ICS 35.240
A 90

GA

中华人民共和国公共安全行业标准

GA/T 1557—2019

信息安全技术　基于 IPv6 的高性能网络审计系统产品安全技术要求

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

2019-04-16 发布　　2019-04-16 实施

中华人民共和国公安部　　发 布

目　　次

前言 …… Ⅰ
1　范围 …… 1
2　规范性引用文件 …… 1
3　术语和定义 …… 1
4　IPv6 网络审计产品描述 …… 2
5　总体说明 …… 3
5.1　安全技术要求分类 …… 3
5.2　安全等级划分 …… 3
6　安全功能要求 …… 3
6.1　信息采集 …… 3
6.2　数据还原 …… 3
6.3　审计记录统计 …… 4
6.4　审计记录分析处理 …… 5
6.5　管理控制要求 …… 6
6.6　标识与鉴别 …… 6
6.7　审计日志 …… 7
6.8　安全管理 …… 7
6.9　数据存储 …… 8
7　环境适应性要求 …… 9
7.1　接入方式 …… 9
7.2　IPv6 协议一致性 …… 9
7.3　IPv6 应用环境适应性 …… 9
7.4　IPv6 管理环境适应性 …… 9
8　性能要求 …… 9
8.1　处理能力 …… 9
8.2　网络影响 …… 9
9　安全保障要求 …… 9
9.1　开发 …… 9
9.2　指导性文档 …… 10
9.3　生命周期支持 …… 11
9.4　测试 …… 11
9.5　脆弱性评定 …… 12
10　不同安全等级要求 …… 12
10.1　安全功能要求 …… 12
10.2　安全保障要求 …… 13

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、公安部网络安全保卫局。

本标准主要起草人：唐迪、王志佳、马海燕、范春玲、俞优、邹春明、顾健。

信息安全技术　基于IPv6的高性能网络审计系统产品安全技术要求

1　范围

本标准规定了基于IPv6的高性能网络审计系统产品的安全功能要求、环境适应性要求、性能要求、安全保障要求和等级划分要求。

本标准适用于基于IPv6的高性能网络审计系统产品的设计、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 20945—2013　信息安全技术　信息系统安全审计产品技术要求和测试评价方法

GB/T 25069—2010　信息安全技术　术语

GA/T 695—2014　信息安全技术　网络通信审计产品技术要求

3　术语和定义

GB/T 18336.3—2015、GB/T 20945—2013、GB/T 25069—2010和GA/T 695—2014界定的以及下列术语和定义适用于本文件。

3.1

基于IPv6的高性能网络审计系统产品　IPv6-based high performance network audit system product

对网络通信进行记录和分析，并针对特定事件采用相应的动作，同时支持IPv4协议、IPv6协议及过度技术，并具有高性能的产品。

3.2

IPv6过渡技术　IPv6 transition technology

用于IPv4向IPv6演进的过渡期内，保证业务共存和互操作的技术。

3.3

IPv4/IPv6隧道技术　IPv4/IPv6 tunneling technology

基于IPv4隧道来传送IPv6数据报文的隧道技术。

3.4

双协议栈技术　dual protocol stack technology

在一台设备上同时启用IPv4协议栈和IPv6协议栈。

3.5

IPv4/IPv6网络地址转换　IPv4/IPv6 network address translation

通过对数据包的转换实现了在网络过渡期IPv4节点和IPv6节点之间的互相访问。