ICS 35.240
A.90

GA

中华人民共和国公共安全行业标准

GA/T XXXX—XXXX

信息安全技术 基于IPv6的高性能网络入侵防御系统产品安全技术要求

Information security technology Security technical requirements for IPv6-based high-performance network intrusion prevention system products

（报批稿）

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

中华人民共和国公安部　发布

目　次

前言 III
1 范围 1
2 规范性引用文件 1
3 术语和定义 1
4 缩略语 2
5 基于 IPv6 的高性能网络入侵防御系统产品描述 2
6 总体说明 3
6.1 安全技术要求分类 3
6.2 安全等级划分 3
7 安全功能要求 3
7.1 入侵事件分析功能要求 3
7.2 入侵事件响应功能要求 3
7.3 入侵事件审计功能要求 4
7.4 管理控制功能要求 4
8 自身安全功能要求 5
8.1 标识与鉴别 5
8.2 安全管理 6
8.3 审计日志 6
9 环境适应性要求 7
9.1 支持纯 IPv6 网络环境 7
9.2 IPv6 网络环境下自身管理 7
9.3 支持 IPv6 过渡网络环境（可选） 7
10 性能要求 7
10.1 吞吐率 7
10.2 延迟 7
10.3 最大并发连接数 8
10.4 最大连接速率 8
10.5 误截和漏截 8
11 安全保障要求 8
11.1 开发 8
11.2 指导性文档 9
11.3 生命周期支持 9
11.4 测试 10
11.5 脆弱性评定 11
12 不同安全等级要求 11
12.1 安全功能要求 11
12.2 自身安全功能要求 12

12.3 安全保障要求.....12

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。

本标准主要起草人：顾建新、邵东、付文彬、顾健、张笑笑、顾玮。

信息安全技术 基于IPv6的高性能网络入侵防御系统产品安全技术要求

1 范围

本标准规定了基于IPv6的高性能网络型入侵防御系统产品的安全功能要求、自身安全功能要求、环境适应性要求、性能要求、安全保障要求以及等级划分。

本标准适用于基于IPv6的高性能网络型入侵防御系统产品的设计、开发及测试。

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/T 18336.3-2015 信息技术 安全技术 信息技术安全评估准则 第3部分：安全保障组件

GB/T 25069-2010 信息安全技术 术语

GB/T 28451-2012 信息安全技术 网络型入侵防御产品技术要求和测试评价方法

3 术语和定义

GB/T 18336.3-2015、GB/T 25069-2010和GB/T 28451-2012界定的以及下列术语和定义适用于本文件。

3.1

基于IPv6的高性能网络型入侵防御系统产品 IPv6-based high performance network intrusion prevention system product

以透明网桥或网关形式部署在网络通路上，通过分析网络流量发现具有入侵特征的网络行为，在其传入被保护网络前进行拦截的产品，能够适用于IPv4、IPv6等不同的高性能网络应用场景。

3.2

安全事件 incident

通过对事件的分析处理，从而识别出一种系统、服务或网络状态的发生，表明一次可能的违反安全规则或某些防护措施失效，或者一种可能与安全相关但以前不为人知的一种情况，极有可能危害业务运行和威胁信息安全。

3.3

入侵 intrusion

任何危害或可能危害资源完整性、保密性或可用性的行为。

3.4

告警 alert

当发现攻击或入侵事件时，高性能入侵防御系统向授权管理员发出的紧急通知。

3.5

误截 false positive

在未出现攻击事件时，入侵防御系统产品对正常网络流量进行拦截的行为。

3.6

漏截 false negative

当攻击事件发生时，入侵防御系统未进行拦截的行为。

4 缩略语

下列缩略语适用于本文件。

IPv6：互联网协议第6版（Internet Protocol Version 6）

NFS：网络文件系统（Network File System）

TFTP：简单文件传输协议（Trivial File Transfer Protocol）

5 基于 IPv6 的高性能网络入侵防御系统产品描述

本标准提出了基于IPv6 的高性能网络入侵防御系统产品的安全功能要求和安全保障要求。网络入侵防御产品通常以网桥、路由或透明模式部属在受保护网络出口，将网络划分为外网和内网，产品功能是在内外网之间建立安全防护点，通过分析网络通信数据内容，根据预先定义的攻击防御规则和其他防护策略，对网络通讯数据进行解析并过滤，抵御来自外网的攻击，保护内网用户资源或者内网服务器，并向被保护的网络提供安全的访问服务请求或者应答。此外，适用于下一代互联网网络环境的入侵防御产品的协议栈除支持IPv4外，还应支持IPv6、IPv4/IPv6过渡技术，并具备较高的处理性能。

