

编号：MSCTC-GFJ-01

信 息 技 术
小型防火墙产品安全检验规范

公安部计算机信息系统安全产品质量监督检验中心

第一版 第0次修订
2003年11月01日颁布

2003年12月01日实施

目 次

前言	III
1 范围.....	1
2 引用标准.....	1
3 小型防火墙定义.....	1
4 安全功能要求.....	1
4.1 用户数据保护功能类 (FDP)	1
4.1.1 完整的客体访问控制 (FDP_ACC. 2)	1
4.1.2 访问授权与拒绝 (FDP_ACF. 4)	1
4.1.3 多种安全属性访问控制 (FDP_ACF. 2)	1
4.1.4 管理员属性修改 (FDP_SAM. 1)	2
4.1.5 管理员属性查询 (FDP_SAQ. 1)	2
4.2 识别与鉴别功能类 (FIA)	2
4.2.1 授权管理员和可信主机鉴别数据初始化 (FIA_ADA. 1)	2
4.2.2 授权管理员和可信主机鉴别数据的基本保护 (FIA_ADP. 1)	2
4.2.3 授权管理员可信主机和主机属性的初始化 (FIA_ATA. 1)	2
4.2.4 授权管理员、可信主机和主机唯一属性定义 (FIA_ATD. 2)	2
4.2.5 授权管理员的基本鉴别 (FIA_UAU. 1)	2
4.2.6 单一使用的鉴别机制 (FIA_UAU. 2)	2
4.2.7 授权管理员、可信主机和主机唯一身份识别 (FIA_UID. 2)	3
4.3 保密功能类 (FEN)	3
4.3.1 符合规定的加密操作 (FCS_COP. 2)	3
4.4 可信安全功能保护类 (FPT)	3
4.4.1 防火墙安全策略的不可旁路性 (FPT_RVM. 1)	3
4.4.2 安全功能区域分割 (FPT_SEP. 1)	3
4.5 安全审计功能类 (FAU)	3
4.5.1 审计数据生成 (FAU_GEN. 1)	3
4.5.2 可理解的格式 (FAU_POP. 1)	3
4.5.3 限制审计跟踪访问 (FAU_PRO. 1)	3

前 言

小型防火墙是专门为中小企业、中小型办公室环境或家庭用户提供安全保护的防火墙产品。

小型防火墙的目的是要在内外网络之间建立一个安全控制点，通过允许、拒绝或重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。

小型防火墙的特点是体积小、硬件配置低、流量性能低，其主要访问控制能力与普通防火墙基本相同，但其部分安全功能要求比普通防火墙低，只能适用于中小企业、中小型办公室环境或家庭用户。

小型防火墙产品的安全功能要求是完全包含在《GB/T 18019-1999 信息技术包过滤防火墙安全技术要求》之内的，因此只能选用《GB/T 18019-1999 信息技术包过滤防火墙安全技术要求》中的部分安全功能要求。

本规范规定了小型防火墙产品的安全技术要求。

本规范起草单位：公安部计算机信息系统安全产品质量监督检验中心。

1 范围

本规范规定了小型防火墙产品的安全技术要求。

本规范适用于小型防火墙产品安全功能的研制、开发、测试、评估和产品的采购。

2 引用标准

GB/T 18019-1999 信息技术包过滤防火墙安全技术要求

3 小型防火墙定义

小型防火墙是专门为中小企业、中小型办公室环境或家庭用户提供安全保护的防火墙产品。

小型防火墙的目的是要在内外网络之间建立一个安全控制点，通过允许、拒绝或重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。

小型防火墙的特点是体积小、硬件配置低、流量性能低，其主要访问控制能力与普通防火墙基本相同，但其部分安全功能要求比普通防火墙低，只能适用于中小企业、中小型办公室环境或家庭用户，建议内网用户一般不超过 10 个。

4 安全功能要求

4.1 用户数据保护功能类（FDP）

4.1.1 完整的客体访问控制（FDP_ACC.2）

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。

以及安全功能策略所包括主体和客体上的所有操作。

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。

4.1.2 访问授权与拒绝（FDP_ACF.4）

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。

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。

4.1.3 多种安全属性访问控制（FDP_ACF.2）

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。

防火墙应执行以下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。

4.1.4 管理员属性修改 (FDP_SAM.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) 与安全有关的管理数据。

4.1.5 管理员属性查询 (FDP_SAQ.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。

4.2 识别与鉴别功能类 (FIA)

4.2.1 授权管理员和可信主机鉴别数据初始化 (FIA_ADA.1)

防火墙应根据 FIA_UAU.1 和 FIA_UAU.2 中规定的鉴别数据提供授权管理员和可信主机鉴别数据的初始化功能。

防火墙应确保只允许授权管理员使用这些功能。

4.2.2 授权管理员和可信主机鉴别数据的基本保护 (FIA_ADP.1)

防火墙应保护存储于设备中的鉴别数据不受未经授权查阅、修改和破坏。

4.2.3 授权管理员可信主机和主机属性的初始化 (FIA_ATA.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。

4.2.4 授权管理员、可信主机和主机唯一属性定义 (FIA_ATD.2)

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须的安全属性。

4.2.5 授权管理员的基本鉴别 (FIA_UAU.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。

4.2.6 单一使用的鉴别机制 (FIA_UAU.2)

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。

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。

4.2.7 授权管理员、可信主机和主机唯一身份识别 (FIA_UID.2)

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。

4.3 保密功能类 (FEN)

4.3.1 符合规定的加密操作 (FCS_COP.2)

防火墙的安全功能应保证其从外部网络到防火墙的远程管理会话的加密符合国家密码管理的有关规定。

4.4 可信安全功能保护类 (FPT)

4.4.1 防火墙安全策略的不可旁路性 (FPT_RVM.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。

4.4.2 安全功能区域分割 (FPT_SEP.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。

4.5 安全审计功能类 (FAU)

4.5.1 审计数据生成 (FAU_GEN.1)

防火墙的安全功能应能够对可审计事件生成一个审计记录：

4.5.2 可理解的格式 (FAU_POP.1)

防火墙的安全功能应使审计记录中的所有审计数据可为人所理解。

4.5.3 限制审计跟踪访问 (FAU_PRO.1)

防火墙的安全功能应只允许授权管理员访问审计记录。