ICS 35.020
L 80

中华人民共和国国家标准

GB/T 25068.4—2010/ISO/IEC 18028-4:2005

信息技术　安全技术　IT 网络安全
第 4 部分:远程接入的安全保护

Information technology—Security techniques—IT network security—Part 4:Securing remote access

(ISO/IEC 18028-4:2005,IDT)

2010-09-02 发布　　2011-02-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

目　　次

前　言

GB/T 25068 在《信息技术　安全技术　IT 网络安全》总标题下，拟由以下 5 个部分组成：

——第 1 部分：网络安全管理；

——第 2 部分：网络安全体系结构；

——第 3 部分：使用安全网关的网间通信安全保护；

——第 4 部分：远程接入的安全保护；

——第 5 部分：使用虚拟专用网的跨网通信安全保护。

本部分为 GB/T 25068 的第 4 部分。

本部分使用翻译法等同采用国际标准 ISO/IEC 18028-4:2005《信息技术　安全技术　IT 网络安全　第 4 部分：远程接入的安全保护》(英文版)。该国际标准中缺少“规范性引用文件”的章条，为保持与该国际标准编排方式的一致，本部分未添加相应的章条。

本部分更正了部分术语(条款 2.10 中 DHCP 全称中的“Control”更正为“Configuration”；条款 2.28 中 RADIUS 全称中的“Access”更正为“Authentication”；条款 2.43 中 TKIP 全称中的“implementation”更正为“integrity”；条款 7.2.2 中 S/MIME 全称中的“exchange”更正为“extensions”)。

本部分更正了部分错误(附录 E.1 中误表示为“行为”的“删除或关闭不必要的服务和应用”和“配置操作系统用户鉴别”更正为“标题”表示形式；附录 E.3 中的“SSI”更正为“SSL”)。

8.4.3 中“窃听威胁只能用加密与之对抗”中的“只能”过于绝对，修改为“大多”，为今后技术发展预留了空间。

8.7 中增加了使用国家加密标准的规定。

本部分的附录 A、附录 B、附录 C、附录 D、附录 E、附录 F 为资料性附录。

本部分由全国信息安全标准化技术委员会(TC 260)提出并归口。

本部分起草单位：黑龙江省电子信息产品监督检验院、中国电子技术标准化研究所、哈尔滨工程大学、北京励方华业技术有限公司、山东省标准化研究院。

本部分主要起草人：王希忠、黄庶、刘亚东、黄俊强、马遥、方舟、王大萌、树彬、张清江、王智、许玉娜、张国印、李健利、冯亚娜、曲家兴、邱益民、王运福。

引　言

在信息技术领域，在组织内部和组织之间使用网络的需求日益增加。因此，安全使用网络的要求必须得到满足。

在远程接入网络领域要求特定措施时，IT 安全宜得到适当安排。GB/T 25068 的本部分为远程接入网络（或使用电子邮件、文件传输，或只是远程工作）提供指南。

信息技术　安全技术　IT网络安全
第4部分:远程接入的安全保护

1　范围

GB/T 25068的本部分规定了安全使用远程接入(使用公共网络将一台计算机远程连接到另一台计算机或某个网络的方法及其IT安全含义)的安全指南。本部分介绍不同类型的远程接入以及使用的协议,讨论与远程接入相关的鉴别问题,并提供安全建立远程接入时的支持。

本部分适用于那些计划使用这种连接或者已经使用这种连接并且需要其安全建立及安全操作方式建议的网络管理员和技术员。

2　术语和定义

下列术语和定义适用于本部分。

2.1

接入点　Access Point;AP

提供从无线网络接入到地面网络的系统。

2.2

高级加密标准　Advanced Encryption Standard;AES

一种对称加密机制。

注:AES提供可变的密钥长度并允许按美国联邦信息处理标准(FIPS)197的规范有效实现。

2.3

鉴别　authentication

确信实体是其所声称身份的措施。在用户鉴别的情况下,通过所知的东西(例如口令)、拥有的东西(例如令牌)或个人特征(生物特征)识别用户。强鉴别既可以基于强机制(例如生物特征),也可以利用这些因子中至少两个(称为"多因子鉴别")。

2.4

回叫　call-back

一种在收到有效标识符(ID)参数后向预先定义或建议位置(和地址)呼叫的机制。

2.5

挑战—握手鉴别协议　Challenge-Handshake Authentication Protocol;CHAP

一种在RFC1994中定义的3次鉴别协议。

2.6

数据加密标准　Data Encryption Standard;DES

一种众所周知的使用56比特密钥的对称加密机制。因其密钥长度短,DES已被AES取代,但仍在多重加密模式中使用,例如,3DES或三重DES(FIPS 46-3)。

2.7

非军事区　de-militarised zone;DMZ

一种本地网络或站点网络的隔离区,其访问借助防火墙实现的特定策略来控制。DMZ不是内部网络的一部分并被认为不太安全。

2.8

拒绝服务　Denial of Service;DoS

一种使系统失去可用性的攻击。

2.9

数字用户线　Digital Subscriber Line;DSL

一种快速访问本地电信回路网络的技术。

2.10

动态主机配置协议　Dynamic Host Configuration Protocol;DHCP

一种在启动时动态提供 IP 地址的互联网协议(RFC 2131)。

2.11

封装安全载荷　Encapsulating Security Payload;ESP

一种基于 IP、对数据提供保密性服务的协议。特别是,ESP 将加密作为一种安全服务来提供,以保护 IP 包的数据内容。ESP 是一个互联网标准(RFC 2406)。

2.12

可扩展鉴别协议　Extensible Authentication Protocol;EAP

一种由远程拨号接入用户鉴别服务(RADIUS)支持并由 IETF 在 RFC 2284 中标准化的鉴别协议。

2.13

文件传输协议　File Transfer Protocol;FTP

一种用于在客户端与服务器之间传输文件的互联网标准(RFC 959)。

2.14

互联网工程任务组　Internet Engineering Task Force;IETF

负责提出和制定互联网技术标准的小组。

2.15

互联网消息访问协议第 4 版　Internet Message Access Protocol v4;IMAP4

一种电子邮件协议,该协议允许访问和管理远程电子邮件服务器上的电子邮件和信箱(在 RFC 2060 中被定义)。

2.16

局域网　Local Area Network;LAN

一种通常在建筑物之内的本地网络。

2.17

调制解调器　modem

为将电话协议作为一种计算机协议使用,而将数字信号调制成模拟信号或反向调制(解调)的硬件或软件。

2.18

多用途互联网邮件扩展[协议]　Multipurpose Internet Mail Extensions;MIME

一种允许通过电子邮件传输多媒体和二进制数据的方法,在 RFC 2045 至 RFC 2049 中被规范。

2.19

网络访问服务器　Network Access Server;NAS

为远程客户端提供对某基础设施访问的系统(通常是计算机)。

2.20

一次性口令　one-time password;OTP

一种仅使用一次(因而对抗重放攻击)的口令。

2.21

被动模式　Passive mode;PASV mode

一种 FTP 连接建立模式。

2.22

口令鉴别协议　Password Authentication Protocol;PAP

一种为点对点协议(PPP)提供的鉴别协议(RFC 1334)。

2.23

个人数字助理　Personal Digital Assistant;PDA

通常指手持式计算机(掌上计算机)。

2.24

点对点协议　Point-to-Point Protocol;PPP

一种在点对点链路上封装网络层协议信息的标准方法。

2.25

邮局协议第 3 版　Post Office Protocol v3;POP3

RFC1939 中定义的电子邮件协议,该协议允许电子邮件客户端索取存储在电子邮件服务器中的电子邮件。

2.26

良好隐私保护　Pretty Good Privacy;PGP

一种基于公钥密码、可公开提供的加密软件程序,其消息格式在 RFC 1991 和 RFC 2440 中被规范。

2.27

用户级交换机　Private Branch Exchange;PBX

一种通常基于计算机的企业级数字电话交换机。

2.28

远程拨号接入用户鉴别服务　Remote Authentication Dial-in User Service;RADIUS

一种用于鉴别远程用户的互联网安全协议(RFC 2138 和 RFC 2139)。

2.29

远程接入服务　Remote Access Service;RAS

通常是提供远程接入的硬件和软件。

2.30

远程接入　remote access

从安全域的外部对某系统的授权访问。

2.31

请求评议　Request for Comment;RFC

由 IETF 提出的互联网标准的标识。

2.32

安全壳　Secure Shell;SSH

一种利用不安全的网络提供安全的远程登录的协议。SSH 虽为专有,但不久将成为 IETF 标准。SSH 最初由 SSH 通信安全组开发。

2.33

安全套接字　Secure Sockets Layer;SSL

一种处于网络层与应用层之间、提供客户端和服务器的鉴别及保密性和完整性服务的协议。SSL 由 Netscape 开发,并构成安全传输层(TLS)的基础。

2.34

安全多用途互联网邮件扩展　Security/Multipurpose Internet Mail Extensions;S/MIME

一种提供安全多用途邮件交换的协议。

注：该协议第3版由5部分组成：RFC 3369和RFC 3370定义消息句法，RFC 2631至RFC 2633定义消息规范、证书处理和密钥协定方法。

2.35

串行线互联网协议　Serial Line Internet Protocol;SLIP

一种在RFC 1055中被规范的、采用电话线(串行线)传输数据的包成帧协议。

2.36

服务集标识符　Service Set Identifier;SSID

一种通常以名字的形式表示的无线接入点标识符。

2.37

简单邮件传输协议　Simple Mail Transfer Protocol;SMTP

一种用于向电子邮件服务器发送电子邮件(外发)的互联网协议(RFC 821及其扩展)。

2.38

传输层安全协议　Transport Layer Security Protocol;TLS

SSL的后继协议，是正式的互联网协议(RFC 2246)。

2.39

统一资源定位符　Uniform Resource Locator;URL

Web服务的地址方案。

2.40

不间断电源　Uninterruptible Power Supply;UPS

通常是一种基于电池的系统，用于在停电、电压下降和电涌时保护设备。

2.41

用户数据报协议　User Datagram Protocol;UDP

一种用于无连接通信的互联网联网协议(RFC 768)。

2.42

虚拟专用网　Virtual Private Network;VPN

利用共享网络的专用网，例如，基于密码隧道协议运行在另一个网络基础设施上的网络。

2.43

WiFi保护接入　WiFi Protected Access;WPA

一种为无线通信提供保密性和完整性的安全增强规范。该规范包括临时密钥完整性协议(TKIP)。WPA是有线等效隐私(WEP)的后继协议。

2.44

有线等效隐私　Wired Equivalent Privacy;WEP

一种采用128比特密钥提供流密码加密的密码协议。该协议被定义在GB 15629.11—2003(无线局域网规范)中。

2.45

无线保真　Wireless Fidelity;WiFi

一种WiFi联盟推动使用无线LAN设备的商标。

2.46

无线局域网　Wireless LAN;WLAN

一种使用无线电频率的网络。最常用的标准是GB 15629.1102—2003和GB 15629.1104—2006，

它们利用 2.4 GHz 频段，分别提供可高达 11 Mbit/s 和 54 Mbit/s 的传输速率。

3 目的

本部分旨在当网络管理员和 IT 安全主管遇到远程接入安全保护问题时提供指南。它提供各种远程接入类型和技术的信息，并帮助目标读者识别适当的措施来保护远程接入抵御已识别的威胁。

它也可能在用户打算从其家庭办公室或在旅途中远程访问他们的办公室时提供帮助。

4 综述

远程接入使得用户能够从本地计算机登录到远程计算机或计算机网络上，并且就像存在直接的局域网链接那样，使用这些远程资源（见图 1）。这里所使用的服务称为远程接入服务（RAS）。RAS 确保远程用户能够访问网络资源。

通常，在以下情形中使用 RAS：

- 链接固定的个人工作站（例如，使得员工能够在家远程办公）；
- 链接移动计算机（例如，支持员工在现场或商务外出时办公）；
- 链接整个局域网（例如，把远地或分支机构的本地网络连接到公司总部的局域网上）；
- 提供对远程计算机的管理访问（例如，用于远程维护）。

RAS 提供一种在如下场景中连接远程用户的简单方式：远程用户建立与主干网的连接，例如，使用调制解调器经由电话网络。只要需要，这种直接连接可能一直存在，并且能够看作是租用线路，仅在需要时才激活。当使用 DSL 或者其他适当技术时，该连接也可能是永久的。

