ICS 35.040
A 90

GA

中华人民共和国公共安全行业标准

GA/T 1177—2014

信息安全技术
第二代防火墙安全技术要求

Information security technology—Security technique requirements for the second generation firewall products

2014-07-24 发布　　2014-09-01 实施

中华人民共和国公安部　　发布

目　　次

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准由公安部网络安全保卫局提出。

本标准由公安部信息系统安全标准化技术委员会提出并归口。

本标准起草单位：公安部计算机信息系统安全产品质量监督检验中心、深圳市深信服电子科技有限公司、网神信息技术（北京）股份有限公司、北京神州绿盟信息安全科技股份有限公司、网御星云信息技术有限公司、启明星辰信息技术有限公司。

本标准主要起草人：邹春明、俞优、宋好好、陆臻、顾健、李焕波、王帆、王刚、段继平、冯涛、黄涛。

信息安全技术
第二代防火墙安全技术要求

1 范围

本标准规定了第二代防火墙产品的安全功能要求、安全保证要求、环境适应性要求、性能要求和安全等级划分。

本标准适用于第二代防火墙产品的设计、开发和测试。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本(包括所有的修改单)适用于本文件。

GB 17859—1999 计算机信息系统安全保护划分准则

GB/T 18336.3—2008 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 20281—2006 信息安全技术 防火墙技术要求和测试评价方法

GB/T 25069—2010 信息安全技术 术语

3 术语和定义

GB 17859—1999、GB/T 20281—2006 和 GB/T 25069—2010 界定的以及下列术语和定义适用于本文件。

3.1

第一代防火墙 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，具备包过滤、网络地址转换(NAT)、状态检测等安全功能。

3.2

第二代防火墙 the second generation firewall

除具备第一代防火墙基本功能之外，还具有应用流量识别、应用层访问控制、应用层安全防护、用户控制、深度内容检测、高性能等特征的控制的系统。

3.3

深度内容检测 deep content inspection

对应用协议进行深入解析，识别出协议中的各种要素(如，针对 http 协议，可具体解析到如 cookie、Get 参数、Post 表单等内容)及协议所承载的业务内容(如，业务系统交互中包含在协议或文件中的数据内容)，并对这些数据进行快速解析，以还原其原始通信的信息。根据解析后的原始信息，检测其中是否包含威胁以及敏感内容。

3.4

SQL 注入 SQL injection

把 SQL 命令插入到 web 表单递交或者页面请求的参数中，以达到欺骗服务器执行恶意 SQL 命令的目的。

3.5

跨站脚本　cross site scripting

恶意攻击者往 web 页面里插入恶意 HTML 代码，当用户浏览该页面时，嵌入 web 页面里面的 HTML 代码会被执行，从而达到恶意攻击用户的目的。

4　缩略语

下列缩略语适用于本文件。

DMZ：非军事区（Demilitarized Zone）
DNAT：目的网络地址转换（Destination NAT）
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）
IP：网际协议（Internet Protocol）
IPV4：互联网协议第四版（Internet Protocol V4）
IPV6：互联网协议第六版（Internet Protocol V6）
MAC：介质访问控制（Media Access Control）
NAT：网络地址转换（Network Address Translation）
P2P：对等网络（Peer-to-peer）
PHP：计算机编程语言（Hypertext Preprocessor）
POP3：邮局协议 3（Post Office Protocol 3）
SSH：安全外壳协议（Secure Shell）
SMTP：简单邮件传送协议（Simple Mail Transfer Protocol）
SNAT：源网络地址转换（Source IP NAT）
SQL：结构化查询语言（Structured Query Language）
SYN：TCP/IP 建立连接时使用的握手信号（Synchronous）
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）
XSS：跨站脚本攻击（Cross Site Scripting）

5　安全技术要求

5.1　总体说明

5.1.1　要求分类

第二代防火墙技术要求分为安全功能、安全保证、环境适应性和性能要求四个大类。其中：

a）　安全功能要求：针对第二代防火墙应具备的安全功能提出具体要求，包括网络层控制、应用层控制和安全运维管理；
b）　安全保证要求：针对第二代防火墙的开发和使用过程提出具体要求，包括配置管理、交付和运行、开发和指南文件等；
c）　环境适应性要求：针对第二代防火墙的部署模式和应用环境提出具体要求；
d）　性能要求：针对第二代防火墙应达到的性能指标作出规定，包括应用层吞吐量、网络层吞吐量、延迟、最大新建连接速率和最大并发连接数。