网络型入侵防御产品保护的资产是受安全策略保护的网络服务和用户资源等，此外，入侵防御产品本身及其内部的重要数据也是受保护的资产。

下图1是网络入侵防御产品的一个典型部署环境，左图是企业内网防护场景，网络入侵防御产品防护企业用户免受来自互联网的威胁，右图是关键服务器防护场景，网络入侵防御产品防护关键服务器免受外部威胁。

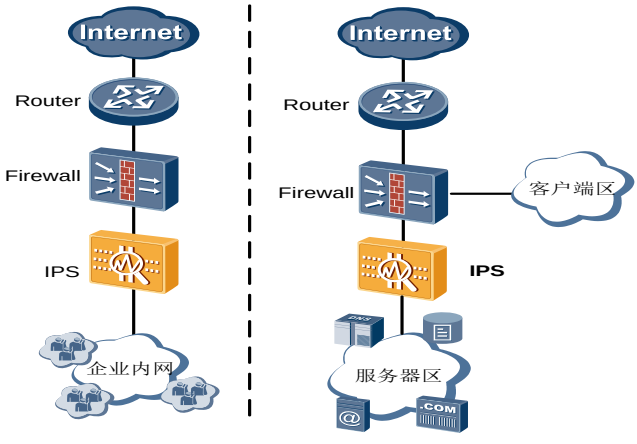


图1 网络入侵防御系统产品典型运行环境

6 总体说明

6.1 安全技术要求分类

本标准将基于IPv6的高性能网络入侵防御系统产品安全技术要求分为安全功能要求、自身安全功能要求、环境适应性、性能要求和安全保障要求。其中，安全功能要求是对产品应具备的安全功能提出具体要求，包括入侵事件分析功能要求、入侵事件响应功能要求、入侵事件审计功能要求、管理控制功能要求；自身安全要求包括标识与鉴别、安全管理和审计日志；安全保障要求针对基于IPv6的高性能网络入侵防御系统产品的生命周期过程提出具体的要求，例如配置管理、交付和运行、开发和指南文件等。

6.2 安全等级划分

基于 IPv6 的高性能网络入侵防御系统产品的安全等级按照其安全功能要求、自身安全功能要求和安全保障要求的强度划分为基本级和增强级，其中安全保障要求参考了 GB/T 18336.3—2015。

7 安全功能要求

7.1 入侵事件分析功能要求

7.1.1 数据收集

产品应具有实时收集流入目标网络内所有数据包的能力。

7.1.2 协议分析

产品应至少但不限于分析基于以下协议的事件：IP、ICMP、ARP、RIP、TCP、UDP、RPC、HTTP、FTP、TFTP、IMAP、SNMP、TELNET、DNS、SMTP、POP3、NETBIOS、NFS、NNTP 等。

7.1.3 入侵发现

产品应能发现协议中的入侵行为。

7.1.4 入侵逃避发现

产品应能发现躲避或欺骗检测的行为，如 IP 碎片重组，TCP 流重组，协议端口重定位，URL 字符串变形，shell 代码变形等。

7.1.5 流量监测

产品应对目标环境中的应用流量进行监测。

7.2 入侵事件响应功能要求

7.2.1 拦截能力

产品应对发现的入侵行为进行预先拦截，防止进入目标网络。

7.2.2 安全告警

产品应在发现并拦截入侵行为时，进行安全警告。

7.2.3 告警方式

产品的告警方式包括屏幕实时提示、E-mail 告警、声音告警、短信息等中的一种或多种方式。

7.2.4 例外规则

为减少对特定内网终端的影响，产品应支持主机隔离；同时为了关键业务系统的连续性，产品应支持添加例外规则。

7.2.5 事件合并

产品应具有对高频度发生的相同安全事件进行合并告警，避免出现告警风暴的能力，其频度可设置。

7.2.6 事件定位

产品应支持事件定位，可以定位到攻击源的地理位置（国家、城市），便于追溯。

7.3 入侵事件审计功能要求

7.3.1 事件生成

产品应能对拦截行为及时生成审计记录。

7.3.2 事件记录

产品应记录并保存拦截到的入侵事件，入侵事件信息应至少包含以下内容：事件名称、事件发生日期时间、源 IP 地址、源端口、源 IP 地理信息、目的 IP 地址、目的端口、危害等级，如果是内网用户滥用行为，还需要记录用户名信息等。

