需要通过一条 IP 通信路径交换上述信息，这时信息是在实 IP 系统中运行的两个安全管理应用之间传递的，安全管理应用将利用通信信息去更新 SMIB。进行这样的更新之前可能需要得到安全主管部门的批准。

9.2 安全管理

IP 网安全管理包括 3 个方面：

— 系统安全管理；

— 安全服务管理；

— 安全机制管理。

此外，还需考虑 IP 网管理本身的安全性。

9.2.1 系统安全管理

系统安全管理涉及 IP 网环境所有安全方面的管理，这方面典型的活动有：

— 安全策略的综合管理，包括修改和一致性维护；

— 同其它 IP 管理功能的交互作用；

— 同安全服务管理和安全机制管理的交互作用；

— 事件处理的管理；

— 安全审计的管理；

— 安全恢复的管理。

9.2.1.1 事件处理管理

在 IP 网内看得见的事件处理管理是远距离报告有关违犯系统安全的明显企图以及修改启动事件报告的门限。

9.2.1.2 安全审计管理

安全审计管理包括：

— 选择拟记录和/或拟在远端收集的事件；

— 启动或停止记录被选事件的审计数据；

— 远程收集被选的审计记录；

— 准备安全审计报告。

9.2.1.3 安全恢复管理

安全恢复管理包括：

— 维护用于对实际的或嫌疑的安全违章作出反应的规则；

— 远程报告有关系统方面的明显违章；

— 安全保密主管部门的相互作用。

9.2.2 安全服务管理

安全服务管理涉及特殊的安全服务，下面是管理特殊安全服务典型的活动：

— 为服务确定和分配安全保护目标；

— 分配和维护为提供所需的安全服务使用的特定安全机制的选择规则；

— 在达成管理协议前协商可使用的安全机制；

— 通过适当的安全机制管理功能去调用特定安全机制，如主管部门提出的安全服务；

— 与其他的安全服务管理功能和安全机制管理功能相互作用。

9.2.3 安全机制管理

安全机制管理涉及特定的安全机制，下面是部分典型的安全机制管理功能：

— 密钥管理；

— 加密管理；

— 数字签名管理；

— 访问控制管理；

— 数据完整性管理；

— 认证管理；

— 通信业务填充管理；

— 路由选择控制管理；

— 公证管理。

9.2.3.1 密钥管理

密钥管理包括：

— 根据所要求的安全级定时生成合适的密钥；

— 根据访问控制的要求，确定哪些实体可以接收每一把密钥的拷贝；

— 使实例 IP 系统中的实体以用安全的方式获取或分配到密钥。

显然，有些密钥管理功能将在 IP 网环境以外完成，包括通过可信手段对密钥进行的物理分配。

在关联期间，为应用交换工作密钥是一种正常的层协议功能，工作密钥可通过对分配中心的访问进行选择，或通过管理协议进行预分配。

9.2.3.2 加密管理

加密管理包括：

— 与密钥管理的交换作用；

— 建立密码参数；

— 密码同步。

加密机制的存在意味着要使用密钥管理和使用共同的密码算法。

加密管理功能所提供保护的区别程度取决于 IP 环境内哪些实体独立拥有密钥；这通常必然要取决于安全保密结构，尤其是密钥管理机制。

共同的密码算法可利用密码算法寄存器或在实体之间预先达成协议来获得。

9.2.3.3 数字签名管理

数字签名管理包括：

— 与密钥管理交互作用；

— 建立密码参数和算法；

— 在通信实体间(可能还有第三者参与)使用协议。

通常数字签名管理与加密管理之间存在极相似之处。

9.2.3.4 访问控制管理

访问控制管理可包括安全属性(包括口令)的分配、对访问控制表或能力表的更新。也可以包括在通信实体与其他提供访问控制服务的实体之间协议的使用。

9.2.3.5 数据完整性管理

数据的完整性管理包括：

— 与密钥管理交互作用；

— 建立密码参数和算法；

— 在通信实体间协议的使用。

当为数据完整性使用密码技术时，数据完整性管理与加密管理之间存在极相似之处。

9.2.3.6 认证管理

认证管理可以包括向要求执行认证的实体散发说明型信息、口令或密钥(使用密钥管理)。也可以包括在通信实体和其他提供认证服务的实体间协议的使用。

9.2.3.7 通信业务填充管理

通信业务填充管理可包括通信业务填充规则的维护，如：

— 预先指定的数据率；

— 指定随机数据率；

— 指定消息特征，如长度；

