ICS 35.020
L 09

中华人民共和国国家标准

GB/T 20010—2005

信息安全技术
包过滤防火墙评估准则

Information security technology —
Packet filtering firewalls evaluation criteria

2005-11-11 发布　　2006-05-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

目　次

前　言

GB 17859—1999《计算机信息系统安全保护等级划分准则》是我国计算机信息系统安全等级管理的重要标准，已于1999年9月13日发布。为促进安全等级管理工作的正常有序开展，特制定一系列相关的标准。本标准是系列标准之一。

本标准文本中，黑体字表示较低等级中没有出现或增强的评估内容。

本标准的附录A中说明防火墙面临的主要威胁和对策。

本标准的附录A是资料性附录。

本标准由全国信息安全标准化技术委员会提出并归口。

本标准起草单位：北京大学软件工程国家工程中心，公安部公共信息网络安全监察局。

本标准主要起草人：王立福、刘学洋、赵学志、张劲飞、张晰。

引　言

防火墙是内部、外部两个网络之间的一个阻隔，通过允许和拒绝经过防火墙的数据流，防止不希望的、未授权的通信，并实现对进、出内部网络的服务和访问的审计和控制。防火墙对网络用户提供访问控制服务和通信安全服务，对网络用户基本上是“透明”的，并且只有授权的管理员方可对防火墙进行管理。

防火墙一般要解决的安全问题可分为被保护系统(即内部网)的安全问题和自身的安全问题。

防火墙产品主要分为两类：包过滤和应用级防火墙。本标准规定了包过滤防火墙的各级安全要求。包过滤防火墙根据安全功能策略建立包过滤规则。过滤规则的主要要素有源 IP 地址、目的 IP 地址、协议号、源端口、目的端口、连接标志和另外一些 IP 选项，以及包到达或发出的接口。

信息安全技术
包过滤防火墙评估准则

1 范围

本标准从信息技术方面规定了按照 GB 17859—1999 的五个安全保护等级对采用“传输控制协议/网间协议(TCP/IP)”的包过滤防火墙产品安全保护等级划分所需要的评估内容。

本标准适用于包过滤防火墙安全保护等级的评估，对于包过滤防火墙的研制、开发、测试和产品采购也可参照使用。

2 规范性引用文件

下列文件中的条款通过本标准的引用而成为本标准的条款。凡是注日期的引用文件，其随后所有的修改单(不包括勘误的内容)或修订版均不适用于本标准，然而，鼓励根据本标准达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件，其最新版本适用于本标准。

GB 17859—1999 计算机信息系统安全保护等级划分准则

3 术语和定义

GB 17859—1999 确立的以及下列术语和定义适用于本标准。

3.1

主机 host

一台与防火墙相互作用的机器，它在防火墙安全功能策略控制下进行通信。

3.2

用户 user

一个在防火墙安全功能策略的控制下，通过防火墙访问外部网络或内部网络的人，此人不具有能影响防火墙安全功能策略执行的特权。

3.3

授权管理员 authorized administrator

能访问、实施、修改防火墙安全功能策略的个人，其职责仅限定于对防火墙的管理，不包括系统管理和网络管理。

3.4

可信主机 trusted host

允许授权管理员对防火墙进行远程管理的机器。

3.5

鉴别数据 authentication data

用来确认授权管理员和可信主机身份的信息。

4 安全环境

4.1 物理方面

对防火墙资源的处理限定在一些可控制的访问设备内，防止未授权的物理访问。所有与实施防火

墙安全策略相关的硬件和软件应受到保护以免于未授权的物理修改。

4.2 人员方面

授权管理员不具敌意并遵守所有的管理员规则。

4.3 连通性方面

防火墙是内、外网络之间的唯一连接点，所有内外网络间的通信应经过防火墙。授权管理员可以从内部或外部网上对防火墙进行远程管理。

5 评估内容

本章给出了各级防火墙所需评估的安全功能内容和安全保证内容。包过滤防火墙执行的安全功能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(发送信息的主机)向另一侧客体(接受信息的主机)发送数据。在主体发送数据之前，未鉴别的端到端策略不需要对主体身份进行鉴别。

5.1 用户自主保护级

5.1.1 访问控制

5.1.1.1 安全属性定义

对于每一个授权管理员、可信主机和主机，防火墙安全功能应为其提供一套唯一的、为了执行安全功能策略所必需的安全属性。

5.1.1.2 属性初始化

防火墙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。

5.1.1.3 属性修改

防火墙安全功能应仅向授权管理员提供修改下述(包含但不仅限于)参数的能力：

a) 标识与角色(例如：配置管理员等)的关系；

b) 源地址、目的地址、传输层协议和请求的服务(例如：源端口号或目的端口号等访问控制属性)；

c) 配置的安全参数(例如：最大鉴别失败次数等数据)。

5.1.1.4 属性查询

防火墙安全功能应仅向授权管理员提供以下查询：源地址、目的地址、传输层协议和请求的服务(例如：源端口号或目的端口号等访问控制属性)。

5.1.1.5 访问授权与拒绝

防火墙安全功能应根据主体和客体的安全属性值[源地址、目的地址、传输层协议和请求的服务(例如：源端口号或目的端口号)等]，提供明确的访问保障能力和拒绝访问能力。

5.1.2 身份鉴别

5.1.2.1 鉴别数据初始化

防火墙安全功能应根据规定的鉴别机制，提供授权管理员和可信主机鉴别数据的初始化功能，并确保仅允许授权管理员使用这些功能。

5.1.2.2 鉴别时机

在所有授权管理员和可信主机请求执行的任何操作之前，防火墙安全功能应确保对每个授权管理员和可信主机进行了身份鉴别。

5.1.2.3 鉴别失败处理

在经过一定次数的鉴别失败以后，防火墙安全功能应能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。

5.1.3 数据完整性

防火墙安全功能应保护储存的鉴别数据和过滤策略不受未授权修改和破坏。

5.1.4 配置管理

开发者应为防火墙产品的不同版本提供唯一的标识。

防火墙产品的每个版本应当使用它们的唯一标识作为标签。

5.1.5 安全功能开发过程

5.1.5.1 功能规约

开发者应提供防火墙的安全功能规约。

功能规约应以非形式方法来描述安全功能与其外部接口，并描述使用外部安全功能接口的目的与方法，在需要的时候，还要提供例外情况和错误信息的细节。

安全功能规约应是内在一致的并能完备地表示安全功能。

5.1.5.2 表示对应性

开发者应在防火墙安全功能表示的所有相邻对之间提供对应性分析。

对于防火墙安全功能表示的每个相邻对，分析应阐明：较为抽象的安全功能表示的所有相关安全功能，应在较具体的安全功能表示中得到正确而完备地细化。

5.1.6 测试

5.1.6.1 功能测试

开发者应测试安全功能，将结果文档化并提供测试文档。

测试文档应包括测试计划、测试过程、预期的测试结果和实际测试结果。测试计划应标识要测试的安全功能，并描述测试的目标。测试过程应标识要执行的测试，并描述每个安全功能的测试概况，这些概况包括对其他测试结果的顺序依赖性。期望的测试结果应表明测试成功后的预期输出。实际测试结果应表明每个被测试的安全功能能按照规定进行运作。

5.1.6.2 覆盖分析

开发者应提供测试覆盖的分析结果。

测试覆盖的分析结果应表明测试文档中所标识的测试与安全功能规约中所描述的安全功能是对应的。

5.1.7 指导性文档

5.1.7.1 管理员指南

开发者应提供系统管理员使用的管理员指南。

管理员指南应说明以下内容：

a) 防火墙管理员可以使用的管理功能和接口；

b) 怎样安全地管理防火墙；

c) 在安全处理环境中应进行控制的功能和权限；

d) 所有对与防火墙的安全操作有关的用户行为的假设；

e) 所有受管理员控制的安全参数，如果可能，应指明安全值；

f) 每一种与管理功能有关的安全相关事件，包括对安全功能所控制的实体的安全特性进行的改变；

g) 所有与系统管理员有关的 IT 环境的安全要求。

管理员指南应与为评估而提供的其他所有文件保持一致。

5.1.7.2 用户指南

开发者应提供用户指南。

用户指南应说明以下内容：

a) 防火墙的非管理用户可使用的安全功能和接口；

b) 防火墙提供给用户的安全功能和接口的用法；

c) 用户可获取但应受安全处理环境控制的所有功能和权限；

d) 防火墙安全操作中用户所应承担的职责；

e) 与用户有关的IT环境的所有安全要求。

用户指南应与为评估而提供的其他所有文件保持一致。

5.1.8 交付与运行

开发者应提供文档说明防火墙的安装、生成和启动的过程。

5.2 系统审计保护级

5.2.1 访问控制

5.2.1.1 安全属性定义

对于每一个授权管理员、可信主机和主机，防火墙安全功能应为其提供一套唯一的、为了执行安全功能策略所必需的安全属性。

5.2.1.2 属性初始化

防火墙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。

5.2.1.3 属性修改

防火墙安全功能应仅向授权管理员提供修改下述(包含但不仅限于)参数的能力：

a) 标识与角色(例如：审计管理员等)的关系；

b) 源地址、目的地址、传输层协议和请求的服务(例如：源端口号或目的端口号等访问控制属性)；

c) 配置的安全参数(例如：最大鉴别失败次数、最大审计存储容量等数据)。

5.2.1.4 属性查询

防火墙安全功能应仅向授权管理员提供以下查询：源地址、目的地址、传输层协议和请求的服务(例如：源端口号或目的端口号等访问控制属性)。

5.2.1.5 访问授权与拒绝

防火墙安全功能应根据主体和客体的安全属性值[源地址、目的地址、传输层协议和请求的服务(例如：源端口号或目的端口号)等]，提供明确的访问保障能力和拒绝访问能力。

5.2.1.6 不可旁路

在与安全有关的操作(例如安全属性的修改、外部网络主机向内部网络主机发送信息等)被允许执行之前，防火墙安全功能应确保其通过安全功能策略的检查。

5.2.1.7 区分安全管理角色

防火墙安全功能：

a) 应将与安全相关的管理功能与其他功能区分开；

b) 应包括安装、配置和管理防火墙安全功能本身所需的所有功能，其中至少应包括：增加和删除主体(发送信息的主机)和客体(接受信息的主机)，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；

