ICS 35.040
L 80

中华人民共和国国家标准

GB/T 18020—1999

信 息 技 术
应用级防火墙安全技术要求

Information technology—
Security requirements for application level firewall

1999-11-11 发布　　2000-05-01 实施

国家质量技术监督局 发布

前　言

本标准规定了网络安全设备——应用级防火墙的安全技术要求。

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。

本标准起草单位：国家信息中心、中国国家信息安全测评认证中心。

本标准主要起草人：叶红、吴亚非、吴世忠、陈晓桦、李正男、严望佳。

目　　次

中华人民共和国国家标准

信 息 技 术
应用级防火墙安全技术要求

GB/T 18020—1999

Information technology—
Security requirements for application level firewall

1 范围

本标准规定了应用级防火墙的安全技术要求。

本标准适用于应用级防火墙安全功能的研制、开发、测试、评估和产品采购。

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构成为本标准的条文。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2部分：安全体系结构

3 定义和记法约定

本章给出本标准中使用的术语和记法约定。

3.1 定义

3.1.1 用户 user

在防火墙之外，但与防火墙相互作用的人，他不具有影响防火墙安全策略执行的特权。

3.1.2 授权管理员 authorized administrator

任何具有旁路或绕过防火墙安全策略权限的授权人，本标准中的“授权管理员”严格定义为防火墙的管理员，他不具有网络管理的职责。

3.1.3 主机 host

在防火墙之外，但与防火墙相互作用的计算机，它不具有影响防火墙安全策略执行的特权。

3.1.4 可信主机 trusted host

任何具有旁路或绕过防火墙安全策略权限的授权计算机。

3.2 记法约定

细化：用于增加某一功能要求的细节，从而进一步限制该项要求。对功能要求的细化用**黑体字**表示。示例见 7.1.2.3。

选择：用于在对某一功能要求的陈述中，突出一个或多个选项，用*带下划线的斜体字表示*。示例见 7.1.5.2。

赋值：用于将一个特定值赋给某个未定参数，如某个口令字的长度。赋值出现在方括号中，[要赋予的值]表示某个值。示例见 7.1.1.3。

4 应用级防火墙概述

本标准规定了应用级防火墙在低风险（敏感但不保密）环境下的最低安全要求。明确了应用级防火

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

墙应阻止的威胁，定义了它的安全目标和使用环境，提出了应用级防火墙的安全功能和安全保证要求。同时，说明了防火墙安全目标及功能和保证要求的基本原则。

防火墙的目的是对进、出内部网的服务访问实行控制和审计。准许、拒绝或重新定向通过防火墙的数据流。虽然防火墙的体系结构和技术多种多样，但防火墙产品基本上可分成两类：包过滤防火墙和应用级防火墙。网络中防火墙的典型位置如图 1 所示。

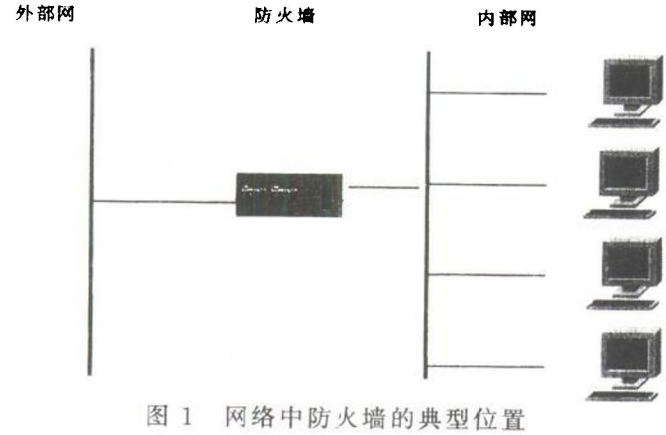

图 1　网络中防火墙的典型位置

应用级防火墙的作用是：仲裁不同网络上客户和服务器之间的通信业务流。应用级防火墙通常与包过滤控制配合使用，以承担对应用级协议包的进一步控制。（例如：FTP、Telnet）。应用级防火墙可以雇用代理服务器筛选数据包。

5　安全环境

符合本标准的防火墙用于敏感但不保密的信息处理环境。防火墙应提供访问控制策略、身份标识与鉴别、远程管理员会话加密、一定的审计能力以及最基本的安全保证。

5.1　安全条件假定

假定防火墙的运行环境符合以下条件：

5.1.1　单一接入（A.SINGLEPT）

如图 1 所示意的那样，防火墙是网络间唯一的互连点。

5.1.2　物理访问控制（A.SECURE）

防火墙和与其直接相连的控制台在物理上是安全的，而且仅供授权人使用。

5.1.3　通信保护（A.COMMS）

信息传输的保护级别应该与信息的敏感性一致（例如：受物理保护的传输媒体，加密），或者明确说明该信息可以明文传输。

5.1.4　用户（A.USER）

应用级防火墙提供的不是通常意义下的计算能力（例如：执行任意代码或应用程序），它对通过防火墙发送通信业务流的用户进行身份标识和鉴别。只有授权管理员才能直接访问和远程访问防火墙。