5.1.2 安全等级划分

按照第二代防火墙安全功能的强度划分安全功能要求的级别，按照 GB/T 18336.3 划分安全保证要求的级别。安全等级突出安全特性，环境适应性要求和性能要求不作为等级划分依据。

依据安全功能的强弱和安全保证要求的高低将安全等级分为基本级和增强级。基本级与增强级的划分见表 1 和表 2。

表 1 安全功能要求等级划分表

安全功能			基本级	增强级
网络层控制	包过滤		5.2.1.1a)～d)、f)～g)	5.2.1.1
	状态检测		5.2.1.2	5.2.1.2
	NAT		5.2.1.3a)～c)	5.2.1.3
	IP/MAC 绑定		5.2.1.4	5.2.1.4
	策略路由		5.2.1.5a)～b)	5.2.1.5
	流量会话管理	带宽管理	5.2.1.6.1 a)	5.2.1.6.1
		流量统计	5.2.1.6.2a)～d)	5.2.1.6.2
		连接数控制	5.2.1.6.3	5.2.1.6.3
		会话管理	5.2.1.6.4	5.2.1.6.4
	抗拒绝服务攻击		5.2.1.7a)	5.2.1.7
应用层控制	应用协议访问控制		5.2.2.1a)～c)	5.2.2.1
	应用内容访问控制		5.2.2.2a)～c)	5.2.2.2
	用户管控		5.2.2.3	5.2.2.3
	入侵防御		5.2.2.4a)～c)	5.2.2.4
	恶意代码防护		5.2.2.5	5.2.2.5
	WEB 攻击防护		—	5.2.2.6
	信息泄露防护		—	5.2.2.7
安全运维管理	运维管理	管理安全	5.2.3.1.1a)～c)	5.2.3.1.1
		管理方式	5.2.3.1.2a)～b)	5.2.3.1.2
		管理能力	5.2.3.1.3a)～c)	5.2.3.1.3
	安全审计	记录事件类型	5.2.3.2.1a)～e)	5.2.3.2.1
		日志内容	5.2.3.2.2	5.2.3.2.2
		日志管理	5.2.3.2.3	5.2.3.2.3
	报警		5.2.3.3	5.2.3.3
	安全管理	管理接口独立	—	5.2.3.4.1
		安全支撑系统	5.2.3.4.2	5.2.3.4.2
		异常处理机制	5.2.3.4.3	5.2.3.4.3
	高可靠性		5.2.3.5a)～b)	5.2.3.5
	升级		—	5.2.3.6

注：“—”表示无此要求。

表 2　安全保证要求等级划分表

安全保证			基本级	增强级
配置管理	部分配置管理自动化		—	5.3.1.1
	配置管理能力	版本号	5.3.1.2.1	5.3.1.2.1
		配置项	5.3.1.2.2	5.3.1.2.2
		授权控制	—	5.3.1.2.3
		产生支持和接受程序	—	5.3.1.2.4
	配置管理范围	配置管理覆盖	—	5.3.1.3.1
		问题跟踪配置管理覆盖	—	5.3.1.3.2
交付与运行	交付程序		5.3.2.1	5.3.2.1
	修改检测		—	5.3.2.2
	安装、生成和启动程序		5.3.2.3	5.3.2.3
开发	功能规范	非形式化功能规范	5.3.3.1.1	5.3.3.1.1
		充分定义的外部接口	—	5.3.3.1.2
	高层设计	描述性高层设计	5.3.3.2.1	5.3.3.2.1
		安全加强的高层设计	—	5.3.3.2.2
	安全功能实现的子集		—	5.3.3.3
	描述性低层设计		—	5.3.3.4
	非形式化对应性证实		5.3.3.5	5.3.3.5
	非形式化产品安全策略模型		—	5.3.3.6
指导性文档	管理员指南		5.3.4.1	5.3.4.1
	用户指南		5.3.4.2	5.3.4.2
生命周期支持	安全措施标识		—	5.3.5.1
	开发者定义的生命周期模型		—	5.3.5.2
	明确定义的开发工具		—	5.3.5.3
测试	测试覆盖	覆盖证据	5.3.6.1.1	5.3.6.1.1
		覆盖分析	—	5.3.6.1.2
	测试:高层设计		—	5.3.6.2
	功能测试		5.3.6.3	5.3.6.3
	独立测试	一致性	5.3.6.4.1	5.3.6.4.1
		抽样	5.3.6.4.2	5.3.6.4.2
脆弱性评定	误用	指南审查	—	5.3.7.1.1
		分析确认	—	5.3.7.1.2
	产品安全功能强度评估		5.3.7.2	5.3.7.2
	脆弱性分析	开发者脆弱性分析	5.3.7.3.1	5.3.7.3.1
		独立的脆弱性分析	—	5.3.7.3.2
		中级抵抗力	—	5.3.7.3.3