c) 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；

d) 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；

e) 应仅允许授权管理员和可信主机承担安全管理职责；

f) 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。

5.2.1.8 管理功能

防火墙安全功能应向授权管理员提供如下管理功能：

a) 能设置和更新与安全相关的数据；

b) 能执行防火墙的安装及初始化、系统启动和关闭、备份和恢复的能力，备份能力应有自动工具的支持；

c) 如果防火墙安全功能支持外部或内部接口的远程管理，那么它应：

1) 具有对两个接口或其中之一关闭远程管理的选择权；

2) 能限制那些可进行远程管理的地址；

3) 能通过加密来保护远程管理对话。

5.2.2 身份鉴别

5.2.2.1 鉴别数据初始化

防火墙安全功能应根据规定的鉴别机制，提供授权管理员和可信主机鉴别数据的初始化功能，并确保仅允许授权管理员使用这些功能。

5.2.2.2 鉴别时机

在所有授权管理员和可信主机请求执行的任何操作之前，防火墙安全功能应确保对每个授权管理员和可信主机进行了身份鉴别。

5.2.2.3 最少反馈

当进行鉴别时，防火墙安全功能应仅将最少的反馈（如：打入的字符数，鉴别的成功或失败）提供给用户。

5.2.2.4 鉴别失败处理

在经过一定次数的鉴别失败以后，防火墙安全功能应能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。

5.2.3 客体重用

在为所有内部或外部网上的主机连接进行资源分配时，防火墙安全功能应保证不提供以前连接的任何信息内容。

5.2.4 审计

5.2.4.1 审计数据生成

防火墙安全功能应能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) 任何对审计记录进行操作的尝试，包括关闭审计功能或子系统，以及受影响客体的标识；

c) 任何读取、修改、破坏审计记录的尝试；

d) 所有对防火墙规则覆盖的客体（内部或外部网络上的主机）执行操作的请求，以及受影响客体的标识；

e) 修改安全属性的所有尝试，以及修改后安全属性的新值；

f) 所有使用安全功能中鉴别数据管理机制的请求；

g) 所有访问鉴别数据的请求，以及访问请求的目标；

h) 所有使用标识机制的尝试；

i) 任何对鉴别机制的使用；

j) 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，以及配置参数的新值。

对于每一个审计记录，防火墙安全功能应至少记录以下信息：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。

5.2.4.2 审计记录管理

防火墙安全功能应使授权管理员能创建、存档、删除和清空审计记录。

5.2.4.3 可理解的格式

防火墙安全功能应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。

5.2.4.4 限制审计记录访问

防火墙安全功能应仅允许授权管理员访问审计记录。

5.2.4.5 可选择查阅审计

防火墙安全功能应提供能按主体 ID(标识符)、客体 ID、日期、时间以及这些参数的逻辑组合等参数对审计数据进行查找和排序的审计查阅工具。

5.2.4.6 防止审计数据丢失

防火墙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,并应限制由于故障和攻击造成的审计事件丢失的数量。

对因故障或存储耗竭而导致审计数据丢失的最大审计存储容量,防火墙的开发者应提供相应的分析结果。

5.2.5 数据完整性

防火墙安全功能应保护储存于设备中的鉴别数据和过滤策略不受未授权修改和破坏。

5.2.6 生存周期支持

开发者应提供开发安全文件。

开发安全文件应描述在防火墙的开发环境中,为保护防火墙设计和实现的机密性和完整性,而在物理上、程序上、人员上以及其他方面所采取的必要的安全措施。开发安全文件还应提供在防火墙的开发和维护过程中执行安全措施的证据。

5.2.7 配置管理

5.2.7.1 授权机制

开发者应使用配置管理系统并提供配置管理文档,以及为防火墙产品的不同版本提供唯一的标识。

配置管理系统应对所有的配置项作出唯一的标识,并保证只有经过授权才能修改配置项。

配置管理文档应包括配置清单和配置管理计划。在配置清单中,应对每一配置项给出相应的描述;在配置管理计划中,应描述配置管理系统是如何使用的。实施的配置管理应与配置管理计划相一致。

配置管理文档还应描述对配置项给出唯一标识的方法,并提供所有的配置项得到有效地维护的证据。

5.2.7.2 配置管理范围

开发者应提供配置管理文档。

配置管理文档应说明配置管理系统至少能跟踪:防火墙实现表示、设计文档、测试文档、用户文档、管理员文档和配置管理文档,并描述配置管理系统是如何跟踪配置项的。

5.2.8 安全功能开发过程

5.2.8.1 功能规约

开发者应提供防火墙的安全功能规约。

功能规约应以非形式方法来描述安全功能与其外部接口,并描述使用外部安全功能接口的目的与方法,在需要的时候,还要提供例外情况和错误信息的细节。

安全功能规约应是内在一致的并能完备地表示安全功能。

5.2.8.2 高层设计

开发者应提供防火墙安全功能的高层设计。

高层设计应以非形式方法表述并且是内在一致的。为说明安全功能的结构，高层设计应将安全功能分解为各个安全功能子系统进行描述，并阐明如何将有助于加强防火墙安全功能的子系统和其他子系统分开。对于每一个安全功能子系统，高层设计应描述其提供的安全功能，标识其所有接口以及哪些接口是外部可见的，描述其所有接口的使用目的与方法，并提供安全功能子系统的作用、例外情况和错误信息的细节。高层设计还应标识安全功能要求的所有基础性的硬件、固件和软件，并且支持由这些硬件、固件或软件所实现的保护机制。

5.2.8.3 表示对应性

开发者应在防火墙安全功能表示的所有相邻对之间提供对应性分析。

对于防火墙安全功能表示的每个相邻对，分析应阐明：较为抽象的安全功能表示的所有相关安全功能，应在较具体的安全功能表示中得到正确而完备地细化。

5.2.9 测试

5.2.9.1 功能测试

开发者应测试安全功能，将结果文档化并提供测试文档。

测试文档应包括测试计划、测试过程、预期的测试结果和实际测试结果。测试计划应标识要测试的安全功能，并描述测试的目标。测试过程应标识要执行的测试，并描述每个安全功能的测试概况，这些概况包括对其他测试结果的顺序依赖性。期望的测试结果应表明测试成功后的预期输出。实际测试结果应表明每个被测试的安全功能能按照规定进行运作。

5.2.9.2 覆盖分析

开发者应提供测试覆盖的分析结果。

测试覆盖的分析结果应表明测试文档中所标识的测试与安全功能规约中所描述的安全功能是对应的，且该对应是完备的。

5.2.9.3 深度

开发者应提供测试深度的分析。

在深度分析中，应说明测试文档中所标识的对安全功能的测试，足以表明该安全功能和高层设计是一致的。

5.2.9.4 独立性测试

开发者应提供证据证明，开发者提供的防火墙经过独立的第三方测试并通过。

5.2.10 指导性文档

5.2.10.1 管理员指南

开发者应提供系统管理员使用的管理员指南。

管理员指南应说明以下内容：

a) 防火墙管理员可以使用的管理功能和接口；

b) 怎样安全地管理防火墙；

c) 在安全处理环境中应进行控制的功能和权限；

d) 所有对与防火墙的安全操作有关的用户行为的假设；

e) 所有受管理员控制的安全参数，如果可能，应指明安全值；

f) 每一种与管理功能有关的安全相关事件，包括对安全功能所控制的实体的安全特性进行的改变；

g) 所有与系统管理员有关的 IT 环境的安全要求。

管理员指南应与为评估而提供的其他所有文件保持一致。

5.2.10.2 用户指南

开发者应提供用户指南。

用户指南应说明以下内容：

a) 防火墙的非管理用户可使用的安全功能和接口；

b) 防火墙提供给用户的安全功能和接口的用法；

c) 用户可获取但应受安全处理环境控制的所有功能和权限；

d) 防火墙安全操作中用户所应承担的职责；

e) 与用户有关的 IT 环境的所有安全要求。

用户指南应与为评估而提供的其他所有文件保持一致。

5.2.11 脆弱性分析

5.2.11.1 指南检查

开发者应提供指南性文档。

在指南性文档中，应确定对防火墙的所有可能的操作方式（包括失败和操作失误后的操作）、它们的后果以及对于保持安全操作的意义。指南性文档中还应列出所有目标环境的假设以及所有外部安全措施（包括外部程序的、物理的或人员的控制）的要求。指南性文档应是完备的、清晰的、一致的、合理的。

