ICS 35.040
L 80

中华人民共和国国家标准

GB/T 20281—2006

信息安全技术
防火墙技术要求和测试评价方法

**Information security technology—
Technique requirements and testing and evaluation approaches for firewall products**

2006-05-31 发布　　2006-12-01 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

中华人民共和国
国家标准
信息安全技术
防火墙技术要求和测试评价方法
GB/T 20281—2006
*
中国标准出版社出版发行
北京复兴门外三里河北街16号
邮政编码:100045
网址 www.bzcbs.com
电话:68523946 68517548
中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销
*
开本 880×1230 1/16 印张 2.25 字数 60 千字
2006年11月第一版 2006年11月第一次印刷
*
书号:155066·1-28270 定价 17.00 元

GB/T 20281-2006

前　言

本标准的附录A为资料性附录。

本标准由全国信息安全标准化技术委员会提出并归口。

本标准由解放军信息安全测评认证中心、北京中科网威信息技术有限公司负责起草。

本标准主要起草人：李京春、钟力、郑传波、付志峰、锁延锋、桂坚勇、陆驿。

目　次

信息安全技术
防火墙技术要求和测试评价方法

1 范围

本标准规定了采用“传输控制协议/网际协议(TCP/IP)”的防火墙类信息安全产品的技术要求和测试评价方法。

本标准适用于采用“传输控制协议/网际协议(TCP/IP)”的防火墙类信息安全产品的研制、生产、测试和评估。

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。凡不注日期的引用文件，其最新版本适用于本标准。

GB/T 5271.8 信息技术 词汇 第8部分：安全(GB/T 5271.8—2001，idt ISO/IEC 2382-8：1998)

GB 17859 计算机信息系统安全保护等级划分准则

GB/T 18336.3 信息技术 安全技术 信息技术安全性评估准则 第3部分：安全保证要求(GB/T 18336.3—2001，idt ISO/IEC 15408-3：1999)

3 术语和定义

GB/T 5271.8、GB 17859 和 GB/T 18336.3 确立的以及下列术语和定义适用于本标准。

3.1

防火墙 firewall

一个或一组在不同安全策略的网络或安全域之间实施访问控制的系统。

3.2

内部网络 internal network

通过防火墙隔离的可信任区域或保护区域，通常是指单位内部的局域网。

3.3

外部网络 external network

通过防火墙隔离的不可信任区域或非保护区域。

3.4

非军事区 demilitary zone

一个网络对外提供网络服务的部分，受防火墙保护，通过防火墙与内部网络和外部网络隔离，执行与内部网络不同的安全策略，也有的称为安全服务网络(secure service network)。