注：“—”表示无此要求。

5.2 安全功能要求

5.2.1 网络层控制

5.2.1.1 包过滤

第二代防火墙应具备包过滤功能，安全策略应：

a) 采用最小安全原则，即除非明确允许，否则就禁止；
b) 包含基于源 IP 地址、目的 IP 地址的访问控制；
c) 包含基于源端口、目的端口的访问控制；
d) 包含基于传输层协议类型的访问控制；
e) 包含基于 MAC 地址的访问控制；
f) 包含基于时间的访问控制；
g) 支持用户自定义，可以是以上条件的部分或全部组合。

5.2.1.2 状态检测

第二代防火墙应具备状态检测功能，支持基于状态检测技术的访问控制。

5.2.1.3 NAT

第二代防火墙应具备 NAT 功能，具体技术要求如下：

a) 支持双向 NAT：SNAT 和 DNAT；
b) SNAT 至少可实现“多对一”地址转换，使得内部网络主机访问外部网络时，其源 IP 地址被转换；
c) DNAT 至少可实现“一对多”地址转换，将 DMZ 的 IP 地址/端口映射为外部网络 IP 地址/端口，使外部网络的主机通过访问映射地址和端口实现对 DMZ 服务器的访问；
d) 支持动态 SNAT 技术，实现“多对多”的 SNAT。

5.2.1.4 IP/MAC 绑定

第二代防火墙应支持自动或管理员手工绑定 IP/MAC 地址，当主机的 IP 地址、MAC 地址与 IP/MAC 绑定表中不一致时，阻止其通过防火墙。

5.2.1.5 策略路由

具有多个相同属性的网络接口（即多个外部网络接口、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) 基于源、目的 IP 的策略路由；
b) 基于协议、端口或应用的策略路由；
c) 基于多链路情况（如最小延时、最大带宽或最少跳数等）进行最优路由的自动选择。

5.2.1.6 流量会话管理

5.2.1.6.1 带宽管理

第二代防火墙应具备带宽管理功能，具体技术要求如下：

a) 能够根据用户/用户组、IP 地址、应用类型，配置最大带宽、保障带宽的参数，划分带宽优先级；
b) 能够支持基于时间段的带宽策略配置。

5.2.1.6.2 流量统计

第二代防火墙应具备以下流量统计功能：

a) 通过 IP 地址、服务类型、时间和协议类型等参数进行流量统计；
b) 根据应用类型、用户等参数对流量进行统计；
c) 实时或以报表形式输出流量统计结果；
d) 按照时间段、用户、应用类型等多条件组合进行流量统计；
e) 根据网站类型进行流量统计；
f) 按照时间段、用户、应用类型、网站类型等多条件组合进行流量统计。

5.2.1.6.3 连接数控制

第二代防火墙应能够限制单 IP 的最大会话数，防止大量非法连接产生时，影响网络性能。

5.2.1.6.4 会话管理

第二代防火墙应能够在会话处于非活跃状态或会话结束后，终止网络连接。

5.2.1.7 抗拒绝服务攻击

第二代防火墙具有抗拒绝服务攻击的能力，包括但不限于：

a) ICMP 洪水攻击、UDP 洪水攻击、SYN 洪水攻击、超大 ICMP 数据包攻击；
b) TearDrop 攻击、LAND 攻击、WinNuke 攻击、Smurf 攻击。

5.2.2 应用层控制

5.2.2.1 应用协议访问控制

第二代防火墙应能够基于应用层协议分析识别各种应用协议并进行控制，应用协议识别库不低于 2 000 种，包括但不限于：

a) HTTP、FTP、TELNET、SSH、SMTP、POP3 等常见应用，如 HTTP 文件下载/内容提交，FTP 上传/下载等；
b) 即时消息、P2P 应用、网络流媒体、网络游戏、股票软件；
c) 动态开放端口的应用识别；
d) 采用隧道加密技术的应用，如翻墙软件或加密代理等；
e) 自定义应用类型的识别。

