



中华人民共和国公共安全行业标准

GA/T 1390.8—2025

信息安全技术 网络安全等级保护 基本要求 第8部分:IPv6网络安全 扩展要求

Information security technology—Baseline for classified protection of
cybersecurity—Part 8: Extended requirements for IPv6 network security

2025-10-13 发布

2026-02-01 实施

中华人民共和国公安部 发布

目 次

前言	Ⅲ
引言	Ⅳ
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 概述	2
5.1 IPv6 over IPv4	2
5.2 IPv4 over IPv6	2
5.3 双栈	2
5.4 单栈	2
6 第一级安全要求	3
6.1 安全通信网络	3
6.2 安全区域边界	3
6.3 安全建设管理	3
6.4 安全运维管理	3
7 第二级安全要求	3
7.1 安全通信网络	3
7.2 安全区域边界	3
7.3 安全计算环境	4
7.4 安全建设管理	4
7.5 安全运维管理	4
8 第三级安全要求	4
8.1 安全通信网络	4
8.2 安全区域边界	5
8.3 安全计算环境	5
8.4 安全建设管理	5
8.5 安全运维管理	5
9 第四级安全要求	5
9.1 安全通信网络	5
9.2 安全区域边界	6
9.3 安全计算环境	6

9.4 安全建设管理6

9.5 安全运维管理6

10 第五级安全要求7

附录A(资料性) IPv6网络攻击列表8

参考文献9

前 言

本文件按照 GB/T 1.1—2020《标准化工作导则 第 1 部分：标准化文件的结构和起草规则》的规定起草。

本文件是 GA/T 1390《信息安全技术 网络安全等级保护基本要求》的第 8 部分。GA/T 1390 已经发布了以下部分：

- 第 2 部分：云计算安全扩展要求；
- 第 3 部分：移动互联安全扩展要求；
- 第 5 部分：工业控制系统安全扩展要求；
- 第 6 部分：边缘计算安全扩展要求；
- 第 7 部分：大数据系统安全扩展要求；
- 第 8 部分：IPv6 网络安全扩展要求；
- 第 9 部分：区块链安全扩展要求。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由公安部网络安全保卫局提出。

本文件由公安部信息系统安全标准化技术委员会归口。

本文件起草单位：公安部第三研究所、公安部网络安全保卫局、公安部第一研究所、清华大学网络科学与网络空间研究院、新华三技术有限公司、华为技术有限公司、昆仑数智科技有限责任公司、联通数字科技有限公司、北京金易星安信息技术有限公司。

本文件主要起草人：朱建兴、陈广勇、赵劲涛、任娟娟、陈建伟、郭丽丹、宫月、敖日格勒、丁闫、万晓兰、刘保君、周世杰、毛盾、刘金刚、王飞。

引 言

GA/T 1390《信息安全技术 网络安全等级保护基本要求》旨在提出不同网络安全保护等级的基线安全要求,指导等级保护对象的安全建设和监督管理。GA/T 1390 拟由以下部分组成。

- 第 1 部分:安全通用要求。旨在提出适用于所有网络安全等级保护对象的安全基线要求。
- 第 2 部分:云计算安全扩展要求。旨在提出适用于云计算平台/系统的安全扩展要求。
- 第 3 部分:移动互联安全扩展要求。旨在提出适用于采用移动互联技术的等级保护对象的安全扩展要求。
- 第 4 部分:物联网安全扩展要求。旨在提出适用于物联网的安全扩展要求。
- 第 5 部分:工业控制系统安全扩展要求。旨在提出适用于工业控制系统的安全扩展要求。
- 第 6 部分:边缘计算安全扩展要求。旨在提出适用于采用边缘计算技术的等级保护对象的安全扩展要求。
- 第 7 部分:大数据系统安全扩展要求。旨在提出适用于采用大数据技术的等级保护对象的安全扩展要求。
- 第 8 部分:IPv6 网络安全扩展要求。旨在提出适用于 IPv6 等级保护对象的安全扩展要求。
- 第 9 部分:区块链安全扩展要求。旨在提出适用于区块链等级保护对象的安全扩展要求。
- 第 10 部分:生成式人工智能安全扩展要求。旨在提出适用于生成式人工智能等级保护对象的安全扩展要求。
- 第 11 部分:低空智联网安全扩展要求。旨在提出适用于低空智联网等级保护对象的安全扩展要求。
- 第 12 部分:智能车联网安全扩展要求。旨在提出适用于智能车联网等级保护对象的安全扩展要求。