5.1.5　授权管理员（A.NOEVIL）

管理员应值得信任、无恶意，能够正确执行各项职责。

5.2　安全威胁

本标准的目的在于提供一种能力，以控制通过防火墙的数据包，限制那些潜在恶意用户的活动能力，阻止他们获得对内部网或者对内部网上的某一主机的访问权。

5.2.1　防火墙阻止的威胁

符合本标准的防火墙应能阻止以下威胁：

5.2.1.1　未授权逻辑访问（T.LACCESS）

未经授权的人可能在逻辑上访问防火墙。未经授权的人是指除防火墙的授权用户之外，所有已经或可能企图访问这个系统的人。

5.2.1.2 假冒网络地址攻击(T.ISPOOF)

一个主体可能假冒成另一个主体获得对特定信息的访问。例如，外部网上的一个用户可能利用假地址伪装成内部网上的用户访问内部资源。

5.2.1.3 针对内部网络的攻击(T.NATTACK)

攻击者利用高层协议和服务，对内部受保护网络或者网上的主机进行攻击，这类攻击可能以拒绝服务和穿透主机或网络结点为目的。

5.2.1.4 审计记录丢失或破坏(T.AUDIT)

攻击者可能采取耗尽审计存储量的方法导致审计记录丢失或破坏。

5.2.1.5 对防火墙的配置和其他与安全相关数据的更改(T.DCORRUPT)

这类攻击包括所有采用读取或修改防火墙的内部代码或数据结构，以及防火墙的配置参数和与安全相关的数据，对防火墙实施的攻击。

5.2.1.6 绕开身份标识和鉴别机制(T.AUTH)

这类攻击企图绕过或欺骗身份识别和鉴别机制，假冒成另一个授权管理员或侵入已建立的会话连接。例如，拦截鉴别信息(如口令字)，重放有效的鉴别交换信息，以及截取会话连接等攻击。

5.2.2 运行环境阻止的威胁

下述威胁必须通过物理控制、过程措施或者管理手段来对付。

5.2.2.1 被保护网上的恶意用户试图向外部用户提供信息(T.INSHARE)

这种威胁是指内部网络用户试图给外部网络上的非授权用户发送信息。由于防火墙主要用于保护内部网络免受外部网络的侵害，因此，它们对抵御这种威胁作用不大。

5.2.2.2 受保护网络上的恶意用户攻击同一网络上的计算机(T.INALL)

防火墙的主要目的是保护防火墙内部的网络用户免受外部用户的侵害。因此，它无法控制不经过防火墙的通信业务流。属于此范畴的攻击是指来自受保护网络内的对本网络服务功能的攻击，以及对同一网段上的计算机的攻击。

5.2.2.3 攻击高层协议和服务(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。符合本标准的防火墙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，仍有可能攻击上述的这些服务。

5.2.2.4 截取传输信息(T.PRIVACY)

攻击者可能截取通过防火墙传输的敏感信息。

6 安全目标

6.1 信息技术安全目标

防火墙应达到的信息技术安全目标如下：

6.1.1 访问仲裁(O.ACCESS)

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，在防火墙连接的网络之间提供受控制的访问，这些控制是根据主体、客体的有关参数以及管理上配置的访问控制规则实现的。

6.1.2 管理员访问(O.ADMIN)

仅限授权的管理者才能访问防火墙，即只允许他们有配置防火墙的能力。

6.1.3 个体身份记录(O.ACCOUNT)

个体身份记录提供了对用户身份的记录能力，并允许基于唯一身份对访问做出判定。鉴别为确定身

份是否真实提供了方法。

6.1.4 防火墙的自保护(O.PROTECT)

为了成功地达到这一目标,防火墙应能把正在处理的数据与需要运算的数据分开,应保护自己不受外部实体的攻击。此外,防火墙还应能保护授权管理员的通信会话。

6.1.5 审计(O.AUDIT)

审计记录对于判定是否存在绕过安全策略的尝试,是否有因配置错误而允许了本应拒绝的访问这类问题起着十分重要的作用。不仅应收集审计数据,还应使其具有可读性并容易使用。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,以帮助管理者做出正确的安全决定。