5.2.11.2 脆弱性分析

开发者应从用户可能破坏安全策略的明显途径出发，对防火墙的各种功能进行分析并提供文档。对被确定的脆弱性，开发者应明确记录采取的措施。

对每一条脆弱性，应有证据显示在使用防火墙的环境中该脆弱性不能被利用。在文档中，还需证明经过标识脆弱性的防火墙可以抵御明显的穿透性攻击。

5.2.12 交付与运行

5.2.12.1 交付

开发者应使用一定的交付程序交付防火墙，并将交付过程文档化。

交付文档应描述在给用户方交付防火墙的各版本时，为维护安全所必需的所有程序。

5.2.12.2 安装生成

开发者应提供文档说明防火墙的安装、生成和启动的过程。

5.3 安全标记保护级

5.3.1 访问控制

5.3.1.1 安全属性定义

对于每一个授权管理员、可信主机和主机，防火墙安全功能应为其提供一套唯一的、为了执行安全功能策略所必需的安全属性。

5.3.1.2 属性初始化

防火墙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。

5.3.1.3 属性修改

防火墙安全功能应仅向授权管理员提供修改下述（包含但不仅限于）参数的能力：

a) 标识与角色（例如：审计管理员等）的关系；

b) 源地址、目的地址、传输层协议和请求的服务（例如：源端口号或目的端口号等访问控制属性）；

c) 配置的安全参数（例如：最大鉴别失败次数、最大审计存储容量等数据）。

5.3.1.4 属性查询

防火墙安全功能应仅向授权管理员提供以下查询：源地址、目的地址、传输层协议和请求的服务（例如：源端口号或目的端口号等访问控制属性）。

5.3.1.5 客体访问控制策略

对于防火墙的主体（未经防火墙鉴别的发送信息的主机）和客体（内部或外部网上的接收信息的主

机)以及安全功能策略(SFP)所包括的主体、客体的所有操作,防火墙安全功能应执行未鉴别的端到端策略,并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。

5.3.1.6 防火墙强制访问控制

防火墙安全功能应通过授权管理员和授权管理员控制的安全功能数据的敏感标记,控制授权管理员对相关安全功能数据的直接访问。

5.3.1.7 访问授权与拒绝

防火墙安全功能应根据主体和客体的安全属性值[源地址、目的地址、传输层协议和请求的服务(例如:源端口号或目的端口号)等],提供明确的访问保障能力和拒绝访问能力。

5.3.1.8 子集信息流控制

防火墙安全功能应根据发出信息的主机地址以及信息流类型等安全属性,确定允许信息流通过或禁止信息流通过。

5.3.1.9 安全功能区域分隔

为保护防火墙安全功能免遭不可信主体(内部或外部网络上的主机)的干扰和篡改,防火墙安全功能应为其自身的执行过程设定一个安全区域,并把防火墙控制范围内的各个主体(内部或外部网络上的主机)的安全区域分隔开。

5.3.1.10 不可旁路

在与安全有关的操作(例如安全属性的修改、外部网络主机向内部网络主机发送信息等)被允许执行之前,防火墙安全功能应确保其通过安全功能策略的检查。

5.3.1.11 区分安全管理角色

防火墙安全功能:

a) 应将与安全相关的管理功能与其他功能区分开;

b) 应包括安装、配置和管理防火墙安全功能本身所需的所有功能,其中至少应包括:增加和删除主体(发送信息的主机)和客体(接受信息的主机),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;

c) 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;

d) 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;

e) 应仅允许授权管理员和可信主机承担安全管理职责;

f) 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。

5.3.1.12 管理功能

防火墙安全功能应向授权管理员提供如下管理功能:

a) 能设置和更新与安全相关的数据;

b) 能执行防火墙的安装及初始化、系统启动和关闭、备份和恢复的能力,备份能力应有自动工具的支持;

c) 如果防火墙安全功能支持外部或内部接口的远程管理,那么它应:

1) 具有对两个接口或其中之一关闭远程管理的选择权;

2) 能限制那些可进行远程管理的地址;

3) 能通过加密来保护远程管理对话。

5.3.2 标记

防火墙安全功能应维护与授权管理员以及授权管理员可直接访问的防火墙中安全功能数据和存储

客体相关的敏感标记。

5.3.3 身份鉴别

5.3.3.1 鉴别数据初始化

防火墙安全功能应根据规定的鉴别机制，提供授权管理员和可信主机鉴别数据的初始化功能，并确保仅允许授权管理员使用这些功能。

5.3.3.2 鉴别时机

在所有授权管理员和可信主机请求执行的任何操作之前，防火墙安全功能应确保对每个授权管理员和可信主机进行了身份鉴别。

5.3.3.3 最少反馈

当进行鉴别时，防火墙安全功能应仅将最少的反馈（如：打入的字符数，鉴别的成功或失败）提供给用户。

5.3.3.4 多鉴别机制

防火墙安全功能应提供多鉴别机制以支持用户多鉴别。

5.3.3.5 鉴别失败处理

在经过一定次数的鉴别失败以后，防火墙安全功能应能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。

5.3.4 客体重用

在为所有内部或外部网上的主机连接进行资源分配时，防火墙安全功能应保证不提供以前连接的任何信息内容。

5.3.5 审计

5.3.5.1 审计数据生成

防火墙安全功能应能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) 任何对审计记录进行操作的尝试，包括关闭审计功能或子系统，以及受影响客体的标识；

c) 任何读取、修改、破坏审计记录的尝试；

d) 所有对防火墙规则覆盖的客体（内部或外部网络上的主机）执行操作的请求，以及受影响客体的标识；

e) 修改安全属性的所有尝试，以及修改后安全属性的新值；

f) 所有使用安全功能中鉴别数据管理机制的请求；

g) 所有访问鉴别数据的请求，以及访问请求的目标；

h) 所有使用标识机制的尝试；

i) 任何对鉴别机制的使用；

j) 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，以及配置参数的新值；

k) 因鉴别尝试不成功的次数超出了设定的限制，导致的会话连接终止，以及会话连接使用的标识符。

对于每一个审计记录，防火墙安全功能应至少记录以下信息：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。

5.3.5.2 用户身份关联

防火墙安全功能应能将每个可审计事件与引起该事件的用户身份相关联。

5.3.5.3 审计记录管理

防火墙安全功能应使授权管理员能创建、存档、删除和清空审计记录。

5.3.5.4 可理解的格式

防火墙安全功能应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。

5.3.5.5 限制审计记录访问

防火墙安全功能应仅允许授权管理员访问审计记录。

5.3.5.6 可选择查阅审计

防火墙安全功能应提供能按主体ID、客体ID、日期、时间以及这些参数的逻辑组合等参数对审计数据进行查找和排序的审计查阅工具。

5.3.5.7 防止审计数据丢失

防火墙安全功能：

a) 应把生成的审计记录储存于一个永久性的审计记录中，并应限制由于故障和攻击造成的审计事件丢失的数量；

b) 一旦审计存储容量达到事先规定的警戒值，应能发出警告信息，并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。

对因故障或存储耗竭而导致审计数据丢失的最大审计存储容量，防火墙的开发者应提供相应的分析结果。

5.3.6 数据完整性

防火墙安全功能应保护储存于设备中的鉴别数据和过滤策略不受未授权修改和破坏。

5.3.7 密码支持

防火墙安全功能应保证其远程管理会话的加密符合国家密码主管部门的有关规定。

5.3.8 生存周期支持

5.3.8.1 开发安全

开发者应提供开发安全文件。

开发安全文件应描述在防火墙的开发环境中，为保护防火墙设计和实现的机密性和完整性，而在物理上、程序上、人员上以及其他方面所采取的必要的安全措施。开发安全文件还应提供在防火墙的开发和维护过程中执行安全措施的证据。

5.3.8.2 生存周期模型

开发者应建立生存周期模型并提供生存周期定义文档。

在生存周期定义文档中，应描述用于开发和维护防火墙的模型。为了对防火墙开发和维护进行必要的控制，该模型应提供相应的支持。

5.3.8.3 工具和技术

开发者应标识用于开发防火墙的工具，并对开发工具中已选择的依赖实现的选项文档化。

在开发工具文档中，应明确定义所有用于实现的开发工具和实现中每个语句的含义，以及所有基于实现的选项的含义。

5.3.9 配置管理

5.3.9.1 部分配置管理

开发者应使用配置管理系统，并提供配置管理计划。

配置管理系统应确保只有已授权开发人员才能对防火墙产品实现进行修改，并支持防火墙基本配置项的生成。

配置管理计划应描述在配置管理系统中使用的工具软件。

5.3.9.2 产生支持和接受程序

开发者应使用配置管理系统并提供配置管理文档，以及为防火墙产品的不同版本提供唯一的标识。

配置管理系统应对所有的配置项作出唯一的标识，并保证只有经过授权才能修改配置项，还应支持防火墙基本配置项的生成。

配置管理文档应包括配置清单、配置管理计划以及接受计划。配置清单用来描述组成防火墙的配置项。在配置管理计划中，应描述配置管理系统是如何使用的。实施的配置管理应与配置管理计划相一致。在接受计划中，应描述对修改过或新建的配置项进行接受的程序。

配置管理文档还应描述对配置项给出唯一标识的方法，并提供所有的配置项得到有效地维护的证据。

5.3.9.3 配置管理范围

开发者应提供配置管理文档。

配置管理文档应说明配置管理系统至少能跟踪：防火墙实现表示、设计文档、测试文档、用户文档、管理员文档、配置管理文档和安全缺陷，并描述配置管理系统是如何跟踪配置项的。

5.3.10 安全功能开发过程

5.3.10.1 安全策略模型

开发者应提供安全策略模型并阐明安全功能规约和安全策略模型之间的对应性。

安全策略模型应是非形式化的。对于所有可以模型化的安全策略，在模型中应描述其规则和特性，并阐明该模型对所有可模型化的安全策略来说是一致的、完备的。在阐明防火墙安全策略模型和安全功能规约之间的对应性时，应说明，所有安全功能规约中的安全功能与安全策略模型是一致的、是完备的。