信息安全技术 网络安全等级保护 基本要求 第8部分:IPv6网络安全 扩展要求

1 范围

本文件规定了 IPv6 网络等级保护对象的网络安全等级保护第一级到第四级的安全扩展要求。

本文件适用于 IPv6 网络等级保护对象的安全建设和监督管理。

注:第五级 IPv6 网络等级保护对象不在本文件中进行描述。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中,注日期的引用文件,仅该日期对应的版本适用于本文件;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 22239—2019 信息安全技术 网络安全等级保护基本要求

GB/T 44810(所有部分) IPv6 网络安全设备技术要求

3 术语和定义

GB/T 22239—2019 界定的以及下列术语和定义适用于本文件。

3.1

IPSec 协议 **Internet protocol security**

开放标准的框架结构,通过使用加密的安全服务以确保在公开网络上进行保密而安全的通信,能从端至端的层面上提供数据完整性保护、数据源鉴别、载荷机密性和抗重放攻击等安全服务。

[来源:GB/T 36968—2018,3.4]

3.2

IPv6 网络 **IPv6 network**

基于互联网协议第 6 版编址方案构建的网络。

3.3

网络切片 **network slicing**

IP 网络为给特定的用户或业务提供专用或共享的网络资源和网络能力,以满足不同的用户和业务差异化连接需求和质量保证。

[来源:YD/T 4267—2023,3.1]

3.4

随流检测 **in-situ flow information telemetry**

通过正常的业务流量检测网络性能。

注:如网络的真实丢包率、时延等性能指标。

4 缩略语

下列缩略语适用于本文件。

DAD:重复地址检测(Duplicate Address Detection)

DNS64:IPv4 与 IPv6 过渡的域名系统(Domain Name System 64)

DS-Lite:轻型双栈(Dual-Stack Lite)

GRE:通用路由封装协议(Generic Routing Encapsulation)

ICMPv6:互联网控制报文协议第六版(Internet Control Message Protocol version 6)

IPv4:互联网协议第四版(Internet Protocol version 4)

IPv6:互联网协议第六版(Internet Protocol version 6)

L3VPN:三层虚拟专用网络(Layer 3 Virtual Private Network)

MPLS:多协议标签交换(Multiprotocol Label Switching)

MTU:路径最大传输单元(Maximum Transmission Unit)

NAT64:IPv4 与 IPv6 过渡的网络地址转换技术(Network Address Translation 64)

NDP:邻居发现协议(Neighbor Discovery Protocol)

SRv6:基于 IPv6 的分段路由技术(Segment Routing over IPv6)

5 概述

5.1 IPv6 over IPv4

在 IPv4 向 IPv6 的过渡初期,IPv4 网络已大量部署,IPv6 over IPv4 是通过隧道技术,使 IPv6 报文在 IPv4 网络中传输,从而实现通过 IPv6 将各相对独立的 IPv6 网络互连。但由于 IPv4 网络无法验证源地址的真实性,攻击者可以将伪造的隧道报文注入目的网络中。

5.2 IPv4 over IPv6

在 IPv4 向 IPv6 过渡的后期,IPv6 网络已被大量部署,IPv4 over IPv6 是通过隧道技术,使 IPv4 报文在 IPv6 网络中传输,从而实现通过 IPv6 将各相对独立的 IPv4 网络互连。但由于 IPv4 over IPv6 不对隧道封装的内容进行检查,攻击者可以将 IPv4 流量承载在 IPv6 报文中,导致原来 IPv4 网络的攻击流量经由 IPv6 的封装后无法被检测进而带来安全风险。