重要提示：对企业的远程接入宜总是通过远程接入服务器来控制。直接拨号接入计算机意味着会有很多风险，因此宜避免使用。企业里的调制解调器只宜在限定的位置使用。

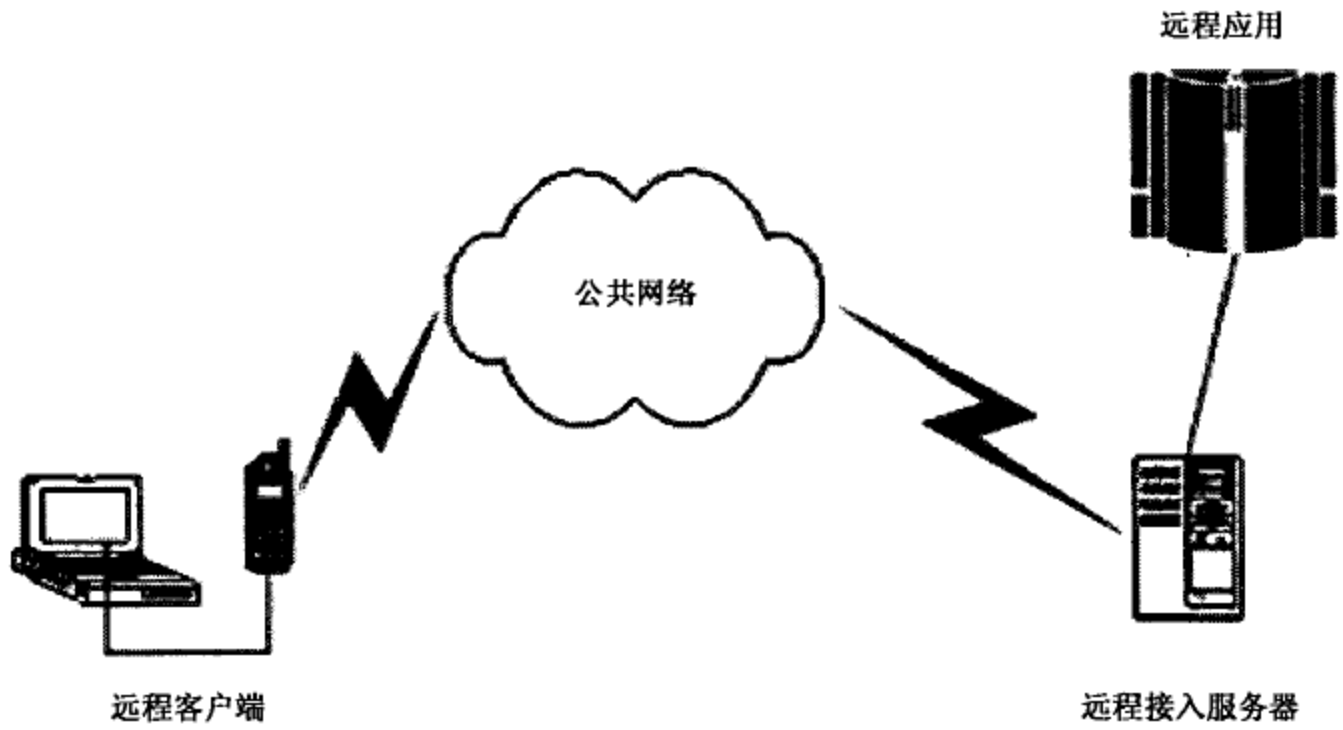

图 1 资源的远程接入

建立 RAS 连接通常需要以下三种组件：

a) 企业网络内的本地网络组件，它提供 RAS（即，已安装 RAS 软件）并且已经准备好接受 RAS 连接。这种组件称为 RAS 服务器或访问服务器。

b) 已安装 RAS 软件并发起 RAS 连接的远程计算机。这种组件称为 RAS 客户端。远程客户端可能是工作站或移动计算机。

c) 在其上建立 RAS 连接的通信介质。在大多数场景中，RAS 客户端使用电信网络建立连接。因此，其最低要求是一条电话线和一个相匹配的调制解调器。根据 RAS 的体系结构，在服务器端能够使用不同的连接技术。

RAS 是按照客户端/服务器体系结构实现的：当通过拨打已安装 RAS 服务器软件的计算机的电话

号码来请求公司的网络资源时，RAS 客户端可以配置成能自动建立 RAS 连接。

另一种方式是，用户能够手动发起 RAS 连接。一些操作系统也允许在系统登录后立即激活 RAS。客户端系统可以是任何一种计算机[例如膝上型计算机、个人数字助理(PDA)、智能电话]。

连接建立之后，客户端系统可以使用各种应用，其中一些可能有安全含义。

5 安全要求

从安全角度来看，RAS 服务器和 RAS 客户端被认为处于规定的安全策略的控制之下，而通信介质被认为在控制之外并且可能处于敌对的环境中。安全机制关注的风险是未授权的实体(例如个人或者过程)可能：

- 获得对 RAS 客户端的访问；
- 获得对 RAS 服务器的访问；
- 阻止对 RAS 服务器的访问(拒绝服务)；
- 窃听 RAS 客户端与 RAS 服务器之间交换的信息；
- 修改交换的信息。

对抗这些风险的安全服务包括保密性服务、鉴别服务和访问控制。因此，下列安全目标适用于 RAS 访问：

鉴别：远程用户必须由 RAS 系统唯一地识别。每次与本地网络建立连接时，必须通过鉴别机制确定用户的身份。在系统访问情况下，必须使用额外的控制机制，以确保远程用户的系统访问受到适当控制(例如，限制访问次数或只能访问得到允许的远程连接点)。

有多种在质量和技术上不同的鉴别用户和过程的方法。最常用但也是最脆弱的方法是使用口令。

访问控制：一旦远程用户已经被鉴别，远程接入服务器必须能够限制用户与网络的交互。为此要求，除了对远程用户的任何特定限制(例如特定的白天时间段、每个用户一个连接)外，还强制对远程用户实施由已授权管理员针对本地网络资源规定的授权和限制。

通信安全：在远程接入的本地资源所在之处，用户数据也必须在已建立的 RAS 连接上传输。通常，适用于本地网络的有关通信保护(保密性、完整性、真实性)的安全要求，对于在 RAS 连接上传输的数据也必须是可实现的。

然而，RAS 通信的保护尤为关键，因为可以使用许多通信介质和协议来进行 RAS 通信，且一般不能假定这些通信处于本地网络操作人员的控制之下。

可用性：当远程接入用于主流业务活动时，RAS 访问的可用性尤其重要。如果 RAS 访问彻底失败或连接带宽不足，业务过程的通畅性可能受到削弱。通过使用替代的或冗余的 RAS 连接，可以将这种风险降低到一定程度。这种方式尤其适用于以互联网作为通信介质的情况，因为互联网对连接和带宽一般都没有保证。

RAS 系统的客户端/服务器体系结构，意味着 RAS 客户端和 RAS 服务器都会因为操作环境的类型和使用方式，而面临特定的风险。

RAS 客户端不必是固定的(例如家庭 PC)，但也可能是移动设备(例如膝上型计算机)。然而，客户端的位置通常不处于局域网操作人员的控制下，所以，必须假定这种环境是不安全的并且暴露于特定威胁，对移动客户端尤其如此。这里特别需要考虑的威胁包括物理威胁，诸如窃取或损坏。

RAS 服务器通常是远程用户希望登录的局域网的一部分。它们处于局域网操作人员的控制下，并因此能被本地适用的安全措施覆盖。因为 RAS 服务器的主要任务是确保只有得到授权的用户才能访问已连接的局域网，所以，RAS 服务器面临的威胁宜被看作属于以未授权访问该局域网为目的的攻击范畴。

6 远程访问连接类型

客户端与远程局域网中的计算机建立连接有多种方式：

- 直接拨号接入到访问服务器；
- 拨号接入到互联网服务提供商(ISP)的访问服务器，并且通过互联网访问远程局域网；
- 通过到另一个网络的永久连接实现非拨号接入。

图 2 示出这些远程连接类型。移动用户 2 通过 ISP 和互联网接入局域网，并由控制互联网与本地网络之间访问的防火墙过滤。移动用户 1 也可能是一个无线局域网(WLAN)用户，因此这里的 RAS 称作接入点(AP)。这种访问服务器也由防火墙控制(虚线)。

注：移动用户可使用拨号、租用线路、宽带或无线连接。

所谓“WLAN 热点”的情形描述为移动用户 2 通过 WLAN 接入点而非本地调制解调器接入。即，一般的互联网接入是经由 WLAN AP 和 ISP 来提供。

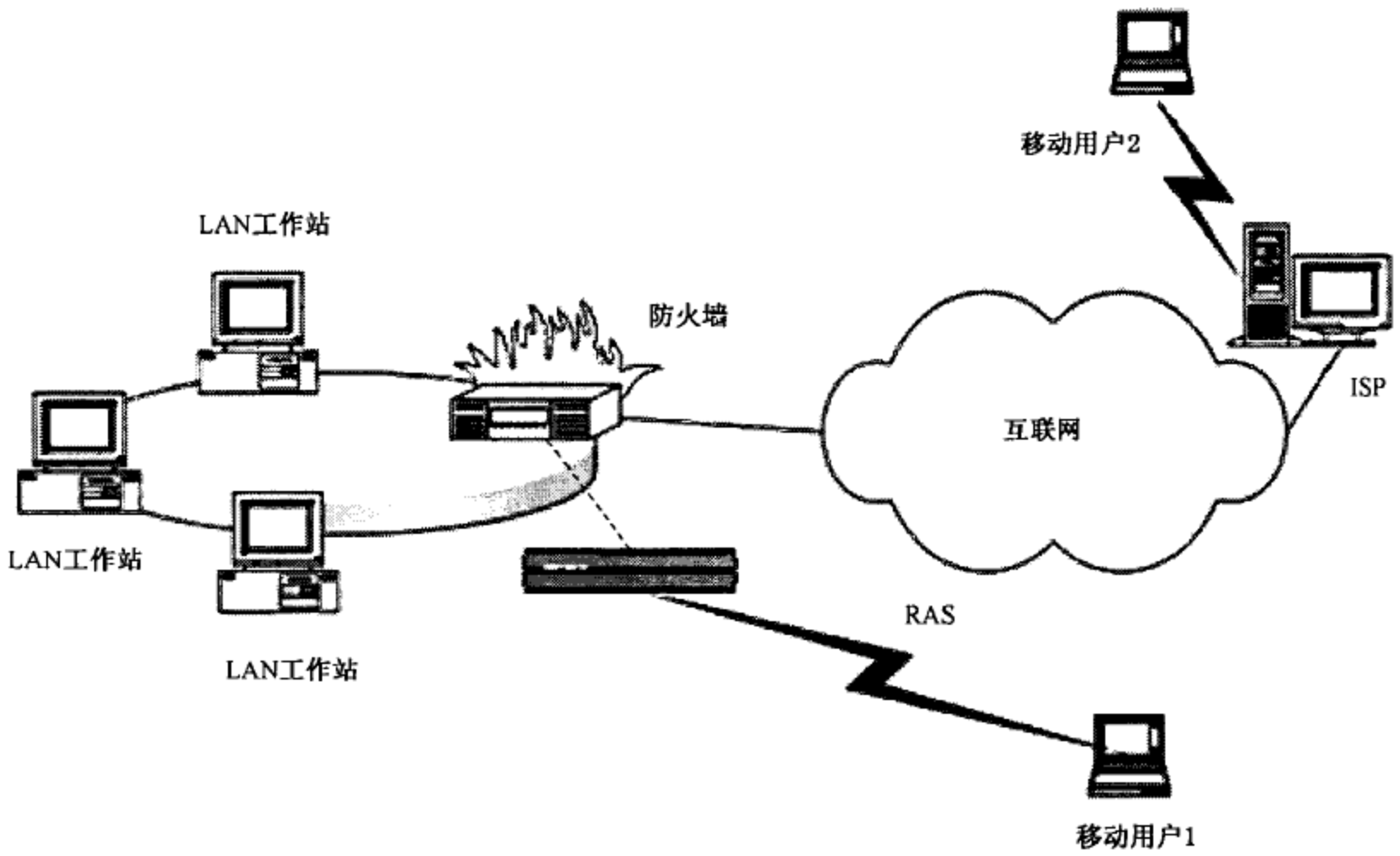

图 2 远程接入的类型

客户端可使用多种方法连接到 ISP。客户端可使用有线和/或无线技术。取决于所使用的方法，可能会发生额外的风险，例如，为了维持保密性，WLAN 要求应用特定的安全措施。

这些方法具有特定的优缺点，须加以考虑。例如，直接拨号接入方法旨在确保只有那些知道拨号号码的授权用户可以远程接入网络。但是，用于扫描可访问的拨号号码的工具(War Dialer)有助于黑客识别正在主动等待进入呼叫的现有调制解调器。对远程用户来说，互联网拨号接入具有按呼叫接入的优点。用户可通过访问本地 ISP 来连接到远程 LAN。但是，这种连接方法可能要求更为复杂和昂贵的服务器设置和配置。

7 远程访问连接技术

7.1 概述

远程接入只宜遵循“需要知晓”的原则来提供。因此，企业必须确定哪些用户应从外部世界访问哪些系统和哪些应用。远程接入的类型宜按照远程使用的服务来定义。

7.2 通信服务器的访问

7.2.1 一般通讯保护

所提供的最常见的访问是对企业内部通信服务的访问，亦即对用户的电子邮件账户、FTP 服务器或 Web 服务器的访问。附录 D 提供有关对安全邮件服务器的实现和操作的核查表，附录 E 在安全地设置和管理 Web 服务器方面提供帮助。

有多种方式来保护服务器与客户端之间的通信，因而提供真实性、保密性和完整性服务，诸如：

a) 安全套接层协议(SSL)提供一种鉴别通信双方(鉴别客户端和服务器)并对双方之间的信息交换进行加密的方法。所有互联网浏览器和 Web 服务器以及几乎所有的操作系统都支持 SSL。互联网工程任务组(IETF)基于 SSL 开发了传输层安全协议(TLS)，将其作为保护客户端/服务器通信的互联网标准(RFC 2246)。

b) IPsec(互联网协议安全)提供鉴别通信双方以及保护所传输信息的方式。IPsec 还提供处理密钥管理问题的功能(见 RFC 2401)。

c) 安全壳(SSH)是在不安全的网络上进行安全的远程登录和其他安全的网络服务的协议。当成功地鉴别了远程用户后，SSH 建立起安全的通信链接，并且提供一系列命令和服务(例如，安全的文件传输)。