6.2 非信息技术安全目标

非信息技术安全目标是指除防火墙技术要求之外还需满足的要求。它们不必实施防火墙硬件和软件的机制,而是通过采用物理的、过程的或管理的方法来达到安全目标。

6.2.1 安装与操作控制(O.INSTALL)

要确保防火墙的交付、安装、管理和操作都是安全可控的。

6.2.2 物理控制(O.PACCESS)

应控制对防火墙的物理访问。

6.2.3 授权管理人员培训(O.TRAIN)

对授权管理员进行培训,以保证建立和维护正确的安全策略和实施水准。

7 安全要求

本章提出了符合本标准的防火墙必须满足的功能和保证要求。

7.1 功能要求

本标准的安全功能要求概括于表1:

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_AFC.2	多种安全属性访问控制
	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
标识与鉴别	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**和用户唯一身份标识
密码支持	FCS_COP.2	符合规定的加密操作

表 1（完）

功能分类	功 能 组 件	
可信安全功能保护	FPT _ RVM. 1	防火墙安全策略的不可旁路性
	FPT _ SEP. 1	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

要求综述：防火墙的安全策略由多级安全功能策略（SFPs）组成。下面定义两种策略，第一种策略称为：**未鉴别的端到端策略**，主要讨论一个内部或外部网络上的主体通过防火墙发送数据流到一个外部或内部网络上的客体。第二种策略称为：**有鉴别的端到端策略**，主要讨论一个内部或外部网络上的主体在发送数据流前，必须通过防火墙的鉴别，才能将数据流传送给一个外部或内部网络上的客体。

7.1.1 用户数据保护类（FDP）

7.1.1.1 完整的客体访问控制（1）（FDP _ ACC. 2）

FDP _ ACC. 2. 1 防火墙的安全功能应在以下方面执行［未鉴别的端到端策略］：

a）［主体：未经防火墙鉴别的主机］；

b）［客体：内部或外部网上的主机］；

［以及安全功能策略（SFP）所包括的主体、客体的所有操作］。

FDP _ ACC. 2. 2 防火墙的安全功能应确保安全功能策略包括了控制范围内的任何主体和客体之间的所有操作。

7.1.1.2 完整的客体访问控制（2）（FDP _ ACC. 2）

FDP _ ACC. 2. 1 防火墙的安全功能应在以下方面执行［有鉴别的端到端策略］：

a）［主体：经防火墙鉴别的用户］；

b）［客体：在内部或外部网络上的主机］；

［以及安全功能策略所包括的主体、客体的所有操作］。

FDP _ ACC. 2. 2 防火墙的安全功能应确保安全功能策略包括了控制范围内的任何主体和客体之间的所有操作。

7.1.1.3 访问授权与拒绝（FDP _ ACF. 4）

FDP _ ACF. 4. 1 防火墙的安全功能应执行：

a）［未鉴别的端到端策略］；

b）［有鉴别的端到端策略］；

根据主体和客体的安全属性值提供明确的访问保障能力。

FDP _ ACF. 4. 2 防火墙的安全功能应执行：

a）［未鉴别的端到端策略］；

b）［有鉴别的端到端策略］；

根据主体和客体的安全属性值提供明确的拒绝访问能力。

7.1.1.4 多种安全属性访问控制(1)(FDP_ACF.2)

FDP_ACF.2.1 防火墙应根据[源地址、目的地址、运输层协议和请求的服务(如源端口号和/或目的端口号)]对客体执行[未鉴别的端到端策略]。

FDP_ACF.2.2 防火墙应执行以下附加规则,以确定受控主体与受控客体之间的操作是否被允许:

a) [防火墙应拒绝从外部网络发出的、但拥有内部网络上的主机源地址的访问或服务请求];

b) [防火墙应拒绝从外部网络发出的、但拥有广播网络上的主机源地址的访问或服务请求];

c) [防火墙应拒绝从外部网络发出的、但拥有保留网络上的主机源地址的访问或服务请求];

d) [防火墙应拒绝从外部网络发出的、但拥有环回网络上的主机源地址的访问或服务请求]。

7.1.1.5 多种安全属性的访问控制(2)(FDP_ACF.2)

FDP_ACF.2.1 防火墙应根据[用户ID、源地址、目的地址、运输层协议和请求的服务(如源端口号和/或目的端口号),以及服务命令(例如:FTP STOR/RUT)]对客体执行[有鉴别的端到端策略]。

