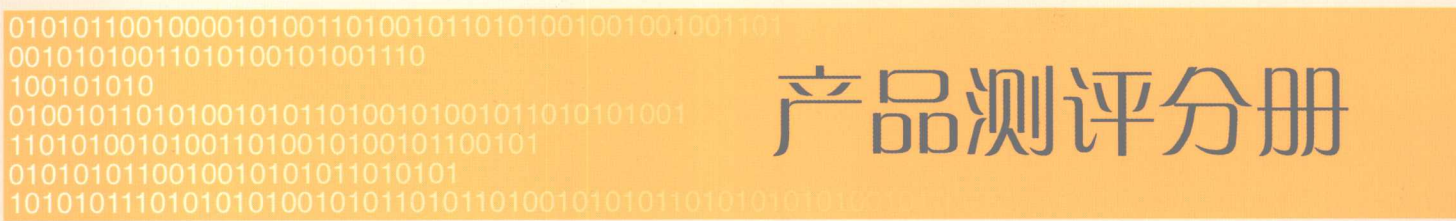
中国标准出版社第四编辑室　编

信息安全标准汇编

信息安全测评卷



产品测评分册

中国标准出版社

信息安全标准汇编

信息安全测评卷

产品测评分册

中国标准出版社第四编辑室　编

中国标准出版社

北　京

图书在版编目（CIP）数据

信息安全标准汇编. 信息安全测评卷. 产品测评分册/中国标准出版社第四编辑室编. —北京：中国标准出版社，2009

ISBN 978-7-5066-5108-0

Ⅰ.信… Ⅱ.中… Ⅲ.信息系统-安全管理-国家标准-汇编-中国 Ⅳ.TP309-65

中国版本图书馆 CIP 数据核字（2008）第 199546 号

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 44 字数 1 334 千字
2009 年 1 月第一版 2009 年 1 月第一次印刷

*

定价 225.00 元

出 版 说 明

在信息化社会，信息技术飞速发展，随之而来的信息技术的安全问题日益突出，它关系到信息系统的正常运行和健康发展，影响到信息化社会的各个方面，不容忽视。国家标准化管理委员会已制定和发布了一系列信息安全国家标准，为我国信息系统的安全提供了技术支持，为信息安全的监督和管理提供了依据和指导。

为满足广大信息技术人员的需求，方便学习和查阅，我们将信息安全国家标准按照信息安全标准体系收集、分类、汇编成卷，共分为以下5卷：

——基础卷

——信息安全管理卷

——信息安全测评卷

——技术与机制卷

——密码技术卷

其中基础卷、信息安全测评卷、技术与机制卷根据需要又分为若干分册。

随着信息安全标准体系的完善和标准制修订情况的变化，本套汇编将陆续分卷分册出版。

本册为信息安全测评卷的产品测评分册，共收入截至2008年11月发布的相关标准21项。

编　　者

2008年11月

前　言

有色金属是国民经济、国防工业、科技发展及人民日常生活必不可少的基础材料和重要的战略物资。农业现代化、工业现代化、国防和科技现代化都离不开有色金属。世界上众多国家尤其是工业发达国家，都竞相发展有色金属工业，增加有色金属的战略储备。

建国近60年来，中国有色金属工业取得了辉煌的成就，兴建了一大批有色金属矿山、冶炼和加工企业，组建了地质、设计、勘察、施工等建设单位和科研、教育、环保、信息等事业单位以及物资供销和进出口贸易单位，形成了一个布局比较合理、体系比较完整的行业。进入21世纪后，中国有色金属工业继续呈现出快速、平稳、健康发展的良好态势。有色金属产品产量持续增长；国内外市场有色金属价格持续在高位波动，规模以上企业尤其是资源型企业经济效益大幅度提高；有色金属进出口额平稳增长。

为了推动有色金属工业走新型工业化道路，达到产品结构调整、清洁生产、环境友好的目的和实现可持续发展的战略目标，有色金属标准化工作坚持密切配合有色金属工业的发展需要，积极推动标准制修订工作，制定了大量新标准来满足市场需求，填补空白。同时对不能满足市场需求的长标龄标准进行了修订，提高了标准整体水平，促进了产品质量的提高。