5.2.2.2 应用内容访问控制

第二代防火墙应能够支持基于应用内容的访问控制策略，具体技术要求如下：

a) 安全策略包含基于 URL 的访问控制，并可针对网站类型进行分类过滤，如成人类，赌博类，娱乐类等；
b) 具备恶意网站过滤的功能，并支持自定义恶意网站；
c) 安全策略包含基于文件类型的访问控制，并可基于文件类型进行下载过滤。包括 HTTP、FTP、邮件附件等；
d) 能够对进出网络的信息内容进行过滤，实现对应用层 HTTP、FTP、TELNET、SMTP 和 POP3 等协议命令级的控制。

5.2.2.3 用户管控

第二代防火墙应具备内网用户管理与识别的功能，应支持：

a) 基于用户名/密码的本地认证方式；
b) LDAP、Radius 等第三方认证服务器对用户身份进行鉴别；
c) 基于用户/用户组进行访问控制。

5.2.2.4 入侵防御

第二代防火墙应具备入侵防御功能，能够检测并抵御的攻击类型包括但不限于：

a) 操作系统类、Web 浏览器、ActiveX 控件、Web 服务器、文件类、FTP 服务器、虚拟化平台软件等漏洞攻击；
b) IP 地址及端口扫描行为；
c) 网络漏洞扫描行为；
d) 恶意软件攻击，如冰河、僵尸网络等；
e) 能够抵御通用服务的口令暴力破解，如 FTP、TELNET、数据库等口令破解。

5.2.2.5 恶意代码防护

第二代防火墙应具有恶意代码检测功能，具体技术要求如下：

a) 支持恶意代码检测，如蠕虫病毒、后门木马、间谍软件等；
b) 支持检测并拦截 HTTP、FTP、电子邮件等协议所携带的恶意代码。

5.2.2.6 WEB 攻击防护

第二代防火墙应具备 WEB 攻击防护的能力，支持：

a) SQL 注入攻击检测与防护，并支持 base64 编码的 SQL 注入攻击检测与防护；
b) XSS 攻击检测与防护；
c) 对常见的 Web 服务器环境 Web 入侵的脚本攻击工具(webshell)的拦截，包含 ASPX、ASP、PHP、JSP 等。

5.2.2.7 信息泄露防护

第二代防火墙应具备对流出的信息流进行检测，防止敏感信息泄露，应支持基于：

a) 关键词对流出防火墙的数据流进行过滤，如 http 上传、外发邮件主题及正文等；
b) 文件类型对流出防火墙的数据流进行过滤，如 http 上传、ftp 上传、外发邮件的附件等。

5.2.3 安全运维管理

5.2.3.1 运维管理

5.2.3.1.1 管理安全

第二代防火墙应具备管理安全功能，具体技术要求如下：

a) 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；
b) 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、主机和用户进行唯一的身份识别；
c) 具有登录失败处理功能，可采取结束会话、限制非法登录次数和当网络登录连接超时自动退出等措施；

d) 对管理员进行分权，可给不同的管理员分配不同的权限；
e) 对同一授权管理员选择两种或两种以上组合的鉴别技术进行身份鉴别。

5.2.3.1.2 管理方式

第二代防火墙应具备多种管理方式，具体技术要求如下：
a) 支持通过 console 端口进行本地管理；
b) 支持通过网络接口进行远程管理，并能够限定可进行远程管理的网络接口和可管理的 IP 地址；
c) 支持通过 SNMP V3 协议对防火墙状态进行监测，监测内容应包括 CPU、内存使用率，防火墙接口状态；
d) 远程管理过程中，管理端与第二代防火墙之间的所有通讯数据应保密传输。

5.2.3.1.3 管理能力

第二代防火墙应具备一定的管理能力，具体技术要求如下：
a) 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；
b) 向授权管理员提供设置、查询和修改各种安全策略的功能；
c) 向授权管理员提供管理审计日志的功能；
d) 能够为管理员提示风险，如入侵事件和恶意代码事件剧增，网络流量、连接数异常等；
e) 能够根据安全风险的情况自动生成针对性的推荐策略；
f) 能够对包过滤的规则进行检查，包括规则互相包含、规则冲突、长时间的无用规则、规则命中数检查等。