FDP_ACF.2.2 防火墙应执行以下附加规则以确定受控主体与受控客体之间的操作是否被允许:

a) [防火墙应拒绝从外部网络发出的、但拥有内部网络上的主机源地址的访问或服务请求];

b) [防火墙应拒绝从外部网络发出的、但拥有广播网络上的主机源地址的访问或服务请求];

c) [防火墙应拒绝从外部网络发出的、但拥有保留网络上的主机源地址的访问或服务请求];

d) [防火墙应拒绝从外部网络发出的、但拥有环回网络上的主机源地址的访问或服务请求]。

7.1.1.6 资源分配时对遗留信息的充分保护(FDP_RIP.3)

FDP_RIP.3.1 防火墙安全功能应确保在为所有客体进行资源分配时,不提供以前的信息内容。

应用注解:该要求用于支持连接所有设备资源(例如,寄存器、缓存器)的管理要求,目的是不允许用户访问以前的会话信息。通常,通过清除或覆盖这些信息来达到该项要求。

要求综述: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。

7.1.1.7 管理员属性修改(FDP_SAM.1)

FDP_SAM.1.1 防火墙应执行*访问控制安全功能策略:*

a) *未鉴别的端到端策略;*

b) *有鉴别的端到端策略;*

以向授权管理员提供修改以下参数的能力:

a) [标识与角色(例如:授权管理员)的关联];

b) [FDP_ACF.2中标识的访问控制属性];

c) [与安全相关的管理数据]。

7.1.1.8 管理员属性查询(FDP_SAQ.1)

FDP_SAQ.1.1 防火墙应执行*访问控制安全功能策略:*

a) *未鉴别的端到端策略;*

b) *有鉴别的端到端策略;*

以向授权管理员提供以下查询能力:

a) [FDP_ACF.2中标识的访问控制属性];

b) [主机名];

c) [用户名]。

7.1.2 标识与鉴别功能类

7.1.2.1 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 防火墙应提供与[FIA _ UAU. 1 和 FIA _ UAU. 2 中规定的鉴别机制]有关的**授权管理员、可信主机**以及用户鉴别数据的初始化功能。

FIA _ ADA. 1. 2 防火墙应确保只允许授权管理员使用这些功能。

7. 1. 2. 2 **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 防火墙安全功能应保护存储于设备中的鉴别数据不被未授权查阅、修改和破坏。

7. 1. 2. 3 鉴别失败的基本处理(FIA _ AFL. 1)

FIA _ AFL. 1. 1 防火墙的安全功能应能够在鉴别尝试[经一个可设定的次数]失败以后,终止**可信主机**或用户建立会话的过程。**最多失败次数仅由授权管理员设定**。

FIA _ AFL. 1. 2 在**可信主机**或用户会话建立过程终止后,防火墙的安全功能应能够关闭**相应的***可信主机或用户的帐号*,直至[授权管理员重新开启]。

7. 1. 2. 4 **授权管理员、可信主机、主机**和用户属性初始化(FIA _ ATA. 1)

FIA _ ATA. 1. 1 防火墙的安全功能应提供用默认值对**授权管理员、可信主机、主机**和用户属性初始化的能力。

7. 1. 2. 5 唯一的**授权管理员、可信主机、主机**和用户属性的定义(FIA _ ATD. 2)

FIA _ ATD. 2. 1 防火墙的安全功能应**为每一个规定的授权管理员、可信主机、主机和用户**提供一套唯一的、为执行安全策略所必需的安全属性。

7. 1. 2. 6 **授权管理员**的基本鉴别(FIA _ UAU. 1)

FIA _ UAU. 1. 1 防火墙的安全功能应鉴别任何通过防火墙控制台履行**授权管理员**职能的管理员身份。

7. 1. 2. 7 单一使用的鉴别机制(FIA _ UAU. 2)

FIA _ UAU. 2. 1 防火墙的安全功能应当在执行任何与**授权管理员、可信主机**或用户相关功能之前,**鉴别授权管理员、可信主机**或用户的身份。

FIA _ UAU. 2. 2 防火墙的安全功能应防止与[远程授权管理员、远程可信主机和用户要求的下述服务相关的鉴别数据重用。

——文件传送协议(FTP);

——超文本传输协议(HTTP);

——登录;

——邮政协议(POP);

——远程登录;

——简单网络管理协议(SNMP);

——Telnet。]

应用注解:只有防火墙提供的服务才需要满足这一要求。

7. 1. 2. 8 **授权管理员、可信主机、主机**和用户唯一身份标识(FIA-UID. 2)

FIA _ UID. 2. 1 防火墙的安全功能应确保每一个授权管理员、可信主机、主机或用户在请求执行任何操作之前,对其进行唯一身份识别。

7. 1. 3 密码支持功能类(FEN)

符合规定的加密操作(FCS _ COP. 2)