为深入贯彻落实《中华人民共和国标准化法》、《国家中长期科学和技术发展规划纲要》，加强有色金属工业标准化工作，提高有色金属产品质量，并满足广大有色金属企业、事业单位和其他行业对有色金属标准的迫切需要，全国有色金属标准化技术委员会和中国标准出版社组织编辑出版了这套《有色金属工业标准汇编》。本套汇编系统地汇集了由国家标准和行业标准主管部门批准发布实施的现行有色金属国家标准、行业标准，各标准汇编分册如下：

变形铝合金材料标准汇编　产品卷
变形铝合金材料标准汇编　方法卷
镁及镁合金标准汇编
钛及钛合金标准汇编
铜及铜合金标准汇编　产品卷
铜及铜合金标准汇编　方法卷
铅及铅合金标准汇编
锌及锌合金标准汇编
镍钴及镍钴合金标准汇编
锡锑及锡锑合金标准汇编
稀有金属及合金标准汇编　产品卷
稀有金属及合金标准汇编　方法卷
半导体材料标准汇编

粉末冶金标准汇编
稀土金属及合金标准汇编
贵金属及合金标准汇编

本汇编分册为《稀有金属及合金标准汇编　产品卷》，收集了截至2008年6月底批准、发布的有色金属国家标准、行业标准共61项，其中国家标准24项，有色行业标准37项。

本汇编分册收入的标准均为现行有效标准。但是，由于客观情况变化，各使用单位在参照执行时，应注意个别标准的修订情况。本汇编收集的国家标准的属性已在本目录上标明(GB或GB/T)，年号用四位数字表示。

鉴于部分国家标准是在国家标准清理整顿前出版的，现尚未修订，故正文部分仍保留原样；读者在使用这些国家标准时，其属性以目录标明的为准(标准正文“引用标准”中标准的属性请读者注意查对)。

标准号中括号内的年代号，表示在该年度确认了该项标准，但未重新出版。由于所收录标准的发布年代不尽相同，我们对标准中所涉及到的有关量和单位的表示方法未做统一改动，这次汇编时只对原标准中技术内容上的错误以及其他明显不妥之处做了更正。

本汇编目录中，凡标准名称后用括号注明国家标准“(原GB××××—××)”的行业标准，均由国家标准转换而来。这些标准因未另出版行业标准文本(即仅给出行业号，正文内容完全不变)，故本汇编中正文部分仍为原国家标准。与此类似的专业标准、部标准转化为行业标准的情况也照此处理。

本汇编分册可供从事稀有金属及合金材料生产、检测、设计和贸易等方面的人员参考使用。

编　者

2008年10月

目　　录

前　　言

本标准是我国国际互联网网络安全标准之一，它对网络代理服务器的最低安全要求作了规定。

本标准由国家信息化办公室提出。

本标准由全国信息技术标准化技术委员会归口。

本标准由公安部第三研究所负责起草，参加起草工作的单位还有电子工业部标准化研究所。

本标准主要起草人：严忠槐、张岚、汪广杰、李富豪、罗韧鸿。

中华人民共和国国家标准

网络代理服务器的安全技术要求

GB/T 17900—1999

Security technical requirements for proxy server

1 范围

本标准规定了网络代理服务器的安全技术要求，并作为网络代理服务器的安全技术检测依据。

2 定义

2.1 用户 user

一个远离代理服务器并与代理服务器相互作用的个人，他没有能够影响代理服务器安全策略执行的特权。

2.2 授权管理员 authorized administrator

任何具有旁路或规避代理服务器安全策略权限的经鉴别过的个人。本标准中，“授权管理员”特指代理服务器的管理员，但其职责不包括网络管理。

2.3 主机 host

一个远离代理服务器并与代理服务器相互作用的计算机，它没有能够影响代理服务器安全策略执行的特权。

2.4 可信主机 trusted host

任何具有旁路或规避代理服务器安全策略权限的计算机。

3 概述

本标准规定了网络代理服务器在低风险环境下的最低安全要求。指出由该类代理服务器所能防止的威胁，定义其实现的安全目标、使用环境以及安全功能和安全保证要求。

网络代理服务器以各种代理服务为基础，通过它提供集中的应用服务。它可以为不同的协议(如Telnet、SMTP、FTP、HTTP 等)进行代理。为在内部、外部两个网络之间建立安全可靠的应用服务，网络代理服务器必须具备安全控制手段，只有合法有效的客户要求才由代理服务器提交给真正的服务器。