5.3 双栈

双栈技术是指在涉及网站业务交互的各类应用系统、网络设备、运营支撑系统的软硬件设备中同时运行 IPv4 和 IPv6 两套协议栈,能够同时处理 IPv4 和 IPv6 数据包。由于双栈部署的网络中同时运行着 IPv4、IPv6 两个逻辑通道,会增加设备或系统的暴露面,网关类防护设备也需同时配置双栈策略,在一定程度上增加了策略管理的复杂度。另外,双栈系统的复杂性也会增加网络节点的数据转发负担,导致网络节点的故障率增加。

5.4 单栈

IPv6 单栈网络就是在网络中关闭 IPv4 协议栈并以 IPv6 协议为核心进行编址、路由和转发的网络。

6 第一级安全要求

6.1 安全通信网络

在网络架构方面应为 IPv6 网络中的主机合理规划并分配具备真实性的可溯源的地址。

6.2 安全区域边界

入侵防范应满足以下要求：

- a) 针对 ICMPv6 报文、NDP 协议部署必要的源验证及安全认证机制或报文抑制机制,对非法报文进行过滤和阻断;
- b) 限制转发 IPv6 路由扩展报文头内的报文,或在网络边界对扩展报文进行过滤。

6.3 安全建设管理

采购和使用的安全产品应符合 GB/T 44810(所有部分)的要求。

6.4 安全运维管理

应编制并保存与保护对象相关的资产清单,包括 IPv6 地址等内容。

7 第二级安全要求

7.1 安全通信网络

7.1.1 网络架构

应为 IPv6 网络中的主机合理规划并分配具备真实性的可溯源的地址。

7.1.2 通信传输

通信传输应满足以下要求：

- a) 采用 IPv6 over IPv4、NAT64、DNS64、DS-Lite 等技术保障与 IPv6 网络间的连通性;
- b) 在隧道场景下,如 SRv6、GRE,实现对流量的检测和防护,其部署不能影响网络切片、随流检测等功能。

7.2 安全区域边界

7.2.1 访问控制

访问控制应满足以下要求：

- a) 采用技术手段实现网络上数据报文源地址真实性;
- b) 采用双栈技术的 IPv6 网络,建立至少与 IPv4 协议栈等同的访问控制策略;
- c) 访问控制措施涵盖 IPv6 MPLS L3VPN、IPv6 over IPv4、IPv4 over IPv6、IPv6 over IPv4 GRE、IPv4 over IPv6 GRE 等所有网络场景;
- d) 在 NAT64、DNS64、DS-Lite 等网络地址转换的网络环境下,在网络关键节点配置与 IPv4 协议相同的访问控制策略。

7.2.2 入侵防范

入侵防范应满足以下要求：

- a) 针对 ICMPv6 报文、NDP 协议部署必要的源验证及安全认证机制或报文抑制机制,对非法报文进行过滤和阻断;
- b) 在不影响业务应用的前提下,限制转发 IPv6 路由扩展报文头内的报文,或在网络边界对扩展报文进行过滤;
- c) 能够检测针对 IPv6 网络特有的攻击,如 NDP 攻击、DAD 攻击等,详见附录 A。

7.3 安全计算环境

安全计算环境应满足以下要求：

- a) 发现在 IPv6 网络内可能存在的已知漏洞,并在经过充分测试评估后,及时修补漏洞;
- b) 能够检测到对 IPv6 网络内重要节点进行入侵的行为,并在发生入侵事件时提供告警。