7.3.3 报表生成

产品应能对入侵事件或者入侵行为生成报表。

7.3.4 报表输出

产品应支持管理员按照自己的要求修改和定制报表内容，并输出成方便阅读的文件格式，至少支持 DOC、PDF、HTML、XLS 等各式中的一种或多种。

7.3.5 报表模板的定制

产品应提供结果报表模板的定制功能。

7.4 管理控制功能要求

7.4.1 管理界面

产品应提供管理界面用于管理、配置入侵防御产品，管理界面应包含配置和管理产品所需的所有功能。

7.4.2 入侵事件库

产品应提供入侵事件库，事件库应包括事件名称、详细描述定义等内容。

7.4.3 事件分级

产品应按照严重程度对事件进行分级，使授权管理员能从大量的信息中捕捉到危险的事件。

7.4.4 功能失效处理

产品应提供功能失效处理机制，当设备出现软硬件问题导致入侵防御功能失效时，用户可根据需要选择拦截或者放行网络流量。

7.4.5 策略配置

产品应提供对入侵防御策略、响应措施进行配置的功能。

7.4.6 事件库更新

产品应具备更新、升级产品事件库的能力，并能保证事件库升级时的安全。

7.4.7 管理接口独立

产品应具备独立的管理接口。

7.4.8 协议定义

产品除支持默认的网络协议集外，还应允许授权管理员定义新的协议，或对协议的端口进行重新定位。

7.4.9 流量控制

产品具备对应用流量进行控制的功能，例如：限制P2P下载流量等。

7.4.10 双机热备

产品应具备双机热备的能力。

7.4.11 自我隐藏

产品应至少提供透明或者网桥接入方式，采取隐藏业务口 IP 地址等措施使自身在网络上不可见，以降低被攻击的可能性。

8 自身安全功能要求

8.1 标识与鉴别

8.1.1 属性定义

产品应为每个管理员规定与之相关的安全属性，如标识、鉴别信息、隶属组、权限等。

8.1.2 属性初始化

产品应提供使用默认值对创建的每个管理员的属性进行初始化的能力。

8.1.3 唯一性标识

产品应为管理员提供唯一标识，并能将标识与该用户的所有可审计事件相关联。

8.1.4 基本鉴别

产品应在执行任何与安全功能相关的操作之前鉴别用户的身份。

8.1.5 鉴别数据保护

产品应保证鉴别数据不被未授权查阅或修改。

8.1.6 鉴别失败处理

当用户鉴别失败的次数达到指定次数后，产品应能终止用户的访问。

8.1.7 超时锁定或注销

产品应具备登录超时锁定或注销功能，在设定的时间段内没有任何操作的情况下，终止会话，需要再次进行身份鉴别才能够重新操作，最大超时时间仅由授权管理员设定。

8.2 安全管理

8.2.1 安全功能管理

授权管理员应能对产品进行以下管理操作：

a) 查看、修改相关安全属性；
b) 启动、关闭全部或部分安全功能；
c) 制定和修改各种安全策略。

8.2.2 安全角色管理

产品应能对管理员角色进行区分：

a) 具有至少两种不同权限的管理员角色；
b) 根据不同的功能模块定义各种不同权限角色。

8.2.3 远程安全管理

若产品支持通过网络进行远程管理，应满足以下技术要求：

a) 对远程会话信息进行保护；
b) 对远程管理主机的地址进行限制。

8.3 审计日志

8.3.1 审计日志生成

产品应对与自身安全相关的以下事件生成审计日志：

a) 用户登录成功和失败；
b) 对安全策略进行更改；
c) 对管理员进行增加、删除和属性修改；
d) 因鉴别失败的次数超出了设定值，导致的会话连接终止；
e) 管理员的其他操作。