符合本标准规定的网络代理服务器不再局限于代理服务，它必须具有访问控制、应用层内容过滤、数据截获处理、安全审计等，以保证本地网络资源的安全和对外部网络访问的控制。

图 1 给出代理服务器在网络中的逻辑示意图。

国家质量技术监督局 1999-11-11 批准　　2000-05-01 实施

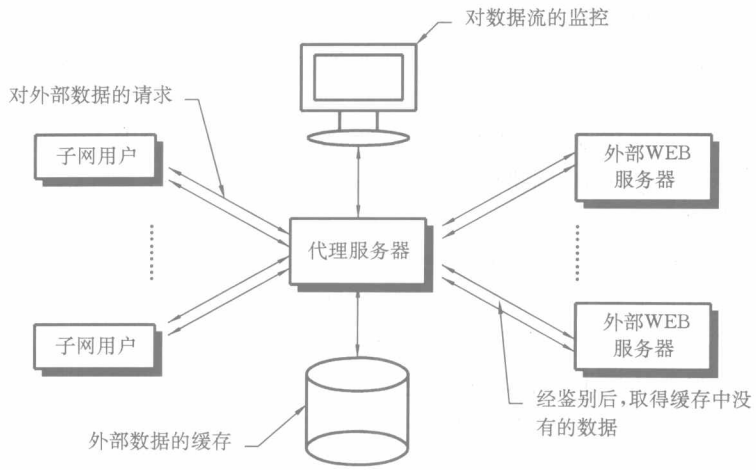


图 1　逻辑图

4　安全环境

遵循本标准的代理服务器应提供访问控制策略，包括身份识别与鉴别、内容过滤、安全审计等。可用于敏感但不保密的信息处理环境。

4.1　安全条件假设

假设在运行环境中存在以下条件：

4.1.1　单输入点(A.SINGLEPT)

如图 1 所示，代理服务器为内部网络与外部网络的唯一连接点。

4.1.2　物理访问控制(A.SECURE)

指代理服务器及相关的控制台在物理上是安全的，而且仅供授权人使用。

4.1.3　通信保护(A.COMMS)

对传输信息的保护应与信息的密级一致，但明确规定以明文传输的信息除外。

4.1.4　用户(A.USER)

代理服务器应提供非一般用途的计算能力，它能对用户交送的各种代理请求进行鉴别和授权。只有授权的管理员才具有直接访问和远程访问的权利。

4.1.5　授权的管理员(A.NOEVIL)

被授权的管理员无恶意和可以信任，并能够正确执行各项职责。

4.2　对安全的威胁

4.2.1　代理服务器应阻止的威胁

4.2.1.1　未授权的逻辑访问(T.LACCESS)

未授权的个人可能得到对代理服务器的逻辑访问权。未授权个人是指具有或者试图得到对系统的访问权的个人，但他不是代理服务器的授权用户。

4.2.1.2　冒用网络地址(T.ISPOOF)

一个主体伪装成另一个主体，试图得到信息访问权。

4.2.1.3　攻击内部受保护网络(T.NATTACK)

攻击者通过高级协议、服务，攻击内部受保护网络或该网络上的某一主机。

4.2.1.4　毁坏审计记录(T.AUDIT)

删除审计存储区文件，使审计记录丢失或毁坏，来逃避检测。

4.2.1.5　修改代理服务器配置及其他安全相关数据(T.DCORRUPT)

修改代理服务器的内部数据结构，篡改代理服务器配置等安全参数。

4.2.1.6 回避身份识别和鉴别机制(T.AUTH)

攻击者试图绕过系统的身份识别和鉴别机制,伪装成一个授权的管理员,或者干扰一个已经创立的进程。

4.2.1.7 受保护网络上的一个有敌意的用户试图向外部用户提供信息(T.INSHARE)