这些方法提供安全的鉴别、保密性和完整性服务，宜附加到通信软件中使用。由于 SSL 事实上是普遍可用的互联网浏览器的一部分，因此，在访问用户的电子邮件账户之前建立 SSL 连接，可以容易地保护 Web 邮件访问。

这些方法之间的主要区别在于，事实上 SSL/TLS 和 IPsec 通常作为下层的通信功能来提供，因而是一种安全网络服务，而 SSH 是一种安全应用。

这些技术也适用于将 FTP 客户端连接到 FTP 服务器，因而允许访问存储在 FTP 服务器上的数据。

注：很多互联网协议，例如，提供终端访问能力的 telnet 或允许文件传输的 FTP，只实现弱鉴别机制，并且一般以明文形式发送口令信息。通过诸如 SSH、SSL/TLS 或 IPsec 之类安全协议在这些互联网协议中形成隧道，不仅提供保密性，还提供对鉴别过程的实质性改进。

注意：很多 Web 服务器只利用 SSL/TLS 提供服务器对用户的鉴别，反之要求用户验证服务器证书则不行。

7.2.2 电子邮件保护

虽然电子邮件是一种通常不为其消息发送提供保密性的服务，但是需满足特定前提条件才允许从外部访问邮件服务器。访问电子邮件服务器的一种常见方式是为邮件账户提供 Web 界面，这就允许用户在旅途中访问他们的电子邮件。这种方法只要求带有浏览器的计算机，即这种方法可在任何可用的计算机上使用。另一方面，这种方法的目的不是让用户下载其邮件和离线答复。

其他方法允许用户使用其标准的电子邮件客户端，但是鉴于电子邮件协议的概念，仍不提供足够的保密性和隐私保护。通常，电子邮件客户端通过以明文鉴别其自身和后面的用户来访问邮局(即，管理所有进入的电子邮件账户的公共程序)。目前使用的两个邮件访问协议(POP3 和 IMAP4)之间的主要区别在于所接收电子邮件的处理方式上：

- POP3 下载所有可用的新电子邮件，且用户能在本地对其进行处理；
- IMAP4 允许用户只下载邮件标题，然后再决定将哪些邮件下载到本地机器。

事实上，由于这些协议均不能独自提供足够的安全机制，强鉴别和传输保密性需额外提供(例如，SSL、SSH)。

注：用户也可以保护电子邮件内容(这不包括发送方地址、接收方地址和主题行)。两个主要的规范是 PGP(良好隐私保护)和 S/MIME(安全多用途互联网邮件扩展)，两者均提供保密性、完整性、真实性和发送方抗抵赖服务。两者均能适当地集成到很多电子邮件客户端程序中。由于发送方地址和接收方地址是以明文传送，所以两者均不能抵御通信流分析。

远程用户可访问的电子邮件服务器宜置于网络的非军事区(DMZ)中。DMZ 的任务就是通过隔离出一些能被内外网络直接访问的计算机，来分隔出内部网络和外部网络。将电子邮件服务器安放在 DMZ 中，意味着这台机器既可从外部网络访问，也可从内部网络访问。为了避免这种做法对内部网络产生风险，需采取一定的措施。

通常，宜避免经由 DMZ 建立外部网络计算机和内部网络计算机之间的在线连接。可以通过配置各自的网关和相应的中间计算机或者使用提供这种隔离的计算机群达到这个目的。

适当的配置需要注意以下问题：

- 邮件服务器应只安装运行特定的应用和最小的操作系统，以避免有可能被滥用作攻击的中间机器。
- 来自外部网络的访问应限定在严格规定的应用上（通过 IP 地址和端口号识别）。
- 来自内部网络的访问也应通过为源地址（内部网络中允许访问的那些计算机）以及目的地址所规定的地址和端口来加以限制。此外，信息流的方向应加以限制。这能够通过路由器或防火墙来实现。

其他通信服务器，诸如 Web 服务器，也可以被置于 DMZ 内，并得到相应的保护。表 1 提供一些在 DMZ 中安放电子邮件服务器时可考虑的端口号和协议。

表 1　电子邮件和相关端口号

端口号	协议名称	描　　述
22	SSH	安全壳登录
25	SMTP	具有 TLS/SSL 能力的常规 SMTP 端口
465	SMTPS	TLS/SSL 上的 SMTP
143	IMAP	常规 IMAP 端口
993	IMAPS	TLS/SSL 上的 IMAP
110	POP3	常规 POP3 端口
995	POP3S	TLS/SSL 上的 POP3

图 3 示出路由器位于互联网一方和位于内部网络一方所要求的不同配置。在这种情况下，从外部对邮件服务器的访问，只允许经由 TLS/SSL 上的 IMAP 和 TLS/SSL 上的 POP 进行，而发送电子邮件可使用常规的 SMTP 来完成。来自内部网络的访问，允许使用没有 TLS/SSL 额外保护的 IMAP 或 POP。这些命令是一种伪命令语言，描述边界防火墙和内部路由器所要求的访问列表命令。通过定义，其他任何端口都被禁止，以避免与其他端口和协议相关的弱点。

可应用额外的防范措施来避免 SMTP 邮件服务器的滥用（例如，限制 SMTP 连接以避免不速之客的电子邮件）。

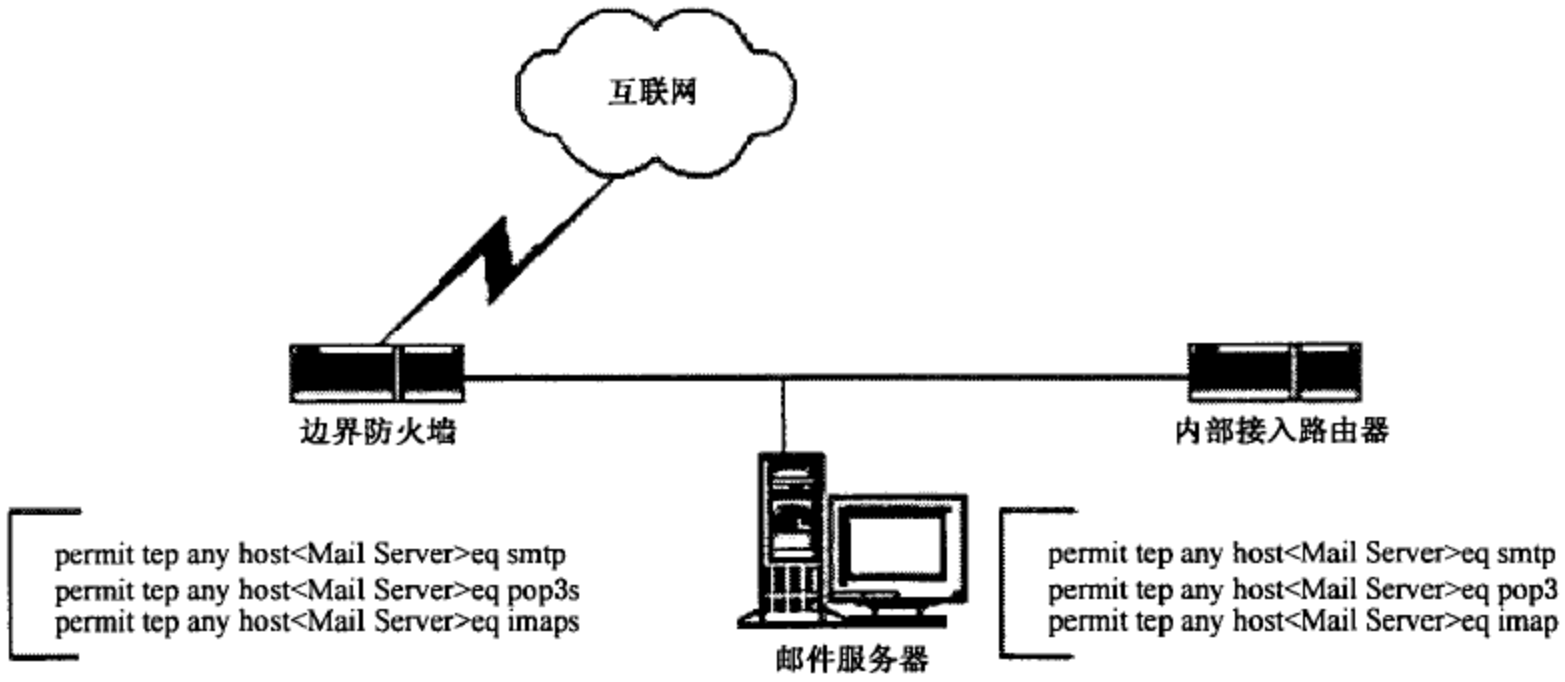

图 3　对 DMZ 内邮件服务器的访问

7.2.3　FTP 连接保护

文件传输协议（FTP）是另一种服务，其服务器可置于 DMZ 内。FTP 指定两种操作模式：

- PORT 模式(也称作正常或主动模式);
- PASV 模式(也称作被动模式)。

这两种模式的区别在于数据通道的建立方式:在 PASV 模式中,命令通道和数据通道由访问 FTP 服务器的 FTP 客户端建立;在 PORT 模式中,FTP 客户端打开命令通道,FTP 服务器在接受该客户端请求时作为回应打开数据通道。指定 FTP 使用端口 21 来构建命令通道;数据通道端口在一定范围内动态分配,通常从端口 1024 开始直至端口 5000。

当为远程客户端提供 FTP 能力时,从大体上说,PORT 模式允许更安全地设置包过滤防火墙。只需向内打开 TCP 端口 21 来建立客户端发起的命令通道。然后向外打开随后的数据通道建立。图 4 示出对包含 FTP 服务器的 DMZ 的适当过滤。

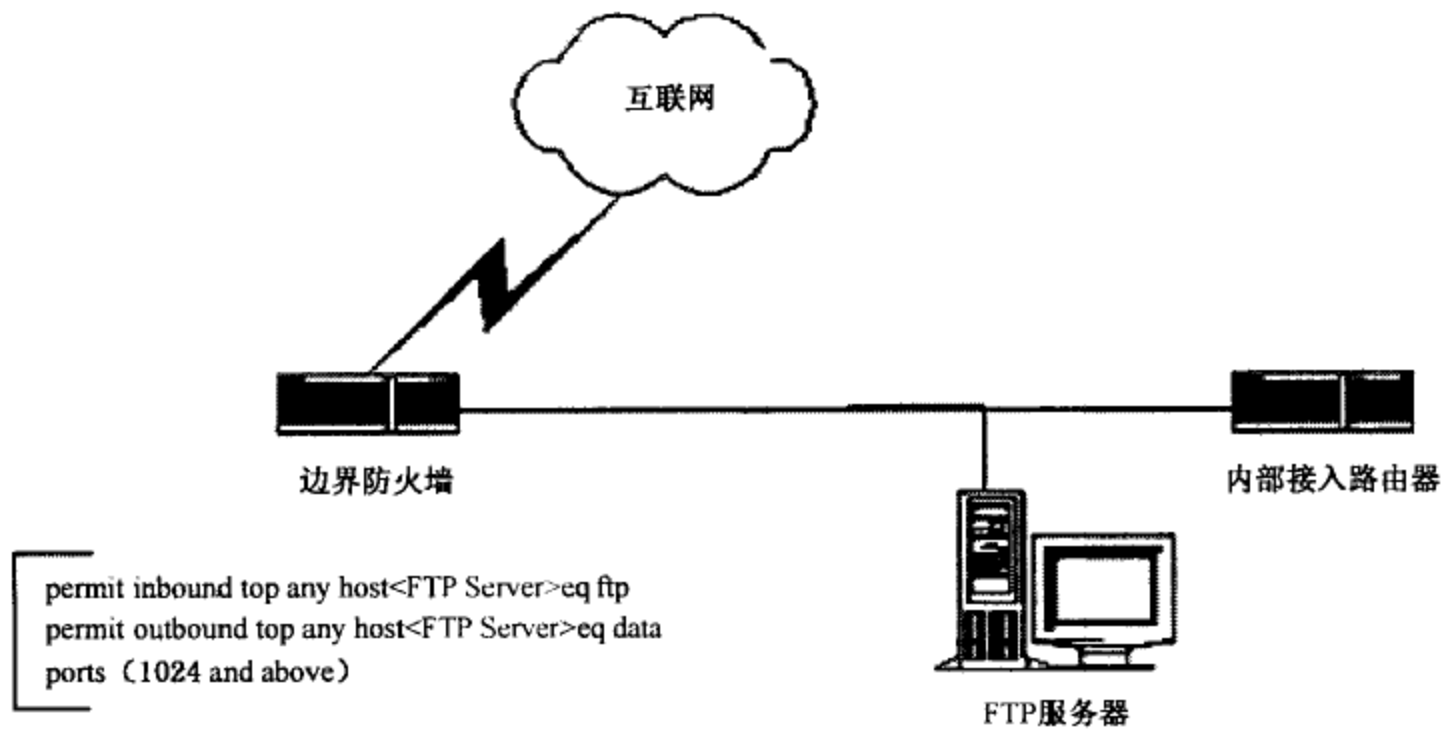

图 4　对 DMZ 内 FTP 服务器的访问

相比之下,使用 PASV 模式连接来实现 FTP 服务器时,要求简单防火墙为进入连接打开从端口 1024 开始的很多端口。这样的设置对防火墙自身隐含很大风险。

遗憾的是,PORT 模式不能与防火墙上的网络地址转换结合使用,因为其数据通道是单独建立的。PASV 模式克服了这个限制,因为所有的通道均由客户端系统发起。实施更复杂的防火墙技术能解决因打开很多端口所隐含的风险。提供状态检测技术的防火墙,允许经请求临时打开进入端口,从而在不要求开启很多入站端口的情况下,允许提供 PASV 模式的 FTP 服务。在防火墙中使用专门的 FTP 代理组件,也能得到同样结果。