每一条审计日志至少应包括事件发生的日期、时间、用户标识、事件描述和结果。若采用远程登录方式对产品进行管理，还应记录管理主机的地址。

8.3.2 审计日志存储

审计日志应存储于掉电非易失性存储介质中。

8.3.3 审计日志管理

产品应提供以下审计日志管理功能：

a) 只允许授权管理员访问审计日志；
b) 对审计日志的查询功能；
c) 保存及导出审计日志。

9 环境适应性要求

9.1 支持纯 IPv6 网络环境

产品应支持纯IPv6网络环境，能够在纯IPv6网络环境下正常工作。

9.2 IPv6 网络环境下自身管理

产品应支持在IPv6网络环境下自身管理。

9.3 支持 IPv6 过渡网络环境（可选）

9.3.1 双协议栈

产品应支持IPv4/IPv6双栈网络环境，能够在IPv4/IPv6双栈网络环境下正常工作。

9.3.2 隧道

9.3.2.1 6over4

产品应支持6over4网络环境，能够在6over4网络环境下正常工作。

9.3.2.2 6to4

产品应支持6to4网络环境，能够在6to4网络环境下正常工作。

9.3.2.3 ISATAP

产品应支持ISATAP网络环境，保证在ISATAP网络环境下正常工作。

10 性能要求

10.1 吞吐率

产品的吞吐率视不同速率的产品有所不同，具体指标要求如下：

a） 对 64 字节短包，百兆产品应不小于线速的 20%，千兆及万兆产品应不小于线速的 35%；
a） 对 512 字节中长包，百兆产品应不小于线速的 70%，千兆及万兆产品应不小于线速的 80%；
b） 对 1518 字节长包，百兆产品应不小于线速的 90%,千兆及万兆产品应不小于线速的 95%；
c） 高性能入侵防御系统产品在不丢包的情况下，对 1518 字节长包，整机处理能力应能够支持 20Gbps。

10.2 延迟

产品的延迟视不同速率的产品有所不同，具体指标要求如下：

a） 对 64 字节短包、512 字节中长包、1518 字节长包，百兆产品的最大延迟不应超过 500us；

b） 对 64 字节短包、512 字节中长包、1518 字节长包，千兆、万兆以及高性能入侵防御系统产品的最大延迟不应超过 90us。

10.3 最大并发连接数

最大并发连接数视不同速率的产品有所不同，具体指标要求如下：

a) 百兆产品的整机最大并发连接数应不小于 10000 个；
b) 千兆产品的整机最大并发连接数应不小于 100000 个；
c) 万兆产品的整机最大并发连接数应不小于 1000000 个；
d) 高性能入侵防御系统产品的整机最大并发连接数应不小于 800 万个。

10.4 最大连接速率

最大连接数视不同速率的产品有所不同，具体指标要求如下：

a) 百兆产品的整机最大连接速率应不小于每秒 1500 个；
b) 千兆产品的整机最大连接速率应不小于每秒 5000 个；
c) 万兆产品的整机最大连接速率应不小于每秒 50000 个；
d) 高性能入侵防御系统产品的整机最大连接速率应不小于每秒 50 万个。

10.5 误截和漏截

10.5.1 误截

在正常背景流量条件下，产品的误截率不可超过 2%。

10.5.2 漏截

在正常背景流量和入侵流量混合条件下，产品的漏截率不可超过 15%。

11 安全保障要求

11.1 开发

11.1.1 安全架构

开发者应提供产品安全功能的安全架构描述，安全架构描述应满足以下要求：

a) 与产品设计文档中对安全功能实施抽象描述的级别一致；
b) 描述与安全功能要求一致的产品安全功能的安全域；
c) 描述产品安全功能初始化过程为何是安全的；
d) 证实产品安全功能能够防止被破坏；
e) 证实产品安全功能能够防止安全特性被旁路。

11.1.2 功能规范

开发者应提供完备的功能规范说明，功能规范说明应满足以下要求：

a） 完全描述产品的安全功能；
b） 描述所有安全功能接口的目的与使用方法；
c） 标识和描述每个安全功能接口相关的所有参数；
d） 描述安全功能接口相关的安全功能实施行为；

e） 描述由安全功能实施行为处理而引起的直接错误消息；
f） 证实安全功能要求到安全功能接口的追溯；
g） 描述安全功能实施过程中，与安全功能接口相关的所有行为；
h） 描述可能由安全功能接口的调用而引起的所有直接错误消息。

