ICS 35.020
L 80

中华人民共和国国家标准

GB/T 18019—1999

信 息 技 术
包过滤防火墙安全技术要求

Information technology —
Security requirements for packet filter firewalls

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
信 息 技 术
包过滤防火墙安全技术要求
GB/T 18019—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 35 千字
2000年6月第一版　2000年6月第一次印刷
印数 1—1 600
*
书号:155066·1-16688　定价 13.00 元
*
标 目 410—25

前　言

本标准规定了采用“传输控制协议/网间协议”的包过滤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：中国国家信息安全测评认证中心、电子部30所。

本标准主要起草人：吴世忠、陈晓桦、龚奇敏、张桂清、杨燕伟、贺卫东、黄元飞。

目　　次

中华人民共和国国家标准

信 息 技 术
包过滤防火墙安全技术要求

GB/T 18019—1999

Information technology —
Security requirements for packet filter firewalls

1 范围

本标准规定了采用“传输控制协议/网间协议(TCP/IP)”的包过滤防火墙产品或系统的安全技术要求。

本标准适用于防火墙产品或系统安全功能的研制、开发、测试、评估和产品的采购。

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 (idt ISO 7498-2:1989)

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 术语定义

本标准采用了GB/T 9387.2中的下列术语和定义：

审计 audit

鉴别 authentication

密钥管理 key management

下列术语适用于本标准。

3.1.1 用户 user

一个在防火墙外与防火墙相互作用的人，此人不具有能够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个人。本标准中的“授权管理员”特指防火墙的管理员，其职责不包括网络管理。

3.1.3 主机 host

一台在防火墙外与防火墙相互作用的机器，它不具有能够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机器。

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。

国家质量技术监督局1999-11-11批准　　2000-05-01实施

示例见7.1.2.3。

选择：用于从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 包过滤防火墙概述

本标准规定包过滤防火墙的最低安全要求，指出该类防火墙应对付的威胁，定义其实现的安全目标及环境，提出安全功能和安全保证要求。

防火墙的目的是要在内部、外部两个网络之间建立一个安全控制点，通过允许、拒绝或重新定向经过防火墙的数据流，实现对进、出内部网络的服务和访问的审计和控制。虽然防火墙的体系结构和技术多种多样，但防火墙产品主要分为两类：包过滤和应用网关。本标准规定了包过滤防火墙的最低安全要求。

符合本标准的防火墙在内外网络之间的位置的逻辑表示如图1所示。包过滤防火墙应根据站点的安全策略，在内部网络和外部网络之间选择性地过滤包。其过滤规则主要是根据源地址、目的地址、协议、源端口、目的端口以及包到达或发出的接口而定。

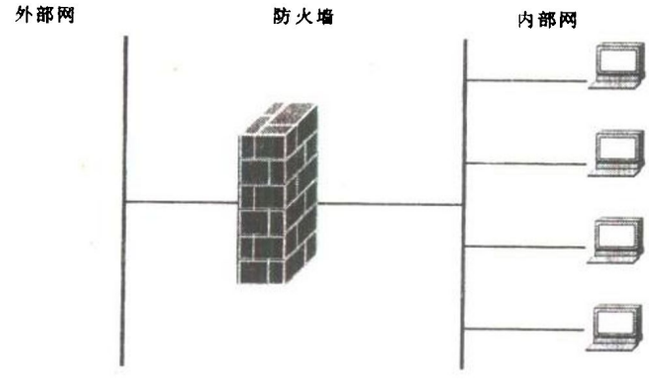

图1 防火墙在网络中的典型位置

5 安全环境

符合本标准的防火墙产品应能提供访问控制策略、身份识别和鉴别、远程管理的加密、安全审计功能和最基本的安全保证。可用于政府部门、企事业单位和商业领域等。

5.1 安全使用的条件

防火墙的使用操作环境应满足以下条件。

5.1.1 连接条件

防火墙的连接条件要求如下：

单一接入：防火墙是内、外网络之间的唯一连接点，见图1。

5.1.2 物理条件

防火墙应满足下列物理条件。

5.1.2.1 物理访问控制

防火墙及其所属的可直接插接的控制端口在物理上是安全的，并只有授权的人员才可访问。

5.1.2.2 通信保护

对已传送的所有信息的保护级别与正在被发送的信息的保护级别相当（例如，受物理保护的传输媒体、加密），但明确规定以明文传输的信息除外。

5.1.3 人员条件

5.1.3.1 用户服务

包过滤防火墙不提供通常意义上的计算能力，对网络用户基本上是“透明”的。只有授权的管理员可直接访问或远程访问。

5.1.3.2 授权管理员

授权的管理员应是可以信赖、且能善尽职守的人。

5.2 防火墙面临的威胁

符合本标准的防火墙应能对付以下威胁。

5.2.1 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。

5.2.2 假冒网络地址攻击 (T.ISPOOF)