FCS _ COP. 2. 1 防火墙的安全功能应保证其远程管理会话加密符合国家密码管理的有关规定。

7. 1. 4 可信安全功能保护类(FPT)

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。

7. 1. 4. 1 防火墙安全策略的不可旁路性(FPT _ RVM. 1)

FPT _ RVM. 1. 1 防火墙的安全功能应确保允许任何与安全有关的操作执行之前,必须通过安全

策略的检查。

7.1.4.2 安全功能区域分隔(FPT _ SEP.1)

FPT _ SEP.1.1 防火墙的安全功能应为其自身的执行过程设定一个安全区域,以保护其免遭不可信主体的干扰和篡改。

FPT _ SEP.1.2 防火墙的安全功能应把防火墙控制范围内的各个主体的安全区域分隔开。

7.1.4.3 区分安全管理角色(FPT _ TSA.2)

FPT _ TSA.2.1 防火墙的安全功能应将与安全相关的管理功能与其他功能区分开。

FPT _ TSA.2.2 在防火墙的安全功能中,与安全相关的管理功能集应包括安装、配置和管理防火墙安全功能所需的所有功能,其中至少应包括[增加和删除主体和客体;查阅访问控制安全属性;分配、修改和撤销访问控制安全属性;查阅和管理审计数据]。

FPT _ TSA.2.3 防火墙的安全功能应把执行与安全相关的管理功能的能力限定为一种安全管理角色,该角色具有一套特别授权的功能和相应的责任。

FPT _ TSA.2.4 防火墙的安全功能应能把授权执行管理功能的**授权管理员和可信主机**与使用防火墙的所有**其他个人或系统**分开。

FPT _ TSA.2.5 防火墙的安全功能应仅允许**授权管理员和可信主机**承担安全管理角色。

FPT _ TSA.2.6 防火墙的安全功能在确认**授权管理员或可信主机**的安全管理角色前,需要接到一个明确的请求。

7.1.4.4 管理功能(FPT _ TSM.1)

FPT _ TSM.1.1 防火墙的安全功能应使授权管理员具有设置和更新[与安全相关的管理数据],**以及对用户授予或取消** FIA _ UAU.2.2 **中各项服务的鉴别能力**。

FPT _ TSM.1.2 防火墙的安全功能应提供给授权管理员[安装和初始化配置防火墙、起动和关闭系统以及备份和恢复]的能力。**备份能力应由自动工具支持**。

如果防火墙的安全功能支持外部或内部接口的远程管理,那么它应该:

a) **具有对内、外两个接口或其中之一关闭远程管理的选择权;**

b) **能够限制那些可进行远程管理的地址;**

c) **能够通过加密来保护远程管理对话。**

7.1.5 安全审计功能类(FAU)

要求概述:下列安全功能要求(FAU 类)规定了安全审计信息的生成、管理、保护和处理。

7.1.5.1 审计数据生成(FAU _ GEN.1)

FAU _ GEN.1.1 防火墙的安全功能应能够对下列可审计事件生成一个审计记录:

a) 审计功能的启动和关闭;

b) 所有与*基本或最低*审计级别有关的可审计事件,**定义在表 2 中的那些**功能组件中;

c) 根据所有包含在安全目标中的功能组件,附加事件*在表 2 中标为"扩展"的事件。*

FAU _ GEN.1.2 防火墙的安全功能应在每一个审计记录中至少记录以下信息:

a) 事件发生的日期和时间,事件的类型,主体身份和*成功或失败*事件。

b) 根据本标准对其他功能组件的可审计事件定义,对每一类审计事件,**附加信息说明在表 2 第 4 列**。

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。	若适用,受影响客体的标识
FAU _ PRO	基本	任何读取、修改、破坏审计跟踪的尝试。	
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

表 2（完）

功能族	级别	可审计事件	附加审计记录内容
FDP _ SAM	基本	修改安全属性的所有尝试，包括拟修改对象的身份。	修改后安全属性的新值
FDP _ SAQ	基本	查询安全属性的所有尝试，包括查询对象的身份。	
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。	
FPT _ TSA	最低	使用某项与安全相关的管理功能。	
FPT _ TSM	基本	所有对安全功能配置参数的修改（设置和更新），无论成功与否。	配置参数的新值

7.1.5.2 审计追踪管理(FAU _ MGT.1)

FAU _ MGT.1.1 防火墙的安全功能应使管理员能*创建、存档、删除和清空*审计记录。

7.1.5.3 可理解的格式(FAU _ POP.1)