— 规范的变更，可能根据一天的时间和/或日历进行更新。

9.2.3.8 路由控制管理

路由控制管理可包括链路或子网的定义；这些链路和子网对特定准则而言被认为是安全或可信赖的。

9.2.3.9 公证管理

公证管理包括：

— 有关公证人的信息的分配；

— 有关公证人与通信实体之间协议的使用；

— 与公证人交互作用。

9.2.4 IP 网管理的安全

所有 IP 网管理的安全和 IP 网管理信息通信的安全对 IP 网安全很重要，IP 网安全管理将选择适合安全服务与安全机制，以保证 IP 网管理协议得到适当的保护。

附录 A
(提示的附录)
GSS-API 实现示范

假设信任凭证的获取已经完成，下层认证技术能够使服务器利用在单个令牌中携带的元素认证客户，也能够使客户用返回的单个令牌认证服务器。下面的示例说明客户和服务器以机制独立方式使用GSS-API 的数据流，建立安全文字，并传送受保护的消息。

（1）客户调用 GSS_Init_sec_context()，通过识别目标名称(targ_name)，建立到服务器的安全文字，并选择互请求标志(mutual_req_flag)，使得在安全文字建立的过程中执行相互认证。GSS_Init_sec_context()返回一个输出令牌(output_token)，并指定互认证序列的待完成 GSS_CONTINUE_NEEDED 状态。如果设置互请求标志，GSS_Init_sec_context()将返回 GSS_COMPLETE 状态。客户向服务器发送输出令牌。

（2）服务器把收到的令牌作为输入令牌(input_token)参数传给 GSS_Accept_sec_context()，GSS_Accept_sec_context 指示 GSS_COMPLETE 状态，在源名称(src_name)中提供客户的认证身份，并且提供一个输出令牌。服务器向客户发送输出令牌。

（3）客户把收到的令牌作为输入令牌参数传给紧接着的一个调用 GSS_Init_sec_context()，此调用处理令牌中包括的数据，从客户方看来是为了完成相互认证。这次调用 GSS_Init_sec_context()返回 GSS_COMPLETE 状态，指示相互认证成功，安全文字建立完成。

（4）客户产生一条数据消息并传给 GSS_Seal()，GSS_Seal 对此消息执行数据源认证，数据完整性，以及可选的机密性处理，并封装成输出消息(output_message)，指示 GSS_COMPLETE 状态。客户向服务器发送输出消息。

（5）服务器把收到的消息传给 GSS_Unseal()，GSS_Unseal 执行解封，如果需要解密，并验证数据源认证的有效性和数据完整性。GSS_Unseal()通过返回 GSS_COMPLETE 状态指示成功有效。

（6）如果假设服务器已经知道此安全文字在一条受保护的消息从客户发送到服务器后不在使用，服务器调用 GSS_Delete_sec_context()冲洗文字级信息，此调用返回文字令牌(context_token)，服务器向客户发送此令牌。

（7）客户把收到的文字令牌传给 GSS_Process_context_token()，它在客户端系统清除文字级信息后返回 GSS_COMPLETE 状态。

附录B
(提示的附录)
安全背景知识

B1 安全背景知识

安全在TCP/IP环境里仅仅是数据处理/数据通信安全的一个方面。若希望它们发挥效力，则在TCP/IP环境里使用的保护措施需要 TCP/IP 以外的支撑措施支持。例如，在系统间流通的信息是可以加密的，但若不采用物理形式对系统的访问进行安全限制，则加密将等于零。此外，TCP/IP 只涉及系统的互连，所以，若希望获得有效的TCP/IP安全措施，这些措施应该同TCP/IP以外的其他措施结合使用。

B1.1 安全方面的要求

“安全”是指减少财产和资源的脆弱性。所谓财产是泛指有价值的东西，脆弱性是任何可以利用的弱点，以达到侵犯某一系统或该系统所包含的信息的目的。所谓威胁是指对安全的潜在危险。

(1) 开放系统考虑安全的动机

- 社会日益依赖于计算机，计算机的访问和连接是通过数据通信实现的，它需要保护以防止各种威胁；
- 在一些国家已颁布有关数据保护的法规，规定制造商必须能够保证系统的安全和隐私权。

