ICS 35.020
L 80

中华人民共和国国家标准

GB/T 17900—1999

网络代理服务器的安全技术要求

Security technical requirements for proxy server

1999-11-11 发布　　2000-05-01 实施

国家质量技术监督局 发布

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
*
中国标准出版社出版
北京复兴门外三里河北街16号
邮政编码:100045
电　　话:68522112
中国标准出版社秦皇岛印刷厂印刷
新华书店北京发行所发行　各地新华书店经售

*
开本 880×1230 1/16　印张 1½　字数 40 千字
2000年6月第一版　2000年6月第一次印刷
印数 1—1 800
*
书号:155066·1-16718　定价 13.00 元
*
标 目 411—23

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。

目　　次

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

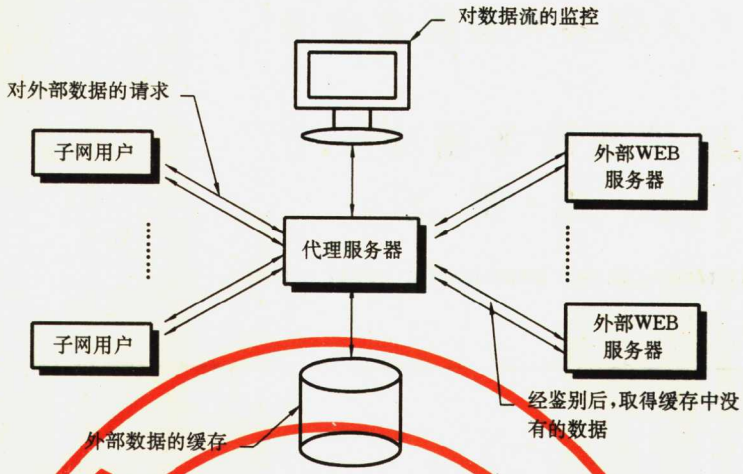

图 1 逻辑图

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：

表 3 保证要求

保证类	保证组件	
配置管理	ACM _ CAP. 1	最低限度的支持
交付与操作	ADO _ IGS. 1	安装、生成和启动过程
开发	ADV _ FSP. 1	代理服务器和安全策略
	ADV _ HLD. 1	高层设计描述
	ADV _ RCR. 1	非形式的一致性证明
指南文件	AGD _ ADM. 1	管理员指南
	AGD _ USR. 1	用户指南
测试	ATE _ IND. 1	独立测试——一致性
	ATE _ COV. 1	测试覆盖面—非形式的
	ATE _ FUN. 1	功能测试
	ATE _ DPT. 1	测试—功能规范
脆弱性分析	AVA _ SOF. 1	代理服务器安全功能强度的评估
	AVA _ VLA. 1	开发者脆弱性分析

6.2.1 最低限度的支持(ACM _ CAP. 1)

ACM _ CAP. 1. 1D 开发者应使用配置管理系统。

ACM _ CAP. 1. 2D 开发者应提供配置管理文件。

ACM _ CAP. 1. 1C 配置管理文件应包括一个配置目录。

ACM _ CAP. 1. 2C 配置目录应描述包括代理服务器的各个配置条目,并应包括代理服务器使用的外部网络服务项目。

ACM _ CAP. 1. 3C 配置管理文件应描述用于唯一识别代理服务器配置项目的方法。

ACM _ CAP. 1. 1E 评估者应确认所提供的信息满足证据的内容和表述的所有要求。

6.2.2 安装、生成和启动过程(ADD _ IGS. 1)

ADD _ IGS. 1. 1D 开发者应提供安全安装、生成和启动代理服务器的文件。

ADD _ IGS. 1. 1C 该文件应描述安全安装、生成和启动代理服务器所必须的步骤。

ADD _ IGS. 1. 1E 评估者应确认所提供的信息满足证据的内容和表述的所有要求。

6.2.3 代理服务器和安全策略(ADV _ FSP. 1)

ADV _ FSP. 1. 1D 开发者应提供一份功能规格说明。

ADV _ FSP. 1. 2D 开发者应提供一个代理服务器安全策略。

ADV _ FSP. 1. 1C 该功能规格说明应使用一种非形式的方法描述代理服务器安全策略。

ADV _ FSP. 1. 2C 该功能规格说明应包括一份所有代理服务器安全功能外部接口的语法和语义的非形式表述。

ADV _ FSP. 1. 3C 该功能规格说明应包括能说明代理服务器安全功能被完整描述的证明。

应用注释:这条要求可以通过安全目标和外部接口指标等文件的组合来达到。

ADV _ FSP. 1. 1E 评估者应确认所提供的信息满足证据的内容和表述的所有要求。

ADV _ FSP. 1. 2E 评估者应判定该功能规格说明与代理服务器安全策略是一致的。

ADV _ FSP. 1. 3E 评估者应判定代理服务器安全功能的描述已满足代理服务器安全目标中的功能要求。

6.2.4 高层设计描述(ADV _ HLD. 1)

