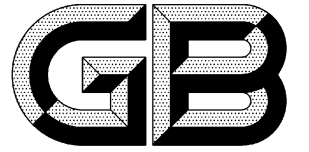


ICS 35.040
L 80



中华人民共和国国家标准

GB/T 18020—1999

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

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

*

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
版权专有 不得翻印

*

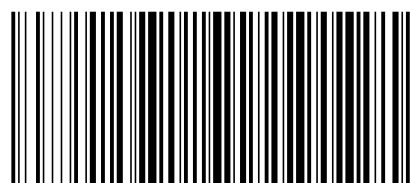
开本 880×1230 1/16 印张 1½ 字数 35 千字
2000年6月第一版 2000年6月第一次印刷
印数 1—1 600

*

书号: 155066·1-16689 定价 14.00 元

*

标目 410—26



GB/T 18020—1999

1999-11-11 发布

2000-05-01 实施

国家质量技术监督局 发布

表 6 安全目标和功能要求之间的关系

	O. ACCESS	O. ADMIN	O. ACCOUNT	O. PROTECT	O. AUDIT
FDP-ACC. 2	×				
FDP-ACF. 4	×				
FDP-ACF. 2	×				
FDP-RIP. 3	×				
FDP-SAM. 1	×	×			
FDP-SAQ. 1	×	×			
FIA-ADA. 1		×	×		
FIA-ADP. 1			×	×	
FIA-AFL. 1		×	×	×	
FIA-ATA. 1			×		
FIA-ATD. 2			×		
FIA-UAU. 1			×		
FIA-UAU. 2			×		
FIA-UID. 2			×		
FCS-COP. 2				×	
FPT-RVM. 1	×			×	
FPT-SEP. 1				×	
FPT-TSA. 2		×			
FPT-TSM. 1		×			
FAU-GEN. 1					×
FAU-MGT. 1					×
FAU-POP. 1					×
FAU-PRO. 1		×			×
FAU-SAR. 1		×			×
FAU-SAR. 3					×
FAU-STG. 3					×

8.4 保证要求基本原则

在厂商没有提供完整开发记录的情况下,只进行中低等级安全评估的独立保证。为此,厂商需要额外承担最低限度的任务是支持功能测试。除此之外,如果在开发中已注意使用了合理标准,则厂商不参加也可以进行评估。所选的保证级别应满足所有的功能相关性,并与设想的威胁环境一致。尤其是,恶意攻击的威胁不应大于中等级别,并且就明显缺陷已对产品做过检查。

目 次

前言 Ⅲ

1 范围 1

2 引用标准 1

3 定义和记法约定 1

3.1 定义 1

3.2 记法约定 1

4 应用级防火墙概述 1

5 安全环境 2

5.1 安全条件假定 2

5.2 安全威胁 2

6 安全目标 3

6.1 信息技术安全目标 3

6.2 非信息技术安全目标 4

7 安全要求 4

7.1 功能要求 4

7.2 保证要求 9

8 基本原则 13

8.1 信息技术安全目标的基本原则 13

8.2 非信息技术安全目标的基本原则 13

8.3 信息技术功能要求的基本原则 14

8.4 保证要求基本原则 16

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)

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。