(2) 要保护的东西：

信息和数据(包括与安全措施相关的软件和“被动”数据如口令等)；
通信和数据处理服务；
装备与设施。

(3) 对通信系统的威胁包括：

对信息和/或其他资源的破坏；
对信息的讹用和修改；
盗窃、搬移或丢失信息和/或其他资源；
泄露信息；
拒绝服务。

威胁可分为偶然型与蓄意型，主动型与被动型：

- 偶然型是非预先计划的事件，如系统故障、操作上的疏忽以及软件差错等。
- 蓄意型包括使用容易获得的监控工具随意窃阅到特殊的系统知识的高级袭击行为。蓄意型若得逞则可视为一种“袭击”。
- 被动型若得逞将不修改系统内的任何信息，而且既不变更系统的操作又不改变系统的状态，如使用无源线切听通信线传输的信息。
- 主动型包括对系统内信息的修改、或改变系统状态和工作。如无权用户恶意改变系统的路由表。

(4) 某些特殊类型的袭击：

在下文中，“授权”是指“授予权力”，它有两种含义：完成某些动作(例如存取数据)的权力，和被授予某实体、代理人或进程的权力。所以所谓合法行为是指授权(而不是调用)完成某些动作的行为。

- 冒充 — 一个实体装扮成另一个实体的行为称为冒充。冒充通常伴随着其他形式的主动型袭击，尤其是重放和修改消息。如，当有效的认证序列出现后，是有可能被截获和重放的。仅拥有一点权力的合法实体可利用伪装的手法冒充拥有更多权力的实体以获得该权力。
- 重放 — 将一消息或其中的一部分加以重复以便产生非法的效果叫做重放。如包含认证信息

的一段消息有可能被另一个实体重放来达到认证自己的身份的目的。

- 更改消息 — 偷偷改变数据传输的内容，并造成非法后果的行为。
- 拒绝服务 — 某一个实体拒绝完成本身的任务，或妨碍其他实体完成他们本身的任务的行为。此袭击有两种可能性：第一种无特定目的，如一个实体抑制所有的消息；第二种是有目标的，如一个实体抑制所有送往特定目的地(如安全审计服务)的消息，包括抑制业务量和生成多余的业务量，也有可能生成某种情况来破坏网络的操作，尤其是当网络包括转节实体时，而后者的路由选择是根据其他转接实体收到的状态报告确定的。
- 内部袭击 — 当一个系统的合法用户表现一种越权行为或不正当行为时。大多数计算机作案与损害系统安全的内部袭击有关。防止方法如下：

— 认证审查工作人员的品德；
— 仔细检查硬件、软件、安全策略和系统布置，保证它们工作正确(可信功能)；
— 审计数据，用来增强对这种袭击的检测能力。

- 外部袭击 — 使用下列技术：

— 搭线法；
— 截收发射信号；
— 冒充系统的授权用户或系统的组成部分；
— 回避认证或访问控制机制。

- 陷门 — 一个系统的实体被改变，使袭击者能够通过命令或事先确定的事件或事件序列上产生越权的效果。如一个口令的认证有可能被修改，从而除了正常效果外，还能够确认袭击者的口令。
- 特洛伊木马 — 当特洛伊木马侵入系统时，它具有双重授权和未授权功能。把消息拷贝到一条无权信道上的中继实体也是特洛伊木马。

B1.2 安全策略

整个安全领域是复杂和广泛的。任何比较完整的分析均产生种类繁多的细节。一个恰当的安全策略应当把注意力集中于最高权威认为必须引起重视的那些方面。重要的是，安全策略应当概括地说明在安全领域内哪些在相关系统的一般操作过程中是允许和不允许的。策略通常是不具体的，它只是提醒你注意至关重要的事情，但不具体告诉你如何获得所希望的结果。策略奠定安全规范的最高层次。

由于策略的概括性很强，刚开始的时候是不可能知道如何把策略同特定的应用结合在一起的。因此，最好的办法是不断地修订策略，在每一个阶段的应用中增加新的细节部分。要想知道这些细节的内容究竟是什么，需要根据一般策略仔细研究具体的应用领域。这个研究应当弄清在试图把策略的条件同具体应用结合在一起的过程中出现的一系列问题。修订策略的过程是根据直接从应用中获得的材料更确切地阐明一般性策略的内容。新阐述的策略使制定实施方案细节的工作更容易些。