当考虑为远程客户端提供 FTP 能力时,重要的是要意识到 FTP 协议本身只提供非常基本的安全措施。FTP 协议不支持保密性,所提供的鉴别服务级别是非常基本的。例如,口令用明文传输,这样做容易遭受重放攻击。

因此,只要可能,FTP 服务的实施宜结合下面安全层的隧道协议(例如 TLS/SLS)或者改进的文件传输应用,比如安全 FTP 或 scp(安全副本),两者均基于 SSH 协议。这两类变体都允许实施强鉴别及提供保密性服务。

7.3　局域网资源的访问

这种访问要求建立机器和特定系统配置。由于远程用户访问网络内的资源对该网络形成高风险,因此,远程接入需满足如下要求。

鉴别:强鉴别机制或双因子鉴别需确保远程用户的身份得到验证。

授权:鉴别成功之后,远程用户获得允许其按规定开展工作的授权。用户以这种方式履行特定的远程用户角色。

访问控制:在访问资源或数据之前,对照远程用户的授权检查其访问。

保密性、真实性和完整性:根据所使用的资源和数据,通信安全需通过提供保密性、真实性和完整性

服务来建立。

这些要求由包括适当鉴别机制的安全隧道协议(与用于虚拟专用网的协议相同)予以满足。更多细节在 GB/T 25068.5 中讨论。

针对远程用户的适当鉴别机制有,例如,一次性口令(OTP)令牌,用户每次访问时输入其个人识别号码(PIN)后便提供一个唯一的口令。这样的令牌提供双因子鉴别,用户需拥有令牌并知道适当的 PIN。

授权可按特定角色建立,特定角色可指派给远程用户组。一个组应获得为完成其正在远程执行的任务所需的授权。以这种方式能够容易地实现远程用户的受限访问。

访问控制可由各自使用的操作系统提供的机制所支持的策略来实施。例如:用户账户策略可定义所要求的权限和限制。操作系统也可为远程用户提供专门制定的组策略。

最常用的协议集与远程拨号接入用户鉴别服务(RADIUS)一起提供。这些协议,最初只是针对远程拨号访问开发的,能够对网络访问进行集中鉴别、授权和计费,并且得到 VPN 和强鉴别机制的支持。这些协议的工作原理如下:

RADIUS 客户端(典型的是接入服务器,诸如拨号接入服务器、VPN 服务器或无线接入点)以 RADIUS 消息的形式,向 RADIUS 服务器发送用户凭证和连接参数信息。RADIUS 服务器对 RADIUS 客户端提出的请求进行鉴别和授权,然后回送一个 RADIUS 应答消息。RADIUS 客户端还向 RADIUS 服务器发送 RADIUS 计费信息。此外,RADIUS 标准支持使用 RADIUS 代理。RADIUS 代理是一台计算机,它在 RADIUS 客户端与 RADIUS 服务器之间,也可能经由其他 RADIUS 代理,来转发 RADIUS 消息。RADIUS 消息从不在访问客户端与访问服务器之间传送。

RADIUS 消息作为用户数据报协议(UDP)消息来发送;UDP 端口 1812 用于 RADIUS 鉴别消息,而 UDP 端口 1813 用于 RADIUS 计费消息。仅有一条 RADIUS 消息包含在 RADIUS 包的 UDP 载荷中。

RFC2865 定义以下 RADIUS 消息类型:

- **Access-Request**:由 RADIUS 客户端发出,对网络访问连接尝试请求鉴别和授权。
- **Access-Accept**:由 RADIUS 服务器发出,以响应 Access-Request 消息。这个消息通知 RADIUS 客户端,该连接尝试已被鉴别和授权。
- **Access-Reject**:由 RADIUS 服务器发出,以响应 Access-Request 消息。这个消息通知 RADIUS 客户端,该连接尝试已被拒绝。如果凭证不真实或连接尝试没有得到授权,RADIUS 服务器就发送该消息。
- **Access-Challenge**:由 RADIUS 服务器发出,以响应 Access-Request 消息。这个消息对要求响应的 RADIUS 客户端是一个挑战。

附录 B 对在微软 Windows 2000 环境中实施和部署 RADIUS 提供支持。

7.4 用于维护的访问

这种类型的远程接入为系统管理员在需要远程管理系统时建立连接而提供。由于此类用户通常拥有对系统的最高访问权限,所以访问需以最安全的方式建立。此外,所进行的任何远程活动均需载入日志以备日后审计,尤其当系统管理外包给服务提供商时。

因此,宜只对需要远程管理的特定计算机提供访问,如下措施是需要的:

- 应只对限定机器上的特定账户提供访问;
- 远程用户与被管理机器之间的通信应使用 SSH 之类工具予以保护;
- 需使用强鉴别机制鉴别用户;
- 允许其远程管理系统的每个用户,都需以适当的机制和规程进行培训;
- 任何动作都应载入日志;
- 执行远程管理后,宜立即审计日志;如果是在上班时间外进行的维护活动,宜在第一时间审计。

回叫机制(需要额外的防范措施,见 8.2)是选项。遵循上述这些要求会限制此类远程接入中所隐含的风险。

8 选择和配置指南

8.1 概述

下面章条将讨论为抵御已识别的威胁所要求的措施。将详细解释所提出的每种措施并指出其优缺点。编写结构是分别介绍 RAS 客户端、RAS 服务器和 RAS 通信这三个领域。综合措施将在最后讨论。

在此,建议不要把对客户端和服务器的威胁截然分开考虑,因为,假如危及 RAS 客户端安全,那么将自动危及 RAS 服务器安全。此外,宜注意,例如在 Windows 环境中,每一个 RAS 客户端也能作为 RAS 服务器使用。因此,应用于 RAS 服务器的威胁同样可应用于 RAS 客户端。

8.2 RAS 客户端的保护

8.2.1 固定 RAS 客户端

固定的客户端可首先被物理保护,即,可将其放置在只有已授权人员才可进入的房间。这种方法可能适合于使用家庭办公室的远程上下班者。

固定的 RAS 客户端可使用电话调制解调器、电缆调制解调器或 DSL 连接来与 RAS 服务器相连。第二种和第三种连接类型要求对永久连接互联网的宽带连接采取额外措施。一种简单的方法就是安装并正确配置所谓的“个人防火墙”,来限制外部对所连接计算机的访问。

8.2.2 所有 RAS 客户端

对所有的 RAS 客户端而言,有几个适用的安全级别来避免计算机的滥用和保护远程连接的安全。

要建立的第一道屏障是计算机硬件本身。保护计算机和避免滥用的一个简单方法是设置引导口令,在引导系统之前强制执行用户识别。该屏障是潜在攻击者的第一个障碍,但它未提供足够的保护。

第二道屏障是操作系统。对于便携式计算机和工作站,宜使用那种具备用户识别和鉴别能力的操作系统。大多数的操作系统提供这种特点。使用的账户宜是普通用户账户而非管理员账户。因为管理员账户具有更多的权限,所以宜只用于管理计算机。还要记住,宜强制使用高质量的口令[1)]。

如果一台计算机存储了对公司很有价值的信息,宜对其采取额外措施:

操作系统宜得到加固,以提供比现成配置更高的安全性。这意味着宜删除操作系统中所有不必要的组件,且只安装需要的应用。此外,对像网络配置这样的特点加以限制,只允许提供该特定系统需要的服务。

强鉴别能够使用智能卡、令牌卡或生物特征[2)]机制来实施。强鉴别(也称作多因子或双因子鉴别)要求用户至少完成两种识别方式[3)]。

硬盘加密防止其中存储的信息泄露。这种保密性服务需使用强算法(见 ISO/IEC 18033-3:2005)

另外一个重要的配置问题是调制解调器的配置。客户端调制解调器的设置方式需考虑一般不接受呼入。因此,需由客户端用户发起连接。

在很多情况下,如果个人防火墙配置正确,可提高安全性。

最后,为避免和限制由恶意代码造成的损害,需安装抗病毒程序并定期更新。

8.3 RAS 服务器的保护

8.3.1 物理和逻辑设置

RAS 服务器的物理安全必须得到保护。通常,RAS 服务器是企业服务器基础设施的一部分,宜具

---

1) 有关口令管理的更多信息见 GB/T 22081。

2) 生物特征指基于人类物理或行为特征来鉴别人。

3) 鉴别通常要求用户提供一些他们知道的(口令)、他们拥有的(令牌卡或智能卡)、他们自身的(生物特征)或者他们的组合,以便提供他们身份的证据。

有与其他服务器相同的物理安全。像其他任何外部服务一样，RAS 服务器宜置于 DMZ 内。这包括将其锁藏在服务器房间中以防止未授权物理接触，以及使用 UPS 以防止断电。所要求的其他措施包括 RAS 服务器的安全设置和配置、安全管理和备份以及恢复规程。

虽然最常见类型的 RAS 服务器仍提供使用电话线或 ISDN 的调制解调器接入，但同时还有其他可用的解决方案，例如，拨号接入企业控制范围之外的本地服务供应商 RAS，进一步的接入由互联网提供，并受企业边界（防火墙系统）的控制和限制。

这种方法的优点是成本低（拨号接入通常是本地呼叫），缺点是客户端需经过两次识别：第一次在 ISP，第二次在远程位置。

8.3.2 RAS 服务器和调制解调器

对于提供调制解调器接入的 RAS 服务器，宜采取若干措施，以确保使用调制解调器不会给基础设施带来额外风险。

计算机的配置宜满足提供 RAS 服务的要求，并且宜忽略所有其他服务。这意味着操作系统被加固，并对其应用所有相关的升级程序和补丁。只允许管理员和维护人员物理接触服务器。不宜为其设置普通用户账户。

如果 RAS 服务器还提供其他的服务，那么需对其进行测试和验证，以确保这些服务组合不引入新的风险。可由软件供应商提供明确的 RAS 配置支持。

还要考虑的其他重要问题包括：数据备份、日志信息收集、日志向管理站点传送（包括其日常评价）以及应急计划编制。

在主动提供远程接入服务之前，应针对已知脆弱性来测试服务器。这些测试应包括本地配置和网络渗透测试。

调制解调器应配置为单向被动工作，在这种情况下，允许呼入。如果可能，该配置应允许在调制解调器上鉴别，然后发起对某个预存号码的回叫（也称为回拨）。这种回叫只在固定客户端或经由移动电话连接的膝上型计算机上执行。这就确保只连接已知的地址（电话号码）并允许限制呼叫实体的开销。

现代电话设备（例如 PBX）提供类似呼叫路由重选的特点，它可直接呼叫非预约的号码。因此，回叫机制需要补充额外的防范措施。

建议客户端的设置中务必安装抗病毒程序，并定期更新。

8.3.3 网络访问服务器

如果远程接入设置为拨号接入到本地互联网服务提供商（ISP），那么，对网络的访问需由网络访问服务器（NAS）控制。对 ISP 的访问将不受企业的直接控制，那里的任何鉴别结果也将不为企业所知。

NAS 必须像任何其他网络设备那样受到保护，即，需将其锁藏起来，只由得到授权的管理员物理接触。设备的管理宜与本地策略一致：如果是网络管理系统在监视其活动，那么管理系统与 NAS 之间的通信流需限制在本地网络之内或以隧道方式隐藏其信息类型。

NAS 是本地企业网络与外部世界之间的一种网关，因此宜适用 GB/T 25068.3 中提出的机制。

8.3.4 无线接入点

尽管无线局域网的接入点（AP）不是典型的远程接入场景，但可用它来提供对网络的接入。因此，像其他无线技术的接入点一样，这样的 AP 宜放置于 DMZ 内从而得到保护。有关无线安全的更多信息见 8.5。

8.4 连接的保护

8.4.1 概述

RAS 客户端与 RAS 服务器之间的连接经过几个阶段。首先是建立连接，然后是操作该连接，用后终止该连接。所有这些通信阶段都要求保护。

下面分别集中讨论保护 RAS 客户端与服务器之间通信连接安全的各个步骤。

8.4.2 连接建立

安全连接的建立要求鉴别远程用户。该鉴别在用于远程接入的协议[4]设置完成后进行。

有不同的用户鉴别方式,它们的安全性也不同。下面提到的前两个协议是在客户端(称为对等端)与服务器(鉴别者)之间使用,第三个协议使用鉴别服务器,它允许包含额外的鉴别方案。