一个主体可能通过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。

5.2.3 针对内部网络的攻击 (T.NATTACK)

攻击者可能利用高层协议和服务，对内部受保护的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。

5.2.4 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。

5.2.5 对防火墙配置和其他与安全有关数据的更改 (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、配置和与安全相关的数据，对防火墙实施的攻击。

5.2.6 绕开身份识别和鉴别机制 (T.AUTH)

这类攻击是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。

5.3 运行环境面临的威胁

以下的可能威胁不是符合本标准的防火墙所能处理的。它们应靠环境、制度程序来对付，可列为对系统的潜在威胁。

5.3.1 受保护网络(内部网)上的恶意用户企图把信息传送给网外用户 (T.INSHARE)

这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。由于防火墙的设计主要是为了保护内部网络免受外部网的侵害，所以难以对付此类威胁。

5.3.2 受保护网络上的恶意用户攻击同一网上的计算机 (T.INALL)

由于防火墙主要是用来保护防火墙内的网络用户免受防火墙外的用户的攻击，因此它无法控制不经过防火墙的通信业务。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，或者对同一网段上的计算机的攻击。

5.3.3 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，那么仍有可能对上述的这些服务攻击。

5.3.4 截取传输的信息 (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 信息技术性安全目标

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)

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,为连接在防火墙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,由防火墙生成的状态信息和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)

此项目标是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。

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连接。

6.1.5 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。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,它们不需防火墙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。

由于防火墙是完整的、独立的专用设备,因此正常工作时不必依靠任何其他设备。但是,为了支持防火墙的安全功能,应达到有关运行环境方面的某些目标。

防火墙的非信息技术安全目标如下。

6.2.1 安装与操作控制 (O.INSTALL)

要确保对防火墙的交付、安装、管理、操作都是安全可控的。

6.2.2 物理控制 (O.PACCESS)

对防火墙的物理访问应可控制。

6.2.3 授权管理员培训 (O.TRAIN)

安全管理员应经过专业培训,并得到资格认可,以建立并保持正确的安全策略和实施水准。

7 安全要求

本章给出了符合本标准的防火墙应满足的安全功能要求。

7.1 功能要求

本标准的安全功能要求由表1的下列项目组成:

7.1.1 用户数据保护功能类(FDP)

要求概述:防火墙的安全策略由一项安全功能策略构成。该策略定义如下:该策略称为未鉴别的端到端策略,用来处理防火墙一侧的主体向另一侧客体发送数据。

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
识别和鉴别	FIA _ ADA. 1	授权管理员和可信主机鉴别数据初始化
	FIA _ ADP. 1	授权管理员和可信主机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、可信主机和主机属性的初始化
	FIA _ ATD. 2	授权管理员、可信主机和主机唯一属性定义
	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、可信主机和主机唯一标识
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	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

7.1.1.1　完整的客体访问控制　(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中的任何主体和客体之间的所有操作。

7.1.1.2　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未鉴别的端到端策略，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未鉴别的端到端策略，根据主体和客体的安全属性值

提供明确的拒绝访问能力。

7.1.1.3 多种安全属性访问控制 (FDP _ ACF.2)

FDP _ ACF.2.1 防火墙应根据[源地址、目的地址、传输层协议和请求的服务(如源端口号或目的端口号)]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]。

7.1.1.4 资源分配时对遗留信息的充分保护 (FDP _ RIP.3)

FDP _ RIP.3.1 防火墙应保证在为所有客体进行资源分配时,不提供以前的任何信息内容。

应用注解:该要求是对用于支持连接的所有设备资源(例如寄存器、缓存器)管理的要求,目的是不让网络用户访问以前的任何会话信息。这样其他任何网络用户的通信中都不会包含别人的信息或会话片段。该要求通常是通过对这些设备资源进行清除或重写来达到。