5.3.10.2 功能规约

开发者应提供防火墙的安全功能规约。

安全功能规约应以非形式方法来描述安全功能与其外部接口，并描述使用外部安全功能接口的目的与方法，在需要的时候，还要提供例外情况和错误信息的细节。

安全功能规约应是内在一致的，能完备地表示安全功能，并提供安全基本原理证明安全功能的表示是完备的。

5.3.10.3 高层设计

开发者应提供防火墙安全功能的高层设计。

高层设计应以非形式方法表述并且是内在一致的。为说明安全功能的结构，高层设计应将安全功能分解为各个安全功能子系统进行描述，并阐明如何将有助于加强防火墙安全功能的子系统和其他子系统分开。对于每一个安全功能子系统，高层设计应描述其提供的安全功能，标识其所有接口以及哪些接口是外部可见的，描述其所有接口的使用目的与方法，并提供安全功能子系统的作用、例外情况和错误信息的细节。高层设计还应标识安全功能要求的所有基础性的硬件、固件和软件，并且支持由这些硬件、固件或软件所实现的保护机制。

5.3.10.4 低层设计

开发者应提供防火墙安全功能的低层设计。

低层设计应是非形式化、内在一致的。在描述防火墙安全功能时，低层设计应采用模块术语，说明每一个安全功能模块的目的，并标识安全功能模块的所有接口和安全功能模块可为外部所见的接口，以及安全功能模块所有接口的目的与方法，适当时，还应提供接口的作用、例外情况和错误信息的细节。

低层设计还应包括以下内容：

a) 以安全功能性术语及模块的依赖性术语，定义模块间的相互关系；

b) 说明如何提供每一个安全策略的强化功能；

c) 说明如何将防火墙加强安全策略的模块和其他模块分离开。

5.3.10.5 安全功能的实现

开发者应为选定的防火墙安全功能子集提供实现表示。

实现表示应无歧义而且详细地定义防火墙安全功能，使得不需要进一步的设计就能生成该安全功能的子集。实现表示应是内在一致的。

5.3.10.6 表示对应性

开发者应在防火墙安全功能表示的所有相邻对之间提供对应性分析。

对于防火墙安全功能表示的每个相邻对，分析应阐明：较为抽象的安全功能表示的所有相关安全功能，应在较具体的安全功能表示中得到正确而完备地细化。

5.3.11 测试

5.3.11.1 功能测试

开发者应测试安全功能，将结果文档化并提供测试文档。

测试文档应包括测试计划、测试过程、预期的测试结果和实际测试结果。测试计划应标识要测试的安全功能，并描述测试的目标。测试过程应标识要执行的测试，并描述每个安全功能的测试概况，这些概况包括对其他测试结果的顺序依赖性。期望的测试结果应表明测试成功后的预期输出。实际测试结果应表明每个被测试的安全功能能按照规定进行运作。

5.3.11.2 覆盖分析

开发者应提供测试覆盖的分析结果。

测试覆盖的分析结果应表明测试文档中所标识的测试与安全功能规约中所描述的安全功能是对应的，且该对应是完备的。

5.3.11.3 深度

开发者应提供测试深度的分析。

在深度分析中，应说明测试文档中所标识的对安全功能的测试，足以表明该安全功能和高层设计是一致的。

5.3.11.4 独立性测试

开发者应提供证据证明开发者提供的防火墙经过独立的第三方测试并通过。

5.3.12 指导性文档

5.3.12.1 管理员指南

开发者应提供系统管理员使用的管理员指南。

管理员指南应说明以下内容：

a) 防火墙管理员可以使用的管理功能和接口；

b) 怎样安全地管理防火墙；

c) 在安全处理环境中应进行控制的功能和权限；

d) 所有对与防火墙的安全操作有关的用户行为的假设；

e) 所有受管理员控制的安全参数，如果可能，应指明安全值；

f) 每一种与管理功能有关的安全相关事件，包括对安全功能所控制的实体的安全特性进行的改变；

g) 所有与系统管理员有关的 IT 环境的安全要求。

管理员指南应与为评估而提供的其他所有文件保持一致。

5.3.12.2 用户指南

开发者应提供用户指南。

用户指南应说明以下内容：

a) 防火墙的非管理用户可使用的安全功能和接口；

b) 防火墙提供给用户的安全功能和接口的用法；

c) 用户可获取但应受安全处理环境控制的所有功能和权限；

d) 防火墙安全操作中用户所应承担的职责；

e) 与用户有关的 IT 环境的所有安全要求。

用户指南应与为评估而提供的其他所有文件保持一致。

5.3.13 脆弱性分析

5.3.13.1 指南检查

开发者应提供指南性文档**并将其文档化**。

在指南性文档中，应确定对防火墙的所有可能的操作方式(包括失败和操作失误后的操作)、它们的后果以及对于保持安全操作的意义。指南性文档中还应列出所有目标环境的假设以及所有外部安全措施(包括外部程序的、物理的或人员的控制)的要求。指南性文档应是完备的、清晰的、一致的、合理的。**在分析文档中，应阐明指南性文档是完备的。**

5.3.13.2 脆弱性分析

开发者应从用户可能破坏安全策略的明显途径出发，对防火墙的各种功能进行分析并提供文档。对被确定的脆弱性，开发者应明确记录采取的措施。

对每一条脆弱性，应有证据显示在使用防火墙的环境中该脆弱性不能被利用。在文档中，还需证明经过标识脆弱性的防火墙可以抵御明显的穿透性攻击。

5.3.14 交付和运行

5.3.14.1 交付

开发者应使用一定的交付程序交付防火墙，并将交付过程文档化。

交付文档应包括以下内容：

a) 在给用户方交付防火墙的各版本时，为维护安全所必需的所有程序；

b) 开发者的向用户提供的防火墙版本和用户收到的版本之间的差异以及如何监测对防火墙的修改；

c) 如何发现他人伪装成开发者修改用户的防火墙。

5.3.14.2 安装生成

开发者应提供文档说明防火墙的安装、生成和启动的过程。

5.4 结构化保护级

5.4.1 访问控制

5.4.1.1 安全属性定义

对于每一个授权管理员、可信主机和主机，防火墙安全功能应为其提供一套唯一的、为了执行安全功能策略所必需的安全属性。

5.4.1.2 属性初始化

防火墙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。

5.4.1.3 属性修改

防火墙安全功能应仅向授权管理员提供修改下述(包含但不仅限于)参数的能力：

a) 标识与角色(例如：审计管理员等)的关系；

b) 源地址、目的地址、传输层协议和请求的服务(例如：源端口号或目的端口号等访问控制属性)；

c) 配置的安全参数(例如：最大鉴别失败次数、最大审计存储容量等数据)。

5.4.1.4 **属性查询**

防火墙安全功能应仅向授权管理员提供以下查询：源地址、目的地址、传输层协议和请求的服务（例如：源端口号或目的端口号等访问控制属性）

5.4.1.5 **客体访问控制策略**

对于防火墙的主体（未经防火墙鉴别的发送信息的主机）和客体（内部或外部网上的接收信息的主机）以及安全功能策略（SFP）所包括的主体、客体的所有操作，防火墙安全功能应执行未鉴别的端到端策略，并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。

5.4.1.6 **防火墙自身强制访问控制**

防火墙安全功能应通过授权管理员和授权管理员控制的安全功能数据的敏感标记，控制授权管理员对相关安全功能数据的直接和间接访问。

5.4.1.7 **访问授权与拒绝**

防火墙安全功能应根据主体和客体的安全属性值[源地址、目的地址、传输层协议和请求的服务（例如：源端口号或目的端口号）等]，提供明确的访问保障能力和拒绝访问能力。

5.4.1.8 **完全信息流控制**

防火墙安全功能应根据：发出信息的主机地址和信息流类型等安全属性，**以及导致信息流入/流出的操作**，确定允许信息流通过或禁止信息流通过。

对于导致信息流入/流出防火墙所保护的任意内部或外部网络上主机的所有操作，防火墙安全功能应保证其被一个信息流控制规则所覆盖。

5.4.1.9 **无非法信息流**

防火墙安全功能应保证没有规避信息流控制规则的非法信息流存在。

5.4.1.10 **安全功能区域分隔**

为保护防火墙安全功能免遭不可信主体（内部或外部网络上的主机）的干扰和篡改，防火墙安全功能应为其自身的执行过程设定一个安全区域，并把防火墙控制范围内的各个主体（内部或外部网络上的主机）的安全区域分隔开。

5.4.1.11 **不可旁路**

在与安全有关的操作（例如安全属性的修改、外部网络主机向内部网络主机发送信息等）被允许执行之前，防火墙安全功能应确保其通过安全功能策略的检查。

5.4.1.12 **区分安全管理角色**

防火墙安全功能：

a) 应将与安全相关的管理功能与其他功能区分开；

b) 应包括安装、配置和管理防火墙安全功能本身所需的所有功能，其中至少应包括：增加和删除主体（发送信息的主机）和客体（接受信息的主机），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；