3.5

安全策略 security policy

有关管理、保护和发布敏感信息的法律、规定和实施细则。

3.6

授权管理员 authorized administrator

具有防火墙管理权限的用户，负责对防火墙的系统配置、安全策略、审计日志等进行管理。

3.7

可信主机　trusted host

赋予权限能够管理防火墙的主机。

3.8

主机　host

一台与防火墙相互作用的机器，它在防火墙安全策略的控制下进行通信。

3.9

用户　user

一个在防火墙安全策略的控制下，通过防火墙访问防火墙的某一个区域的人，此人不具有能影响防火墙安全策略执行的权限。

3.10

吞吐量　throughput

防火墙在不丢包情况下转发数据的能力，一般以所能达到线速的百分比(或称通过速率)来表示。

3.11

延迟　delay

数据帧的最后一个位的末尾到达防火墙内部网络输入端口至数据帧的第一个位的首部到达防火墙外部网络输出端口之间的时间间隔。

3.12

TCP 最大并发连接数　maximum concurrent TCP connection capacity

防火墙所能保持的最大 TCP 并发连接数量。

3.13

TCP 最大连接速率　maximum TCP connection establishment rate

防火墙在单位时间内所能建立的最大 TCP 连接数，一般是每秒的连接数。

4　符号和缩略语

DMZ	非军事区	Demilitary Zone
DNAT	目的网络地址转换	Destination NAT
DNS	域名系统	Domain Name System
FTP	文件传输协议	File Transfer Protocol
HTTP	超文本传输协议	Hypertext Transfer Protocol
ICMP	网间控制报文协议	Internet Control Messages Protocol
IDS	入侵检测系统	Intrusion Detection System
IP	网际协议	Internet Protocol
NAT	网络地址转换	Network Address Translation
POP3	邮局协议 3	Post Office Protocol 3
PBR	策略路由	Policy-based Routing
SMTP	简单邮件传送协议	Simple Mail Transfer Protocol
SNAT	源网络地址转换	Source NAT
SSN	安全服务网络	Secure Service Network
STP	生成树协议	Spanning Tree Protocol
TCP	传输控制协议	Transport Control Protocol
UDP	用户数据报协议	User Datagram Protocol
URL	统一资源定位器	Uniform Resource Locator

USB	通用串行总线	Universal Serial Bus
VLAN	虚拟局域网	Virtual Local Area Network
VPN	虚拟专用网	Virtual Private Network
VRRP	虚拟路由器冗余协议	Virtual Router Redundancy Protocol

5 技术要求

5.1 总体说明

5.1.1 技术要求分类

本标准将防火墙通用技术要求分为功能、性能、安全和保证要求四个大类。其中，功能要求是对防火墙产品应具备的安全功能提出具体的要求，包括包过滤、应用代理、内容过滤、安全审计和安全管理等；性能要求对防火墙产品应达到的性能指标作出规定，例如吞吐量、延迟、最大并发连接数和最大连接速率；安全要求是对防火墙自身安全和防护能力提出具体的要求，例如抵御各种网络攻击；保证要求则针对防火墙开发者和防火墙自身提出具体的要求，例如管理配置、交付与操作、指南文件等。

5.1.2 安全等级

本标准依据 GB 17859 和 GB/T 18336.3，并根据国内测评认证机构、测评技术和我国防火墙产品开发现状，对防火墙产品进行安全等级划分。安全等级分为一级、二级、三级三个逐级提高的级别，功能强弱、安全强度和保证要求高低是等级划分的具体依据。安全等级突出安全特性，性能高低不作为等级划分依据。

5.2 功能要求

5.2.1 一级产品功能要求

5.2.1.1 功能要求列表

一级产品的功能要求由表 1 所列项目组成。

表 1 一级产品功能要求细目

功能分类	功能项目要求
包过滤	支持默认禁止原则
	支持基于 IP 地址的访问控制
	支持基于端口的访问控制
	支持基于协议类型的访问控制
应用代理	支持应用层协议代理
NAT	支持双向 NAT
流量统计	支持根据 IP 地址、协议、时间等参数对流量进行统计
	支持统计结果的报表形式输出
安全审计	支持记录来自外部网络的被安全策略允许的访问请求
	支持记录来自内部网络和 DMZ 的被安全策略允许的访问请求
	支持记录任何试图穿越或到达防火墙的违反安全策略的访问请求
	支持记录防火墙管理行为
	审计记录内容
	支持日志的访问授权
	支持日志的管理
	提供日志管理工具

表 1（续）

功能分类	功能项目要求
管理	支持对授权管理员的口令鉴别方式
	支持对授权管理员、可信主机、主机和用户进行身份鉴别
	支持本地和远程管理
	支持设置和修改安全管理相关的数据参数
	支持设置、查询和修改安全策略
	支持管理审计日志

5.2.1.2 **包过滤**

防火墙应具备包过滤功能，具体技术要求如下：

a) 防火墙的安全策略应使用最小安全原则，即除非明确允许，否则就禁止；

b) 防火墙的安全策略应包含基于源 IP 地址、目的 IP 地址的访问控制；

c) 防火墙的安全策略应包含基于源端口、目的端口的访问控制；

d) 防火墙的安全策略应包含基于协议类型的访问控制。

5.2.1.3 **应用代理**

应用代理型和复合型防火墙应具备应用代理功能，且应至少支持 HTTP、FTP、TELNET、POP3 和 SMTP 等协议的应用代理。

5.2.1.4 **NAT**

包过滤型和复合型防火墙应具备 NAT 功能，具体技术要求如下：

a) 防火墙应支持双向 NAT：SNAT 和 DNAT；

b) SNAT 应至少可实现“多对一”地址转换，使得内部网络主机正常访问外部网络时，其源 IP 地址被转换；

c) DNAT 应至少可实现“一对多”地址转换，将 DMZ 的 IP 地址映射为外部网络合法 IP 地址，使外部网络主机通过访问映射地址实现对 DMZ 服务器的访问。