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。

7.1.1.5 管理员属性修改 (FDP _ SAM.1)

FDP _ SAM.1.1 防火墙应执行*访问控制的功能策略(SFP):未鉴别的端到端策略*,向授权管理员提供修改下述参数的能力:

a) [标识与角色(例如: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]。

7.1.1.6 管理员属性查询 (FDP _ SAQ.1)

DP _ SAQ.1.1 防火墙应执行*访问控制的功能策略:未鉴别的端到端策略*,向授权管理员提供以下查询:

a) [FDP _ ACF.2 中标识的访问控制属性];

b) [主机名]。

7.1.2 识别与鉴别功能类 (FIA)

7.1.2.1 **授权管理员和可信主机**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**授权管理员和可信主机**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 **授权管理员和可信主机**鉴别数据的基本保护 (FIA _ ADP.1)

FIA _ ADP.1.1 防火墙应保护储存于设备中的鉴别数据不受未授权查阅、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**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**会话建立过程终止后,防火墙的安全功能应能够关闭*可信主机的帐号*,直至[授权管理员重新开启]。

7.1.2.4 **授权管理员、可信主机和主机**属性的初始化 (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、可信主机和主机**属性初始化的能力。

7.1.2.5 **授权管理员、可信主机和主机**唯一属性定义 (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、可信主机和主机**提供一套唯一的、为了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**通过防火墙的控制口**履行**授权管理员**功能的管理员身份。

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鉴别任何声称要履行**授权管理员和可信主机**功能的**管理员和主机**的身份。

FIA _ UAU.2.2 防火墙应预防与[远程管理和远程可信主机操作]有关的鉴别数据的重用。

7.1.2.8 **授权管理员、可信主机和主机**唯一身份识别 (FIA _ UID.2)

FIA _ UID.2.1 防火墙的安全功能应确保在所有**授权管理员、可信主机和主机**请求执行的任何操作之前，对每个**授权管理员、可信主机和主机**进行唯一身份识别。

7.1.3 保密功能类 (FEN)

7.1.3.1 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的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任何与安全有关的操作被允许执行之前，都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。

应用注解：该项可选。

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 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；查阅安全属性；分配、修改和撤销安全属性；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职责，该职责具有一套特别授权的功能和响应的责任。

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只允许**授权管理员和可信主机**承担安全管理职责。

FPT _ TSA.2.6 防火墙的安全功能应在提出一个明确的请求以后，才会让**授权管理员和可信主机**承担安全管理职责。

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能够设置和更新[与安全相关的数据]。

FPT _ TSM. 1.2　防火墙的安全功能应向授权管理员提供能够执行[防火墙的安装及初始配置，系统启动和关闭功能，备份和恢复]的能力。**备份能力应有自动工具的支持。**

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：下列功能安全要求(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）在安全目标包括的所有功能性项目中，**在表 2 中**定义为*基本审计*级别的所有可审计事件；

c）安全目标包括的所有功能性项目中，*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）在本标准对其他功能性项目的可审计事件定义的基础上，**表 2 第 4 列对每一类审计事件所说明的附加信息。**

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	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	受影响的客体的标识
FDP _ SAM	基本	修改安全属性的所有尝试，包括拟修改的客体的身份	修改后安全属性的新值
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 _ 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　审计跟踪管理　(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 _ POP. 1.1　防火墙的安全功能应使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)

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”)]。

应用注解：**防火墙**的开发者应详细描述审计查阅工具的功能，特别是应说清楚根据与安全相关的属性查找和排序的能力。

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(CC)”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

7.2.1.1 最低限度的支持 (ACM _ CAP.1)

7.2.1.1.1 开发者应使用配置管理系统 (ACM _ CAP.1.1D)

7.2.1.1.2 开发者应提供配置管理文件。 (ACM _ CAP.2D)

7.2.1.1.3 配置管理文件应包括一个配置目录。 (ACM _ CAP.1C)

7.2.1.1.4 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. 2C)

7.2.1.1.5 配置管理文件应描述用于唯一识别防火墙的配置项的方法。 (ACM _ CAP. 3C)

7.2.1.1.6 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。 (ACM _ CAP. 1E)