ADV _ HLD. 1. 1D 开发者应提供代理服务器安全功能的高层设计说明。

ADV _ HLD. 1. 1C 高层设计的表述应是非形式的。

ADV _ HLD. 1. 2C 高层设计应根据子系统来描述代理服务器安全功能的结构。

ADV _ HLD. 1. 3C 高层设计应描述由代理服务器安全功能的每个子系统提供的安全功能。

ADV _ HLD. 1. 4C 高层设计应描述代理服务器安全功能子系统的接口。

ADV _ HLD. 1. 5C 高层设计应标明所有低层的硬件、固件和(或)代理服务器安全功能所需的软件,并说明由使用硬件、固件、软件实现的保护机制提供的功能。

ADV _ HLD. 1. 1E 评估者应确认所提供的信息满足证据的内容和表述的所有要求。

ADV _ HLD. 1. 2E 评估者应判定代理服务器安全目标中的功能要求已被代理服务器安全功能的描述满足。

6. 2. 5 非形式的一致性证明(ADV _ RCR. 1)

ADV _ RCR. 1. 1D 开发者应提供证据说明所提供的最扼要的代理服务器安全功能介绍是准确、完整的,并且是在代理服务器安全目标中陈述的功能要求的完全实现。

ADV _ RCR. 1. 1C 对于代理服务器同一安全功能两个相邻层的表述,开发者应证明在较高层抽象表述的所有部分在较底层抽象中得到了细化。

ADV _ RCR. 1. 2C 对于代理服务器同一安全功能的两个相邻层的表述,其对应关系可以用非形式化方法表述。

ADV _ RCR. 1. 1E 评估者应确认所提供的信息满足证据的内容和表述的所有要求。

ADV _ RCR. 1. 2E 评估者应分析在代理服务器安全目标中陈述的功能要求和以最低层抽象之间的对应关系进行分析,以保证正确性、一致性和完整性。

6. 2. 6 管理员指南(AGD _ ADM. 1)

AGD _ ADM. 1. 1D 开发者必须向系统管理人员提供管理员指南。

AGD _ ADM. 1. 1C 管理员指南应描述如何用安全的方式管理代理服务器。

AGD _ ADM. 1. 2C 管理员指南应包括对于应该在安全处理环境下受控制的功能和优先权的警告。

AGD _ ADM. 1. 3C 管理员指南应包括统一和有效使用代理服务器安全功能中安全功能的指导。

AGD _ ADM. 1. 4C 管理员指南应描述两种类型功能之间的区别:一种是管理员控制安全参数的功能,另一种是只允许管理员获得信息的功能。

AGD _ ADM. 1. 5C 管理员指南应对管理员控制下的所有安全参数进行描述。

AGD _ ADM. 1. 6C 管理员指南应描述各种与安全相关的事件,这些事件都是需要执行与管理功能相关的功能,包括在代理服务器安全功能控制下改变实体的安全特征。

AGD _ ADM. 1. 7C 管理员指南应包括安全功能如何相互作用的指导。

AGD _ ADM. 1. 8C 管理员指南应包括怎样配置代理服务器的指令。

AGD _ ADM. 1. 9C 管理员指南应描述所有在安全安装代理服务器过程中可能使用的配置选项。

AGD _ ADM. 1. 10C 管理员指南应描述与安全管理相关的详细过程。

AGD _ ADM. 1. 11C 管理员指南应与提交评估的所有其他文件一致。

AGD _ ADM. 1. 1E 评估者应确认所提供的信息满足证据的内容和表述的所有要求。

AGD _ ADM. 1. 2E 评估者应确认安装过程应产生一个安全的配置。

6. 2. 7 用户指南(AGD _ USR. 1)

AGD _ USR. 1. 1D 开发者应提供用户指南。

AGD _ USR. 1. 1C 用户指南应描述用户可使用的代理服务器安全功能和接口。

AGD _ USR. 1. 2C 用户指南应包括使用代理服务器提供的安全功能的指导。

AGD _ USR. 1. 3C 用户指南应包括对于应该在安全处理环境下受控制的功能和优先权的警告。

AGD _ USR. 1. 4C 用户指南应包括与用户可见的安全功能之间交互作用的描述。

AGD _ USR. 1. 5C 用户指南应与提交评估的所有其他文件一致。

AGD_USR.1.1E 评估者应确认所提供的信息满足证据的内容和表述的所有要求。

6.2.8 独立测试——一致性(ATE_IND.1)

ATE_IND.1.1D 开发者应提供用于测试的代理服务器。

ATE_IND.1.1C 代理服务器应适合测试。

ATE_IND.1.1E 评估者应确认所提供的信息满足证据的内容和表述的所有要求。

6.2.9 测试覆盖面——非形式的(ATE_COV.1)

ATE_COV.1.1D 开发者应提供对测试范围的分析。

ATE_COV.1.1C 测试范围的分析应说明在测试文件中确定的测试覆盖了代理服务器的安全功能。

ATE_COV.1.1E 评估者应确认所提供的信息满足证据的内容和表述的所有要求。

6.2.10 功能测试(ATE_FUN.1)