(1) 安全策略的组成部分

- 授权：上面讨论的威胁均包括授权与未授权行为的概念，授权内容的说明均在安全策略的条文中给出。安全策略的总纲可以作出这样的声明：“不得把信息提供给未授权用户，不允许未授权用户存取信息，不得把信息透露给未授权用户，不得把任何资源提供给未授权用户”。授权的性质是区分各种策略的依据。策略可根据授权的性质划分为基于规则的和基于身份的两种：前者是基于少量普遍实施的一般属性或灵敏度类别的规则；后者是基于特定身份化属性的授权准则。某些属性被认为同符合该属性的实体永远保持联系，其他一些属性可能是可以传给其他实体的占有物(如能力)。此外，授权服务还可划分为由主管部门规定和通过动态选择两种类型。安全策略将确定哪些系统安全要素要强制执行(如基于规则和基于身份的安全策略，若存在)，哪些是根据用户需要选择的。
- 基于身份的安全策略：基于身份的安全策略部分地符合所谓“需要知道”的安全策略。其目的是对数据或资源存取进行筛选。根据存取权，信息是掌握在存取者手里抑或是被存取的数据

的一部分。基于身份的策略基本上有两种实施方法：第一种的例子是特权或能力的概念，即授予用户的特权或赋予用户的能力，或者为用户执行任务的进程使用的特权或能力；第二种的例子是存取控制表(ACL)。

- 基于规则的安全策略：在基于规则的安全策略中，授权通常取决于敏感度。在保密系统里，数据和/或资源应当贴上保密标签。为某些用户执行任务的进程可以获得同发起者的身份相适应的保密标签。

(2) 安全策略、通信与标签

标签的概念在数据通信环境中是至关重要的，携带属性的标签扮演着各种角色。有些数据项在通信过程中移动位置，有些进程与实体启动通信，有些则作出响应，有些信道与系统的其他资源本身在通信过程中被使用，所有这些都可以贴上表示各种属性的标签。安全策略必须指出如何把上述属性用来提供必要的安全保护；为标签上的特定属性确定适当的安全内容时，可能要进行协商。当安全标签贴在存取进程和被存取的数据时，使用基于身份的存取控制所需的附加信息必须放在相关的标签里。当安全策略是基于直接或通过进程存取数据的用户的身份时，机密标签应当包括有关用户身份的信息。有关特定标签的规则应当在安全管理信息库(SMIB)内的安全保密策略中阐述，和/或根据要求同端系统进行协商。标签的后面可附上一些属性，说明标签的敏感度、详细处理和分配方法、规定时间和安排上的限制条件，以及详细说明端系统的特殊要求。

- 进程标签　在认证中，给启动与响应某一通信实例的实体或进程贴上明确的标签和适当的属性是至关重要的，因此，安全管理信息库应充分保存对主管部门实施的策略记为重要的一些属性的相关信息。
- 数据项标签　当数据在通信实例的过程中移动时，每个数据均被牢牢地同其标签栓在一起(这种耦合是重要的，在一些情况下是基于规则的策略所规定的，要求在把数据项递交给应用实体之前先把标签贴在该数据项作为该数据项的一部分)。此外，用于保持数据完整性的技术亦应当保证准确地选择标签和耦合标签。这些属性可应用于开放系统互连基本参考模型中的数据链路层的路由选择控制功能。

B1.3　安全机制

安全保密策略可根据策略目标与使用的机制，单独使用或组合使用各种机制实现。在一般情况下，机制共有以下 3 种(互相重叠的)类别：

预防；

检测；

恢复。

适合于数据通信环境的安全保密机制有以下 11 种。

（1）密码技术与加密

密码技术涉及许多安全服务与机制。密码功能可作为加密、解密、数据完整性、认证交换、口令存储和检查等功能的一部分，协助达到保密、完整性和/或认证目的。在保密服务的应用中，加密功能把高度机密的数据(即要保护的数据)转换为机密度稍差的形式。当使用于完整性或认证服务时，密码技术被用来计算不能伪造的功能。

加密首先是用来把明文转换为密文。解密时可以产生两种结果：明文或隐蔽的密文。为一般性除了目的使用明文在计算上是可行的，它的语义学内容是可供存取的。由于密文的语义学内容是隐蔽的，因此，除非使用特殊的方法(如解密或准确的匹配)，要处理密文在算法上是行不通的。当不希望导出原来的明文时，往往故意设法使加密功能成为不可逆过程。