5.2.1.5 **流量统计**

防火墙应具备流量统计功能，具体技术要求如下：

a) 防火墙应能够通过 IP 地址、网络服务、时间和协议类型等参数或它们的组合进行流量统计；

b) 防火墙应能够实时或者以报表形式输出流量统计结果。

5.2.1.6 **安全审计**

防火墙应具备安全审计功能，具体技术要求如下：

a) 记录事件类型

1) 被防火墙策略允许的从外部网络访问内部网络、DMZ 和防火墙自身的访问请求；

2) 被防火墙策略允许的从内部网络和 DMZ 访问外部网络服务的访问请求；

3) 从内部网络、外部网络和 DMZ 发起的试图穿越或到达防火墙的违反安全策略的访问请求；

4) 试图登录防火墙管理端口和管理身份鉴别请求。

b) 日志内容

1) 数据包发生的时间，日期必须包括年、月、日，时间必须包括时、分、秒；

2) 数据包的协议类型、源地址、目标地址、源端口和目标端口等。

c) 日志管理

1) 防火墙应只允许授权管理员访问日志；

2） 防火墙管理员应支持对日志存档、删除和清空的权限；

3） 防火墙应提供能查阅日志的工具，并且只允许授权管理员使用查阅工具；

4） 防火墙应提供对审计事件一定的检索和排序的能力，包括对审计事件以时间、日期、主体ID、客体ID等排序的功能。

5.2.1.7 管理

防火墙应具备管理功能，具体技术要求如下：

a） 管理安全

1） 支持对授权管理员的口令鉴别方式，且口令设置满足安全要求；

2） 防火墙应在所有授权管理员、可信主机、主机和用户请求执行任何操作之前，对每个授权管理员、可信主机、主机和用户进行惟一的身份识别。

b） 管理方式

1） 防火墙应支持通过console端口进行本地管理；

2） 防火墙应支持通过网络接口进行远程管理。

c） 管理能力

1） 防火墙向授权管理员提供设置和修改安全管理相关的数据参数的功能；

2） 防火墙向授权管理员提供设置、查询和修改各种安全策略的功能；

3） 防火墙向授权管理员提供管理审计日志的功能。

5.2.2 二级产品功能要求

5.2.2.1 功能要求列表

二级产品除需满足一级产品的功能要求外，还需增加如表2所示的功能要求。

表2 二级产品增加的功能要求细目

功能分类	功能项目要求
包过滤	支持基于MAC地址的访问控制
	支持基于时间的访问控制
	支持基于用户自定义安全策略的访问控制
状态检测	支持基于状态检测技术的访问控制
深度包检测	支持基于URL的访问控制
	支持基于电子邮件信头的访问控制
应用代理	支持应用层协议代理
NAT	支持动态NAT
IP/MAC地址绑定	支持IP/MAC地址绑定
	支持检测IP地址盗用
动态开放端口	支持FTP的动态端口开放
策略路由	支持根据数据包信息来设置路由策略
	支持设置多个路由表
带宽管理	支持客户端占用带宽大小限制
双机热备	支持物理设备状态检测
	支持VRRP和STP协议
负载均衡	支持将网络负载均衡到多台服务器

表 2（续）

功能分类	功能项目要求
安全审计	支持记录对防火墙系统自身的操作
	支持记录在防火墙管理端口上的认证请求
	支持对日志事件和防火墙所采取的相应措施的描述
	支持日志记录存储和备份的安全
	支持日志管理工具管理日志
	支持日志的统计分析和报表生成
	支持日志的集中管理
管　理	支持智能卡、USB 钥匙等身份鉴别信息载体
	支持鉴别失败处理
	支持授权管理员、可信主机、主机和用户的惟一安全属性
	支持远程管理安全
	支持防火墙状态和网络数据流状态监控