最常见的鉴别方案使用口令鉴别协议(PAP)。PAP 是一种两次握手协议,按照这种方案,鉴别者(服务器)接收对等端(客户端)的凭证,并基于这些凭证决定是否允许访问。这些凭证用明文传送,通常包含用户 ID 和口令。因此该协议不提供抵御重放攻击的保护。

挑战—握手鉴别协议(CHAP)是一种更好的鉴别方案。CHAP 是一种 3 次握手协议,按照这种方案,鉴别者向对等端发送一个"challenge(挑战)"。这个挑战是唯一的,每次发送的挑战都必须改变。对等端根据自己的 ID 参数(称为"秘密")和"challenge"计算出一个散列值来应答。鉴别者将自己的计算值与该结果进行比较并决定是否允许访问。所传送的凭证使用散列算法(通常使用 MD5)加密。由于挑战不可预测,所以 CHAP 抵御重放攻击。

7.3 中介绍的远程拨号接入用户鉴别服务(RADIUS)提供一种更一般的鉴别方法。

RADIUS 服务器通常集中存储用户的 ID 参数,即,它保存远程用户的共享秘密。如果用户想要访问网络中的系统,它就向 RADIUS 服务器发送一个"访问请求",其中包含用户 ID、口令、该用户访问的系统 ID 和系统端口。口令以加密的方式掩蔽呈现。RADIUS 服务器或者响应该请求,或者将其转发给另一个 RADIUS 服务器。如果 RADIUS 服务器响应该请求,它将首先验证所传输的数据是有效的。一个有效的标识至少包括用户 ID 和口令,还可能包括系统地址和系统提供的端口。如果请求被转发到另一个 RADIUS 服务器,那么最初被寻址的 RADIUS 服务器就成为客户端。在这些方法中可能要强制进行附加鉴别,例如,UNIX 鉴别、Windows 2000 鉴别或 NOVELL 鉴别。RADIUS 服务器也可使用鉴别方案 PAP 和 CHAP。

所要使用的其他强鉴别可能包括使用数字证书或使用令牌的鉴别。在这些方法中,鉴别不仅依赖于用户所知的东西,还依赖于是否拥有令牌或证书,所以称作双因子鉴别。生物特征鉴别也可能包含在内。

注:较早的网络服务"终端访问控制器访问控制系统(TACACS)"以及由它演化而来的 XTACACS 和 TACACS+ 现在仍存在,但是它们的重要性不及 RADIUS。

8.4.3 通信加密

窃听威胁大多用加密与之对抗。链接加密是把通信限制在拥有适当加密设备的设施上进行。内容加密更灵活,并且允许与未提供加密的服务器连接。它也提供仅在各自加密端点之间的保密性。

内容加密的一个实例是使用类似"良好隐私(PGP)"的软件,这种软件包提供基于公钥密码技术的加密,因此也允许抗抵赖和真实性之类的服务。

重要提示:使用加密程序时,要确保使用的密钥足够长。此外,要制定规程并按照这些规程,对通过电子邮件收到的公钥证书,在引入和使用它们之前,对它们的真实性和有效性进行验证。

对远程接入来说,足以保护通信内容的方式是通过使用虚拟专用网(VPN)来提供的。有许多可用的产品提供这种保护。要确保 VPN 只使用标准化的协议。关于这个主题的指南在 GB/T 25068.5 中给出。

8.5 无线安全

无线协议可在远程接入范围内的不同场景中使用:

- 诸如蓝牙之类的协议用于将移动电话、调制解调器或宽带访问部件本地连接到远程接入客户端系统;
- 无线局域网协议(诸如由 GB 15629.11—2003 系列标准定义的协议)可用于将远程接入客户端

4) 对调制解调器访问而言,早期使用的协议是串行线互联网协议(SLIP),它只允许简单鉴别;现在的点对点协议(PPP)提供更可靠的协议和更有效的鉴别。

系统连接到公共或专用网络。

在大多数场景中，提供远程接入能力的组织，对于所涉及的无线通信协议的配置或设置，没有影响或只有非常有限的影响：

例如，使用机场提供的公共无线局域网访问设施（称为热点），移动用户可连接到远程接入客户端系统。该例中的无线接入基础设施通常是由 ISP 运营，而用户或其组织对配置问题没有任何影响。

尽管无线协议提供一些安全性服务，但是在远程接入范围内各种场景的环境中，不能依赖于这些安全性服务。

因此，如果允许无线协议与实现远程接入能力相结合，就需要通过使用在 8.3 中介绍的更高等级协议的能力，来实现所要求的诸如鉴别或保密性之类的所有安全性服务。常用的方法是使用诸如 IPsec 或 SSL/TLS 之类的隧道协议来提供强鉴别和保密性。

在组织能配置无线接入基础设施的情形下，要求额外的技术措施来保护接入点。目前有三种基本方法来保护对 AP 的访问；这些方法已被纳入到几个 GB 15629.11—2003 协议中。

- 服务集标识符（SSID）；
- 介质访问控制（MAC）地址过滤；
- 有线等效隐私（WEP）或者 WiFi 保护接入（WPA）。

即使这三种方法一起使用，也不能为组织提供充分的安全性。

SSID 提供一种机制，可把无线网络分割成由一个或多个 AP 提供服务的多个网络。每个接入点都带有制造商默认的指出该 AP 制造商的 SSID，以及其他可能与各自 AP 相关的信息。因此宜把 SSID 改变成内部的、不容易猜测的 SSID，而且这种 SSID 既不提供有关本组织运营该 AP 的信息，也不提供该设备自身的信息。对 AP 的最低安全要求是禁止广播其 SSID。否则，任何正在接听的设备都能记录该 SSID，并且能通过呼叫正确的 SSID 来尝试连接到该 AP。因此，强烈建议这些 AP 按照禁止广播模式来配置，尽管还有其他方式来记录未被广播的 SSID。

SSID 标识 AP，而 MAC 地址标识计算机的网络接口。每个网络接口卡都有唯一的 MAC 地址。为增强无线局域网的安全性，如果可能，AP 宜使用有效客户端计算机的 MAC 地址对其加以标识[5)]。尽管可能发生 MAC 地址欺骗，但是，使用 MAC 地址将增加一些对无线局域网访问的保护。

众所周知，WEP 有一些根本的脆弱性，它们影响保密性、完整性和真实性。但是，它为通信提供使用 40 比特或 104 比特的共享密钥加密。这种密钥加上一个 24 比特的初始化向量，形成长度为 64 或 128 比特的密钥。鉴于这些协议的已知弱点，宜频繁改变 WEP 密钥，以增强安全性。WPA（WEP 的后继者）如果通过提供临时共享密钥进行正确配置，就可以克服这些弱点。

此外，建议使用动态主机配置协议（DHCP）或静态地址；DHCP 协议由具有“客户端预留”特点（即，计算机的 MAC 地址与规定的 IP 地址绑定）的 AP 提供。

在使用不可路由 IP 地址的情况下，要把内部 IP 子网地址（通常是 192.168.0.0）改变为另一个子网地址。此外，禁止对 WAP 和无线路由器的无线管理访问，以避免被攻击者修改。

最后，定期评价无线局域网的状态。

附录 F 中提供关于无线局域网安全的详细核查表。

8.6 组织措施

组织措施宜包括远程接入策略，它定义用户、管理员和安全人员的不同角色。相关人员的责任也需定义。关于适当的网络策略的更多信息（包括远程接入）在 GB/T 25068.1 中给出。附录 A 提供远程接入策略的一个实例。

对于一些移动装置（例如 PDA、智能电话），实现充分的技术防范措施可能是不可行的；因此可能需要额外的组织措施来对抗风险。

---

5) 在大的无线环境或某些操作情形中，基于 MAC 地址过滤来限制访问可能是不可行的。

组织措施所涉及到的其他主题包括:应急计划、备份、灾难恢复、人员培训、用户意识和用户培训。

关于这些主题的更多信息参见 ISO/IEC 13335 和 GB/T 22081—2008。

8.7 法律考量

远程接入技术的实施宜考虑任何适用的国内法律法规限制或要求,特别是国家加密标准的使用规定。

实施者宜确保远程接入部署具备足够的合同和其他法律规定,以确保万一发生意外时的追索权。

9 结论

远程接入要求有周密策划的方法,从适当的安全策略着手并且涵盖技术方法以及组织和法律方法。

附 录 A
（资料性附录）
远程接入安全策略示例

A.1 目的

本附录的目的是规定从任意主机连接到<公司名称>网络的标准。这些标准的设计是为了尽量减少因未授权使用<公司名称>资源而可能导致<公司名称>承受的损失。这些损失包括：丢失敏感数据或公司保密数据、知识产权，损害公众形象，破坏<公司名称>的关键内部系统等。

A.2 范围

本附录适用于所有使用<公司名称>拥有的或个人拥有的计算机或工作站连接到<公司名称>网络的<公司名称>雇员、承包商、供应商和代理商。本策略适用于为<公司名称>工作而使用的远程访问连接，包括阅读或发送电子邮件、查看内网上的 Web 资源。

本附录所涉及的远程接入实施包括(但不限于)：拨号接入调制解调器、帧中继、ISDN、DSL、VPN、SSH 和电缆调制解调器等。

A.3 策略

A.3.1 概述

a) 对<公司名称>的公司网络拥有远程接入权限的<公司名称>雇员、承包商、供应商和代理商，有责任确保把他们的远程访问连接作为用户与<公司名称>的现场连接一样来对待。

b) 对于享有固定费率服务的雇员，允许其直系家庭成员使用个人计算机通过<公司名称>网络对互联网进行一般的娱乐性访问。<公司名称>雇员有责任确保其家庭成员不违反<公司名称>的任何策略，不从事违法活动，不利用这种访问谋求外部商业利益。<公司名称>雇员要为滥用访问造成的后果承担责任。

c) 关于通过远程接入方法访问公司网络时保护信息的细节以及<公司名称>网络的可接受使用，请见以下策略：

   1) 可接受加密策略；
   2) 虚拟专用网(VPN)策略；
   3) 无线通信策略；
   4) 可接受使用策略。

d) 关于<公司名称>远程访问连接选项的更多信息，包括如何订购或取消连接服务、成本对比、故障诊断与排除等，要到“远程接入服务(RAS)”网站了解。

A.3.2 要求

a) 必须严格控制安全远程接入。这种控制将通过一次性口令鉴别或使用强口令短语的公钥/私钥来强制执行。关于创建强口令短语的信息，见“口令策略”。

b) <公司名称>任何雇员在任何时候都不宜将其登录口令或电子邮件口令透露给任何人，甚至包括其家庭成员。

c) 拥有远程接入权限的<公司名称>雇员和承包商必须确保其远程连接到<公司名称>网络的<公司名称>拥有的或个人的计算机或工作站，不同时连接到其他网络上，处于该用户完全控制之下的个人网络除外。

d) 拥有远程接入<公司名称>网络权限的<公司名称>雇员和承包商绝对不能使用非<公司名

称>的电子邮件账户(即,Hotmail、Yahoo、AOL)或其他外部资源进行<公司名称>的业务活动,从而确保公事从不与私事混淆。

e) 为接入<公司名称>网络而配置的 ISDN 专线路由器必须满足 CHAP 的最低鉴别要求。

f) 任何时候都不允许为了分割隧道或双归宿而重新配置家庭用户设备。

g) 帧中继必须满足 DLCI 标准的最低鉴别要求。

h) 非标准的硬件配置必须得到“远程接入服务”的认可,并且必须由 InfoSec 认可对硬件接入的安全配置。

i) 通过远程接入技术连接到<公司名称>各个内部网络的所有主机,必须使用最新的抗病毒软件(这里填写公司软件网站的 URL),上述主机包括个人计算机。第三方的连接必须符合“第三方协议”中规定的要求。

j) 用于连接到<公司名称>网络的个人设备必须满足<公司名称>拥有的设备进行远程接入的要求。

k) 希望对<公司名称>生产网络实施非标准远程接入方案的组织或个人,必须先得到“远程接入服务”和 InfoSec 的认可。

A.4 强制执行

任何雇员,一经发现违反本策略,都可能受到纪律处分,直至终止雇佣关系。

A.5 术语和定义

术 语	定 义
电缆调制解调器	电缆公司,诸如 AT&T 宽带,通过电缆提供互联网访问。
TV 同轴电缆	电缆调制解调器使用同轴电缆,能以高于 1.5Mbps 的速率从互联网接收数据。目前,电缆只在某些区域可用。
挑战—握手鉴别协议(CHAP)	挑战—握手鉴别协议是一种使用单向散列函数的鉴别方法。
数据链路连接标识符(DLCI)	数据链路连接标识符(DLCI)是帧中继网络中分配给永久虚电路(PVC)端点的唯一编号。DLCI 识别帧中继网络中用户访问通道内一个特定 PVC 端点,且只对此通道有局部意义。
拨号调制解调器	一种通过电话线将计算机彼此相连以发送通信信息的外部设备。调制解调器将计算机的数字信号调制成模拟信号以在电话线上发送,然后解调回数字信号以被另一端的计算机读取。因此,“调制解调器”这个名字是指调制器/解调器。
双宿	一台计算机或网络设备同时连接到一个以上的网络。这样的例子包括:在经由本地以太网连接登录到公司网络的同时,拨号进入 AOL 或其他互联网服务提供商(ISP);在<公司名称>提供的远程接入家用网络上的同时,连接到另一个网络,诸如配偶的远程接入;配置一个依据包的不同目的地拨号进入<公司名称>网络或某 ISP 的 ISDN 路由器。
数字用户线(DSL)	数字用户线(DSL)是一种与电缆调制解调器竞争的高速互联网访问形式。DSL 使用标准电话线工作并支持高于 2 Mbps 的数据下行速率(至用户)和较慢的上行速率(至互联网)。
帧中继	帧中继是一种能从 ISDN 速率逐渐增加到 T1 线速率的通信方法。帧中继按照固定费率而不是使用次数来收费。帧中继通过电话公司网络连接。