5.2.3.2 安全审计

5.2.3.2.1 记录事件类型

第二代防火墙应具备安全审计功能，记录事件类型要求如下：
a) 被防火墙包过滤策略允许/禁止的访问请求；
b) 被防火墙应用访问控制策略允许/禁止的访问请求；
c) 检测及防护的各类应用防护事件；
d) 从内部网络、外部网络和 DMZ 发起的到达防火墙的访问请求；
e) 试图登录防火墙管理端口和管理身份鉴别请求，包括鉴别成功和失败事件；
f) 对防火墙的重要管理配置操作：如增加/删除管理员、增加/删除/修改安全策略、配置/修改重要安全参数等。

5.2.3.2.2 日志内容

第二代防火墙应具备安全审计功能，日志内容要求如下：
a) 事件发生的日期时间，日期应包括年、月、日，时间应包括时、分、秒；
b) 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) 攻击防护日志应记录各种类型攻击事件的详细描述；
d) 管理日志应包括主体、客体、事件描述。

5.2.3.2.3 日志管理

第二代防火墙应具备安全审计功能，日志管理要求如下：

a) 只允许授权管理员访问日志；
b) 管理员支持对日志存档、删除和清空的权限；
c) 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；
d) 支持以标准 syslog 方式把日志数据外发到统一日志服务器，对日志数据进行集中分析报表；
e) 提供对审计事件一定的检索能力，检索条件包括时间、日期、主体 ID、客体 ID 等。

5.2.3.3 报警

第二代防火墙应具有报警功能，具体要求如下：
a) 对入侵事件、攻击事件等进行报警，并记录报警数据，应包括事件发生的日期时间、级别、源目的 IP 地址、对应的应用类型、事件描述；
b) 对系统运行状态异常进行报警，如 CPU、内存、带宽等超过设定阈值，并记录报警数据；
c) 对报警事件应支持至少两种方式进行报警，如邮件、声音或短信等。

5.2.3.4 安全管理

5.2.3.4.1 管理接口独立

防火墙可配置独立的管理接口，与业务接口分离。

5.2.3.4.2 安全支撑系统

第二代防火墙的支撑系统应满足以下要求：
a) 确保其支撑系统不提供多余的网络服务；
b) 不含可能导致产品权限丢失、拒绝服务等高风险安全漏洞；
c) 若支持 Web 方式管理，管理界面应不含 SQL 注入、跨站脚本等高风险安全漏洞。

5.2.3.4.3 异常处理机制

第二代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所保存的状态；
b) 日志信息不会丢失；
c) 管理员重新认证。

5.2.3.5 高可靠性

第二代防火墙应具备高可靠性，具体技术要求如下：
a) 支持物理设备状态检测。当一台防火墙自身出现断电或其他故障时，另外一台防火墙应及时发现并接管主防火墙进行工作，切换时间不超过 5 s；
b) 具备基于链路状态检测的双机热备功能，当一台防火墙直接相连的链路发生故障而无法正常工作时，另外一台防火墙应及时发现并接管主防火墙进行工作，切换时间不超过 5 s；
c) 能够支持主/主模式的双机部署；
d) 具备操作系统冗余保证系统稳定性。

5.2.3.6 升级

第二代防火墙应具备升级功能，具体技术要求如下：
a) 能对应用类型识别库、漏洞特征库、网址库、恶意代码库等进行升级；
b) 支持通过升级包以离线方式升级；

c) 支持手动或定期在线升级；

d) 采取相应措施保证升级过程安全。

5.3 安全保证要求

5.3.1 配置管理

5.3.1.1 部分配置管理自动化

配置管理系统应提供一种自动方式来支持产品的生成，通过该方式确保只能对产品的实现表示进行已授权的改变。

配置管理计划应描述在配置管理系统中所使用的自动工具，并描述在配置管理系统中如何使用自动工具。

5.3.1.2 配置管理能力

5.3.1.2.1 版本号

开发者应为产品的不同版本提供唯一的标识。

5.3.1.2.2 配置项

开发者应使用配置管理系统并提供配置管理文档。

配置管理文档应包括一个配置清单，配置清单应唯一标识组成产品的所有配置项并对配置项进行描述，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维护的证据。