11.1.3 实现表示

开发者应提供全部安全功能的实现表示，实现表示应满足以下要求：
a） 提供产品设计描述与实现表示实例之间的映射，并证明其一致性；
b） 按详细级别定义产品安全功能，详细程度达到无须进一步设计就能生成安全功能的程度；
c） 以开发人员使用的形式提供。

11.1.4 产品设计

开发者应提供产品设计文档，产品设计文档应满足以下要求：
a） 根据子系统描述产品结构；
b） 标识和描述产品安全功能的所有子系统；
c） 描述安全功能所有子系统间的相互作用；
d） 提供的映射关系能够证实设计中描述的所有行为能够映射到调用它的安全功能接口；
e） 根据模块描述安全功能；
f） 提供安全功能子系统到模块间的映射关系；
g） 描述所有安全功能实现模块，包括其目的及与其他模块间的相互作用；
h） 描述所有实现模块的安全功能要求相关接口、其他接口的返回值、与其他模块间的相互作用及调用的接口；
i） 描述所有安全功能的支撑或相关模块，包括其目的及与其他模块间的相互作用。

11.2 指导性文档

11.2.1 操作用户指南

开发者应提供明确和合理的操作用户指南，操作用户指南与为评估而提供的其他所有文档保持一致，对每一种用户角色的描述应满足以下要求：
a） 描述在安全处理环境中被控制的用户可访问的功能和特权，包含适当的警示信息；
b） 描述如何以安全的方式使用产品提供的可用接口；
c） 描述可用功能和接口，尤其是受用户控制的所有安全参数，适当时指明安全值；
d） 明确说明与需要执行的用户可访问功能有关的每一种安全相关事件，包括改变安全功能所控制实体的安全特性；
e） 标识产品运行的所有可能状态（包括操作导致的失败或者操作性错误），以及它们与维持安全运行之间的因果关系和联系；
f） 充分实现安全目的所必需执行的安全策略。

11.2.2 准备程序

开发者应提供产品及其准备程序，准备程序描述应满足以下要求：
a） 描述与开发者交付程序相一致的安全接收所交付产品必需的所有步骤；
b） 描述安全安装产品及其运行环境必需的所有步骤。

11.3 生命周期支持

11.3.1 配置管理能力

开发者的配置管理能力应满足以下要求：

a) 为产品的不同版本提供唯一的标识；
b) 使用配置管理系统对组成产品的所有配置项进行维护，并唯一标识配置项；
c) 提供配置管理文档，配置管理文档描述用于唯一标识配置项的方法；
d) 配置管理系统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；
e) 配置管理文档包括一个配置管理计划，配置管理计划描述如何使用配置管理系统开发产品。实施的配置管理与配置管理计划相一致；
f) 配置管理计划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。

11.3.2 配置管理范围

开发者应提供产品配置项列表，并说明配置项的开发者。配置项列表应包含以下内容：

a) 产品、安全保障要求的评估证据和产品的组成部分；
b) 实现表示、安全缺陷报告及其解决状态。

11.3.3 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。在给用户方交付产品的各版本时，交付文档应描述为维护安全所必需的所有程序。

11.3.4 开发安全

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。

11.3.5 生命周期定义

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。

11.3.6 工具和技术

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地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。

11.4 测试

11.4.1 测试覆盖

开发者应提供测试覆盖文档，测试覆盖描述应满足以下要求：

a) 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间的对应性；
b) 表明上述对应性是完备的，并证实功能规范中的所有安全功能接口都进行了测试。

11.4.2 测试深度

开发者应提供测试深度的分析。测试深度分析描述应满足以下要求：

a) 证实测试文档中的测试与产品设计中的安全功能子系统和实现模块之间的一致性；
b) 证实产品设计中的所有安全功能子系统、实现模块都已经进行过测试。

11.4.3 功能测试

开发者应测试产品安全功能，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，标识要执行的测试，并描述执行每个测试的方案，这些方案包括对于其他测试结果的任何顺序依赖性；
b) 预期的测试结果，表明测试成功后的预期输出；
c) 实际测试结果和预期的一致性。