c) 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；

d) 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；

e) 应仅允许授权管理员和可信主机承担安全管理职责；

f) 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。

5.4.1.13 **管理功能**

防火墙安全功能应向授权管理员提供如下管理功能：

a) 能设置和更新与安全相关的数据；

b) 能执行防火墙的安装及初始化、系统启动和关闭、备份和恢复的能力，备份能力应有自动工具的支持；

c) 如果防火墙安全功能支持外部或内部接口的远程管理，那么它应：

1) 具有对两个接口或其中之一关闭远程管理的选择权；

2) 能限制那些可进行远程管理的地址；

3) 能通过加密来保护远程管理对话。

5.4.2 标记

防火墙安全功能应维护与授权管理员以及授权管理员可直接或间接访问的防火墙中安全功能数据和存储客体相关的敏感标记。

5.4.3 身份鉴别

5.4.3.1 鉴别数据初始化

防火墙安全功能应根据规定的鉴别机制，提供授权管理员和可信主机鉴别数据的初始化功能，并确保仅允许授权管理员使用这些功能。

5.4.3.2 鉴别时机

在所有授权管理员和可信主机请求执行的任何操作之前，防火墙安全功能应确保对每个授权管理员和可信主机进行了身份鉴别。

5.4.3.3 最少反馈

当进行鉴别时，防火墙安全功能应仅将最少的反馈（如：打入的字符数，鉴别的成功或失败）提供给用户。

5.4.3.4 多鉴别机制

防火墙安全功能应提供多鉴别机制以支持用户多鉴别。

5.4.3.5 鉴别失败处理

在经过一定次数的鉴别失败以后，防火墙安全功能应能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。

5.4.3.6 用户-主体绑定

防火墙应把合适的用户安全属性关联到代表用户活动的主体上。

5.4.4 客体重用

在为所有内部或外部网上的主机连接进行资源分配时，防火墙安全功能应保证不提供以前连接的任何信息内容。

5.4.5 审计

5.4.5.1 审计数据生成

防火墙安全功能应能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) 任何对审计记录进行操作的尝试，包括关闭审计功能或子系统，以及受影响客体的标识；

c) 任何读取、修改、破坏审计记录的尝试；

d) 所有对防火墙规则覆盖的客体（内部或外部网络上的主机）执行操作的请求，以及受影响客体的标识；

e) 修改安全属性的所有尝试，以及修改后安全属性的新值；

f) 所有使用安全功能中鉴别数据管理机制的请求；

g) 所有访问鉴别数据的请求，以及访问请求的目标；

h) 所有使用标识机制的尝试；

i) 任何对鉴别机制的使用；

j) 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，以及配置参数的新值；

k) 因鉴别尝试不成功的次数超出了设定的限制，导致的会话连接终止，以及会话连接使用的标识符；

l) 开启和关闭任何审计记录分析机制；

m) 在信息流控制中，对信息流请求的所有裁决；

n) 可信路径功能的所有尝试过的使用。

对于每一个审计记录，防火墙安全功能应至少记录以下信息：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。

5.4.5.2 用户身份关联

防火墙安全功能应能将每个可审计事件与引起该事件的用户身份相关联。

5.4.5.3 审计记录管理

防火墙安全功能应使授权管理员能创建、存档、删除和清空审计记录。

5.4.5.4 可理解的格式

防火墙安全功能应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。

5.4.5.5 限制审计记录访问

防火墙安全功能应仅允许授权管理员访问审计记录。

5.4.5.6 可选择查阅审计

防火墙安全功能应提供能按主体 ID、客体 ID、日期、时间以及这些参数的逻辑组合等参数对审计数据进行查找和排序的审计查阅工具。

5.4.5.7 防止审计数据丢失

防火墙安全功能：

a) 应把生成的审计记录储存于一个永久性的审计记录中，并应限制由于故障和攻击造成的审计事件丢失的数量；

b) 一旦审计存储容量达到事先规定的警戒值，应能发出警告信息，并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。

对因故障或存储耗竭而导致审计数据丢失的最大审计存储容量，防火墙的开发者应提供相应的分析结果。

5.4.5.8 潜在侵害分析

防火墙安全功能应能用一系列规则去监控审计事件，并根据这些规则指示出防火墙的潜在侵害。这些规则包括：

a) 已知的用来指示潜在安全攻击的已定义的可审计事件的子集的积累或组合；

b) 任何其他用户定义的规则。

5.4.6 数据完整性

防火墙安全功能应保护储存于设备中的鉴别数据和过滤策略不受未授权修改和破坏。

5.4.7 可信路径

在授权管理员登录和鉴别(包括远程登录和鉴别)时，防火墙安全功能应提供与授权管理员之间的可信通信路径。该路径上的通信只能由授权管理员初始化。

5.4.8 密码支持

防火墙安全功能应保证其远程管理会话的加密符合国家密码主管部门的有关规定。

5.4.9 生存周期支持

5.4.9.1 开发安全

开发者应提供开发安全文件。

开发安全文件应描述在防火墙的开发环境中，为保护防火墙设计和实现的机密性和完整性，而在物理上、程序上、人员上以及其他方面所采取的必要的安全措施。开发安全文件还应提供在防火墙的开发和维护过程中执行安全措施的证据。

5.4.9.2 生存周期模型

开发者应利用标准化的生存周期模型来开发和维护防火墙并提供生存周期定义文档。

在生存周期定义文档中，应描述用于开发和维护防火墙的模型，解释选择该模型的原因，并阐明实际使用的模型与标准化的生存周期模型是相符的。为对防火墙开发和维护进行必要的控制，该模型应提供相应的支持并解释如何用该模型来开发和维护防火墙。

5.4.9.3 工具和技术

开发者应标识用于开发防火墙的工具并对开发工具中已选择的依赖实现的选项文档化。开发者还应描述所应用的实现标准。

在开发工具文档中，应明确定义所有用于实现的开发工具和实现中每个语句的含义，以及所有基于实现的选项的含义。

5.4.10 配置管理

5.4.10.1 部分配置管理

开发者应使用配置管理系统，并提供配置管理计划。

配置管理系统应确保只有已授权开发人员才能对防火墙产品实现进行修改，并支持防火墙基本配置项的生成。

配置管理计划应描述在配置管理系统中使用的工具软件。

5.4.10.2 产生支持和接受程序

开发者应使用配置管理系统并提供配置管理文档，以及为防火墙产品的不同版本提供唯一的标识。

配置管理系统应对所有的配置项作出唯一的标识，并保证只有经过授权才能修改配置项，还应支持防火墙基本配置项的生成。

配置管理文档应包括配置清单、配置管理计划以及接受计划。配置清单用来描述组成防火墙的配置项。在配置管理计划中，应描述配置管理系统是如何使用的。实施的配置管理应与配置管理计划相一致。在接受计划中，应描述对修改过或新建的配置项进行接受的程序。

配置管理文档还应描述对配置项给出唯一标识的方法，并提供所有的配置项得到有效地维护的证据。

5.4.10.3 配置管理范围

开发者应提供配置管理文档。

配置管理文档应说明配置管理系统至少能跟踪：防火墙实现表示、设计文档、测试文档、用户文档、管理员文档、配置管理文档、安全缺陷以及开发工具及相关信息，并描述配置管理系统是如何跟踪配置项的。

5.4.11 安全功能开发过程

5.4.11.1 安全策略模型

开发者应提供安全策略模型并阐明安全功能规约和安全策略模型之间的对应性，在适当时，应给出对应性的严格证明。

安全策略模型应是形式化的。对于所有可以模型化的安全策略，在模型中应描述其规则和特性，并

阐明该模型对所有可模型化的安全策略来说是一致的、完备的。在阐明防火墙安全策略模型和安全功能规约之间的对应性时，应说明，所有安全功能规约中的安全功能与安全策略模型是一致的、是完备的。**当安全功能规约是半形式化时，阐明安全策略模型与安全功能规约之间的对应性时也应半形式化；如果安全功能规约是形式化的，则阐明安全策略模型与安全功能规约之间的对应性也应形式化。**

5.4.11.2 **功能规约**

开发者应提供防火墙的安全功能规约。

安全功能规约应以**半形式化风格**来描述安全功能与其外部接口，**在需要时，可用非形式化、解释性的文字来支持安全功能规约的描述**。安全功能规约还应描述使用外部安全功能接口的目的与方法，在需要的时候，应提供例外情况和错误信息的细节。

安全功能规约应是内在一致的，能完备地表示安全功能，并提供安全基本原理证明安全功能的表示是完备的。

5.4.11.3 **高层设计**

开发者应提供防火墙安全功能的高层设计。

高层设计应以**半形式化方法**表述并且是内在一致的。为说明安全功能的结构，高层设计应将安全功能分解为各个安全功能子系统进行描述，并阐明如何将有助于加强防火墙安全功能的子系统和其他子系统分开。对于每一个安全功能子系统，高层设计应描述其提供的安全功能，标识其所有接口以及哪些接口是外部可见的，描述其所有接口的使用目的与方法，并提供安全功能子系统**所有的**作用、例外情况和错误信息的**完整**细节。高层设计还应标识安全功能要求的所有基础性的硬件、固件和软件，并且支持由这些硬件、固件或软件所实现的保护机制。

5.4.11.4 **低层设计**

开发者应提供防火墙安全功能的低层设计。

低层设计应是**半形式化**、内在一致的。在描述防火墙安全功能时，低层设计应采用模块术语，说明每一个安全功能模块的目的，并标识安全功能模块的所有接口和安全功能模块可为外部所见的接口，以及安全功能模块所有接口的目的与方法，适当时，还应提供接口**所有的**作用、例外情况和错误信息的**完整**细节。

低层设计还应包括以下内容：

a) 以安全功能性术语及模块的依赖性术语，定义模块间的相互关系；

b) 说明如何提供每一个安全策略的强化功能；

c) 说明如何将防火墙加强安全策略的模块和其他模块分离开。

5.4.11.5 **模块化**

为避免设计模块之间出现不必要的交互作用，开发者应以模块化方法设计和构建防火墙安全功能，并提供防火墙安全功能的结构化描述。

结构化描述应标识所有的防火墙安全功能模块并描述每一个安全功能模块的目的、接口、参数和影响。结构化描述还应阐明安全功能设计是如何避免各模块之间不必要的交互作用的。

5.4.11.6 **安全功能的实现**

开发者应为**全部**防火墙安全功能提供实现表示。

实现表示应无歧义而且详细地定义**全部**防火墙安全功能，使得不需要进一步的设计就能生成安全功能。实现表示应是内在一致的**并能描述实现各部分之间的关系**。

5.4.11.7 **表示对应性**

开发者应在防火墙安全功能表示的所有相邻对之间提供对应性分析。

对于防火墙安全功能表示的每个相邻对，分析应阐明：较为抽象的安全功能表示的所有相关安全功

能，应在较具体的安全功能表示中得到正确而完备地细化。并且如果某个相邻对的各部分都至少是半形式化时，相应的对应性阐明也应是半形式化的。

5.4.12 测试

5.4.12.1 功能测试

开发者应测试安全功能，将结果文档化并提供测试文档。

测试文档应包括测试计划、测试过程、预期的测试结果和实际测试结果。测试计划应标识要测试的安全功能，并描述测试的目标。测试过程应标识要执行的测试，并描述每个安全功能的测试概况，这些概况包括对其他测试结果的顺序依赖性。期望的测试结果应表明测试成功后的预期输出。实际测试结果应表明每个被测试的安全功能能按照规定进行运作。