此类威胁涉及的是内部(受保护)网络的用户企图把信息传送给外部网络的非授权用户。

4.2.2 由运行环境阻止的威胁

以下威胁可以通过物理控制操作规程或管理手段来防止。

4.2.2.1 受保护网络上的一个有敌意的用户攻击同一网络上的计算机(T.INALL)

此类威胁指来自受保护网络内的对本网络服务功能的攻击,或者对同一网段上的计算机的攻击。

4.2.2.2 对高层协议和服务的攻击(T.SERVICES)

此类威胁针对传输层以上的协议层(和利用这些协议的服务,如超文本传输协议 HTTP)中的漏洞。符合本标准的代理服务器可以完全拒绝对特定主机或主机群的访问,但是,如果允许数据包通过的话,那么仍有可能对上述的这些服务攻击。

4.2.2.3 截取传输的信息(T.PRIVACY)

攻击者可能截取通过代理服务器传输的敏感信息。

5 安全目标

5.1 信息技术性安全目标

代理服务器应达到的信息技术安全目标如下。

5.1.1 访问仲裁(O.ACCESS)

目标是通过允许或拒绝从一个主体(发送实体)传到一个客体(接受实体)的信息流,为连接在代理服务器上的两个网络之间提供受控制的访问,这些控制是根据主体、客体的有关参数,由代理服务器生成的状态信息和管理上配置的访问控制规则实现的。

5.1.2 管理员访问(O.ADMIN)

此项目标是仅限授权的管理者才能访问代理服务器,即只允许他们有配置代理服务器的能力。

5.1.3 个体身份记录(O.ACCOUNT)

个体记录提供对用户的记录能力,并允许基于唯一身份对访问作出判定。鉴别为确定身份是否真实提供了方法。

5.1.4 代理服务器的自我保护(O.PROTECT)

为了成功地达到这一目标,代理服务器应能够从其正在处理的数据中分离出自身的控制信息而保护自己不受外部实体的攻击。此外,代理服务器还应能保护授权管理员的通信会话连接。

5.1.5 审计(O.AUDIT)

对于判定是否存在绕过安全策略尝试,是否因配置错误而不知觉地允许了本应拒绝的访问,审计记录起着重要的作用。代理服务器不仅应收集审计数据,还应使其具有可读性并较易使用。审计记录应受到充分保护,并应了解丢失审计记录的可能性有多大,以帮助授权管理员做出正确的安全决定。

5.2 非信息技术安全目标

非信息技术性安全目标是指除代理服务器技术要求之外还需满足的要求,它们不需代理服务器硬件和软件的机制实现。而是通过采用物理的、过程的或管理的方法来达到。

代理服务器的非信息技术安全目标如下。

5.2.1 安装与操作控制(O.INSTALL)

确保代理服务器在运输、安装、保管、操作中的系统安全。

5.2.2 物理控制(O.PACCESS)

控制对代理服务器的物理访问。

5.2.3 授权管理员培训(O.TRAIN)

加强对授权管理员的培训,使他们具有建立和维护一定的安全策略的实际能力。

6 信息技术安全要求

本章给出了符合本标准的代理服务器应满足的功能要求和安全要求。

6.1 功能要求

本标准的功能安全要求由表1的下列项目组成:

表1 功能要求

功能分类	功能组件	
用户数据保护	FDP_ACC.2	完整的客体访问控制
	FDP_ACF.4	访问授权与拒绝
	FDP_ACF.2	多种安全属性的访问控制
	FDP_IFC.2	完整的信息流控制
	FDP_IFF.8	信息流授权与拒绝
	FDP_RIP.3	资源分配时对遗留信息的充分保护
	FDP_SAM.1	管理员属性修改
	FDP_SAQ.1	管理员属性查询
识别与鉴别	FIA_ADA.1	授权管理员、可信主机和用户鉴别数据初始化
	FIA_ADP.1	授权管理员、可信主机和用户鉴别数据的基本保护
	FIA_AFL.1	鉴别失败的基本处理
	FIA_ATA.1	授权管理员、可信主机、主机和用户属性的初始化
	FIA_ATD.2	授权管理员、可信主机、主机和用户唯一属性定义
	FIA_UAU.1	授权管理员的基本鉴别
	FIA_UAU.2	单一使用的鉴别机制
	FIA_UID.2	授权管理员、可信主机、主机和用户的唯一标识
密码支持	FCS_COP.2	符合规定的加密操作
可信安全功能的保护	FPT_RVM.1	代理服务器安全策略的不可旁路性
	FPT_SEP.1	代理服务器安全功能区域分隔
	FPT_TSA.2	区分安全管理角色
	FPT_TSM.1	管理功能
安全审计	FAU_GEN.1	审计数据生成
	FAU_MGT.1	审计跟踪管理
	FAU_POP.1	可理解的格式
	FAU_PRO.1	限制审计跟踪访问
	FAU_SAR.1	限制审计查阅
	FAU_SAR.3	可选择查阅审计
	FAU_STG.3	防止审计数据丢失

要求概述：代理服务器安全策略由多项安全功能策略组成。定义如下三个安全策略：策略一，**未鉴别的端到端策略**，负责处理正在通过代理服务器由内部网络向外部网客体或由外部网络向内部网络客体发送信息的主体。策略二，**已鉴别的端到端策略**，负责处理相关的内部或外部网络上的主体，当它在通过代理服务器向外部或内部网络的客体发送信息时，必须在代理服务器上被鉴别。策略三，**关键词过滤策略**，负责处理正在通过代理服务器由内部网络向外部网客体或由外部网络向内部网络客体发送的信息，并根据预置关键词对非加密明文信息作出授权或拒绝的决定。

6.1.1 完整的客体访问控制(FDP _ ACC.2)

FDP _ ACC.2.1 代理服务器安全功能应在如下实体上执行未鉴别的端到端策略：

a) 主体：未经代理服务器鉴别的主机；

b) 客体：内部或外部网上的主机；

以及被安全功能策略覆盖的所有主体与客体间的操作。

FDP _ ACC.2.2 代理服务器安全功能应在如下实体上执行已鉴别的端到端策略：

a) 主体：已在代理服务器鉴别的用户；

b) 客体：内部或外部网上的主机；

以及被安全功能策略覆盖的所有主体与客体间的操作。

FDP _ ACC.2.3 代理服务器应保证任何在代理服务器安全功能控制范围内的主体与客体间的操作都被安全功能策略覆盖。

6.1.2 访问授权与拒绝(FDP _ ACF.4)

FDP _ ACF.4.1 代理服务器安全功能应保证：

——未鉴别的端到端策略

——已鉴别的端到端策略

根据主体和客体的安全属性值，提供明确的准许访问的能力。

FDP _ ACF.4.2 代理服务器安全功能应保证：

——未鉴别的端到端策略

——已鉴别的端到端策略

根据主体和客体的安全属性值，提供明确的拒绝访问的能力。

6.1.3 多种安全属性的访问控制(FDP _ ACF.2)

FDP _ ACF.2.1 代理服务器安全功能应保证：

对基于源地址、目的地址、传输层协议和所请求的服务客体实现

——未鉴别的端到端策略

FDP _ ACF.2.2 代理服务器安全功能应保证：

对基于用户 ID、源地址、目的地址、传输层协议和所请求的服务的客体实现

——已鉴别的端到端策略

FDP _ ACF.2.3 代理服务器安全功能应保证如下附加规则以判定受控主体与受控客体间的操作是否被允许：

a) 代理服务器应拒绝源于一个外部未受保护网络上鉴别过的用户，但有一个内部，受保护网络上主机的源地址的访问或服务请求；

b) 代理服务器应拒绝源于一个外部未受保护网络上鉴别过的用户，但有一个广播网络源地址的访问或服务请求；

c) 代理服务器应拒绝源于一个外部未受保护网络上鉴别过的用户，但有一个私有的，保留网络主机源地址的访问或服务请求；

d) 代理服务器应拒绝源于一个外部未受保护网络上鉴别过的用户，但有环回网络上一个主机源地址的访问或服务请求。

6.1.4 完整的信息流控制(FDP _ IFC.2)

