ICS 35.040
A 90

GA

中华人民共和国公共安全行业标准

GA/T 1728—2020

信息安全技术　基于 IPv6 的高性能网络入侵检测系统产品安全技术要求

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

2020-05-13 发布　　2020-08-01 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、公安部第三研究所、网神信息技术（北京）股份有限公司。

本标准主要起草人：宋好好、顾建新、武腾、邹春明、陆臻、沈亮、顾健、李博、杨柳。

信息安全技术　基于IPv6的高性能网络入侵检测系统产品安全技术要求

1　范围

本标准规定了基于IPv6的高性能网络入侵检测系统产品的安全功能要求、环境适应性要求、性能要求、安全保障要求及安全等级划分。

本标准适用于基于IPv6的高性能网络入侵检测系统产品的设计、开发与测试。

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

3　术语和定义

GB/T 18336.3—2015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

事件　event

一种系统、服务或网络状态的发生或者改变的记录信息，可作为分析安全事件的基础。

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

入侵检测　intrusion detection

通过对计算机网络或计算机系统中的若干关键点收集信息并对其进行分析，从中发现网络或系统中是否有违反安全策略的行为和被攻击的迹象。

3.5

探测器　sensor

用于收集可能指示出入侵行为或者滥用信息系统资源的实时事件，并对收集到的信息进行初步分析的入侵检测系统组件。

3.6

告警　alert

当攻击或入侵发生时，高性能入侵检测系统向授权管理员发出的紧急通知。

3.7

响应　response

当攻击或入侵发生时，针对信息系统及存储的数据采取的保护并恢复正常运行环境的行为。

3.8

误报　false positive

高性能入侵检测系统在未发生攻击时告警，或者发出错误的告警信息。

3.9

漏报　false negative

当攻击发生时高性能入侵检测系统未告警。

4　缩略语

下列缩略语适用于本文件。

ARP：地址解析协议（Address Resolution Protocol）

DNS：域名系统（Domain Name System）

FTP：文件传输协议（File Transfer Protocol）

HTML：超文本标记语言（Hypertext Markup Language）

ICMP：网际控制报文协议（Internet Control Message Protocol）

IDS：入侵检测系统（Intrusion Detection System）

IMAP：因特网消息访问协议（Internet Message Access Protocol）

IP：网际协议（Internet Protocol）

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

NFS：网络文件系统（Network File System）

POP3：邮局协议的第三个版本（Post Office Protocol 3）

RIP：路由选择信息协议（Routing Information Protocol）

RPC：远程过程调用（Remote Procedure Call）

SMTP：简单邮件传送协议（Simple Mail Transfer Protocol）

SNMP：简单网络管理协议（Simple Network Management Protocol）

TCP：传输控制协议（Transport Control Protocol）

TELNET：远程登录（Telecommunication Network）

TFTP：普通文件传送协议（Trivial File Transfer Protocol）

UDP：用户数据报协议（User Datagram Protocol）

5　基于 IPv6 的高性能网络入侵检测系统产品描述

基于 IPv6 的高性能网络入侵检测系统产品以网络上的数据包作为数据源，监听所保护网络内的所有数据包并进行分析，从而发现异常行为并报警。

基于 IPv6 的高性能网络入侵检测系统产品采用旁路模式接入目标网络。在旁路模式下，高性能入侵检测系统旁路连接在目标网络中，通过采集交换机镜像口网络通信数据工作。图 1 为基于 IPv6 的高性能网络入侵检测系统产品旁路模式的一个典型运行环境。