综合业务数字网(ISDN)	有两种综合业务数字网或 ISDN:BRI 和 PRI。BRI 用于家庭办公室/远程接入。BRI 有两个 64 k 比特(合计 128 k 比特)“承载”通道和一个传输信号信息的 D 通道。
远程接入	通过非<公司名称>控制的网络、设备或介质,对<公司名称>公司网络的访问。
分割隧道	当经由 VPN 隧道连接到<公司名称>公司网络时,同时从远程设备(PC、PDA、WAP 电话等)直接访问一个非<公司名称>网络(诸如互联网或家庭网络)。虚拟专用网(VPN)是一种经由贯穿互联网的“隧道”访问远程网络的方法。

附 录 B
（资料性附录）
RADIUS 实施和部署的最佳实践

B.1 概述

本附录为在微软 Windows 2000 环境和操作系统中使用 RADIUS 提供建议。

为解决 RADIUS 安全问题，宜遵守以下实施和部署的最佳实践。

B.2 实施的最佳实践

实施 RADIUS 客户端、服务器或代理时，为解决 RADIUS 安全问题，使用以下最佳实践：为了给整个 RADIUS 消息提供数据保密性，使用 ESP 和诸如三重 DES 之类的加密算法实施 IPsec。

这种方法在 RFC 3162 中描述。通过使用 IPsec 协议给完整的 RADIUS 消息加密，来保护敏感的 RADIUS 字段（诸如 Access-Request 消息中的“Request Authenticator”字段）和属性（诸如“User-Password”、“Tunnel-Password”和“MPPE-Key”属性）免于被查看。攻击者在能够分析 RADIUS 消息内容之前，必须首先对 ESP 所保护的 RADIUS 消息进行解密。建议支持基于证书的 IPsec 鉴别，以防止攻击者发起对 RADIUS 服务器的在线攻击。

另外一种方案，或与 IPsec 的使用相结合，宜做到以下几点：

a） 允许配置和使用长度至少为 32 位十六进制数或至少 22 个键盘字符的共享秘密。

b） 实现所有的 Access-Request 消息均使用 Message-Authenticator 属性。

对于 RADIUS 客户端，实现所有的 Access-Request 消息均使用 Message-Authenticator 属性并允许其配置。对于 RADIUS 服务器或代理，实现所有的 Access-Request 消息均在需要时使用 Message-Authenticator 属性，并允许其配置。

c） 为请求鉴别者实现密码随机生成器。

在实施 RADIUS 时，为了给访问客户端鉴别提供附加保护，使用以下的最佳实践：

a） 使用强鉴别方法实现 EAP 和 EAP 类型。

EAP-TLS 是一个良好的强 EAP 方法实例。它要求访问客户端与 RADIUS 服务器交换证书。所有的 EAP 消息都要求 Message-Authenticator 属性，该属性对未用 IPsec 保护的 Access-Request 消息提供保护。

b） 使用相互鉴别来实现鉴别方法。

使用相互鉴别时，连接的两个端点均鉴别其对等端。如果其中一个鉴别失败，就拒绝该连接尝试。例如，EAP-TLS 和 MS-CHAP 第 2 版是相互鉴别的方法。使用 EAP-TLS 时，RADIUS 服务器验证访问客户端的用户证书，而访问客户端验证 RADIUS 服务器的计算机证书。使用 MS-CHAP 第 2 版时，访问客户端和访问服务器均提供所知的用户账户口令的证据。

c） 如果实施 PAP 鉴别，默认其为禁用。

例如，OTP/令牌卡使用 PAP 发送鉴别信息。如果必须实施 PAP，默认其为禁用，并实施长共享密钥和给请求鉴别者加密。因为 IEEE802.1X 不支持 PAP，该问题只适用于 PPP 连接。

d） 如果实施 CHAP 鉴别，使用强 CHAP 挑战。

CHAP 挑战类似于 RADIUS 的请求鉴别者，宜是随机的、加密的。

e） 如果实施 MS-CHAP 鉴别，则不支持 LAN 管理器对 MS-CHAP 挑战的应答或口令更改进行编码。

B.3 部署的最佳实践

在部署 RADIUS 解决方案时，为解决 RADIUS 安全问题，使用以下的部署最佳实践：为了给整个 RADIUS 消息提供数据保密性，配置 RADIUS 客户端和服务器，对所有的 RADIUS 通信流使用具有 ESP 的 IPsec，而 ESP 具有 3DES。

对于 RADIUS 通信流，具有 3DES 的 IPsec ESP 的配置，取决于 IPsec 的实施。例如，在活动目录服务域环境中，如果正使用 Windows 2000 路由和远程接入服务作为访问服务器，Windows 2000 IAS 作为 RADIUS 服务器，那么采用对所有进出 UDP 端口 1812 和 1813 的通信流使用 ESP 和 3DES 加密的规则，就能为适当的系统容器配置主动 IPsec 策略。更多信息见 Windows 2000 服务器帮助手册。

另外一种方案，或与 IPsec 的使用相结合，宜做到以下几点：

a) 使用强共享秘密，该秘密是长度至少为 32 个十六进制数的随机序列，或是长度至少为 22 个字符的大小写字母、数字、标点符号的随机序列。理想情况下，共享秘密宜由计算机生成。

b) 每个＜RADIUS 客户端，RADIUS 服务器＞对，使用不同的共享秘密。

c) 要求所有的 Access-Request 消息均使用 Message-Authenticator 属性。

将每个 RADIUS 客户端配置成发送所有 Access-Request 消息的 Message-Authenticator 属性。将每个 RADIUS 服务器配置成要求每个 RADIUS 客户端发送所有 Access-Request 消息的 Message-Authenticator 属性。

d) 所使用的 RADIUS 客户端、服务器和代理使用加密的强请求鉴别者。

在部署 RADIUS 时，为了给访问客户端鉴别提供附加保护，使用以下的最佳实践：

a) 如果不要求使用 PAP，访问服务器和 RADIUS 服务器均禁用 PAP。

对于安全连接，PAP 唯一可接受的用法是同时使用 OTP 和令牌卡鉴别，其口令在此处具有高熵且每次使用时都改变。然而，PAP 的启用允许配置错误的访问客户端与其访问服务器协商 PAP 并发送未保护的用户账号口令。更好的解决方案是对 OTP 和令牌卡鉴别使用 EAP 和 EAP 类型。

b) 如果要求使用 MS-CHAP，禁用 LAN 管理器编码。

如果正使用 Windows 2000 IAS，就在 IAS 服务器上将注册表键值 HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\RemoteAccess\Policy\Allow LM Authentication 设置为 0。

c) 使用具有强鉴别方法的 EAP 和 EAP 类型。

无线接入点的 IEEE802.1X 鉴别要求使用 EAP，使用 Message-Authenticator 属性来保护每个 Access-Request 消息，且不支持 PAP 鉴别。

d) 使用相互鉴别方法，诸如 EAP-TLS 或 MS-CHAP 第 2 版。

附 录 C
（资料性附录）
FTP 的两种模式

有两种 FTP 模式：

- PORT 模式 FTP；
- PASV 模式 FTP。

C.1 PORT 模式 FTP

PORT 模式是传统的 FTP 模式。PORT FTP 连接的事件序列如下：

a) FTP 客户端：打开随机应答的高端端口（就本例而言，假设是端口 TCP 6000 和 TCP 6001）。

b) FTP 客户端：从其 TCP 6000 端口向 FTP 服务器的 TCP 21 端口发送一个打开命令通道的请求。

c) FTP 服务器：从其 TCP 21 端口向 FTP 客户端的 TCP 6000 端口（命令通道链接）发送一个确认。命令通道在此时被建立。

d) FTP 客户端：向 FTP 服务器发送数据请求（PORT 命令）。FTP 客户端在 PORT 命令中包含它打开的用于接收数据的数据端口号。本例中，FTP 客户端已打开 TCP 6001 端口来接收数据。

e) FTP 服务器：在 FTP 客户端的 PORT 命令所指明的端口上，FTP 服务器打开一个到 FTP 客户端的“新”向内连接。例如，FTP 服务器源端口是 TCP 20 端口。本例中，FTP 服务器从自身拥有的 TCP 20 端口向 FTP 客户端的 TCP 6001 端口发送数据。

在此会话中建立了两个连接：由 FTP 客户端发起的向外连接和 FTP 服务器建立的向内连接。注意：PORT 命令（在命令通道上发送）中包含的信息存储在包的数据区。

C.2 PASV 模式 FTP

最常见的 FTP 实现是被动模式或 PASV 模式。在最常见的浏览器上，PASV 模式的 FTP 连接是默认的。PASV 模式的主要优点之一是服务器不需要创建到 FTP 客户端的新向内连接。稍后将看到，该优点使得 PASV 模式 FTP 对防火墙稍友好一些。

PASV 模式 FTP 的事件序列如下：

a) FTP 客户端：打开随机应答的高端端口（就本例而言，假设使用端口 TCP 6000 和 TCP 6001）。

b) FTP 客户端：从其 TCP 6000 端口向 FTP 服务器的 TCP 21 端口发送一个打开命令通道的请求。

c) FTP 服务器：从其 TCP 21 端口向 FTP 客户端的 TCP 6000 端口发送一个确认。命令通道在此时被建立。

d) FTP 客户端：发送 PASV 命令，请求 FTP 服务器打开一个 FTP 客户端能连接的端口号以建立数据通道。

e) FTP 服务器端：在命令通道上发送 FTP 客户端能发起连接的 TCP 端口号以建立数据通道。本例中，FTP 服务器打开端口 7000。

f) FTP 客户端：打开从自身拥有的应答端口 TCP 6001 至 FTP 服务器的数据通道 7000 的新连接。数据传送通过此通道发生。

注意：PASV 模式的 FTP 客户端发起所有的连接。FTP 服务器从不需要创建回到 FTP 客户端的新连接。

附 录 D
（资料性附录）
安全邮件服务核查表

下列核查表有助于规划、配置和操作邮件服务器。涉及的主题包括操作系统、邮件安全、内容过滤等。

D.1 邮件服务器操作系统核查表

完成	动 作
	规划邮件服务器的配置和部署
○	识别邮件服务器的功能
○	识别将通过邮件服务器存储、处理和传输的信息类别
○	识别信息的安全要求
○	识别用于运行邮件服务器的专用主机
○	识别邮件服务器所提供或支持的网络服务
○	识别邮件服务器的用户和用户类别，并确定每类用户的权限
○	识别邮件服务器的用户鉴别方法
	为邮件服务器选择适当的操作系统
○	使脆弱性的暴露最少化
○	有能力将管理活动或根级活动限制为只有授权用户才能进行
○	有能力拒绝对服务器信息的访问，而不是试图使其可用
○	有能力关闭可能被构建到操作系统或服务器软件中的不需要的网络服务
○	可接受的保险和债务成本（一些保险公司对某些操作系统收费更多）
○	拥有有经验的员工来安装、配置、保护和维护操作系统
	修补和升级操作系统
○	识别和安装操作系统的所有必要的补丁和升级程序
○	识别和安装与操作系统一同引入的应用和服务的所有必要的补丁和升级程序
	删除或关闭不必要的服务和应用
○	关闭或删除不必要的服务和应用
	配置操作系统用户鉴别
○	删除或关闭不需要的默认账户和组
○	关闭非交互式账户
○	为特定计算机创建用户组
○	为特定计算机创建用户账户
○	检查组织的口令策略，并适当地设置账户口令（例如长度、复杂性）
○	将计算机配置成在有限次登录尝试失败后拒绝登录
○	安装并配置其他安全机制以增强鉴别
	测试操作系统的安全性
○	初始安装后测试操作系统以确定脆弱性
○	定期（例如按季度）测试操作系统以确定新的脆弱性