FDP _ IFC.2.1 代理服务器安全功能应在如下实体上执行关键词过滤策略：

a) 主体：内部或外部网上的主机或用户；

b) 客体：内部或外部网上的主机或用户；

以及被安全功能策略覆盖的所有主体与客体间的操作。

FDP _ IFC.2.2 代理服务器应保证任何在代理服务器安全功能控制范围内的主体与客体间的操作都被安全功能策略覆盖。

6.1.5 信息流授权与拒绝(FDP _ IFF.8)

FDP _ IFF.8.1 代理服务器安全功能应保证关键词过滤策略，根据主体和客体的安全属性值明确地对信息流授权。

FDP _ IFF.8.2 代理服务器安全功能应保证关键词过滤策略，根据主体和客体的安全属性值明确地拒绝信息流。

6.1.6 资源分配时对遗留信息的充分保护(FDP _ RIP.3)

FDP _ RIP.3.1 代理服务器安全功能应保证在为所有客体分配资源时，不提供以前的任何信息内容。

应用注释：该要求需要管理用于支持连接的所有资源(如：寄存器、缓冲区)，使得不允许访问以前会话中的信息。该要求通常通过清除或覆盖这些资源来满足。

要求概述：下述两项要求(FDP _ SAM.1，FDP _ SAQ.1)确定了支持管理员完成其职能所必需的能力，特别是查阅和修改与安全相关参数的能力。这些要求将在后续的对与安全有关数据初始化的要求中予以详述或补充。随后的识别与鉴别组的要求与有关安全参数(如鉴别数据)的定义、管理和使用的需要紧密相关。

6.1.7 管理员属性修改(FDP _ SAM.1)

FDP _ SAM.1.1 代理服务器安全功能应执行如下访问控制安全功能策略。

——未鉴别的端到端策略

——已鉴别的端到端策略

以保证管理员可以修改：

——标识与角色的联系(如：授权的管理员)；

——由 FDP _ ACF.2 标识的访问控制属性；

——与安全相关的管理数据。

6.1.8 管理员属性查询(FDP _ SAQ.1)

FDP _ SAQ.1.1 代理服务器安全功能应执行如下访问控制安全功能策略。

—未鉴别的端到端策略

—已鉴别的端到端策略

以保证管理员可以查询：

——FDP _ ACF.2 标识的访问控制属性；

——主机名；

——用户名。

6.1.9 授权管理员、可信主机和用户鉴别数据初始化(FIA _ ADA.1)

FIA _ ADA.1.1 代理服务器安全功能应能够提供与 FIA _ UAU.1 和 FIA _ UAU.2 规定的鉴别机制相关的授权管理员、可信主机和用户鉴别数据的初始化功能。

FIA _ ADA.1.2 代理服务器安全功能应限制只能由管理员使用这些功能。

6.1.10 授权管理员、可信主机和用户鉴别数据的基本保护(FIA _ ADP.1)

FIA _ ADP.1.1 代理服务器安全功能应防止未授权的查阅、修改、销毁存储在代理服务器中的鉴别数据。

6.1.11 鉴别失败的基本处理(FIA _ AFL.1)

FIA _ AFL.1.1 代理服务器安全功能应有能力在一定次数的鉴别失败后,中断可信主机或用户会话的建立过程。失败次数限值应只能由授权管理员设置。

FIA _ AFL.1.2 中断可信主机或用户会话的建立过程后,代理服务器安全功能应能够使相应的可信主机帐号或用户帐号失效,直到授权管理员解除对会话的封锁。

6.1.12 授权管理员、可信主机、主机和用户属性的初始化(FIA _ ATA.1)

FIA _ ATA.1.1 代理服务器安全功能应提供用缺省值对授权管理员、可信主机、主机和用户属性初始化的能力。

6.1.13 授权管理员、可信主机、主机和用户唯一属性定义(FIA _ ATD.2)

FIA _ ATD.2.1 代理服务器安全功能应为定义的每一个授权管理员、可信主机、主机和用户提供执行代理服务器安全策略所必须的唯一的安全属性集合。

6.1.14 授权管理员的基本鉴别(FIA _ UAU.1)