7.4 安全建设管理

采购和使用的安全产品应符合 GB/T 44810(所有部分)的要求。

7.5 安全运维管理

7.5.1 资产管理

应编制并保存与保护对象相关的资产清单,包括 IPv6 地址等内容。

7.5.2 密码管理

应实现 IPv6 网络环境下对密钥的产生、分发、存储、使用、更新、归档、撤销、备份、恢复和销毁等环节的管理。

7.5.3 应急预案管理

应制定针对 IPv6 网络拒绝服务攻击、NDP 攻击等场景的应急预案,如,包括应急处理流程、系统恢复流程等内容。

8 第三级安全要求

8.1 安全通信网络

8.1.1 网络架构

应为 IPv6 网络中的主机合理规划并分配具备真实性的可溯源的地址。

8.1.2 通信传输

通信传输应满足以下要求：

- a) 在通信前实现不同 IPv6 网络间的双向认证;
- b) 在不同 IPv6 网络间采用 IPSec 等协议实现通信过程中数据的完整性及保密性;
- c) 采用 IPv6 over IPv4、NAT64、DNS64、DS-Lite 等技术保障与 IPv6 网络间的连通性;
- d) 在隧道场景下,如 SRv6、GRE,实现对流量的检测和防护,其部署不能影响网络切片、随流检测等功能。

8.2 安全区域边界

8.2.1 访问控制

访问控制应满足以下要求：

- a) 采用技术手段实现网络上数据报文源地址真实性；
- b) 采用双栈技术的IPv6网络,建立至少与IPv4协议栈等同的访问控制策略；
- c) 访问控制措施涵盖IPv6 MPLS L3VPN、IPv6 over IPv4、IPv4 over IPv6、IPv6 over IPv4 GRE、IPv4 over IPv6 GRE等所有网络场景；
- d) 在NAT64、DNS64、DS-Lite等网络地址转换的网络环境下,在网络关键节点配置与IPv4协议相同的访问控制策略。

8.2.2 入侵防范

入侵防范应满足以下要求：

- a) 针对ICMPv6报文、NDP协议部署必要的源验证及安全认证机制或报文抑制机制,对非法报文进行过滤和阻断；
- b) 在不影响业务应用的前提下,限制转发IPv6路由扩展报文头内的报文,或在网络边界对扩展报文进行过滤；
- c) 能够检测、限制或阻断针对IPv6网络特有的攻击,如NDP攻击、DAD攻击等,详见附录A。

8.3 安全计算环境

安全计算环境应满足以下要求：

- a) 发现在IPv6网络内可能存在的已知漏洞,并在经过充分测试评估后,及时修补漏洞；
- b) 能够检测到对IPv6网络内重要节点进行入侵的行为,并在发生入侵事件时提供告警和阻断。

8.4 安全建设管理

采购和使用的安全产品应符合GB/T 44810(所有部分)的要求。

8.5 安全运维管理

8.5.1 资产管理

应编制并保存与保护对象相关的资产清单,包括IPv6地址等内容。

8.5.2 密码管理

应实现IPv6网络环境下对密钥的产生、分发、存储、使用、更新、归档、撤销、备份、恢复和销毁等环节的管理。

8.5.3 应急预案管理

应制定IPv6网络环境下重要事件的应急预案,包括应急处理流程、系统恢复流程等内容。

9 第四级安全要求

9.1 安全通信网络

9.1.1 网络架构

应为IPv6网络中的主机合理规划并分配具备真实性的可溯源的地址。

9.1.2 通信传输

通信传输应满足以下要求：

- a) 在通信前实现不同 IPv6 网络间的双向认证；
- b) 在不同 IPv6 网络间采用 IPSec 等协议实现通信过程中数据的完整性及保密性；
- c) 采用 IPv6 over IPv4、NAT64、DNS64、DS-Lite 等技术保障与 IPv6 网络间的连通性；
- d) 在隧道场景下，如 SRv6、GRE，实现对流量的检测和防护，其部署不能影响网络切片、随流检测等功能。