7.2.2 交付和操作保证

7.2.2.1 安装、生成和启动过程 (ADO _ IGS. 1)

7.2.2.1.1 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. 1D)

7.2.2.1.2 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. 1C)

7.2.2.1.3 评估者应确认所提供的信息满足内容和表述上的所有要求。 (ADO _ IGS. 1. 1E)

7.2.3 开发过程保证

7.2.3.1 防火墙和安全策略 (ADV _ FSP. 1)

7.2.3.1.1 开发者应提供防火墙的功能规范。 (ADV _ FSP. 1. 1D)

7.2.3.1.2 开发者应提供防火墙的安全策略。 (ADV _ FSP. 1. 2D)

7.2.3.1.3 功能规范应以非形式方法来描述安全策略。 (ADV _ FSP. 1. 1C)

7.2.3.1.4 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. 2C)

7.2.3.1.5 功能规范应包括能证明安全功能已完全实现了的证据。 (ADV _ FSP. 1. 3C)

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。

7.2.3.1.6 评估者应确认所提供的信息满足内容和表述上的所有要求。 (ADV _ FSP. 1. 1E)

7.2.3.1.7 评估者应确认功能规范与安全策略是一致的。 (ADV _ FSP. 1. 2E)

7.2.3.1.8 评估者应确认安全功能的表述是否包含了安全目标(ST)中的每一项功能要求。 (ADV _ FSP. 1. 3E)

7.2.3.2 高层设计描述 (ADV _ HLD. 1)

7.2.3.2.1 开发者应提供防火墙安全功能的高层设计。 (ADV _ HLD. 1. 1D)

7.2.3.2.2 高层设计应以非形式方法表述。 (ADV _ HLD. 1. 1C)

7.2.3.2.3 高层设计应根据子系统来描述安全功能的结构。 (ADV _ HLD. 1. 2C)

7.2.3.2.4 高层设计应描述由安全功能的每一个子系统提供的安全功能。 (ADV _ HLD. 1. 3C)

7.2.3.2.5 高层设计应标明安全功能子系统的接口。 (ADV _ HLD. 1. 4C)

7.2.3.2.6 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. 5C)

7.2.3.2.7 评估者应确认所提供的信息满足内容和表述上的所有要求。 (ADV _ HLD. 1. 1E)

7.2.3.2.8 评估者应确认安全功能的表述是否包含了安全目标(ST)中的每一项功能要求。 (ADV _ HLD. 1. 2E)

7.2.3.3 非形式的一致性证明 (ADV _ RCR. 1)

7.2.3.3.1 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. 1D)

7.2.3.3.2 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. 1C)

7.2.3.3.3 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化方法表述。 (ADV _ RCR. 1. 2C)

7.2.3.3.4 评估者应确认所提供的信息满足内容和表达上的所有要求。 (ADV _ RCR. 1. 1E)

7.2.3.3.5 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。 (ADV _ RCR. 1. 2E)

7.2.4 指南文件保证

7.2.4.1 管理员指南 (AGD_ADM.1)

7.2.4.1.1 开发者应提供能满足系统管理者需要的管理员指南。 (AGD_ADM.1.1D)

7.2.4.1.2 管理员指南应描述怎样以安全的方式管理防火墙。 (AGD_ADM.1.1C)

7.2.4.1.3 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.1.2C)

7.2.4.1.4 管理员指南应对一致、有效地使用安全功能提供指导。 (AGD_ADM.1.3C)

7.2.4.1.5 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.1.4C)

7.2.4.1.6 管理员指南应描述管理员控制下的所有安全参数。 (AGD_ADM.1.5C)

7.2.4.1.7 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.1.6C)

7.2.4.1.8 管理员指南应包括安全功能如何相互作用的指导。 (AGD_ADM.1.7C)

7.2.4.1.9 管理员指南应包括怎样配置防火墙的指令。 (AGD_ADM.1.8C)

7.2.4.1.10 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.1.9C)

7.2.4.1.11 管理员指南应充分描述与安全管理相关的详细过程。 (AGD_ADM.1.10C)

7.2.4.1.12 管理员指南应与提交评估的所有其他文件一致。 (AGD_ADM.1.11C)

7.2.4.1.13 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.1.1E)