5.2.2.2　**包过滤**

防火墙应具备包过滤功能，具体技术要求如下：

a）　防火墙的安全策略可包含基于 MAC 地址的访问控制；

b）　防火墙的安全策略可包含基于时间的访问控制；

c）　防火墙应支持用户自定义的安全策略，安全策略可以是 MAC 地址、IP 地址、端口、协议类型和时间的部分或全部组合。

5.2.2.3　**状态检测**

防火墙应具备状态检测功能。

5.2.2.4　**深度包检测**

防火墙应具备深度包检测功能，具体技术要求如下：

a）　防火墙的安全策略应包含基于 URL 的访问控制；

b）　防火墙的安全策略应包含基于电子邮件中的 Subject、To、From 域等进行的访问控制。

5.2.2.5　**应用代理**

应用代理型和复合型防火墙应具备 DNS 协议的应用代理。

5.2.2.6　**NAT**

包过滤型和复合型防火墙应具备 NAT 功能，具体技术要求如下：

a）　防火墙应支持动态 SNAT 技术，实现“多对多”的 SNAT；

b）　防火墙应支持动态 DNAT 技术，实现“多对多”的 DNAT。

5.2.2.7　**IP/MAC 地址绑定**

防火墙应具备 IP/MAC 地址绑定功能，具体技术要求如下：

a）　防火墙应支持自动或管理员手工绑定 IP/MAC 地址；

b）　防火墙应能够检测 IP 地址盗用，拦截盗用 IP 地址的主机经过防火墙的各种访问。

5.2.2.8　**动态开放端口**

防火墙应具备动态开放端口功能，支持主动模式和被动模式的 FTP。

5.2.2.9 策略路由

具有多个相同属性网络接口(多个外部网络接口、多个内部网络接口或多个 DMZ 网络接口)的防火墙应具备策略路由功能,具体技术要求如下:

a) 防火墙应能够根据数据包源目的地址、进入接口、传输层接口或数据包负载内容等参数来设置路由策略;

b) 防火墙应能够设置多个路由表,且每个路由表能包含多条路由信息。

5.2.2.10 带宽管理

防火墙应具备带宽管理功能,能够根据安全策略中管理员设定的大小限制客户端占用的带宽。

5.2.2.11 双机热备

防火墙应具备双机热备功能,具体技术要求如下:

a) 防火墙应支持物理设备状态检测。当主防火墙自身出现断电或其他故障时,备防火墙应及时发现并接管主防火墙进行工作。

b) 在路由模式下,防火墙可支持 VRRP 协议。

c) 在透明模式下,防火墙可支持 STP 协议。

5.2.2.12 负载均衡

防火墙应具备负载均衡功能,能够根据安全策略将网络流量均衡到多台服务器上。

5.2.2.13 安全审计

防火墙应具备安全审计功能,具体技术要求如下:

a) 记录事件类型

1) 每次重新启动,包括防火墙系统自身的启动和安全策略重新启动;

2) 所有对防火墙系统时钟的手动修改操作。

b) 日志内容

1) 指明在管理端口上的认证请求是成功还是失败,若认证请求失败必须记录失败的原因;

2) 对日志事件和防火墙采取的相应措施进行详细的描述。

c) 日志管理

1) 防火墙应支持把日志存储和备份在一个安全、永久性的地方;

2) 防火墙应支持只能使用日志管理工具管理日志;

3) 防火墙应支持对日志的统计分析和生成报表的功能;

4) 日志应该可以发送到日志服务器上集中管理。

5.2.2.14 管理

防火墙应具备安全管理功能,具体技术要求如下:

a) 应支持智能卡、USB 钥匙等身份鉴别信息载体;

b) 身份鉴别在经过一个可设定的鉴别失败最大次数后,防火墙应终止可信主机或用户建立会话的过程;

c) 防火墙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惟一的为执行安全策略所必需的安全属性;

d) 远程管理过程中,管理端与防火墙之间的所有通讯应加密确保安全;