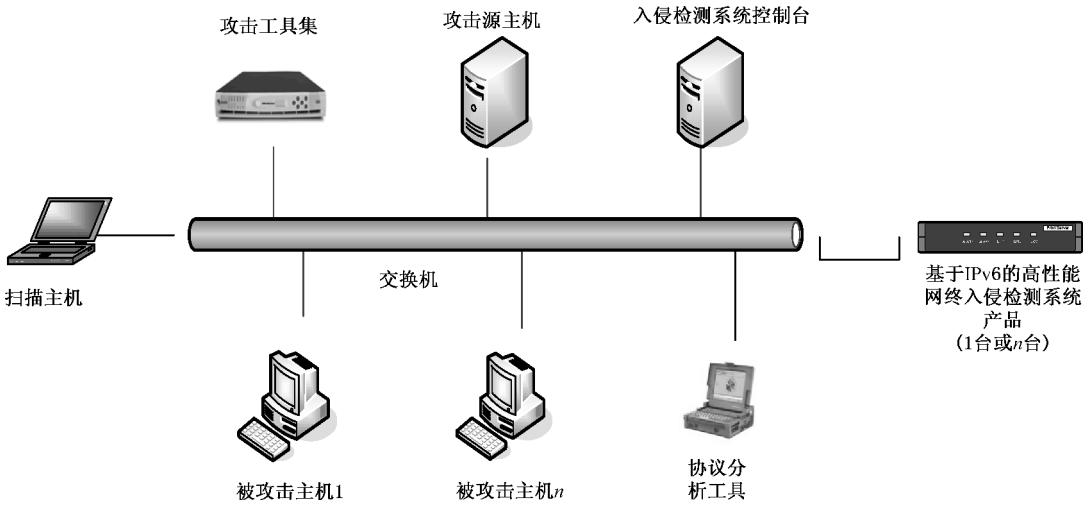

图 1　基于 IPv6 的高性能网络入侵检测系统产品典型运行环境

6　总体说明

6.1　安全技术要求分类

本标准将基于 IPv6 的高性能网络入侵检测系统产品安全技术要求分为安全功能要求、网络环境适应性要求、性能要求、安全保障要求 4 个大类。其中，安全功能要求是对基于 IPv6 的高性能网络入侵检测系统产品应具备的安全功能提出的具体要求，包括数据探测功能要求、入侵分析功能要求、入侵响应功能要求等；网络环境适应性要求是对基于 IPv6 的高性能网络入侵检测系统产品应具备的网络环境适应性提出的具体要求，包括支持纯 IPv6 网络环境和 IPv6 网络环境下自身管理等；性能要求是对基于 IPv6 的高性能网络入侵检测系统产品应具备的性能提出的具体要求，包括误报率和漏报率等；安全保障要求是针对基于 IPv6 的高性能网络入侵检测系统产品的开发和使用文档的内容提出的具体要求，例如开发、指导性文档、生命周期支持、测试、脆弱性评定等。

6.2　安全等级

基于 IPv6 的高性能网络入侵检测系统产品的安全等级按照其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　数据探测功能要求