5.3.1.2.3 授权控制

开发者提供的配置管理文档应包括一个配置管理计划，配置管理计划应描述如何使用配置管理系统。实施的配置管理应与配置管理计划相一致。

开发者应提供所有的配置项得到有效地维护的证据，并应保证只有经过授权才能修改配置项。

5.3.1.2.4 产生支持和接受程序

开发者提供的配置管理文档应包括一个接受计划，接受计划应描述用来接受修改过的或新建的作为产品组成部分的配置项的程序。

配置管理系统应支持产品的生成。

5.3.1.3 配置管理范围

5.3.1.3.1 配置管理覆盖

配置管理范围应至少包括产品实现表示、设计文档、测试文档、指导性文档、配置管理文档，以确保它们的修改是在一个正确授权的可控方式下进行的。

配置管理文档应至少能跟踪上述内容，并描述配置管理系统是如何跟踪这些配置项的。

5.3.1.3.2 问题跟踪配置管理覆盖

配置管理范围应包括安全缺陷，确保安全缺陷置于配置管理系统之下。

5.3.2 交付与运行

5.3.2.1 交付程序

开发者应使用一定的交付程序交付产品，并将交付过程文档化。

交付文档应描述在给用户方交付产品的各版本时，为维护安全所必需的所有程序。

5.3.2.2 修改检测

交付文档应描述如何提供多种程序和技术上的措施来检测修改，或检测开发者的主拷贝和用户方所收到版本之间的任何差异。还应描述如何使用多种程序来发现试图伪装成开发者，甚至是在开发者没有向用户方发送任何东西的情况下，向用户方交付产品。

5.3.2.3 安装、生成和启动程序

开发者应提供文档说明产品的安装、生成和启动的过程。

5.3.3 开发

5.3.3.1 功能规范

5.3.3.1.1 非形式化功能规范

开发者应提供一个功能规范，功能规范应满足以下要求：

a) 使用非形式化风格来描述产品安全功能及其外部接口；

b) 内在一致；

c) 描述所有外部接口的用途与使用方法，适当时应提供效果、例外情况和错误消息的细节；

d) 完备地表示产品安全功能。

5.3.3.1.2 充分定义的外部接口

功能规范应包括安全功能是完备地表示的基本原理。

5.3.3.2 高层设计

5.3.3.2.1 描述性高层设计

开发者应提供产品安全功能的高层设计，高层设计应满足以下要求：

a) 表示应非形式化；

b) 内在一致；

c) 按子系统描述安全功能的结构；

d) 描述每个安全功能子系统所提供的安全功能；

e) 标识安全功能所要求的任何基础性的硬件、固件或软件，以及在这些硬件、固件或软件中实现的支持性保护机制所提供功能的一个表示；

f) 标识安全功能子系统的所有接口；

g) 标识安全功能子系统的哪些接口是外部可见的。

5.3.3.2.2 安全加强的高层设计

开发者提供的安全加强的高层设计应满足以下要求：

a) 描述产品的功能子系统所有接口的用途与使用方法，适当时应提供效果、例外情况和错误消息的细节；
b) 把产品分成安全策略实施和其他子系统来描述。

5.3.3.3 安全功能实现的子集

开发者应为选定的安全功能子集提供实现表示。实现表示应当无歧义且详细地定义安全功能，无须进一步设计就能生成安全功能。实现表示应内在一致。

5.3.3.4 描述性低层设计

开发者应提供产品安全功能的低层设计，低层设计应满足以下要求：
a) 表示应非形式化；
b) 内在一致；
c) 按模块描述安全功能；
d) 描述每个模块的用途；
e) 根据所提供的安全功能性和对其他模块的依赖关系两方面来定义模块间的相互关系；
f) 描述每个安全策略实施功能是如何被提供的；
g) 标识安全功能模块的所有接口；
h) 标识安全功能模块的哪些接口是外部可见的；
i) 描述安全功能模块所有接口的用途和用法，适当时应提供效果、例外情况和错误消息的细节；
j) 把产品分为安全策略实施模块和其他模块来描述。

5.3.3.5 非形式化对应性证实

开发者应提供产品安全功能表示的所有相邻对之间的对应性分析。

对于产品安全功能所表示的每个相邻对，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且完备地细化。

5.3.3.6 非形式化产品安全策略模型

开发者应提供安全策略模型，安全策略模型应满足以下要求：
a) 表示应是非形式化的；
b) 描述所有能被模型化的安全策略的规则与特征；
c) 包含合理性，即论证该模型相对所有能被模型化的安全策略来说是一致的，且是完备的；
d) 阐明安全策略模型和功能规范之间的对应性，即论证所有功能规范中的安全功能对于安全策略模型来说是一致的，且是完备的。