7.2.4.1.14 评估者应确认安装过程能产生一个安全的配置。 (AGD_ADM.1.2E)

7.2.4.2 用户指南 (AGD_USR.1)

7.2.4.2.1 开发者应提供用户指南。 (AGD_USR.1.1D)

7.2.4.2.2 用户指南应描述用户可使用的安全功能和接口。 (AGD_USR.1.1C)

7.2.4.2.3 用户指南应包含使用防火墙提供的安全功能的指导。 (AGD_USR.1.2C)

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

7.2.4.2.5 用户指南应描述那些用户可见的安全功能之间的相互作用。 (AGD_USR.1.4C)

7.2.4.2.6 用户指南应与提交评估的所有其他文件一致。 (AGD_USR.1.5C)

7.2.4.2.7 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_USR.1.1E)

7.2.5 测试保证

7.2.5.1 独立测试——一致性 (ATE_IND.1)

7.2.5.1.1 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.1.1D)

7.2.5.1.2 防火墙应适合于测试。 (ATE_IND.1.1C)

7.2.5.1.3 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。 (ATE_IND.1.1E)

7.2.5.2 测试覆盖面非形式分析 (ATE_COV.1)

7.2.5.2.1 开发者应提供一个对测试覆盖范围的分析。 (ATE_COV.1.1D)

7.2.5.2.2 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.1.1C)

7.2.5.2.3 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。 (ATE_COV.1.1E)

7.2.5.3 功能测试 (ATE_FUN.1)

7.2.5.3.1 开发者应测试防火墙安全功能,并记录其结果。 (ATE_FUN.1.1D)

7.2.5.3.2 开发者应提供测试文件。 (ATE_FUN.1.2D)

7.2.5.3.3 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. 1C)

7.2.5.3.4 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. 2C)

7.2.5.3.5 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实际情况。 (ATE _ FUN. 1. 3C)

7.2.5.3.6 测试文件中的测试结果应给出每一项测试的预期结果。 (ATE _ FUN. 1. 4C)

7.2.5.3.7 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. 5C)

7.2.5.3.8 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。 (ATE _ FUN. 1. 1E)

7.2.5.4 测试——功能规范 (ATE _ DPT. 1)

7.2.5.4.1 开发者应提供对测试深度的分析。 (ATE _ DPT. 1. 1D)

7.2.5.4.2 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. 1C)

7.2.5.4.3 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。 (ATE _ DPT. 1. 1E)

7.2.6 脆弱性分析保证

7.2.6.1 防火墙安全功能强度的评估 (AVA _ SOF. 1)

7.2.6.1.1 开发者应确定防火墙适合作安全功能强度分析的安全机制。 (AVA _ SOF. 1. 1D)

7.2.6.1.2 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. 2D)

7.2.6.1.3 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. 1C)

7.2.6.1.4 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. 2C)

7.2.6.1.5 安全强度分为**中等或高等**两档。 (AVA _ SOF. 1. 3C)

7.2.6.1.6 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。 (AVA _ SOF. 1. 1E)

7.2.6.1.7 评估者应确认所有需要强度分析的安全机制已确定。 (AVA _ SOF. 1. 2E)

7.2.6.1.8 评估者应确认各项强度声明已确认。 (AVA _ SOF. 1. 3E)

7.2.6.2 开发者脆弱性分析 (AVA _ VLA. 1)

7.2.6.2.1 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. 1D)

7.2.6.2.2 开发者应明确记录对被确定的脆弱性的处置。 (AVA _ VLA. 1. 2D)

7.2.6.2.3 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. 1C)

7.2.6.2.4 评估者应确认所提供的信息符合证据在内容和表述上的所有要求。 (AVA _ VLA. 1. 1E)

7.2.6.2.5 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。 (AVA _ VLA. 1. 2E)

8 基本原理

8.1 信息技术安全目标的基本原理

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 IT 安全目标之间的映射关系

	O. ACCESS	O. ADMIN	O. ACCOUNT	O. PROTECT	O. AUDIT
T. LACESS		×	×		
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理

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、O. TRAIN 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、AUDIT、T. DCORRUPT 和 T. AUTH 威胁是必需的。

表 5 威胁和非 IT 安全目标之间的映射关系

	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理

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的暴露。该组件确保用户不能意外的得到不该属于他们的数