7.1.1　数据收集

产品应具有实时获取受保护网段内用于检测分析数据包的能力。

7.1.2　协议分析

产品至少但不限于应监视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 行为监测

产品至少但不限于应监视以下攻击行为：端口扫描、强力攻击、木马后门攻击、拒绝服务攻击、缓冲区溢出攻击、IP 碎片攻击、网络蠕虫攻击等。

7.1.4 流量监测

产品应监视整个网络或者某一特定协议、地址、端口的报文流量和字节流量。

7.2 入侵分析功能要求

7.2.1 数据分析

产品应对收集的数据包进行分析，发现攻击事件。

7.2.2 分析方式

产品应以模式匹配、协议分析、人工智能等一种或多种方式进行入侵分析。

7.2.3 防躲避能力

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。

7.2.4 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。

7.2.5 事件关联

产品应具有把不同的事件关联起来，发现低危害事件中隐含的高危害攻击的能力。

7.3 入侵响应功能要求

7.3.1 安全告警

当产品检测到入侵时，应自动采取相应动作以发出安全警告。

7.3.2 告警方式

产品应能通过屏幕实时提示、E-mail、声音、短消息等方式告警。

7.3.3 排除响应

产品应允许管理员定义对被检测网段中指定的目标主机或特定的事件不予告警，降低误报。

7.3.4 定制响应

产品应允许管理员对被检测网段中指定的目标主机或特定的事件定制不同的响应方式，以对特定的事件突出告警。

7.3.5 防火墙联动

产品应具有与防火墙进行联动的能力，可按照设定的联动策略自动调整防火墙配置。

7.3.6 全局预警

产品应具有全局预警功能，通过控制台可在设定全局预警的策略后，将局部出现的重大安全事件通知其上级控制台或者下级控制台。

7.3.7 入侵管理

产品应具有全局安全事件的管理能力，可与安全管理中心或网络管理中心进行联动。

7.3.8 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）。

7.4 管理控制功能要求

7.4.1 图形界面

产品应提供图形化的管理界面用于管理、配置产品。管理配置界面应包含配置和管理产品所需的所有功能。

7.4.2 事件数据库

产品的事件数据库应包括事件定义和分析、详细的漏洞修补方案、可采取的对策等。

7.4.3 事件分级

产品应按照事件的严重程度将事件分级。

7.4.4 策略配置

产品应提供产品策略配置方法和手段。

7.4.5 产品升级

产品应具有更新、升级产品和事件库的能力。

7.4.6 统一升级

产品应提供由控制台对各探测器的事件库进行统一升级的功能。

7.4.7 分布式部署

产品应具有本地或异地分布式部署、远程管理的能力。

7.4.8 集中管理

产品应设置集中管理中心，对分布式、多级部署的入侵检测系统进行统一集中管理，形成多级管理结构。

7.4.9 同台管理

对同一个厂家生成的产品，如果同时具有网络型入侵检测系统和主机型入侵检测系统，二者宜被同一个控制台统一进行管理。

7.4.10 端口分离

产品的探测器应配备不同的端口分别用于产品管理和网络数据监听。

7.4.11 硬件失效处理

对于硬件产品，系统失效时应及时向授权管理员报警。

7.4.12 多级管理

产品应具有多级管理的能力。

7.5 检测结果处理要求

7.5.1 事件记录

产品应记录并保存检测到的入侵事件。

入侵事件信息应至少包含以下内容：事件发生时间、源地址、目的地址、危害等级、事件详细描述以及解决方案建议等。

7.5.2 事件可视化

管理员应能通过管理界面实时清晰地查看入侵事件。

7.5.3 报告生成

产品应能生成详尽的检测结果报告。

7.5.4 报告查阅

产品应具有浏览检测结果报告的功能。

7.5.5 报告输出

检测结果报告应可输出成方便管理员阅读的文件格式，如 Word 文件、HTML 文件、文本文件等。

7.6 产品灵活性要求

7.6.1 报告定制

产品应支持授权管理员按照自己的要求修改和定制报告内容。

7.6.2 窗口定义

产品应支持管理员自定义窗口显示的内容和显示方式。

7.6.3 事件定义

产品应允许授权管理员自定义事件，或者对默认提供的事件作修改，并提供定义方法。

7.6.4 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。

7.6.5 通用接口

产品应提供对外的通用接口，以便与其他安全设备（如网络管理软件、防火墙等）共享信息或规范化联动。

7.7 身份鉴别

7.7.1 管理员鉴别

产品应在管理员执行任何与安全功能相关的操作之前对管理员进行鉴别。

7.7.2 鉴别失败的处理

当管理员鉴别尝试失败连续达到指定次数后，产品应锁定该账号或登录 IP。最多失败次数仅由授权管理员设定。

7.7.3 鉴别数据保护

产品应保护鉴别数据不被未授权查阅和修改。

7.7.4 超时设置

产品应具有管理员登录超时重新鉴别功能。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管理产品。最大超时时间仅由授权管理员设定。

7.7.5 多鉴别机制

产品应提供多种鉴别方式，或者允许授权管理员执行自定义的鉴别措施，以实现多重身份鉴别措施。多鉴别机制应同时使用。

7.7.6 会话锁定

产品应允许管理员锁定自己的交互会话，锁定后需要再次进行身份鉴别才能够重新管理产品。

7.8 管理员管理

7.8.1 标识唯一性

产品应保证所设置的管理员标识全局唯一。

7.8.2 用户属性定义

产品应为每一个管理员保存安全属性表，属性应包括：管理员标识、鉴别数据、授权信息或管理组信息、其他安全属性等。

7.8.3 安全行为管理

产品应仅允许授权管理员对产品的功能具有禁止、修改的能力。

7.8.4 管理员角色

产品应设置多个角色，不同的角色具有不同的管理权限，以增加产品管理的安全性。

7.8.5 安全属性管理

产品应仅允许授权角色可以对指定的安全属性进行查询、修改、删除、改变其默认值等操作。

7.9 安全审计

7.9.1 审计数据生成

产品应能为下述可审计事件产生审计记录：审计级别以内的所有可审计事件（如鉴别失败等重大事件）等。应在每个审计记录中至少记录如下信息：事件的日期和时间、事件类型、主体身份、事件的结果（成功或失败）等。