5.3.4 指导性文档

5.3.4.1 管理员指南

开发者应提供管理员指南，管理员指南应与为评估而提供的其他所有文档保持一致。

管理员指南应说明以下内容：
a) 管理员可使用的管理功能和接口；
b) 怎样安全地管理产品；
c) 在安全处理环境中应被控制的功能和权限；

d) 所有对与产品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实体的安全特性进行的改变；

g) 所有与管理员有关的 IT 环境安全要求。

5.3.4.2 用户指南

开发者应提供用户指南，用户指南应与为评估而提供的其他所有文档保持一致。

用户指南应说明以下内容：

a) 产品的非管理员用户可使用的安全功能和接口；

b) 产品提供给用户的安全功能和接口的使用方法；

c) 用户可获取但应受安全处理环境所控制的所有功能和权限；

d) 产品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。

5.3.5 生命周期支持

5.3.5.1 安全措施标识

开发者应提供开发安全文档。

开发安全文档应描述在产品的开发环境中，为保护产品设计和实现的保密性和完整性所必需的所有物理的、程序的、人员的和其他方面的安全措施，并应提供在产品的开发和维护过程中执行安全措施的证据。

5.3.5.2 开发者定义的生命周期模型

开发者应建立一个生命周期模型对产品的开发和维护进行的必要控制，并提供生命周期定义文档描述用于开发和维护产品的模型。

5.3.5.3 明确定义的开发工具

开发者应明确定义用于开发产品的工具，并提供开发工具文档无歧义的定义实现中每个语句的含义和所有依赖于实现的选项的含义。

5.3.6 测试

5.3.6.1 测试覆盖

5.3.6.1.1 覆盖证据

开发者应提供测试覆盖的证据。

在测试覆盖证据中，应表明测试文档中所标识的测试与功能规范中所描述的产品的安全功能是对应的。

5.3.6.1.2 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功能规范中所描述的产品的安全功能之间的对应性是完备的。

5.3.6.2 测试:高层设计

开发者应提供测试深度的分析。

深度分析应证实测试文档中所标识的测试足以证实该产品的功能是依照其高层设计运行的。

5.3.6.3 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。

测试文档应包括以下内容:

a) 测试计划,应标识要测试的安全功能,并描述测试的目标;
b) 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,这些概况应包括对于其他测试结果的顺序依赖性;
c) 预期的测试结果,应表明测试成功后的预期输出;
d) 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。

5.3.6.4 独立测试

5.3.6.4.1 一致性

开发者应提供适合测试的产品,提供的测试集合应与其自测产品功能时使用的测试集合相一致。

5.3.6.4.2 抽样

开发者应提供一组相当的资源,用于安全功能的抽样测试。

5.3.7 脆弱性评定

5.3.7.1 误用

5.3.7.1.1 指南审查

开发者应提供指导性文档,指导性文档应满足以下要求:

a) 标识所有可能的产品运行模式(包括失败或操作失误后的运行)、它们的后果以及对于保持安全运行的意义;
b) 完备的、清晰的、一致的、合理;
c) 列出关于预期使用环境的所有假设;
d) 列出对外部安全措施(包括外部程序的、物理的或人员的控制)的所有要求。

5.3.7.1.2 分析确认

开发者应提供完备的分析文档论证指导性文档。

5.3.7.2 产品安全功能强度评估

开发者应对指导性文档中所标识的每个具有安全功能强度声明的安全机制进行安全功能强度分析,并说明安全机制达到或超过定义的最低强度级别或特定功能强度度量。

5.3.7.3 脆弱性分析

5.3.7.3.1 开发者脆弱性分析

开发者应执行脆弱性分析,并提供脆弱性分析文档。

开发者应从用户可能破坏安全策略的明显途径出发，对产品的各种功能进行分析并提供文档。对被确定的脆弱性，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产品的环境中，该脆弱性不能被利用。

5.3.7.3.2 独立的脆弱性分析

开发者应提供文档证明经过标识脆弱性的产品可以抵御明显的穿透性攻击。

5.3.7.3.3 中级抵抗力

开发者应提供文档证明产品可以抵御中级强度的穿透性攻击，并提供证据说明对脆弱性的搜索是系统化的。

5.4 环境适应性要求

5.4.1 工作模式

5.4.1.1 透明模式

第二代防火墙应支持透明模式。

5.4.1.2 路由模式

第二代防火墙应支持路由模式。

5.4.2 下一代互联网支持(有则适用)