FAU _ POP1.1 防火墙的安全功能应能使存储于永久性审计记录中的所有审计数据可为人所理解。

7.1.5.4 限制审计跟踪访问(FAU _ PRO.1)

FAU _ PRO.1.1 防火墙的安全功能应只允许授权管理员访问审计记录。

7.1.5.5 限制审计查阅(FAU _ SAR.1)

FAU _ SAR.1.1 防火墙的安全功能应提供具有查阅审计数据能力的工具。

FAU _ SAR.1.2 防火墙应只允许授权管理员使用审计查阅工具。

7.1.5.6 可选择查阅审计(FAU _ SAR.3)

FAU _ SAR.3.1 防火墙的安全功能应提供能对审计数据进行查找和排序的审计查阅工具：

a）[主体 ID；

b）客体 ID；

c）日期；

d）时间；

e）上述各参数的逻辑组合(如“和”、“与”)]。

应用注释：防火墙开发者应该详细描述审计查阅工具的功能，尤其是必须描述基于安全相关属性的查找和排序能力。

7.1.5.7 防止审计数据丢失(FAU _ STG.3)

FAU _ STG.3.1 防火墙的安全功能应把生成的审计记录，储存于一个永久性的审计记录中。

FAU _ STG.3.2 防火墙的安全功能应限制由于*故障和攻击*造成的审计事件丢失的数量。

FAU _ STG.3.3 一旦审计存储耗尽，防火墙应能保证在授权管理员所采取的审计行为以外，*防止*其他可审计行为的出现。

应用注解：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。

7.2 保证要求

防火墙的安全保证要求是对防火墙产品或系统的开发研制及供应商提出的管理性规定。这些要求与“信息技术安全评估通用准则”中的安全保证要求是一致的。内容见下表。

表 3 保证要求

保证分类	保证组件	
配置管理	ACM_CAP.1	最低限度的支持
交付和操作	ADO_IGS.1	安装、生成和启动过程
开发	ADV_FSP.1	防火墙和安全策略
	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——非形式分析
	ATE_FUN.1	功能测试
	ATE_DPT.1	测试——功能规范
脆弱性分析	AVA_SOF.1	防火墙安全功能强度的评估
	AVA_VLA.1	开发者脆弱性分析

7.2.1 配置管理保证类(ACM)

7.2.1.1 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 配置目录应描述防火墙的各个配置项目，**并应包括防火墙使用的外部网络的服务项目。**

ACM_CAP.1.3C 配置管理文件应描述用来唯一识别防火墙配置项的方法。

ACM_CAP.1.1E 评估者应该确信所提供的信息满足在内容和表述上的所有要求。

7.2.2 交付和操作保证类(ADO)

7.2.2.1 安装、生成和启动过程(ADO_IGS.1)

ADO_IGS.1.1D 开发者应以文件方式说明用于防火墙的安全安装、生成和启动的过程。

ADO_IGS.1.1C 说明文件中应描述防火墙的安全安装、生成和启动所必须的步骤。

ADO_IGS.1.1E 评估者应确认所提供的信息满足在内容和表述上的所有要求。

7.2.3 开发保证类(ADV)

7.2.3.1 防火墙和安全策略(ADV_FSP.1)

ADV_FSP.1.1D 开发者应提供防火墙的功能规范。

ADV_FSP.1.2D 开发者应提供防火墙的安全策略。

ADV_FSP.1.1C 功能规范应以非形式方法来描述安全策略。

ADV_FSP.1.2C 功能规范应包括以非形式方法表述的所有外部安全功能接口的语法和语义。

ADV_FSP.1.3C 功能规范应包括能证明安全功能已完全实现了的证据。

应用注解：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在内容和表述上的所有要求。

ADV_FSP.1.2E 评估者应确认功能规范与安全策略是一致的。

ADV_FSP.1.3E 评估者应确认安全功能的表述是否包含了安全目标中的每一项功能要求。

7.2.3.2 高层设计描述(ADV _ HLD.1)

ADV _ HLD.1.1D 开发者应提供防火墙安全功能的高层设计。

ADV _ HLD.1.1C 高层设计应以非形式方法表述。

ADV _ HLD.1.2C 高层设计应根据子系统来描述安全功能的结构。

ADV _ HLD.1.3C 高层设计应描述由安全功能的每个子系统提供的安全功能。

ADV _ HLD.1.4C 高层设计标明安全子系统接口。

ADV _ HLD.1.5C 高层设计应说明安全功能所需的所有底层硬件、固件和软件,以及其中已实现的保护机制所提供的功能。

ADV _ HLD.1.1E 评估者应确认所提供的信息满足在内容和表述上的所有要求。

ADV _ HLD.1.2E 评估者应确认安全功能的表述是否包含了安全目标中的每一项功能要求。

7.2.3.3 非形式的一致性证明(ADV _ RCR.1)