5.4.12.2 覆盖分析

开发者应提供测试覆盖的分析结果。

测试覆盖的分析结果应表明测试文档中所标识的测试与安全功能规约中所描述的安全功能是对应的，且该对应是完备的。

5.4.12.3 深度

开发者应提供测试深度的分析。

在深度分析中，应说明测试文档中所标识的对安全功能的测试，足以表明该安全功能和高层设计以及低层设计是一致的。

5.4.12.4 独立性测试

开发者应提供证据证明，开发者提供的防火墙经过独立的第三方测试并通过。

5.4.13 指导性文档

5.4.13.1 管理员指南

开发者应提供系统管理员使用的管理员指南。

管理员指南应说明以下内容：

a) 防火墙管理员可以使用的管理功能和接口；

b) 怎样安全地管理防火墙；

c) 在安全处理环境中应进行控制的功能和权限；

d) 所有对与防火墙的安全操作有关的用户行为的假设；

e) 所有受管理员控制的安全参数，如果可能，应指明安全值；

f) 每一种与管理功能有关的安全相关事件，包括对安全功能所控制的实体的安全特性进行的改变；

g) 所有与系统管理员有关的 IT 环境的安全要求。

管理员指南应与为评估而提供的其他所有文件保持一致。

5.4.13.2 用户指南

开发者应提供用户指南。

用户指南应说明以下内容：

a) 防火墙的非管理用户可使用的安全功能和接口；

b) 防火墙提供给用户的安全功能和接口的用法；

c) 用户可获取但应受安全处理环境控制的所有功能和权限；

d) 防火墙安全操作中用户所应承担的职责；

e) 与用户有关的 IT 环境的所有安全要求。

用户指南应与为评估而提供的其他所有文件保持一致。

5.4.14 脆弱性分析

5.4.14.1 隐蔽通道分析

开发者应对每个信息流控制策略都搜索隐蔽通道并提供隐蔽通道分析的文档。

分析文档应包括以下内容：

a) 标识隐蔽通道并且估计它们的容量；

b) 描述用于确定隐蔽通道存在的程序，以及进行隐蔽通道分析所需要的信息；

c) 描述在进行隐蔽通道分析期间所作的全部假设；

d) 描述在最坏的情况下，对通道容量进行估计的方法；

e) 为每个可标识的隐蔽通道描述其最坏的利用情形。

5.4.14.2 分析确认

开发者应提供指南性文档并将其文档化。

在指南性文档中，应确定对防火墙的所有可能的操作方式(包括失败和操作失误后的操作)、它们的后果以及对于保持安全操作的意义。指南性文档中还应列出所有目标环境的假设以及所有外部安全措施(包括外部程序的、物理的或人员的控制)的要求。指南性文档应是完备的、清晰的、一致的、合理的。在分析文档中，应阐明指南性文档是完备的。

5.4.14.3 脆弱性分析

开发者应从用户可能破坏安全策略的明显途径出发，对防火墙的各种功能进行分析并提供文档。对被确定的脆弱性，开发者应明确记录采取的措施。

对每一条脆弱性，应有证据显示在使用防火墙的环境中该脆弱性不能被利用。在文档中，还需证明经过标识脆弱性的防火墙可以抵御穿透性攻击，并说明对脆弱性的搜索是系统化的。

5.4.15 交付与运行

5.4.15.1 交付

开发者应使用一定的交付程序交付防火墙，并以文档的形式将交付程序提供给用户。

交付文档应包括以下内容：

a) 在给用户方交付防火墙的各版本时，为维护安全所必需的所有程序；

b) 开发者的向用户提供的防火墙版本和用户收到的版本之间的差异以及如何监测对防火墙的修改；

c) 如何发现他人伪装成开发者修改用户的防火墙。

5.4.15.2 安装生成

开发者应提供文档说明防火墙的安装、生成和启动的过程。

5.5 访问验证保护级

5.5.1 访问控制

5.5.1.1 安全属性定义

对于每一个授权管理员、可信主机和主机，防火墙安全功能应为其提供一套唯一的、为了执行安全功能策略所必需的安全属性。

5.5.1.2 属性初始化

防火墙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。

5.5.1.3 属性修改

防火墙安全功能应仅向授权管理员提供修改下述(包含但不仅限于)参数的能力：

a) 标识与角色(例如：审计管理员等)的关系；

b) 源地址、目的地址、传输层协议和请求的服务(例如：源端口号或目的端口号等访问控制属

性）；

c） 配置的安全参数（例如：最大鉴别失败次数、最大审计存储容量等数据）。

5.5.1.4 **属性查询**

防火墙安全功能应仅向授权管理员提供以下查询：源地址、目的地址、传输层协议和请求的服务（例如：源端口号或目的端口号等访问控制属性）。

5.5.1.5 **客体访问控制策略**

对于防火墙的主体（未经防火墙鉴别的发送信息的主机）和客体（内部或外部网上的接收信息的主机）以及安全功能策略（SFP）所包括的主体、客体的所有操作，防火墙安全功能应执行未鉴别的端到端策略，并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。

5.5.1.6 **防火墙自身强制访问控制**

防火墙安全功能应通过授权管理员和授权管理员控制的安全功能数据的敏感标记，控制授权管理员对相关安全功能数据的直接和间接访问。

5.5.1.7 **访问授权与拒绝**

防火墙安全功能应根据主体和客体的安全属性值[源地址、目的地址、传输层协议和请求的服务（例如：源端口号或目的端口号）等]，提供明确的访问保障能力和拒绝访问能力。

5.5.1.8 **完全信息流控制**

防火墙安全功能应根据：发出信息的主机地址和信息流类型等安全属性，以及导致信息流入/流出的操作，确定允许信息流通过或禁止信息流通过。

对于导致信息流入/流出防火墙所保护的任意内部或外部网络上主机的所有操作，防火墙安全功能应保证其被一个信息流控制规则所覆盖。

5.5.1.9 **无非法信息流**

防火墙安全功能应保证没有规避信息流控制规则的非法信息流存在。

5.5.1.10 **完全的访问监控器**

防火墙的未隔离部分应为自身执行维护一个安全区域，防止不可信主体（内部或外部网络上的主机）的干扰和篡改；

防火墙安全功能应对其控制范围内的主机的安全区域之间强行分离；

防火墙安全功能应对防火墙安全功能中与访问控制或信息流控制功能策略有关的部分，维护一个自身执行的安全区域，防止被其他的安全功能和该功能策略不可信主体（内部或外部网络上的主机）干扰或篡改。

5.5.1.11 **不可旁路**

在与安全有关的操作（例如：安全属性的修改、外部网络主机向内部网络主机发送信息等）被允许执行之前，防火墙安全功能应确保其通过安全功能策略的检查。

5.5.1.12 **区分安全管理角色**

防火墙安全功能：

a） 应将与安全相关的管理功能与其他功能区分开；

b） 应包括安装、配置防火墙安全功能所需的所有功能；

c） 应包括管理防火墙安全功能本身所需的所有功能，其中至少应包括：增加和删除主体（发送信息的主机）和客体（接受信息的主机），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；

d） 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；

e) 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；

f) 应仅允许授权管理员和可信主机承担安全管理职责；

g) 应在提出一个明确的请求以后，才允许授权管理员和可信主机承担安全管理职责。

5.5.1.13 **管理功能**

防火墙安全功能应向授权管理员提供如下管理功能：

a) 能设置和更新与安全相关的数据；

b) 能执行防火墙的安装及初始化、系统启动和关闭、备份和恢复的能力，备份能力应有自动工具的支持；

c) 如果防火墙安全功能支持外部或内部接口的远程管理，那么它应：

1) 具有对两个接口或其中之一关闭远程管理的选择权；

2) 能限制那些可进行远程管理的地址；

3) 能通过加密来保护远程管理对话。

5.5.2 **标记**

防火墙安全功能应维护与授权管理员以及授权管理员可直接或间接访问的防火墙中安全功能数据和存储客体相关的敏感标记。

5.5.3 **身份鉴别**

5.5.3.1 **鉴别数据初始化**

防火墙安全功能应根据规定的鉴别机制，提供授权管理员和可信主机鉴别数据的初始化功能，并确保仅允许授权管理员使用这些功能。

5.5.3.2 **鉴别时机**

在所有授权管理员和可信主机请求执行的任何操作之前，防火墙安全功能应确保对每个授权管理员和可信主机进行了身份鉴别。

5.5.3.3 **最少反馈**

当进行鉴别时，防火墙安全功能应仅将最少的反馈(如：打入的字符数，鉴别的成功或失败)提供给用户。

5.5.3.4 **多鉴别机制**

防火墙安全功能应提供多鉴别机制以支持用户多鉴别。

5.5.3.5 **重鉴别**

防火墙安全功能应规定重鉴别条件，在对应的条件下，对用户进行重鉴别。

5.5.3.6 **鉴别失败处理**

在经过一定次数的鉴别失败以后，防火墙安全功能应能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。

5.5.3.7 **用户-主体绑定**

防火墙应把合适的用户安全属性关联到代表用户活动的主体上。

5.5.4 **客体重用**

在为所有内部或外部网上的主机连接进行资源分配时，防火墙安全功能应保证不提供以前连接的任何信息内容。

5.5.5 **审计**

5.5.5.1 **审计数据生成**

防火墙安全功能应能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) 任何对审计记录进行操作的尝试，包括关闭审计功能或子系统，以及受影响客体的标识；