ATE_FUN.1.1D 开发者应测试代理服务器的安全功能,并将结果记录在文件中。

ATE_FUN.1.2D 开发者应提供测试文件。

ATE_FUN.1.1C 测试文件应由测试计划、测试过程描述和测试结果组成。

ATE_FUN.1.2C 测试计划应确定要被测试的安全功能,并描述所做测试的目标。

ATE_FUN.1.3C 测试过程描述应确定要进行的测试,并且描述每一安全功能测试的详细步骤。

ATE_FUN.1.4C 测试文件中的测试结果应给出每项测试的预期结果。

ATE_FUN.1.5C 开发者执行测试所得的结果应证明每项安全功能与设计目标相符。

ATE_FUN.1.1E 评估者应确认所提供的信息满足证据的内容和表述的所有要求。

6.2.11 测试——功能规范(ATE_DPT.1)

ATE_DPT.1.1D 开发者应提供对测试深度的分析。

ATE_DPT.1.1C 深度分析应证明测试文件中确定的测试足够表明代理服务器的运行符合代理服务器安全功能规范。

ATE_DPT.1.1E 评估者应确认所提供的信息满足证据的内容和表述的所有要求。

6.2.12 代理服务器安全功能强度的评估(AVA_SOF.1)

AVA_SOF.1.1D 开发者应确定代理服务器安全功能强度的分析适合于所有代理服务器安全机制。

AVA_SOF.1.2D 开发者应对每一确定的安全机制进行代理服务器安全功能强度分析。加密与鉴别机制应满足有关规定和国家标准。

AVA_SOF.1.1C 对于安全功能对抗威胁的能力,代理服务器安全功能强度分析应判定标明的代理服务器安全机制所受的影响。

AVA_SOF.1.2C 代理服务器安全功能强度分析应证明标明的安全功能强度与代理服务器安全目标一致。

AVA_SOF.1.3C 安全强度分为中等或高等两档。

AVA_SOF.1.1E 评估者应确认所提供的信息满足证据的内容和表述的所有要求。

AVA_SOF.1.2E 评估者应确认所有需要进行强度分析的代理服务器安全机制都已经确定。

AVA_SOF.1.3E 评估者应确认各项强度声明已被确定。

6.2.13 开发者脆弱性分析(AVA_VLA.1)

AVA_VLA.1.1D 开发者应作出一份代理服务器查找用户用常规方法扰乱代理服务器安全策略的分析文件。

AVA_VLA.1.2D 开发者应作出确认的脆弱性的特征的文件。

AVA_VLA.1.1C 对每一种脆弱性,应有证据说明在代理服务器的预期环境中脆弱性不能被利用。

AVA_VLA.1.1E 评估者应确认所有需要进行强度分析的代理服务器安全机制都已经确定。

AVA_VLA.1.2E 评估者应进行基于开发者脆弱性分析的入侵测试,以保证明显的脆弱性已被标明。

7 基本原理

7.1 信息技术安全目标的基本原理

7.1.1 访问仲裁(O. ACCESS)

此安全目标对防止 T. ISPOOF,T. NATTACK 和 T. DCORRUPT 威胁是必需的。

7.1.2 管理员访问(O. ADMIN)

此安全目标对防止 T. LACCESS、T. ISPOOF 和 T. DOCCRRUPT 威胁是必需的。

7.1.3 个体身份记录(O. ACCOUNT)

此安全目标对防止 T. LACCESS 威胁是必需的。

7.1.4 代理服务器的自我保护(O. PROTECT)

此安全目标对防止 T. DCORRUPT 和 T. AUTH 威胁是必需的。

7.1.5 审计(O. AUDIT)

此安全目标对防止 T. NATTACK、T. DOCRRUPT 和 T. AUTH 威胁是必需的。

信息技术安全目标与威胁关系见表 4。

表 4 信息技术安全目标与威胁关系

	O. ACCESS	O. ADMIN	O. ACCOUNT	O. PROTECT	O. AUDIT
T. LACCESS		×	×		
T. ISPOOF	×	×			
T. NATTACK	×				×
T. AUDIT					×
T. DCORRUPT	×	×		×	×
T. AUTH				×	

7.2 非信息技术安全目标的基本原理

7.2.1 安装与操作控制(O. INSTALL)

此安全目标对防止 T. LACCESS、T. ISPOOF、T. NATTACK、T. AUDIT、T. DCORRUPT 和 T. AUTH 威胁是必需的。

7.2.2 实体控制(O. PACCESS)

此安全目标对防止 T. ISPOOF、T. NATTACK 和 T. DCORRUPT 威胁是必需的。

7.2.3 授权管理员的培训(O. TRAIN)

此安全目标对防止 T. LACCESS、T. ISPOOF、T. NATTACK、T. AUDIT、T. DCORRUPT 和 T. AUTH 威胁是必需的。

非信息技术安全目标与威胁关系见表 5。

表 5 非信息技术安全目标与威胁的关系

	O. INSTALL	O. PACCESS	O. TRAIN
T. LACCESS	×		×
T. ISPOOF	×	×	×
T. NATTACK	×	×	×
T. AUDIT	×		×
T. DCORRUPT	×	×	×
T. AUTH	×		×