7.9.2 审计数据可用性

审计数据的记录方式应便于管理员理解。

7.9.3 审计查阅

产品应为授权管理员提供从审计记录中读取全部审计信息的功能。

7.9.4 受限的审计查阅

除了具有明确读访问权限的授权管理员之外，产品应禁止所有非授权管理员对审计记录的读访问。

7.10 事件数据安全

7.10.1 安全数据管理

产品应仅限于指定的授权角色访问事件数据，禁止其他管理员对事件数据的操作。

7.10.2 数据存储安全

产品应在发生事件数据存储器空间将耗尽等情况时，采取措施避免最新事件数据丢失。

7.10.3 数据存储告警

产品应在发生事件数据存储器空间将耗尽等情况时，自动产生告警，并采取措施避免事件数据丢失。产生告警的剩余存储空间大小应由授权管理员自主设定。

7.11 通信安全

7.11.1 通信保密性

若产品采用远程方式管理，应保证远程管理数据保密传输；若产品由多个组件组成，应保证控制命令、传输数据等信息在组件间保密传输。

7.11.2 通信稳定性

产品应采取点到点协议等保证通信稳定性的方法，保证各部件和控制台之间传递的信息不因网络故障而丢失或延迟。

7.11.3 升级安全

产品应确保事件库和版本升级时的数据安全，应确保升级包是由开发商提供的。

7.12 产品自身安全

7.12.1 自我隐藏

产品应采取隐藏探测器 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。

7.12.2 自我监测

产品在启动和正常工作时，应周期性地或者按照授权管理员的要求执行自检，以验证产品自身执行的正确性。

8 网络环境适应性要求

8.1 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。

8.2 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。

8.3 支持 IPv6 过渡网络环境（可选）

8.3.1 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。

8.3.2 隧道

8.3.2.1 6over4

产品应支持 6over4 网络环境，能够在 6over4 网络环境下正常工作。

8.3.2.2 6to4

产品应支持 6to4 网络环境，能够在 6to4 网络环境下正常工作。

8.3.2.3 ISATAP

产品应支持 ISATAP 网络环境，保证在 ISATAP 网络环境下正常工作。

9 性能要求

9.1 误报率

产品应按照测评方法中指定的测试方法、测试工具、测试环境和测试步骤测试产品的误报率。产品应将误报率控制在应用许可范围的 15%内，不能对正常使用产品产生较大影响。

9.2 漏报率

产品应按照测评方法中指定的测试方法、测试工具、测试环境和测试步骤测试产品的漏报率，在正常网络流量和各种指定的网络背景流量下，分别测试产品未能对声称能够检测的入侵行为进行告警的数据。系统应将漏报率控制在应用许可范围的 15%内，不能对正常使用产品产生较大影响。

9.3 监控流量

产品应按照测评方法中指定的测试方法、测试工具、测试环境和测试步骤测试产品的监控流量，支持 15Gbit/s 的背景负荷量。

9.4 监控并发连接数

产品应按照测评方法中指定的测试方法、测试工具、测试环境和测试步骤测试产品的监控并发连接数，监控并发连接数大于或等于500万个/s。

9.5 监控新建TCP连接速率

产品应按照测评方法中指定的测试方法、测试工具、测试环境和测试步骤测试产品的监控新建TCP连接速率，监控新建TCP连接速率大于或等于50万/s。

9.6 还原能力

产品应对入侵行为进行内容恢复和还原；当背景数据流低于网络有效带宽的80%时，系统应保证入侵行为的获取和还原能够正常进行。

10 安全保障要求

10.1 开发

10.1.1 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。

10.1.2 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。

10.1.3 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。

10.1.4 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。

10.2 指导性文档

10.2.1 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须执行的安全策略。

10.2.2 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。

10.3 生命周期支持

10.3.1 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配置项的程序。

10.3.2 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。

10.3.3 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。

10.3.4 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。

10.3.5 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必要控制，并提供生命周期定义文档来描述用于开发和维护产品的模型。

10.3.6 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表示中每个语句的含义和所有依赖于实现的选项的含义。

10.4 测试

10.4.1 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。

10.4.2 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。

10.4.3 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测试结果的一致性。

10.4.4 独立测试

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

10.5 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。

11 不同安全等级的要求

11.1 安全功能要求

不同安全等级的基于 IPv6 的高性能网络入侵检测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 的高性能网络入侵检测系统产品的安全功能要求