D.2 邮件服务器与邮件内容安全核查表

完成	动　　作
	加固邮件服务器应用
○	将服务器软件安装在专用主机上
○	安装所需的最少互联网服务
○	应用所有补丁或升级程序来改正已知脆弱性
○	删除或关闭所有由邮件服务器应用安装的但并不需要的服务(例如基于 Web 的邮件、FTP、远程管理)
○	从服务器上删除所有供应商文档
○	对服务器应用适当的安全模板或加固脚本
○	重新配置 SMTP、POP 和 IMAP 服务标签(和所需的其他设置),不报告邮件服务器和操作系统的类型和版本
○	禁用危险或不必要的邮件命令(例如 VRFY 和 EXPN)
	配置操作系统和邮件服务器访问控制
○	限制邮件服务应用只访问计算资源的子集
○	通过由邮件服务器强制的附加访问控制来限制用户的访问,这要求更细粒度的访问控制等级
○	将邮件服务器应用配置成只在唯一的个人用户和组身份下执行并且其访问有限制性控制
○	确保邮件服务器不在超级或系统级权限或者管理员权限下运行
○	将主机操作系统配置成邮件服务器能写入日志文件但不能读取
○	将主机操作系统配置成邮件服务器应用创建的临时文件只限定在特定的、被适当保护的子目录中
○	将主机操作系统配置成对邮件服务器应用所创建的所有临时文件的访问仅限于创建这些文件的邮件服务器进程
○	确保邮件服务器不能在邮件服务器专用的特定文件结构之外保存文件
○	将邮件服务器配置成在 Linux 和 Unix 主机的 chroot“监牢”中运行
○	将用户邮箱安装在与操作系统和邮件服务器应用不同的硬盘或逻辑分区上
○	限制所允许的附件大小
○	确保日志文件存储在大小适当的位置
	应对恶意附件和内容
○	实施集中式病毒扫描器(在邮件网关、防火墙或邮件服务器上)
○	在所有客户端主机上安装病毒扫描器
○	每周或特定病毒爆发时,更新所有扫描器上的所有病毒数据库
○	就病毒的危害及如何把这些危害降低到最低限度来培训用户
○	爆发发生时通知用户
○	将内容过滤器配置成阻止可疑消息
○	将内容过滤器配置成阻止 UCE 消息
○	如要求,配置词法分析

表（续）

完成	动　　作
○	创建内容过滤策略
○	如要求，为电子邮件增添法律免责声明
○	将邮件服务器配置成阻止来自开放转发黑名单的邮件
○	如要求，将邮件服务器配置成阻止来自特定域的邮件
○	将被鉴别的邮件配置成依赖服务器
○	将邮件服务器配置成使用加密鉴别
○	将邮件服务器配置成支持只经由 SSL/TLS 且被认为是必要的 Web 访问

D.3　网络基础设施核查表

完成	动　　作
	网络位置
○	邮件服务器位于内部网络上并受邮件网关和/或防火墙保护，或邮件服务器位于 DMZ 内
	防火墙的配置
○	邮件服务器由防火墙保护
○	面临较大威胁或较脆弱的邮件服务器，由应用层防火墙保护
○	防火墙控制互联网与邮件服务器之间的所有通信流
○	如需要，防火墙阻止除 TCP 25 端口（SMTP）、TCP 110 端口（POP3）、TCP 143 端口（IMAP）、TCP 398 端口（LDAP）和 TCP 636 端口（安全 LDAP）外所有到邮件服务器的向内通信流
○	防火墙（与入侵检测系统相结合）阻止 IDS 报告正在攻击组织网络的 IP 地址或子网
○	防火墙使用适当的方法将可疑活动通知网络管理员或邮件服务器管理员
○	防火墙提供内容过滤（应用层防火墙）
○	配置防火墙以抵御 DoS 攻击
○	防火墙将关键事态记入日志
○	防火墙和防火墙操作系统被修补到最新或最安全级别
	入侵检测系统
○	配置 IDS 以监视所有防火墙或过滤路由器之前的网络通信流（基于网络的 IDS）
○	配置 IDS 以监视防火墙之后进出邮件服务器的网络通信流
○	配置 IDS 以监视对邮件服务器上关键文件的更改（基于主机的 IDS 或文件完整性检查器）
○	IDS（与防火墙相结合）阻止正在攻击组织网络的 IP 地址或子网
○	IDS 使用适当的方法将攻击通知网络管理员或邮件服务器管理员
○	配置 IDS 以检测端口扫描探测器
○	配置 IDS 以检测 DoS 攻击
○	配置 IDS 以将事态记入日志
○	频繁地（每周）用新的攻击特征码升级 IDS
○	配置 IDS 以监视邮件服务器主机上可用的系统资源（基于主机的 IDS）

表（续）

完成	动　　作
	网络交换机
○	在邮件服务器网段上使用网络交换机以抵御网络窃听
○	用高安全模式配置网络交换机以抵御 ARP 欺骗和 ARP 布毒攻击
○	配置网络交换机以将网段上所有通信流发送给 IDS 主机(基于网络的 IDS)

D.4　邮件客户端安全核查表

完成	动　　作
	修补和升级邮件客户端
○	将电子邮件客户端升级到最安全版本
○	对电子邮件客户端应用所有必需的补丁
○	对浏览器应用所有必需的补丁[针对与浏览器(例如 Outlook 和 Netscape)集成在一起的电子邮件客户端]
	邮件客户端安全
○	确保操作系统升级到最安全补丁级别
○	将操作系统配置成只允许适当用户访问本地存储的消息和邮件客户端配置文件
○	保护或删除 Windows 脚本主机(只限于 Windows 主机)
○	将与 Windows 脚本主机相关联文件的默认动作由执行改为编辑(只限于 Windows 主机)
○	确保将操作系统配置为显示全部文件扩展名(只限于 Windows 主机)
○	确保操作系统强制实施最小权限的概念,因为恶意代码在其被启动的安全环境下运行(即用户访问级别)
○	确保操作系统的关键组件免受恶意代码攻击
○	使用文件加密系统来保护本地存储在用户硬盘上的邮件(对膝上型计算机特别重要)
○	配置客户端操作系统,使其在固定休止期后自动锁定

D.5　邮件服务器的安全管理核查表

完成	动　　作
	日志的记录
○	记录 IP 栈设置错误
○	记录解析器配置问题(例如 DNS、NIS、WINS)
○	记录邮件服务器配置错误(例如,与 DNS 不匹配、本地配置错误、别名数据库过时)
○	记录不当的文件和目录许可,不安全的符号链接和硬链接
○	记录过时的别名数据库
○	记录欠缺的系统资源(例如磁盘空间、内存、CPU)
○	记录别名数据库重建
○	记录(成功的和失败的)登录

表（续）

完成	动　　作
○	记录安全问题(例如垃圾邮件)
○	记录丢失的通信(网络问题)
○	记录协议失败
○	记录连接超时
○	记录连接拒绝
○	记录 VRFY 和 EXPN 命令的使用
○	记录代表发送
○	记录代理发送
○	记录下载
○	记录异常的地址
○	记录消息的收集统计
○	记录错误消息的创建
○	记录交付失败(永久性错误)
○	记录被延迟的消息(暂时性错误)
○	在分离(Syslog)的主机上存储日志
○	根据组织要求将日志归档
○	每天评审日志
○	每周评审日志(用于分析较长期的趋势)
○	使用自动日志文件分析工具
	邮件服务器备份
○	创建邮件服务器备份策略
○	每天至每周对邮件服务器进行增量备份
○	每周至每月对邮件服务器进行完全备份
○	定期将备份归档
	从受损中恢复
○	查阅组织的安全策略(这一点宜优先于此处提供的其他建议)
○	断开一个(或多个)受损系统与网络的连接,或设法容忍攻击以便能够收集更多证据
○	调查其他“相似”主机以确定攻击者是否也损害了其他系统
○	适当时咨询管理层、法律顾问和执法部门(如果需要起诉,立即联系执法部门)
○	分析入侵
○	恢复系统
○	重新将系统连接到网络
○	测试系统以确保安全性
○	监视系统和网络是否有征兆表明,攻击者正企图再次访问系统或网络
○	记录经验教训

附 录 E
（资料性附录）
安全 Web 服务核查表

下列核查表的目的是支持安全 Web 服务器的规划、安装和操作。

E.1 Web 服务器操作系统核查表

完成	动 作
	规划 Web 服务器配置和部署
○	识别 Web 服务器的功能
○	识别将通过 Web 服务器存储、处理和传输的信息类别
○	识别信息的安全要求
○	识别如何将信息发布到 Web 服务器
○	识别运行 Web 服务器的专用主机
○	识别将由 Web 服务器提供或支持的网络服务
○	识别 Web 服务器的用户和用户类别，并确定每类用户的权限
○	识别 Web 服务器的用户鉴别方法
	为 Web 服务器选择适当的操作系统
○	使脆弱性的暴露最少化
○	有能力将管理活动或超级权限活动限制为只有授权用户才能进行
○	有能力拒绝对服务器信息的访问，而不是试图使其可用
○	有能力关闭可能被构建到操作系统或服务器软件中的不需要的网络服务
○	可接受保险和债务的成本（一些保险公司对某些操作系统收费更多）
○	拥有有经验的员工来安装、配置、保护和维护操作系统
	修补和升级操作系统
○	识别和安装操作系统的所有必要的补丁和升级程序
○	识别和安装与操作系统一同引入的应用和服务的所有必要的补丁和升级程序
	删除或关闭不必要的服务和应用
○	删除或关闭不必要的服务和应用
	配置操作系统用户鉴别
○	删除或关闭不需要的默认账户和组
○	关闭非交互式账户
○	为特定计算机创建用户组
○	为特定计算机创建用户账户
○	检查组织的口令策略，并适当地设置账户口令（例如长度、复杂性）
○	将计算机配置成在有限次登录尝试失败后拒绝登录
○	安装并配置其他安全机制以增强鉴别
	测试操作系统的安全性
○	初次安装后测试操作系统以确定脆弱性
○	定期（例如按季度）测试操作系统以确定新的脆弱性

E.2 安全 Web 服务器安装与配置核查表

完成	动　　作
	安全地安装 Web 服务器
○	在专用主机上安装服务器软件
○	安装所需的最少互联网服务
○	应用所有补丁和升级程序来改正已知的脆弱性
○	为 Web 内容创建专用物理盘或逻辑分区(与操作系统和服务器应用分隔开)
○	删除或关闭所有由 Web 服务器应用安装的但不需要的服务(例如 gopher、FTP、远程管理)
○	删除所有示例文档、脚本和可执行代码
○	从服务器上删除所有供应商文档
○	对服务器应用适当的安全模板或加固脚本
○	重新配置 HTTP 服务标签(和所需的其他设置),不报告 Web 服务器和操作系统的类型和版本
	配置 Web 服务器主机操作系统访问控制
○	配置成 Web 内容文件能被 Web 服务进程读取但不能写入
○	配置成 Web 服务进程不能写入保存公共 Web 内容的目录
○	配置成只有得到授权的 Web 服务器管理进程能写入 Web 内容文件
○	配置成 Web 应用能写入 Web 服务器日志文件,但日志文件不能被 Web 服务器应用读取
○	配置成 Web 服务器应用仅限于在特定的、受到适当保护的子目录中创建临时文件
○	配置成对邮件服务器应用所创建的任何临时文件的访问仅限于创建这些文件的 Web 服务进程
○	在与操作系统和 Web 应用不同的硬盘或逻辑分区上安装 Web 内容
○	配置成在允许上载到 Web 服务器时,对专用于上载的硬盘空间大小加以限制
○	配置成日志文件被存储在大小适当的位置
	配置安全的 Web 内容目录
○	专门给 Web 内容一个硬盘或逻辑分区,并建立仅与 Web 服务器内容文件(包括图形但不包括脚本和其他程序)相关的子目录
○	对于作为 Web 服务器内容的一部分被执行的所有外部脚本或程序(例如 CGI、ASP),专门定义一个目录
○	关闭不是专门在管理账户控制下的脚本的执行。该动作通过创建和控制用于包含授权脚本的一个分开目录的访问来完成
○	为计算机创建用户组
○	关闭硬链接或符号链接(又称作 Windows 的快捷方式)的使用
○	定义一个完整的 Web 内容访问矩阵。识别 Web 服务器文档内的哪些文件夹和文件是受限的和哪些是可访问的(被哪些用户)
○	检查组织的口令策略,并适当地设置账户口令(例如长度、复杂性)
○	适当时使用 robots.txt 文件
	使用文件完整性检查器
○	安装文件完整性检查器以保护 Web 服务器配置文件、口令文件和 Web 内容
○	每当升级或内容改变时,更新文件完整性校验和
○	在受保护的一次性写入介质上保存校验和
○	定期比较校验和

E.3 Web 内容核查表

完成	动　　作
	确保任何以下类型的信息都无法在公共 Web 服务器上或经由公共 Web 服务器得到
○	涉密的或敏感的记录
○	内部人事规则和规程
○	保密的或专有的信息
○	调查记录
○	财务记录(已公开提供的记录除外)
○	组织的物理规程和信息安全规程
○	有关组织网络和信息系统基础设施的信息
○	无所有者书面许可的版权资料
○	标明所采取的安全措施类型的隐私保护或安全策略
	为许可的公共 Web 内容建立组织级的文件化正规策略和过程
○	识别宜在 Web 上发布的信息
○	识别目标读者
○	识别因发布信息而可能造成的负面分歧
○	识别哪些人宜负责创建和发布这些特定信息
○	提供适合 Web 出版的风格和格式指南
○	对信息的敏感性和发放/发布控制(包括聚合信息的敏感性)提供适当评审
○	确定适当的访问及安全控制
○	对 Web 内容源代码内所包含的信息提供指南
	Web 用户隐私的考量
○	已发布的隐私策略
○	未经用户明确许可,禁止收集能识别个人的数据
○	禁止使用“持久的”cookie
○	在已发布的隐私保护策略中清晰标识会话 cookie 的使用(如果使用的话)
	客户端主动内容的安全考量
○	仅在绝对需要时才使用
○	若无用户明确许可,不得采取任何行动
○	不得使用高风险的客户端主动内容
○	如果可能,提供替代方案(例如与 PDF 文件一起提供的纯文本)
	服务器端主动内容的安全考量
○	简单、易于理解的代码
○	受限或不可读写文件
○	受限或不可与其他程序交互(例如 sendmail)
○	不要求具有 suid 权限的运行