ADV _ RCR.1.1D 开发者应证明所提供的对安全功能的扼要表述,准确、一致并且完整地反应了安全目标中的功能要求。

ADV _ RCR.1.1C 对于同一安全功能的两个相邻层的表述,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方法表述。

ADV _ RCR.1.1E 评估者应确认所提供的信息满足在内容和表述上的所有要求。

ADV _ RCR.1.2E 评估者应对安全目标中所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,以保证准确、一致和完整。

7.2.4 指南文件保证类(AGD)

7.2.4.1 管理员指南(AGD _ ADM.1)

AGD _ ADM.1.1D 开发者应提供能满足系统管理者需要的管理员指南。

AGD _ ADM.1.1C 管理员指南应描述怎样以安全的方式管理防火墙。

AGD _ ADM.1.2C 对于应该控制在安全处理环境中的功能和特权,管理员指南应有警告。

AGD _ ADM.1.3C 管理员指南应对一致、有效地使用安全功能提供指导。

AGD _ ADM.1.4C 管理员指南应说明两种类型功能之间的差别:一种是允许管理员控制安全参数,而另一种是只允许管理员获得信息。

AGD _ ADM.1.5C 管理员指南应描述管理员控制下的所有安全参数。

AGD _ ADM.1.6C 管理员指南应描述各类需要执行管理功能的安全相关事件,包括在安全功能控制下改变实体的安全特性。

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防火墙的指令。

AGD _ ADM.1.9C 管理员指南应描述在防火墙的安全安装过程中,可能要使用的所有配置选项。

AGD _ ADM.1.10C 管理员指南应充分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给评估的其他文件一致。

AGD _ ADM.1.1E 评估者应确认所提供的信息能满足在内容和表述上的所有要求。

AGD _ ADM.1.2E 评估者应确认安装过程能产生一个安全的配置。

7.2.4.2 用户指南(AGD _ USR.1)

AGD _ USR.1.1D 开发者须提供用户指南。

AGD _ USR.1.1C 用户指南应描述用户可使用的安全功能和接口。

AGD_USR.1.2C 用户指南应该包含使用防火墙提供的安全功能的指导。

AGD_USR.1.3C 对于应该控制在安全处理环境中的功能和特权，用户指南应有警告。

AGD_USR.1.4C 用户指南应描述用户可见的安全功能之间的相互作用。

AGD_USR.1.5C 用户指南应与提交给评估的其他文件一致。

AGD_USR.1.1E 评估者应确认所提供的信息能满足在内容和表述上的所有要求。

7.2.5 测试保证类(ATE)

7.2.5.1 独立测试——一致性(ATE_IND.1)

ATE_IND.1.1D 开发者应向国家授权的信息安全产品测评认证机构提供用于测试的防火墙。

ATE_IND.1.1C 防火墙应适合于测试。

ATE_IND.1.1E 评估者应确认所提供的信息能满足在内容和表述上的所有要求。

7.2.5.2 测试覆盖面——非形式分析(ATE_COV.1)

ATE_COV.1.1D 开发者应提供对测试覆盖范围的分析。

ATE_COV.1.1C 测试覆盖范围分析应证明测试文件中确定的测试项目能覆盖防火墙的安全功能。

ATE_COV.1.1E 评估者应确认所提供的信息能满足在内容和表述上的所有要求。

7.2.5.3 功能测试(ATE_FUN.1)

ATE_FUN.1.1D 开发者应该测试防火墙的安全功能，并记录其结果。

ATE_FUN.1.2D 开发者应提供测试文件。

ATE_FUN.1.1C 测试文件应包括测试计划、测试过程描述和测试结果。

ATE_FUN.1.2C 测试计划应确定将要测试的安全功能，并描述将要达到的测试目标。

ATE_FUN.1.3C 测试过程的描述应确定将要进行的测试，并描述测试每一安全功能的具体情况。

ATE_FUN.1.4C 测试文件中的测试结果应给出每一次测试所预期的结果。

ATE_FUN.1.5C 开发者得到的测试结果应能证明每一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能满足在内容和表述上的所有要求。

7.2.5.4 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，充分表明了防火墙的运行符合安全功能规范。

ATE_DPT.1.1E 评估者应确认所提供的信息能满足在内容和表述上的所有要求。

7.2.6 脆弱性分析保证类(AVA)

7.2.6.1 防火墙安全功能强度的评估(AVA_SOF.1)