c) 任何读取、修改、破坏审计记录的尝试；

d) 所有对防火墙规则覆盖的客体（内部或外部网络上的主机）执行操作的请求，以及受影响客体的标识；

e) 修改安全属性的所有尝试，以及修改后安全属性的新值；

f) 所有使用安全功能中鉴别数据管理机制的请求；

g) 所有访问鉴别数据的请求，以及访问请求的目标；

h) 所有使用标识机制的尝试；

i) 任何对鉴别机制的使用；

j) 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，以及配置参数的新值；

k) 因鉴别尝试不成功的次数超出了设定的限制，导致的会话连接终止，以及会话连接使用的标识符；

l) 开启和关闭任何审计记录分析机制；

m) 在信息流控制中，对信息流请求的所有裁决；

n) 可信路径功能的所有尝试过的使用；

o) **数据鉴别中，有效证据产生成功或者失败。**

对于每一个审计记录，防火墙安全功能应至少记录以下信息：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。

5.5.5.2 用户身份关联

防火墙安全功能应能将每个可审计事件与引起该事件的用户身份相关联。

5.5.5.3 审计记录管理

防火墙安全功能应使授权管理员能创建、存档、删除和清空审计记录。

5.5.5.4 可理解的格式

防火墙安全功能应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。

5.5.5.5 限制审计记录访问

防火墙安全功能应仅允许授权管理员访问审计记录。

5.5.5.6 可选择查阅审计

防火墙安全功能应提供能按主体 ID、客体 ID、日期、时间以及这些参数的逻辑组合等参数对审计数据进行查找和排序的审计查阅工具。

5.5.5.7 防止审计数据丢失

防火墙安全功能：

a) 应把生成的审计记录储存于一个永久性的审计记录中，并应限制由于故障和攻击造成的审计事件丢失的数量；

b) 一旦审计存储容量达到事先规定的警戒值，应能发出警告信息，并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。

对因故障或存储耗竭而导致审计数据丢失的最大审计存储容量，防火墙的开发者应提供相应的分析结果。

5.5.5.8 潜在侵害分析

防火墙安全功能应能用一系列规则去监控审计事件，并根据这些规则指示出防火墙的潜在侵害。这些规则包括：

a) 已知的用来指示潜在安全攻击的已定义的可审计事件的子集的积累或组合；

b) 任何其他用户定义的规则。

5.5.5.9 复杂攻击探测

对于已知入侵方案的事件序列和指示出对防火墙的一个潜在攻击的签名事件，防火墙安全功能应能维护其内部表示，并比较系统行为的记录与签名事件和事件序列。为辨明系统行为，可以对用来决定系统行为的信息进行检查。当一个系统事件或事件序列被发现与一个表示对防火墙的潜在攻击的签名事件匹配时，防火墙安全功能应能指出一个对防火墙的攻击即将到来。

5.5.6 数据完整性

5.5.6.1 基本数据鉴别

对通过防火墙的信息流，防火墙安全功能应具备产生有效性证据的能力，并能向信息的接收者提供验证指定信息的有效性的证据。

5.5.6.2 鉴别数据的保护

防火墙安全功能应保护储存于设备中的鉴别数据和过滤策略不受未授权修改和破坏。

5.5.7 可信路径

在授权管理员登录和鉴别(包括远程登录和鉴别)时，防火墙安全功能应提供与授权管理员之间的可信通信路径。该路径上的通信只能由授权管理员或者防火墙安全功能激活，并在逻辑上与其他路径上的通信相隔离。

5.5.8 可信恢复

对于防火墙服务中断或失败，当不能自动恢复时，防火墙安全功能应进入维护方式，该方式提供将防火墙返回到一个保护状态的能力。

5.5.9 密码支持

防火墙安全功能应保证其远程管理会话的加密符合国家密码主管部门的有关规定。

5.5.10 生存周期支持

5.5.10.1 开发安全

开发者应提供开发安全文件。

开发安全文件应描述在防火墙的开发环境中，为保护防火墙设计和实现的机密性和完整性，而在物理上、程序上、人员上以及其他方面所采取的必要的安全措施。开发安全文件还应提供在防火墙的开发和维护过程中执行安全措施的证据，这些证据应能证明安全措施在维护防火墙的秘密性和完整性方面达到了必要的保护级别。

5.5.10.2 生存周期模型

开发者应利用标准化的和可测量的生存周期模型来开发和维护防火墙并衡量防火墙的开发。开发者还应提供生存周期定义文档。

在生存周期定义文档中，应描述用于开发和维护防火墙的模型，解释选择该模型的原因，并阐明实际使用的模型与标准化的可测量的生存周期模型是相符的。在描述模型时，需要说明使用该模型衡量防火墙开发所需的算术参数和/或度量的细节。为对防火墙开发和维护进行必要的控制，该模型应提供相应的支持并解释如何用该模型来开发和维护防火墙。生存周期文档还应提供利用标准化的可测量的生存周期模型对防火墙开发进行测量的结果。

5.5.10.3 工具和技术

开发者应标识用于开发防火墙的工具并对开发工具中已选择的依赖实现的选项文档化。开发者还应描述在实现防火墙的所有部分时所应用的实现标准。

在开发工具文档中，应明确定义所有用于实现的开发工具和实现中每个语句的含义，以及所有基于

实现的选项的含义。

5.5.11 配置管理

5.5.11.1 完全配置管理

开发者应使用配置管理系统，并提供配置管理计划。

配置管理系统应具备以下功能：

a) 确保只有已授权开发人员才能对防火墙产品实现进行修改；

b) 支持防火墙基本配置项的生成；

c) 记录防火墙各种版本之间的变化；

d) 列出因给定的配置项的修改而受到影响的其他配置项。

配置管理计划应描述在配置管理系统中使用的工具软件。

5.5.11.2 高级支持

开发者应使用配置管理系统并提供配置管理文档，以及为防火墙产品的不同版本提供唯一的标识。

配置管理系统应具备以下功能：

a) 对所有的配置项作出唯一的标识；

b) 保证只有经过授权才能修改配置项；

c) 支持防火墙基本配置项的生成；

d) 保证开发配置项的人不是令配置管理系统接受该配置项的人；

e) 标识组成安全功能的配置项；

f) 支持审计所有对防火墙的修改，并在审计记录中要包括作者、日期、时间等信息；

g) 有能力标识所有用于生成防火墙的源配置项。

配置管理文档包括配置清单、配置管理计划、接受计划和集成程序。配置清单用来描述组成防火墙的配置项。在配置管理计划中，描述了配置管理系统是如何使用的，实施的配置管理应与配置管理计划相一致。接受计划描述对修改过或新建的配置项进行接受的程序。集成程序应描述在防火墙开发过程中如何使用配置管理系统。

配置管理文档还应包括以下内容：

a) 对配置项给出唯一标识的方法；

b) 阐明通过配置管理系统的使用以及开发安全措施，足以保证仅允许已授权的开发人员修改防火墙；

c) 阐明通过使用集成程序，足以确保以授权的方式正确完成防火墙的生成；

d) 阐明通过配置管理系统，足以确保开发配置项的人不是令配置管理系统接受该配置项的人；

e) 证明对所有配置项的修改都进行了充分而适当的复查；

f) 证明所有的配置项都被有效地维护。

5.5.11.3 配置管理范围

开发者应提供配置管理文档。

配置管理文档应说明配置管理系统至少能跟踪：防火墙实现表示、设计文档、测试文档、用户文档、管理员文档、配置管理文档、安全缺陷以及开发工具及相关信息，并描述配置管理系统是如何跟踪配置项的。

5.5.12 安全功能开发过程

5.5.12.1 安全策略模型

开发者应提供安全策略模型并阐明安全功能规约和安全策略模型之间的对应性，在适当时，应给出对应性的严格证明。

安全策略模型应是形式化的。对于所有可以模型化的安全策略，在模型中应描述其规则和特性，并阐明该模型对所有可模型化的安全策略来说是一致的、完备的。在阐明防火墙安全策略模型和安全功能规约之间的对应性时，应说明所有安全功能规约中的安全功能与安全策略模型是一致的、是完备的。当安全功能规约是半形式化时，阐明安全策略模型与安全功能规约之间的对应性时也应半形式化；如果安全功能规约是形式化的，则阐明安全策略模型与安全功能规约之间的对应性也应形式化。

5.5.12.2 **功能规约**

开发者应提供防火墙的安全功能规约。

安全功能规约应以**形式化风格**来描述安全功能与其外部接口，在需要时，可用非形式化、解释性的文字来支持安全功能规约的描述。安全功能规约还应描述使用外部安全功能接口的目的与方法，在需要的时候，应提供例外情况和错误信息的细节。