密码功能使用密码变量，并在字长、数据单元和或数据单元流上进行操作。两个密码变量是密钥与初始向量，前者引导特定转换，后者是某些密码协议为了保持密码文本的表面随机性所需要的，该密钥一般必须保持秘密。密码功能和初始向量可以起到增加时延和加大带宽消耗的作用，这导致在现行的系统中使用“透明”或“插入”密码术附加信息的操作复杂化。

加密和解密使用的密码变量分为对称和不对称两种，不对称算法使用的密钥在数学上是彼此有关的，已知一把密钥要推导另一把密钥在计算上是不可行的，这种算法也称“公钥”算法，因为其中的一把密钥可以公开。

只要在算法上行得通，密文是可以在不知道密钥的情况下加以分析而还原为明文的。这种情况多发生在使用脆弱的或有缺陷的密码功能的场合。窃听与业务量分析能导致对密码系统的袭击，包括插入、删除和改变信息字段、重放原来的有效密文和冒充行为等。

由于上述原因，设计密码协议时应当考虑防御各种袭击和业务流分析，业务流机密性是对付业务流分析的一种反措施，其目的是隐藏数据的存在或不存在及其特性。当需要通过转接点传递密文时，它在转节点和网关上的地址必须用明码表示。若数据只在每一条链路上加密，然后在转接点和网关上解密(因此容易受到攻击)，则这种结构称为“逐条链路加密”。若只有地址(和类似的控制数据)是在转接点或网关上使用明码表示，则这种结构称为“端到端加密”。从安全保密的观点来看，端到端加密更优越，但结构复杂，尤其是当包括带内电子密钥分配(密钥管理)时。为了达到多种安全保密目的，可混合使用这两种结构。数据的完整性往往可通过计算密码校验值达到，校验值可分一步或几步计算，它是密码变量和数据的数学函数，这些校验值同被保护的数据是有关联的。

密码技术能够提供下列保护：

- 防止信息流被窃听和/或被修改；
- 防止(业务量)通信被分析；
- 防止被拒绝；
- 防止假冒；
- 防止非法连接；
- 防止信息被修改。

（2）密钥的管理

密钥管理采用密码算法，包括密钥的产生、分布和控制。密钥管理方法是根据参与管理成员对使用密钥的环境的评价选择的，对环境的考虑包括存在哪些威胁(组织内部和外部)、使用的技术、提供密码服务的总体结构与位置以及密码服务提供者物理结构与位置等。

密钥管理要考虑的事项：

- 对于每一把密钥(隐含的或明确定义的)，应根据时间、使用情况或其它准 则使用其“寿命”；
- 具有不同功能的密钥应分别贴上不同的标志，保证严格按功能合理使用密钥，如机密性服务的专用密钥不应当用于完整性服务，反之亦然。
- 非开放系统互连的考虑，如密钥物理分布与存档。

有关对称密钥算法的密钥管理需要考虑的事项：

- 在密钥管理协议中使用保密服务传递密钥；
- 使用密钥等级结构。应考虑不同情况，如：

只使用数据加密密钥的“平坦”密钥等级，该数据加密密钥是从集合中以明显方式或隐含方式根据密钥的身份或标志选择的；多层密钥等级；密钥的加密密钥不能用来保护数据，反之亦然。

- 分担责任，保证没有一个人能够拥有重要密钥的完整拷贝。

有关不对称密钥算法的密钥管理需要考虑的事项：

- 在密钥管理协议中使用保密服务传递密钥；
- 为了传递公开密钥，在密钥管理协议中使用完整性服务，或提供源证实功能的抗抵赖服务。

这些服务可借助于对称和/或不对称密码算法提供。

（3）数字签名机制

数字签名机制是一种可用来提供安全服务的特殊技术，要求使用不对称密码算法，其主要特性是不使用专用密钥就不可能建立署名的数据单元。这意味着：

- 除了持有专用密钥的用户，任何人都不可能建立署名的数据单元；

- 接收者不可能建立署名的数据单元。

因此，只需使用公开的信息就能够准确地识别某一个数据单元的签名者为专用密钥的唯一主人，一旦参与者之间发生冲突，就有可能求助于可信赖的第三方去鉴别数据单元的真伪，证明该数据单元的署名者的身份。有些场合可能需要附加特性：