AVA_SOF.1.1D 开发者应确定防火墙适合做安全功能强度分析的安全机制。

AVA_SOF.1.2D 开发者应对确定的每一机制进行安全功能强度分析。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，防火墙安全功能强度分析应能判定所标明的安全机制对其产生的影响。

AVA_SOF.1.2C 防火墙安全功能强度分析应证明所标明的安全功能强度与安全目标是一致的。

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能满足在内容和表述上的所有要求。

AVA_ADM.1.2E 评估者应确认所有需要强度分析的防火墙安全机制已被确定。

AVA_SOF.1.3E 评估者应确认所有强度声明已经确定。

7.2.6.2 开发者脆弱性分析(AVA_VLA.1)

AVA_VLA.1.1D 开发者应从用户可能破坏安全策略的明显途径方面,对防火墙的各种功能进行分析并提供文件。

AVA_VLA.1.2D 开发者应明确记录对确定的脆弱性的处置。

AVA_VLA.1.1C 对每一条脆弱性应有证据显示,该脆弱性在使用防火墙的环境中不能被利用。

AVA_VLA.1.1E 评估者应确认所提供的信息能满足在内容和表述上的所有要求。

AVA_VLA.1.2E 评估者应在开发者脆弱性分析的基础上进行渗透测试,以确保明显的薄弱点已得到加强。

8 基本原则

8.1 信息技术安全目标的基本原则

8.1.1 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。

8.1.2 管理员访问(O.ADMIN)

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

8.1.3 个体身份记录(O.ACCOUNT)

此安全目标对防止 T.LACCESS 威胁是必需的。

8.1.4 防火墙的自保护(O.PROTECT)

此安全目标对防止 T.DCORRUPT 和 T.AUTH 威胁是必需的。

8.1.5 审计(O.AUDIT)

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

表 4 威胁与信息技术安全目标之间的关系

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

8.2 非信息技术安全目标的基本原则

8.2.1 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。

8.2.2 物理控制(O.PACCESS)

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

8.2.3 授权管理员培训(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。

表 5 威胁和非信息技术安全目标之间的关系

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

8.3 信息技术功能要求的基本原则

8.3.1 完整的客体访问控制(FDP _ ACC. 2)

该组件用于定义防火墙的访问控制功能,它直接支持访问仲裁安全目标(O. ACCESS)。

8.3.2 访问授权与拒绝(FDP _ ACF. 4)

该组件要求防火墙具有对访问控制功能的配置能力,实际上就是允许管理员实现其安全策略。该组件直接支持访问仲裁安全目标(O. ACCESS)。

8.3.3 多种安全属性访问控制(FDP _ ACF. 2)

该组件规定防火墙的访问控制功能,它直接支持访问仲裁安全目标(O. ACCESS)。

8.3.4 资源分配时对遗留信息的充分保护(FDP _ RIP. 3)

该组件用于避免遗留数据在存储体中暴露。该组件确保用户不能意外的得到不该属于他们的数据,以支持访问控制策略。它支持访问仲裁安全目标(O. ACCESS)。

8.3.5 管理员属性修改(FDP _ SAM. 1)

该组件要求管理员是唯一能够配置和修改防火墙访问控制功能的人。该组件直接支持访问仲裁安全目标(O. ACCESS)和管理员访问安全目标(O. ADMIN)。

8.3.6 管理员属性查询(FDP _ SAQ. 1)

该组件允许管理员具有查询自己设置的访问控制规则的能力。该组件直接支持管理员访问安全目标(O. ADMIN)和访问仲裁安全目标(O. ACCESS)。

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

该组件支持授权管理员对鉴别数据的初始化并始终对其进行管理。该组件支持个体身份记录安全目标(O. ACCOUNT)和管理员访问安全目标(O. ADMIN)。

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

该组件提供用户鉴别数据的保护,这样做对满足个体身份记录安全目标(O. ACCOUNT)和防火墙自保护安全目标(O. PROTECT)是很关键的。

8.3.9 鉴别失败的基本处理(FIA _ AFL. 1)

该组件用于防止对防火墙反复、隐蔽的攻击,特别是像对身份和口令等鉴别数据的猜测尝试。它直接支持防火墙自保护安全目标(O. PROTECT),同时支持管理员访问安全目标(O. ADMIN)和个体身份记录安全目标(O. ACCOUNT)。

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

按照定义和初始化用户属性的需要,该组件支持个体身份记录安全目标(O. ACCOUNT)。

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

该组件支持 FDT _ TSA. 2 中的依赖性,满足定义共享属性的需要,且直接支持个体身份记录安全目标(O. ACCOUNT)。

8.3.12 授权管理员的基本鉴别(FIA _ UAU. 1)