安全功能规约应是内在一致的，能完备地表示安全功能，并提供安全基本原理证明安全功能的表示是完备的。

5.5.12.3 **高层设计**

开发者应提供防火墙安全功能的高层设计。

高层设计应以**形式化方法**表述并且是内在一致的。为说明安全功能的结构，高层设计应将安全功能分解为各个安全功能子系统进行描述，并阐明如何将有助于加强防火墙安全功能的子系统和其他子系统分开。**高层设计应证明所标识的分离方法，包括任何保护机制，足以确保将加强的非安全功能与加强的安全功能清晰而有效地分离出来。**对于每一个安全功能子系统，高层设计应描述其提供的安全功能，标识其所有接口以及哪些接口是外部可见的，描述其所有接口的使用目的与方法，并提供安全功能子系统所有的作用、例外情况和错误信息的完整细节。高层设计还应标识安全功能要求的所有基础性的硬件、固件和软件，支持由这些硬件、固件或软件所实现的保护机制，**并证明安全功能机制足以实现在高层设计中标识的安全功能。**

5.5.12.4 **低层设计**

开发者应提供安全策略的低层设计。

低层设计应是**形式化**、内在一致的。在描述防火墙安全功能时，低层设计应采用模块术语，说明每一个安全功能模块的目的，并标识安全功能模块的所有接口和安全功能模块可为外部所见的接口，以及安全功能模块所有接口的目的与方法，适当时，还应提供接口所有的作用、例外情况和错误信息的完整细节。

低层设计还需要包括以下内容：

a) 以安全功能性术语及模块的依赖性术语，定义模块间的相互关系；

b) 说明如何提供每一个安全策略的强化功能；

c) 说明如何将防火墙加强安全策略的模块和其他模块分离开。

5.5.12.5 **模块化**

开发者在设计和构建防火墙安全功能时，应以如下方式进行：

a) 模块方式，避免设计模块之间出现不必要的交互作用；

b) 分层的方式，使得设计层次之间的交互作用最小化；

c) 安全功能部分复杂度最小化的方式，使得访问控制和信息流控制策略简单到足以分析。

开发者还应提供结构化描述并确认那些与安全无关的功能已从安全功能中排除出去。

结构化描述应标识所有的防火墙安全功能模块以及描述每一个安全功能模块的目的、接口、参数和影响，**并指明安全功能的哪些部分是加强访问控制和信息流控制策略的。结构化描述还应阐明如下内容：**

a) 安全功能设计是如何避免各模块之间不必要的交互作用的；

b) 分层结构以及分层结构如何使交互作用最小化；

c) 加强访问控制和信息流控制策略的安全功能部分是如何构建的以及是如何使其复杂性降为最低。

5.5.12.6 安全功能的实现

开发者应为全部防火墙安全功能提供实现表示。

实现表示应无歧义而且详细地定义全部防火墙安全功能，使得不需要进一步的设计就能生成安全功能。实现表示应是内在一致的并能描述实现各部分之间的关系。

5.5.12.7 表示对应性

开发者应在防火墙安全功能表示的所有相邻对之间提供对应性分析。对于那些形式化的安全功能表示的相邻对，开发者应严格证明其对应性。

对于防火墙安全功能表示的每个相邻对，分析应阐明：较为抽象的安全功能表示的所有相关安全功能，应在较具体的安全功能表示中得到正确而完备地细化。并且如果某个相邻对的各部分都至少是半形式化的，则相应的对应性阐明也应是半形式化的；如果某个相邻对的各部分都是形式化的，则相应的对应性阐明也应是形式化的。

5.5.13 测试

5.5.13.1 功能测试

开发者应测试安全功能，将结果文档化并提供测试文档。

测试文档应包括测试计划、测试过程、预期的测试结果和实际测试结果。测试计划应标识要测试的安全功能，并描述测试的目标。测试过程应标识要执行的测试，并描述每个安全功能的测试概况，这些概况包括对其他测试结果的顺序依赖性以及对顺序依赖性的分析。期望的测试结果应表明测试成功后的预期输出。实际测试结果应表明每个被测试的安全功能能按照规定进行运作。

5.5.13.2 覆盖分析

开发者应提供测试覆盖的分析结果。

测试覆盖的分析结果应表明测试文档中所标识的测试与安全功能规约中所描述的安全功能是对应的，且该对应是完备的。对于安全功能规约所标识的安全功能的所有外部接口，测试覆盖的分析应严格地阐明这些外部接口已经被完备测试过了。

5.5.13.3 深度

开发者应提供测试深度的分析。

在深度分析中，应说明测试文档中所标识的对安全功能的测试，足以表明该安全功能是根据高层设计、低层设计以及实现表示而运作的。

5.5.13.4 独立性测试

开发者应提供证据证明，开发者提供的防火墙经过独立的第三方测试并通过。

5.5.14 指导性文档

5.5.14.1 管理员指南

开发者应提供系统管理员使用的管理员指南。

管理员指南应说明以下内容：

a) 防火墙管理员可以使用的管理功能和接口；

b) 怎样安全地管理防火墙；

c) 在安全处理环境中应进行控制的功能和权限；

d) 所有对与防火墙的安全操作有关的用户行为的假设；

e) 所有受管理员控制的安全参数，如果可能，应指明安全值；

f) 每一种与管理功能有关的安全相关事件，包括对安全功能所控制的实体的安全特性进行的改变；

g) 所有与系统管理员有关的 IT 环境的安全要求。

管理员指南应与为评估而提供的其他所有文件保持一致。

5.5.14.2 **用户指南**

开发者应提供用户指南。

用户指南应说明以下内容：

a) 防火墙的非管理用户可使用的安全功能和接口；

b) 防火墙提供给用户的安全功能和接口的用法；

c) 用户可获取但应受安全处理环境控制的所有功能和权限；

d) 防火墙安全操作中用户所应承担的职责；

e) 与用户有关的 IT 环境的所有安全要求。

用户指南应与为评估而提供的其他所有文件保持一致。

5.5.15 **脆弱性分析**

5.5.15.1 **隐蔽通道分析**

开发者应对每个信息流控制策略都搜索隐蔽通道并提供隐蔽通道分析的文档。

分析文档应包括以下内容：

a) 标识隐蔽通道并且估计它们的容量；

b) 描述用于确定隐蔽通道存在的程序，以及进行隐蔽通道分析所需要的信息；

c) 描述在进行隐蔽通道分析期间所作的全部假设；

d) 描述在最坏的情况下，对通道容量进行估计的方法；

e) 为每个可标识的隐蔽通道描述其最坏的利用情形；

f) **阐明用于标识隐蔽通道的方法是系统化的。**

5.5.15.2 **分析确认**

开发者应提供指南性文档并将其文档化。

在指南性文档中，应确定对防火墙的所有可能的操作方式(包括失败和操作失误后的操作)、它们的后果以及对于保持安全操作的意义。指南性文档中还应列出所有目标环境的假设以及所有外部安全措施(包括外部程序的、物理的或人员的控制)的要求。指南性文档应是完备的、清晰的、一致的、合理的。在分析文档中，应阐明指南性文档是完备的。

5.5.15.3 **脆弱性分析**

开发者应从用户可能破坏安全策略的明显途径出发，对防火墙的各种功能进行分析并提供文档。对被确定的脆弱性，开发者应明确记录采取的措施。

对每一条脆弱性，应有证据显示在使用防火墙的环境中该脆弱性不能被利用。在文档中，还需证明经过标识脆弱性的防火墙可以抵御穿透性攻击，并说明对脆弱性的搜索是系统化的。**对于防火墙所提供的证明，文档中要给出完备的分析。**

5.5.16 **交付与运行**

5.5.16.1 **交付**

开发者应使用一定的交付程序交付防火墙，并以文档的形式将交付程序提供给用户。

交付文档应包括以下内容：

a) 在给用户方交付防火墙的各版本时，为维护安全所必需的所有程序；

b) 开发者的向用户提供的防火墙版本和用户收到的版本之间的差异以及如何监测对防火墙的修改；

c) 如何发现他人伪装成开发者修改用户的防火墙。

5.5.16.2 **安装生成**

开发者应提供文档说明防火墙的安装、生成和启动的过程。

附 录 A
（资料性附录）
防火墙面临的威胁和对策

A.1 防火墙可能面对的主要威胁

a) 一个外部主机可能通过假冒成另一个主机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。这是针对内部网络安全的威胁；

b) 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；

c) 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。这是针对防火墙自身安全的威胁；

d) 对防火墙配置和其他与安全有关数据的更改，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。这些攻击是针对防火墙自身安全的威胁；

e) 攻击者企图绕过或欺骗标识和鉴别机制，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（例如：口令字）、截取会话连接等攻击；

f) 攻击者试图通过重复猜测鉴别数据，以使用该鉴别数据发起对防火墙本身或防火墙保护的子网的攻击；

g) 攻击者利用其他已授权用户或授权管理员遗留的有效身份和鉴别数据，假冒该用户或管理员访问防火墙或防火墙保护的内部网。

A.2 防火墙可采用降低威胁的方法

a) 访问仲裁。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；

b) 管理员访问。仅限授权的管理员才能访问防火墙，即仅允许他们有配置防火墙的能力；

c) 个体身份标识。个体身份标识提供对用户的标识能力，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；

d) 防火墙的自保护。防火墙应把正在处理的数据与需要运算的数据分开，应保护自己不受攻击。此外，防火墙还应能保护授权管理员的通信会话连接；

e) 审计。对于判定是否存在绕过安全功能策略尝试，是否因配置错误而不自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；

f) 防止鉴别数据重用。防火墙应防止网络用户及授权管理员的鉴别数据重用；

g) 安全启动和恢复。当防火墙启动或从一次中断恢复时，不能影响到它自身或和它相联接的网络的资源；

h) 会话加密。如果防火墙允许授权管理员从与防火墙互连的网络上远程登录访问防火墙，则防火墙应通过加密技术保护防火墙与授权管理员的会话。

参 考 文 献

[1] GB/T 18019—1999 信息技术 包过滤防火墙安全技术要求

[2] ISO/IEC 15408：1999（所有部分） Common Criteria for Information Technology Security Evaluation