安全功能要求		基本级	增强级
数据探测功能要求	数据收集	7.1.1	7.1.1
	协议分析	7.1.2	7.1.2
	行为监测	7.1.3	7.1.3
	流量监测	7.1.4	7.1.4
入侵分析功能要求	数据分析	7.2.1	7.2.1
	分析方式	7.2.2	7.2.2
	防躲避能力	—	7.2.3
	事件合并	—	7.2.4
	事件关联	—	7.2.5
入侵响应功能要求	安全告警	7.3.1	7.3.1
	告警方式	7.3.2	7.3.2
	排除响应	—	7.3.3
	定制响应	—	7.3.4
	防火墙联动	—	7.3.5
	全局预警	—	7.3.6
	入侵管理	—	7.3.7
	事件定位	—	7.3.8
管理控制功能要求	图形界面	7.4.1	7.4.1
	事件数据库	7.4.2	7.4.2
	事件分级	7.4.3	7.4.3
	策略配置	7.4.4	7.4.4
	产品升级	7.4.5	7.4.5
	统一升级	7.4.6	7.4.6
	分布式部署	—	7.4.7
	集中管理	—	7.4.8

表 1（续）

安全功能要求		基本级	增强级
管理控制功能要求	同台管理	—	7.4.9
	端口分离	—	7.4.10
	硬件失效处理	—	7.4.11
	多级管理	—	7.4.12
检测结果处理要求	事件记录	7.5.1	7.5.1
	事件可视化	7.5.2	7.5.2
	报告生成	7.5.3	7.5.3
	报告查阅	7.5.4	7.5.4
	报告输出	7.5.5	7.5.5
产品灵活性要求	报告定制	7.6.1	7.6.1
	窗口定义	—	7.6.2
	事件定义	—	7.6.3
	协议定义	—	7.6.4
	通用接口	—	7.6.5
身份鉴别	管理员鉴别	7.7.1	7.7.1
	鉴别失败的处理	7.7.2	7.7.2
	鉴别数据保护	7.7.3	7.7.3
	超时设置	—	7.7.4
	多鉴别机制	—	7.7.5
	会话锁定	—	7.7.6
管理员管理	标识唯一性	7.8.1	7.8.1
	用户属性定义	7.8.2	7.8.2
	安全行为管理	7.8.3	7.8.3
	管理员角色	—	7.8.4
	安全属性管理	—	7.8.5
安全审计	审计数据生成	7.9.1	7.9.1
	审计数据可用性	7.9.2	7.9.2
	审计查阅	7.9.3	7.9.3
	受限的审计查阅	7.9.4	7.9.4
事件数据安全	安全数据管理	7.10.1	7.10.1
	数据存储安全	—	7.10.2
	数据存储告警	—	7.10.3

表 1（续）

安全功能要求		基本级	增强级
通信安全	通信保密性	7.11.1	7.11.1
	通信稳定性	7.11.2	7.11.2
	升级安全	7.11.3	7.11.3
产品自身安全	自我隐藏	7.12.1	7.12.1
	自我监测	7.12.2	7.12.2

11.2 安全保障要求

不同安全等级的基于 IPv6 的高性能网络入侵检测系统产品的安全保障要求如表 2 所示。

表 2 不同安全等级的基于 IPv6 的高性能网络入侵检测系统产品的安全保障要求

安全功能要求		基本级	增强级
开发	安全架构	10.1.1	10.1.1
	功能规范	10.1.2 a)～f)	10.1.2
	实现表示	—	10.1.3
	产品设计	10.1.4 a)～d)	10.1.4
指导性文档	操作用户指南	10.2.1	10.2.1
	准备程序	10.2.2	10.2.2
生命周期支持	配置管理能力	10.3.1a)～c)	10.3.1
	配置管理范围	10.3.2a)	10.3.2
	交付程序	10.3.3	10.3.3
	开发安全	—	10.3.4
	生命周期定义	—	10.3.5
	工具和技术	—	10.3.6
测试	测试覆盖	10.4.1a)	10.4.1
	测试深度	—	10.4.2
	功能测试	10.4.3	10.4.3
	独立测试	10.4.4	10.4.4
脆弱性评定		10.5a)	10.5b)

中华人民共和国公共安全
行业标准
信息安全技术 基于IPv6的高性能网络入侵检测系统产品安全技术要求
GA/T 1728—2020
*
中国标准出版社出版发行
北京市朝阳区和平里西街甲2号(100029)
北京市西城区三里河北街16号(100045)
网址:www.spc.org.cn
服务热线:400-168-0010
2020年10月第一版
*
书号:155066·2-35613

GA/T 1728-2020