e) 防火墙向授权管理员提供监控防火墙状态和网络数据流状态的功能。

5.2.3 三级产品功能要求

5.2.3.1 功能要求列表

三级产品除需满足一、二级产品的功能要求外,还需增加如表 3 所示的功能要求。

表 3　三级产品增加的功能要求细目

功能分类	功能项目要求
深度包检测	支持基于文件类型的访问控制
	支持基于用户的访问控制
	支持基于关键字的访问控制
应用代理	支持透明应用代理
动态开放端口	支持以 H.323 协议建立视频会议
	支持 SQL * NET 数据库协议
	支持 VLAN
带宽管理	支持动态客户端带宽管理
双机热备	支持链路状态检测的双机热备
负载均衡	支持集群工作模式的负载均衡
VPN	支持 IPSec 协议
	支持建立“防火墙至防火墙”和“防火墙至客户机”两种形式的 VPN
	支持 VPN 认证
	加密算法和验证算法符合国家密码管理的有关规定
协同联动	支持与其他安全产品的协同联动
	支持联动安全产品的身份鉴别
安全审计	支持记录协同联动响应行为事件
	支持日志存储耗尽处理机制
管　理	支持生物特征鉴别方式
	支持管理员权限划分

5.2.3.2　深度包检测

防火墙应具备深度包检测功能，具体技术要求如下：

a)　防火墙的安全策略应包含基于文件类型的访问控制；

b)　防火墙的安全策略应包含基于用户的访问控制；

c)　防火墙的安全策略可包含基于关键字的访问控制，对 HTTP 网页数据和电子邮件正文数据进行检查。

5.2.3.3　应用代理

应用代理型和复合型防火墙应具备透明应用代理功能，支持 HTTP、FTP、TELNET、SMTP、POP3 和 DNS 等协议。

5.2.3.4　动态开放端口

防火墙应具备动态开放端口功能，具体技术要求如下：

a)　防火墙应支持以 H.323 协议建立视频会议；

b)　防火墙应支持 SQL * NET 数据库协议；

c)　防火墙应支持 VLAN 协议。

5.2.3.5　带宽管理

防火墙应具备带宽管理功能，能够根据安全策略和网络流量动态调整客户端占用的带宽。

5.2.3.6　双机热备

防火墙应具备基于链路状态检测的双机热备功能，当主防火墙直接相连的链路发生故障而无法正

常工作时，备防火墙应及时发现并接管主防火墙进行工作。

5.2.3.7 负载均衡

防火墙应具备基于集群工作模式的负载均衡功能，使得多台防火墙能够协同工作均衡网络流量。

5.2.3.8 VPN

防火墙可具备 VPN 功能，具体技术要求如下：

a) 防火墙应支持以 IPSec 协议为基础构建 VPN；

b) 防火墙应支持建立“防火墙至防火墙”和“防火墙至客户机”两种形式的 VPN；

c) 防火墙应支持预共享密钥和 X.509 数字证书两种认证方式来进行 VPN 认证；

d) 防火墙所使用的加密算法和验证算法应符合国家密码管理的有关规定。

5.2.3.9 协同联动

防火墙应具备与其他安全产品的协同联动功能(例如与 IDS)，具体技术要求如下：

a) 防火墙应按照一定的安全协议与其他安全产品协同联动，并支持手工与自动方式来配置联动策略；

b) 防火墙应在协同联动前对与其联动的安全产品进行身份鉴别。

5.2.3.10 安全审计

防火墙应具备安全审计功能，具体技术要求如下：

a) 防火墙应记录协同联动响应行为事件；

b) 防火墙日志存储耗尽，防火墙应能采取相应的安全措施，包括向管理员报警、基于策略的最早产生的日志删除和系统工作停止。

5.2.3.11 管理

防火墙应具备管理功能，具体要求如下：

a) 支持指纹、虹膜等生物特征鉴别方式的管理员身份鉴别；

b) 防火墙应支持管理员权限划分，至少需分为两个部分，可将防火墙管理、安全策略管理或审计日志管理权限分割。

5.3 性能要求

5.3.1 吞吐量