表（续）

完成	动　　作
○	使用明确的路径名称(即不依赖于路径变量)
○	没有同时具有写入和执行许可的目录
○	所有可执行文件均被放在专门的文件夹中
○	SSL 是关闭的
○	所有的用户输入均被验证
○	动态创建的页面不生成危险的元字符
○	字符集编码宜在每个页面被明确设置
○	宜根据给定的编码方案,扫描用户数据中是否有表示特殊字符的字节序列
○	宜检验 Cookie 中是否有任何特殊字符
○	使用加密机制给以脚本形式输入的口令加密
○	对于被用户名和口令限制的 Web 应用,如果没有经过适当的登录过程,不宜访问应用中的任何 Web 页面
○	删除所有示例脚本
○	在未验证源代码的情况下,任何第三方脚本或可执行代码均不得使用

E.4　Web 鉴别和加密核查表

完成	动　　作
	Web 鉴别和加密技术
○	对于要求最低保护且有明确规定的少量读者的 Web 资源,配置基于地址的鉴别
○	对于要求附加保护但有明确规定的少量读者的 Web 资源,配置基于地址的鉴别作为第二道防线
○	对于要求最低保护但无明确规定的读者的 Web 资源,配置基本鉴别或摘要鉴别(较好)
○	对于要求抵御恶意 bot 的 Web 资源,配置基本鉴别或摘要鉴别(较好)
○	对于要求最高保护的 Web 资源,配置 SSL/TLS
	配置 SSL/TLS
○	对要求最低鉴别但要求加密的配置,使用自签名证书
○	对要求服务器鉴别和加密的配置,使用第三方颁发的证书
○	对要求客户端中级鉴别的配置,将服务器配置成要求经由 SSL/TLS 的用户名和口令
○	对要求客户端高级鉴别的配置,将服务器配置成要求经由 SSL/TLS 的客户端证书
○	对要求中级加密的组织,使用 DES
○	对要求高级加密的组织,使用 RC4(高级)或 3DES(最高级)
○	配置文件完整性检查器以监视 Web 服务器证书
○	如果 Web 服务器上只使用 SSL/TLS,确保经由 TCP 80 端口的访问是关闭的
○	如果到 Web 服务器的大部分通信流将经由加密的 SSL/TLS,确保在 Web 服务器上使用适当的日志记录和检测机制(因为网络监视对加密的 SSL/TLS 会话是无效的)

E.5 网络基础设施核查表

完成	动　　作
	网络位置
○	Web 服务器置于 DMZ 内或外包给适当保护防火墙的组织
○	DMZ 不放置在防火墙的第三个(或更多)接口上
	防火墙配置
○	Web 服务器由防火墙保护
○	面临较大威胁或较脆弱的 Web 服务器,由应用层防火墙保护
○	防火墙控制互联网与 Web 服务器之间的所有通信流
○	防火墙阻止除 TCP 80 端口(HTTP)和/或 TCP 443 端口(HTTPS)之外所有到 Web 服务器的向内通信流
○	防火墙(与 IDS 相结合)阻止 IDS 报告正在攻击组织网络的 IP 地址或子网
○	防火墙通过适当的方法将可疑活动通知网络管理员或 Web 管理员
○	防火墙提供内容过滤
○	配置防火墙以抵御服务攻击
○	防火墙检测异常的或已知的 URL 请求攻击
○	防火墙将关键事态记入日志
○	防火墙和防火墙操作系统修补到最新或最安全等级
	入侵监测系统(IDS)
○	基于主机的 IDS,用于主要运行 SSL/TLS 的 Web 服务器
○	配置 IDS 以监视任何防火墙或过滤路由器之前的网络通信流(基于网络的 IDS)
○	配置 IDS 以监视防火墙之后进出 Web 服务器的网络通信流
○	配置 IDS 以监视 Web 服务器上关键文件的更改(基于主机的 IDS 或文件完整性检查器)
○	IDS(与防火墙相结合)阻止正在攻击组织网络的 IP 地址或子网
○	IDS 通过适当的方法将攻击通知网络管理员或 Web 管理员
○	配置 IDS 以检测端口扫描探测
○	配置 IDS 以检测 DoS
○	配置 IDS 以检测异常的 URL 请求
○	配置 IDS 以将事态记入日志
○	频繁地(每周)用新的攻击特征码升级 IDS
○	配置 IDS 以监视 Web 服务器主机上可用的系统资源(基于主机的 IDS)
	网络交换机
○	在 Web 服务器网段上使用网络交换机以抵御网络窃听
○	用高安全模式配置网络交换机以防范 ARP 欺骗和 ARP 布毒攻击
○	配置网络交换机以将网段上所有通信流发送给 IDS 主机(基于网络的 IDS)

E.6 安全 Web 服务器管理核查表

完成	动　　作
	日志记录
○	使用组合日志格式来存储传输日志,或人工配置用组合日志格式描述的信息使之成为传输日志的标准格式
○	如果组合日志格式不可用,启用来源日志或代理日志
○	为不同的虚拟 Web 站点建立不同的日志文件名,这些虚拟 Web 站点可能作为单独的物理 Web 服务器的一部分而实现
○	使用 RFC 1413 中规范的远程用户身份
○	在分离的(syslog)主机上存储日志
○	按照组织要求将日志归档
○	每天评审日志
○	每周评审日志(用于分析较长期的趋势)
○	使用自动日志文件分析工具
	Web 服务器备份
○	创建 Web 服务器备份策略
○	每天至每周对 Web 服务器进行增量备份
○	每周至每月对 Web 服务器进行完全备份
○	定期将备份归档
○	维护 Web 站点的授权副本
	从受损中恢复
○	查阅组织的安全策略(这一点宜优先于此处提供的其他建议)
○	断开受损系统与网络的连接,或设法容忍攻击以便能收集更多证据
○	调查其他“相似”主机以确定攻击者是否也损害了其他系统
○	适当时咨询管理层、法律顾问和执法部门(如果需要起诉,立即联系执法部门)
○	分析入侵
○	恢复系统
○	重新将系统连接到网络
○	测试系统以确保安全性
○	监视系统和网络是否有征兆表明,攻击者正企图再次访问系统或网络
○	记录经验教训
	安全测试
○	定期对 Web 服务器和支撑网络进行脆弱性扫描
○	测试之前更新脆弱性扫描器
○	改正被脆弱性扫描器识别的任何缺陷
	远程管理和内容更新
○	使用强鉴别机制(例如公/私钥对、双因子鉴别)

表（续）

完成	动　　作
○	对于能通过 IP 地址对 Web 服务器的内容进行远程管理和更新的主机以及到内部网络的主机予以限制
○	使用安全协议(例如安全壳、HTTPS)
○	强制执行远程管理和内容更新的最少权限概念(即试图使远程管理/更新账户的访问权限最少)
○	更改来自远程管理工具或应用的所有默认账户或口令
○	不允许从互联网上穿越防火墙进行远程管理
○	禁止在内部网络上设置来自 Web 服务器的任何文件共享，反之亦然

附 录 F
（资料性附录）
无线局域网安全核查表

完成	动 作
○	针对无线技术的使用制定组织安全策略
○	确保网络用户受到计算机安全意识的充分培训
○	执行风险评估以了解需要保护的组织资产价值
○	确保客户端网络接口卡(NIC)和 IP 支持固件的升级，以便在安全补丁可用时加以部署(在购买之前)
○	定期进行全面的安全评估(包括验证在 GB 15629.11 无线局域网中不存在流氓 AP)，以充分了解无线网络的安全态势
○	确保在组织的建筑物或建筑群的周边具有外部边界保护
○	完成站点调查以测量和建立组织的 AP 覆盖
○	获得所有的 AP 和 GB 15629.11 无线设备的完整清单
○	实证测试 AP 范围边界以确定准确的无线覆盖范围
○	确保 AP 通道中至少有 5 个通道与其他任何相邻的无线网络不同，以避免干扰
○	将 AP 置于建筑物内部而不是靠近外墙和窗户
○	将 AP 置于安全区域以防止未授权的物理接触和用户操纵
○	确保 AP 在未被使用的所有时间内是关闭的
○	确保 AP 的复位功能仅在需要时被使用，且只被授权组成员调用
○	使用复位功能时，将 AP 恢复到最新的安全设置
○	将 AP 中的默认 SSID 更改为不容易猜测的值
○	关闭“广播 SSID”特性使得客户端的 SSID 必须与 AP 的 SSID 相匹配
○	确认 SSID 字符串不反映组织的名称(部、科和街道等)或产品
○	禁用 AP 的广播信标
○	了解并确保所有默认参数均被更改
○	禁用 AP 上所有不安全且非基本的管理协议
○	启用无线局域网产品的所有安全特性，包括密码鉴别和 WEP/WPA 的隐私特性
○	确保加密密钥的长度至少是 128 比特或尽可能长
○	确保默认共享的密钥定期被更安全的唯一密钥替换
○	在有线基础设施和无线网络之间，安装适当配置的防火墙(AP 或连接多个 AP 的集线器)
○	在所有无线客户端上安装抗病毒和个人防火墙软件
○	部署 MAC 访问控制列表
○	部署用于无线通信的基于 IPsec 的虚拟专用网(VPN)技术
○	确保所使用的加密在给定网络数据的敏感性和计算机的处理器速度下尽可能地强大
○	确保所有的 AP 都有强壮的管理口令并且所有口令均被定期更改

表（续）

完成	动　　作
○	确保 GB 15629.11 的“特设模式(adhoc mode)”被关闭
○	如果可能，在网络上使用静态 IP 寻址
○	使用具有“客户端保留”特性的 DHCP
○	对于 AP 的管理接口，启用用户鉴别机制
○	确保目的地为 AP 的管理通信流在专用有线子网上

参 考 文 献

[1] ISO/IEC TR 13335-4:2000 Information technology—Guidelines for the management of IT Security—Part 4:Selection of safeguards

[2] ISO/IEC TR 13335-5:2001 Information technology—Guidelines for the management of IT Security—Part 5:Management guidance on network security

[3] GB/T 22081—2008 信息技术 安全技术 信息安全管理实用规则(ISO/IEC 27002:2005, IDT)

[4] ISO/IEC 18033-3 Information technology—Security techniques—Encryption algorithms—Part 3:Block ciphersl

[5] NIST Special Publication 800-44:2002 Guidelines on Securing Public Web Servers

[6] NIST Special Publication 800-45:2002 Guidelines on Electronic Mail Security

[7] NIST Special Publication 800-46:2002 Security for Telecommuting and Broadband Communications

[8] NIST Special Publication 800-48:2002 Wireless Network Security:802.11,Bluetooth,and Handheld Devices

[9] IETF RFC 768 User Datagram Protocol(1980)

[10] IETF RFC 821 Simple Mail Transfer Protocol(1982)

[11] IETF RFC 959 File Transfer Protocol(1985)

[12] IETF RFC 1055 Nonstandard for transmission of IP datagrams over serial lines:SLIP(1988)

[13] IETF RFC 1334 PPP Authentication Protocol(1992)

[14] IETF RFC 1413 Identification Protocol(1993)

[15] IETF RFC 1939 Post Office Protocol—Version 3(1996)

[16] IETF RFC 1991 PGP Message Exchange Formats(1996)

[17] IETF RFC 1994 PPP Challenge Handshake Authentication Protocol(CHAP)(1996)

[18] IETF RFC 2045 to IETF RFC 2049 Multipurpose Internet Mail Extensions(MIME)(1996)

[19] IETF RFC 2060 Internet Message Access Protocol—Version 4rev1(1996)

[20] IETF RFC 2131 Dynamic Host Configuration Protocol(1997)

[21] IETF RFC 2139 RADIUS Accounting(1997)

[22] IETF RFC 2246 The TLS Protocol Version 1.0(1999)

[23] IETF RFC 2284 PPP Extensible Authentication Protocol(EAP)(1998)

[24] IETF RFC 2401 Security Architecture for the Internet Protocol(1998)

[25] IETF RFC 2406 IP Encapsulating Security Payload(ESP)(1998)

[26] IETF RFC 2440 OpenPGP Message Format(1998)

[27] IETF RFC 2631 Diffie-Hellman Key Agreement Method(1999)

[28] IETF RFC 2632 S/MIME Version 3 Certificate Handling(1999)

[29] IETF RFC 2633 S/MIME Version 3 Message Specification(1999)

[30] IETF RFC 2865 Remote Authentication Dial In User Service(RADIUS)(2000)

[31] IETF RFC 3162 RADIUS and IPv6(2001)

[32] IETF RFC 3369 Cryptographic Message Syntax(CMS)(2002)

[33] IETF RFC 3370 Cryptographic Message Syntax(CMS) Algorithms(2002)

中 华 人 民 共 和 国
国 家 标 准
信息技术 安全技术 IT网络安全
第4部分:远程接入的安全保护
GB/T 25068.4—2010/ISO/IEC 18028-4:2005
*
中国标准出版社出版发行
北京复兴门外三里河北街16号
邮政编码:100045
网址 www.spc.net.cn
电话:68523946 68517548
中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销
*
开本 880×1230 1/16 印张 2.75 字数 73 千字
2011年1月第一版 2011年1月第一次印刷
*
书号:155066·1-40819 定价 39.00元

GB/T 25068.4-2010