5.4.2.1 支持纯 IPv6 网络环境

第二代防火墙应支持纯 IPv6 网络环境，能够在纯 IPv6 网络环境下正常工作，实现第二代防火墙的安全功能要求。

5.4.2.2 协议一致性

第二代防火墙应支持 IPv6 协议一致性检查：

a) IPv6 Core(核心协议)协议一致性。

b) IPv6 NDP 协议一致性。

c) IPv6 Autoconfig(自动编码)协议一致性。

d) IPv6 PMTU 协议一致性。

e) ICMPv6 协议一致性。

5.4.2.3 协议健壮性

第二代防火墙应保证协议的健壮性，能够抵御 IPv6 网络环境下畸形协议报文攻击。畸形协议报文包括：

a) IPv6 Core 协议畸形报文；

b) ICMPv6 畸形报文；

c) 其他协议畸形报文。

5.4.2.4 IPv6 网络环境下自身管理

第二代防火墙应支持在 IPv6 网络环境下自身管理。

5.4.2.5 支持能力

第二代防火墙应至少支持以下一种 IPv6 过渡网络环境：

a) 双协议栈：IPv4/IPv6 双栈网络环境，能够在 IPv4/IPv6 双栈网络环境下正常工作；

b) 协议转换：将 IPv4 和 IPv6 两种协议相互转换，能够在协议转换网络环境下正常工作；

c) 隧道：至少支持以下一种隧道工作模式：

1) 6over4 网络环境，能够在 6over4 网络环境下正常工作；

2) ISATAP 网络环境，保证在 ISATAP 网络环境下正常工作。

5.5 性能要求

5.5.1 应用层吞吐量

流量参考场景构成如下：HTTP Text，20%；HTTP Audio，4%；HTTP Video 5%，SMB，8%；SMTP，12%；POP3，12%；FTP，10%；SSH，2%；TELNET，2%；PostgreSQL 5%；其他，20%。

应用层吞吐量视不同速率的第二代防火墙有所不同，具体指标要求如下：

a) 第二代防火墙在不阻断正常连接的情况下，应达到的单向应用层吞吐量指标：

1) 千兆第二代防火墙应用层吞吐量应不小于 900 Mbps；

2) 万兆第二代及万兆以上防火墙应用层吞吐量应不小于 8 Gbps；

b) 开启入侵防御、恶意代码防御及应用识别功能的情况下，按照上述流量场景，防火墙不能误拦截正常的 TCP 连接，第二代防火墙应用层吞吐量下降不超过原来的 30%。

5.5.2 网络层吞吐量

网络层吞吐量视不同速率的第二代防火墙有所不同，具体指标要求如下：

a) 第二代防火墙在不丢包的情况下，一对相应速率的端口在具有多条(200 条)包过滤规则的条件下应达到的双向吞吐量指标：

1) 对 64 字节短包，千兆第二代防火墙应不小于线速的 50%，万兆第二代防火墙应不小于线速的 70%；

2) 对 512 字节中长包，千兆第二代防火墙应不小于线速的 85%，万兆第二代防火墙应不小于线速的 90%；

3) 对 1518 字节长包，千兆第二代防火墙应不小于线速的 95%，万兆第二代防火墙应不小于线速的 98%；

b) 在开启入侵防御、恶意代码防御及应用识别功能的条件下，第二代防火墙吞吐量下降不超过原来的 30%。

5.5.3 延迟

延迟视不同速率的第二代防火墙有所不同，在最大吞吐量 90%的条件下，具体延迟指标要求如下：

a) 千兆第二代防火墙的 64 字节短包平均延迟不应超过 500 μs；

b) 万兆第二代防火墙的 64 字节短包平均延迟不应超过 90 μs；

c) 在开启入侵防御、恶意代码防御及应用识别功能的条件下，第二代防火墙平均延迟增加应不超过原来的 50%。

5.5.4 最大新建连接速率

最大新建连接速率视不同速率的第二代防火墙有所不同，具体指标要求如下：

a） 千兆第二代防火墙的最大新建连接数速率应不小于30 000个/s；

b） 万兆第二代防火墙的最大新建连接数速率应不小于150 000个/s。

5.5.5 最大并发连接

最大并发连接数视不同速率的第二代防火墙有所不同，具体指标要求如下：

a） 千兆第二代防火墙的最大并发连接数应不小于200万个；

b） 万兆第二代防火墙的最大并发连接数应不小于500万个。