防火墙的吞吐量视不同速率的防火墙有所不同，具体指标要求如下。

a) 防火墙在只有一条允许规则和不丢包的情况下，应达到的吞吐量指标：

1) 对 64 字节短包，十兆和百兆防火墙应不小于线速的 20%，千兆及千兆以上防火墙应不小于线速的 35%；

2) 对 512 字节中长包，十兆和百兆防火墙应不小于线速的 70%，千兆及千兆以上防火墙应不小于线速的 80%；

3) 对 1 518 字节长包，十兆和百兆防火墙应不小于线速的 90%，千兆及千兆以上防火墙应不小于线速的 95%。

b) 在添加大数量访问控制规则(不同的 200 余条)的情况下，防火墙的吞吐量下降应不大于原吞吐量的 3%。

5.3.2 延迟

防火墙的延迟视不同速率的防火墙有所不同，具体指标要求如下：

a) 十兆防火墙的最大延迟不应超过 1 ms；

b) 百兆防火墙的最大延迟不应超过 500 μs；

c) 千兆及千兆以上防火墙的最大延迟不应超过 90 μs；

d) 在添加大数量访问控制规则(不同的 200 余条)的情况下，防火墙延迟所受的影响应不大于原来的 3%。

5.3.3 最大并发连接数

最大并发连接数视不同速率的防火墙有所不同，具体指标要求如下：

a) 十兆防火墙的最大并发连接数应不小于 1 000 个；

b) 百兆防火墙的最大并发连接数应不小于 10 000 个；

c) 千兆及千兆以上防火墙的最大并发连接数应不小于 100 000 个。

5.3.4 最大连接速率

最大连接速率视不同速率的防火墙有所不同，具体技术要求如下：

a) 十兆防火墙的最大连接速率应不小于每秒 500 个；

b) 百兆防火墙的最大连接速率应不小于每秒 1 500 个；

c) 千兆及千兆以上防火墙的最大连接速率应不小于每秒 5 000 个。

5.4 安全要求

5.4.1 一级产品安全要求

5.4.1.1 安全要求列表

一级产品的安全要求由表 1 所列项目组成。

表 4 一级产品安全要求细目

安全分类	安全要求
抗渗透	抵御各种基本的拒绝服务攻击
	检测和记录端口扫描行为
	抵御源 IP 地址欺骗攻击
	抵御 IP 碎片包攻击
恶意代码防御	拦截典型木马攻击行为
支撑系统	支撑系统不提供多余的网络服务
	支撑系统应不含任何高、中风险安全漏洞
非正常关机	安全策略恢复到关机前的状态
	日志信息不会丢失
	管理员重新认证

5.4.1.2 抗渗透

防火墙具备一定的抗攻击渗透能力，具体技术要求如下：

a) 能够抵御 Syn Flood、Ping of Death 和 UDP Flood 等基本的拒绝服务攻击，保护自身并防止受保护网络受到攻击；

b) 能够检测和记录端口扫描行为；

c) 能够抵御源 IP 地址欺骗攻击；

d) 能够抵御 IP 碎片包攻击。

5.4.1.3 恶意代码防御

防火墙应具备基本的恶意代码防御能力，能够拦截典型的木马攻击行为。

5.4.1.4 支撑系统

防火墙的底层支撑系统应满足如下技术要求：

a) 确保其支撑系统不提供多余的网络服务；

b) 不含任何导致防火墙权限丢失、拒绝服务和敏感信息泄露的安全漏洞。

5.4.1.5 非正常关机

防火墙在非正常条件（比如掉电、强行关机）关机再重新启动后，应满足如下技术要求：

a) 安全策略恢复到关机前的状态；

b) 日志信息不会丢失；

c) 管理员重新认证。

5.4.2 二级产品安全要求

5.4.2.1 安全要求列表

二级产品除需满足一级产品的安全要求外，还需增加如表5所示的安全要求。

表5 二级产品增加的安全要求细目

安全分类	安全要求
抗渗透	抵御各种典型的拒绝服务攻击
	检测和记录漏洞扫描行为
	拦截典型邮件炸弹工具发送的垃圾邮件
恶意代码防御	检测并拦截激活的蠕虫、木马、间谍软件等恶意代码的行为
支撑系统	构建于安全增强的操作系统之上