FIA _ UAU.1.1 当授权的管理员通过控制台访问代理服务器时,代理服务器安全功能应在授权管理员执行任何功能前鉴别其身份。

6.1.15 单一使用的鉴别机制(FIA _ UAU.2)

FIA _ UAU.2.1 代理服务器安全功能应在执行相应授权管理员、可信主机或用户的任何功能前,鉴别授权管理员、可信主机或用户所声明的身份。

FIA _ UAU.2.2 代理服务器安全功能应防止请求如下服务的远程授权管理员、远程可信主机和用户相关的鉴别数据重复使用:

——文件传输协议(FTP);

——超文本传输协议(HTTP);

——登录(login);

——邮政协议(POP);

——远程登录(rlogin);

——简单网络管理协议(SNMP);

——远程终端仿真(Telnet)。

应用说明:该要求仅需在提供这些服务的代理服务器上满足。

6.1.16 授权管理员、可信主机、主机和用户的唯一标识(FIA _ UID.2)

FIA _ UID.2.1 代理服务器安全功能应在执行授权管理员、可信主机或用户请求的任何操作前,唯一地识别每一个授权用户、可信主机、主机或用户。

6.1.17 符合规定的加密操作(FCS _ COP.2)

FCS _ COP.2.1 代理服务器安全功能应保证其远程管理会话的加密符合国家密码管理的有关规定。

要求概述:下面两项要求(FPT _ RVM.1 和 FPT _ SEP.1)规定了保护内部代码和数据结构的基础性体系结构的能力,并能够表明安全策略始终是有效的。

6.1.18 代理服务器安全策略的不可旁路性(FPT _ RVM.1)

FPT _ RVM.1.1 代理服务器安全功能应保证在任何与安全相关的操作被允许进行前代理服务器安全策略总是被使用,并是成功的。

6.1.19 代理服务器安全功能区域分隔(FPT _ SEP.1)

FPT _ SEP.1.1 代理服务器安全功能应为其自身的执行维护一个安全区域,以保护其免遭不可信主体的干扰和篡改。

FPT _ SEP.1.2 代理服务器安全功能应将代理服务器安全功能控制范围内的各个主体的安全区域分

隔开。

6.1.20 区分安全管理角色(FPT _ TSA.2)

FPT _ TSA.2.1 代理服务器安全功能应能够将与安全相关的管理功能与其他功能区分开。

FPT _ TSA.2.2 代理服务器安全功能中与安全相关的管理功能的集合应包括安装、配置和管理代理服务器安全功能所需要的所有功能。至少,此集合应包括:增加和删除主体和客体;查阅访问控制安全属性;分配、修改和取消访问控制安全属性;查阅和管理审计数据。

FPT _ TSA.2.3 代理服务器安全功能应将执行与安全相关的管理功能的能力,限制到具有特定的授权功能和责任的一个安全管理角色上。

FPT _ TSA.2.4 代理服务器安全功能应能够从所有使用代理服务器的个体和系统集中区分出具有管理功能的授权管理员和可信主机的集合。

FPT _ TSA.2.5 代理服务器安全功能应只允许授权管理员和可信主机承担安全管理职能。

FPT _ TSA.2.6 代理服务器安全功能应需要一个明确的请求,以使授权管理员和可信主机承担安全管理职能。

6.1.21 管理功能(FPT _ TSM.1)

FPT _ TSM.1.1 代理服务器安全功能应提供给授权管理员设置和修改与安全相关的管理数据的能力,并能给予或取消 FIA _ UAU.2.2 中服务的用户鉴别。

FPT _ TSM.1.2 代理服务器安全功能应提供给授权管理员执行安装和初始化代理服务器,及使系统起动与关闭、备份与恢复的功能的能力,备份能力应被自动的工具支持。

如果代理服务器安全功能支持从内部或外部接口远程管理的能力,则代理服务器安全功能应:

a) 有可以禁止从内部和外部接口远程管理的选择权;

b) 能够限制可以执行远程管理的地址;

c) 能够通过加密保护远程管理会话。

要求概述:余下的功能安全要求(FAU 类)涉及产生、管理、保护和处理安全审计信息的需要。

6.1.22 审计数据生成(FAU _ GEN.1)