- 发送者不可能否认自己曾发送署名的数据单元。

发送者也可以要求保证接收者事后不否认他收到该署名的数据单元的事实，为此，可使用提供传递证明的抗否认型服务和适当使用数字签名、数据完整性和公证机制。

（4）访问控制机制

访问控制机制是用于实施只允许授权用户访问资源的限制策略的一种机制，采用的技术包括访问控制表、口令、资格级别、标签或标志，拥有这些东西的用户可用它来指出自己的访问权。在使用资格级别的情况下，应当防止假冒和以可以信赖的方式传递资格信息。

（5）数据完整性机制

数据完整性机制是利用密码技术对数据的完整性进行保护，对数据任何形式的非法改动都将被检测出。

（6）认证交换机制

- 当对等实体与通信手段均可信赖时，对等实体的身份可通过口令加以证实；
- 当实体信任其对等实体但不信任通信手段时，为了防止主动性攻击，可以同时使用口令与密码技进行保护；为了防止重放攻击，需要使用双向握手或时戳；具有防重放保护的相互认证可通过三方握手来实现；
- 当实体不信任其对等实体或信任通信手段时，可采用抗否认型服务，这可通过使用数字签名和/或公证机制实现。这些机制还可与上述机制结合使用。

（7）业务填充机制

采用生成假业务和填充协议数据单元达到固定长度，可提供防业务流分析的有限保护。为了获得成功，填充后的真假数据单元加密和伪装。

（8）路由控制机制

适用于数据传送的路由选择规范可用来保证数据只通过物理上保证安全的路由传递，或保证机密信息只通过受适当保护的路由传送。

（9）公证机制

公证机制是建立在可信赖的第三方的概念上，以保证两个实体间交换的信息的某些特征。

（10）物理和人员的安全保密

为了保证提供完整的保护，始终有必要采取物理安全保密措施，这往往是昂贵的，故常用其他技术代替。虽然所有的系统最终将依赖于某种形式的物理安全保密和操作人员的可信赖程度，物理和人员安全保密的考虑不属于本要求的范围。

（11）可信赖的硬件/软件

为了信任某一实体工作正常，可采用下列方法：核实与确认、检测与记录已知的未遂攻击以及指定可信赖人员在有安全保障的环境里建立实体。此外，还需要采取预防措施防止实体在其运行寿命周期内因意外变动或被蓄意更改遭受破坏。为了维护安全，还必须信任系统内的一些实体工作正常。有关建立信任的方法不属于本技术要求。

B2 安全服务与安全机制布置

- 对等实体认证：　应该在网络层、传输层和应用层提供；
- 数据源认证：　应该在网络层、传输层和应用层提供；
- 访问控制：　应该在网络层、传输层和应用层提供；
- 机密性：　应该在链路层、网络层、传输层和应用层提供；

- 完整性：　　应该在网络层、传输层和应用层提供；
- 抗抵赖性　　应该在应用层提供。

具体理由及详细解释请参阅[ISO/IEC 7498-2，Annex B]或[GB/T 9387.2，附件 B]。

B3　应用时加密位置的选取

大多数应用并不要求在一个层以上提供加密机制，层的选择取决于下列重要因素：

- 若要求提供全业务流机密性，则可选择物理层加密机制或传输安全保密机制。若在转接点上能提供物理安全和可信赖的路由选择以及类似功能，则全部安全保密要求将得到满足。
- 若要求提供高可靠性的保护和抗抵赖或选择域保护，则应选择应用层加密机制。选择域保护可能是极为重要的，因为加密算法消耗大量的处理能力。在应用层内的加密机制能够提供无恢复的安全、抗抵赖以及所有机密性服务。
- 若希望为全部端系统至端系统通信提供简单的总保护和/或提供一个外部加密装置，则应当选择网络层加密机制。这将能够提供无恢复的机密性和完整性服务。
- 若要求提供有恢复的完整性机制和高可靠性保护，则应当选择传输层加密机制。这将能够提供有或无恢复的机密性和完整性服务。
- 在未来的实现中，不建议使用链路层的加密机制。
- 当涉及上述两个或多个的关键问题时，可能需要在一个层以上提供加密机制。

中华人民共和国
通信行业标准
IP网络安全技术要求——安全框架
YD/T 1163—2001
*
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
电话:67132792
北京鸿佳印刷厂印刷

*
开本:880×1230　1/16　　2001年12月第1版
印张:3.25　　2001年12月北京第1次印刷
字数:91千字　　印数:1－2 000
ISBN 7-115-663/01-165
定价:18.00元
本书如有印装质量问题,请与本社联系 电话:(010)67129223