5.4.2.2 抗渗透

防火墙应具备较强的抗攻击渗透能力，具体技术要求如下：

a) 能够抵御各种典型的拒绝服务攻击和分布式拒绝服务攻击，保护自身并防止受保护网络遭受攻击；

b) 能够检测和记录漏洞扫描行为，包括对受保护网络的扫描；

c) 拦截典型邮件炸弹工具发送的垃圾邮件。

5.4.2.3 恶意代码防御

防火墙应具备较强的恶意代码防御能力，能够检测并拦截激活的蠕虫、木马、间谍软件等恶意代码的操作行为。

5.4.2.4 支撑系统

防火墙的支撑系统应构建于安全增强的操作系统之上。

5.4.3 三级产品安全要求

5.4.3.1 安全要求列表

三级产品除需满足一、二级产品的安全要求外，还需增加如表6所示的安全要求。

表6 三级产品增加的安全要求细目

安全分类	安全要求
抗渗透	能够抵御网络扫描行为，不返回扫描信息
	支持黑名单或特征匹配等方式的垃圾邮件拦截策略配置
恶意代码防御	检测并拦截被HTTP网页和电子邮件携带的恶意代码
	恶意代码检测告警
支撑系统	构建于安全操作系统之上

5.4.3.2 抗渗透

防火墙应具备很强的抗攻击渗透能力，具体技术要求如下：

a) 能够抵御网络扫描行为，不返回扫描信息；

b) 支持黑名单或特征匹配等方式的垃圾邮件拦截策略配置。

5.4.3.3 恶意代码防御

防火墙应具备很强的恶意代码防御能力，具体技术要求如下：

a) 检测并拦截被 HTTP 网页和电子邮件携带的恶意代码；

b) 发现恶意代码后及时向防火墙控制台告警；

c) 至少每月升级一次，支持在线和离线升级。

5.4.3.4 支撑系统

防火墙的支撑系统可构建于安全操作系统之上。

5.5 保证要求

5.5.1 说明

保证要求采用增量描述方法。通常，二级产品的保证要求应包括一级产品的保证要求，三级产品的保证要求应包括一级和二级产品的保证要求；在某些项目，高等级产品的保证要求比低等级产品的保证要求更为严格，则不存在增量的关系。

5.5.2 一级产品保证要求

5.5.2.1 配置管理

配置管理应满足如下要求：

a) 开发者应为防火墙产品的不同版本提供惟一的标识；

b) 开发者应针对不同用户提供惟一的授权标识；

c) 配置项应有惟一的标识。

5.5.2.2 交付与运行

交付与运行应满足如下要求：

a) 评估者应审查开发者是否提供了文档说明防火墙的安装、生成、启动和使用的过程。用户能够通过此文档了解安装、生成、启动和使用过程。

b) 防火墙运行稳定。

c) 对错误输入的参数，不应导致防火墙出现异常，且给出提示信息。

5.5.2.3 安全功能开发过程

5.5.2.3.1 功能设计

功能设计应满足如下要求：

a) 功能设计应当使用非形式化风格来描述防火墙安全功能与其外部接口；

b) 功能设计应当是内在一致的；

c) 功能设计应当描述使用所有外部防火墙安全功能接口的目的与方法，适当的时候，要提供结果影响例外情况和错误信息的细节；

d) 功能设计应当完整地表示防火墙安全功能；

e) 功能设计应是防火墙安全功能要求的精确和完整的示例。

5.5.2.3.2 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，具体要求如下：

a) 防火墙各种安全功能表示(如防火墙功能设计、高层设计、低层设计、实现表示)之间的对应性是所提供的抽象防火墙安全功能表示要求的精确而完整的示例；

b) 防火墙安全功能在功能设计中进行细化，抽象防火墙安全功能表示的所有相关安全功能部分，在具体防火墙安全功能表示中应进行细化。

5.5.2.4 指导性文档

5.5.2.4.1 管理员指南

开发者应提供供系统管理员使用的管理员指南，该指南应包括如下内容：

a) 防火墙可以使用的管理功能和接口；

b) 怎样安全地管理防火墙；

c) 对一致、有效地使用安全功能提供指导；