FAU _ GEN.1.1 代理服务器安全功能应能够对下列可审计事件产生一个审计记录:

a) 启动和关闭审计功能;

b) 由表 2 中的功能组成部分中,定义为基本或最低级别的所有可审计事件;

c) 基于包括在安全目标中的所有功能组成部件的,在表 2 中说明为"扩展"的附加事件。

FAU _ GEN.1.2 代理服务器安全功能在每一条审计记录中应至少记录如下信息:

a) 事件发生的时期和时间、事件的类型、主体的身份及事件的成败与否;

b) 对每一种审计事件类型,表 2 第四列说明的附加信息。

表 2 可审计事件

功能族	级别	可审计事件	附加审计记录内容
FAU _ MGT	基本	任何对审计跟踪进行操作的尝试,包括关闭审计功能或子系统	如适用,受影响客体的标识
FAU _ PRO	基本	任何对审计跟踪读取、修改和破坏的尝试	
FDP _ ACF	基本	所有对安全功能策略覆盖的客体执行操作的请求	受影响客体的标识
FDP _ SAM	基本	修改安全属性的所有尝试,包括拟修改客体的身份	
FDP _ SAQ	基本	查询安全属性的所有尝试,包括拟修改客体的身份	
FDP _ IFF	基本	任何包含关键词的信息流	

表 2（完）

功能族	级别	可审计事件	附加审计记录内容
FIA _ ADA	基本	所有使用安全功能中鉴别数据管理机制的请求	
FIA _ ADP	基本	所有访问鉴别数据的请求	访问请求的目标
FIA _ AFL	扩展	因鉴别尝试不成功的次数超出了设定的限值，导致的会话连接终止	使用的标识符
FIA _ UAU	基本	任何对鉴别机制的使用	
FIA _ UID	基本	所有使用标识机制（包括所提供的身份）的尝试	
FIA _ TSA	最低	使用与某项安全相关的管理功能	
FIA _ TSM	基本	所有对代理服务器安全功能配置参数的修改（设置和更新），无论成功与否	配置参数的更新

6.1.23 审计跟踪管理（FAU _ MGT. 1）

FAU _ MGT. 1.1 代理服务器安全功能应提供给授权管理员创建、归档、删除和清空审计跟踪记录的能力。

6.1.24 可理解的格式（FAU _ POP. 1）

FAU _ POP. 1.1 代理服务器安全功能应能使存储在永久审计跟踪中的审计数据可为人理解。

6.1.25 限制审计跟踪访问（FAU _ PRO. 1）

FAU _ PRO. 1.1 代理服务器安全功能应只允许授权管理员访问审计跟踪。

6.1.26 限制审计查阅（FAU _ SAR. 1）

FAU _ SAR. 1.1 代理服务器安全功能应提供具有查阅审计数据能力的审计查阅工具。

FAU _ SAR. 1.2 代理服务器安全功能应只允许授权管理员使用审计查阅工具。

6.1.27 可选择查阅审计（FAU _ SAR. 3）

FAU _ SAR. 3.1 代理服务器安全功能应提供基于如下审计数据进行查找和排序的查阅工具：

a）主体标识；

b）客体标识；

c）日期；

d）时间；

e）以上参数的任何逻辑组合（如："与"，"或"）。

应用注释：代理服务器的开发者应详细描述审计查阅工具的功能，特别是应清楚说明根据与安全相关的属性查找和排序的能力。

6.1.28 防止审计数据的丢失（FAU _ STG. 3）

FAU _ STG. 3.1 代理服务器安全功能应将产生的审计记录在一个永久审计跟踪中。

FAU _ STG. 3.2 代理服务器安全功能应减少由于故障和攻击导致的审计事件丢失的数目。

FAU _ STG. 3.3 当审计存储空间用尽时，代理服务器安全功能应能够防止可审计事件的发生，除了那些由授权管理员产生的。

应用注释：对因故障或存储耗竭而导致审计数据丢失的最大容量，防火墙的开发者应提供相应的分析结果。

6.2 保证要求

保证要求针对开发者，由表 3 给出：