11.4.4 独立测试

开发者应提供一组与其自测安全功能时使用的同等资源，以用于安全功能的抽样测试。

11.5 脆弱性评定

基于已标识的潜在脆弱性，产品能够抵抗以下攻击行为：

a) 具有基本攻击潜力的攻击者的攻击；
b) 具有增强型基本攻击潜力的攻击者的攻击。

12 不同安全等级要求

12.1 安全功能要求

不同安全等级的基于 IPv6 的高性能网络入侵防御系统产品的安全功能要求如表 1 所示。

表1 不同安全等级的基于 IPv6 的高性能网络入侵防御系统产品的安全功能要求

安全功能要求		基本级	增强级
入侵事件分析要求	数据收集	7.1.1	7.1.1
	协议分析	7.1.2	7.1.2
	入侵发现	7.1.3	7.1.3
	入侵逃避发现	——	7.1.4
	流量监测	——	7.1.5
入侵事件响应功能要求	拦截能力	7.2.1	7.2.1
	安全告警	7.2.2	7.2.2
	告警方式	7.2.3	7.2.3
	例外规则	——	7.2.4
	事件合并	——	7.2.5
	事件定位	——	7.2.6
入侵事件审计功能要求	事件生成	7.3.1	7.3.1
	事件记录	7.3.2	7.3.2
	报表生成	——	7.3.3
	报表输出	——	7.3.4
	报表模板的定制	——	7.3.5
管理控制功能要求	管理界面	7.4.1	7.4.1
	入侵事件库	7.4.2	7.4.2
	事件分级	7.4.3	7.4.3

表 1（续）

安全功能要求		基本级	增强级
管理控制功能要求	功能失效处理	7.4.4	7.4.4
	策略配置	7.4.5	7.4.5
	事件库更新	7.4.6	7.4.6
	管理接口独立	7.4.7	7.4.7
	协议定义	——	7.4.8
	流量控制	——	7.4.9
	双机热备	——	7.4.10
	自我隐藏	——	7.4.11

12.2 自身安全功能要求

不同安全等级的基于 IPv6 的高性能网络入侵防御系统产品的自身安全功能要求如表 2 所示。

表2 不同安全等级的基于 IPv6 的高性能网络入侵防御系统产品的自身安全功能要求

自身安全功能要求		基本级	增强级
标识与鉴别	属性定义	8.1.1	8.1.1
	属性初始化	8.1.2	8.1.2
	唯一性标识	8.1.3	8.1.3
	基本鉴别	8.1.4	8.1.4
	鉴别数据保护	8.1.5	8.1.5
	鉴别失败处理	——	8.1.6
	超时锁定或注销	——	8.1.7
安全管理	安全功能管理	8.2.1	8.2.1
	安全角色管理	8.2.2 a)	8.2.2
	远程安全管理	8.2.3	8.2.3
审计日志	审计日志生成	8.3.1 a) ～c)	8.3.1
	审计日志存储	8.3.2	8.3.2
	审计日志管理	8.3.3	8.3.3

12.3 安全保障要求

不同安全等级的基于 IPv6 的高性能网络入侵防御系统产品的安全保障要求如表 3 所示。

表3 不同安全等级的基于 IPv6 的高性能网络入侵防御系统产品的安全保障要求

安全保障要求		基本级	增强级
开发	安全架构	11.1.1	11.1.1
	功能规范	11.1.2 a) ～f)	11.1.2
	实现表示	——	11.1.3
	产品设计	11.1.4 a) ～d)	11.1.4

表 3（续）

安全保障要求		基本级	增强级
指导性文档	操作用户指南	11.2.1	11.2.1
	准备程序	11.2.2	11.2.2
生命周期支持	配置管理能力	11.3.1 a) ～c)	11.3.1
	配置管理范围	11.3.2 a)	11.3.2
	交付程序	11.3.3	11.3.3
	开发安全	——	11.3.4
	生命周期定义	——	11.3.5
	工具和技术	——	11.3.6
测试	测试覆盖	11.4.1 a)	11.4.1
	测试深度	——	11.4.2
	功能测试	11.4.3	11.4.3
	独立测试	11.4.4	11.4.4
脆弱性评定		11.5 a)	11.5 b)