9.2 安全区域边界

9.2.1 访问控制

访问控制应满足以下要求：

- a) 采用技术手段实现网络上数据报文源地址真实性；
- b) 采用双栈技术的 IPv6 网络，建立至少与 IPv4 协议栈等同的访问控制策略；
- c) 访问控制措施涵盖 IPv6 MPLS L3VPN、IPv6 over IPv4、IPv4 over IPv6、IPv6 over IPv4 GRE、IPv4 over IPv6 GRE 等所有网络场景；
- d) 在 NAT64、DNS64、DS-Lite 等网络地址转换的网络环境下，在网络关键节点配置与 IPv4 协议相同的访问控制策略。

9.2.2 入侵防范

入侵防范应满足以下要求：

- a) 针对 ICMPv6 报文、NDP 协议部署必要的源验证及安全认证机制或报文抑制机制，对非法报文进行过滤和阻断；
- b) 在不影响业务应用的前提下，限制转发 IPv6 路由扩展报文头内的报文，或在网络边界对扩展报文进行过滤；
- c) 能够检测、限制或阻断针对 IPv6 网络特有的攻击，如 NDP 攻击、DAD 攻击等，详见附录 A；
- d) IPv6 网络内设备均使用经过允许的接入地址，建立允许通信的地址清单，针对 IPv6 地址段进行地址过滤，并阻断 IPv6 仿冒地址接入。

9.3 安全计算环境

安全计算环境应满足以下要求：

- a) 发现在 IPv6 网络内可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞；
- b) 能够检测到对 IPv6 网络内重要节点进行入侵的行为，并在发生入侵事件时提供告警和阻断。

9.4 安全建设管理

采购和使用的安全产品应符合 GB/T 44810(所有部分)的要求。

9.5 安全运维管理

9.5.1 资产管理

应编制并保存与保护对象相关的资产清单，包括 IPv6 地址等内容。

9.5.2 密码管理

应实现 IPv6 网络环境下对密钥的产生、分发、存储、使用、更新、归档、撤销、备份、恢复和销毁等环节的管理。

9.5.3 应急预案管理

应制定 IPv6 网络环境下重要事件的应急预案,包括应急处理流程、系统恢复流程等内容。

10 第五级安全要求

略。

附 录 A
(资料性)
IPv6 网络攻击列表

IPv6 网络攻击是指通过互联网或局域网对 IPv6 网络资源、网络系统及相关信息进行非法、破坏性攻击的行为。IPv6 网络主要攻击类型见表 A.1。

表 A.1 IPv6 网络攻击

名称	目标
NDP 攻击	攻击者基于五种类型的 ICMPv6 消息,实现地址解析,重复地址检测,路由器发现以及路由重定向等功能。ND 协议的协议功能、实现原理均与 IPv4 中的 ARP 类似,同样,在 IPv4 中对 ARP 的某些攻击方式也适用于 ND 协议
DAD 攻击	攻击者通过 NS 或 NA 报文进行干扰,使得受害主机的 DAD 过程失败,无法获取到 IP 地址
IPv6 扩展头攻击	攻击者通过构造包含异常数量扩展头的报文对防火墙进行 DOS 攻击
IPv6 分片攻击	攻击者借助端系统对 IP 数据包进行分段与重组的功能构造恶意数据包
IPv6 源地址泛洪攻击	原理同 IPv4 泛洪攻击
IPv6 路由协议攻击	在 IPv6 网络环境下,由于部分路由协议仅是扩展而来,机制并未发生变化,因此路由攻击依旧存在
IPv6 仿冒伪造攻击	攻击者伪造 IPv6 地址,使得通信双方误认为他们在直接通信,实际上攻击者在中间拦截并篡改了通信内容

参 考 文 献

- [1] GB/T 22240—2020 信息安全技术 网络安全等级保护定级指南
- [2] GB/T 25069—2022 信息安全技术 术语
- [3] GB/T 25070—2019 信息安全技术 网络安全等级保护安全设计技术要求
- [4] GB/T 28448—2019 信息安全技术 网络安全等级保护测评要求
- [5] GB/T 36968—2018 信息安全技术 IPSec VPN技术规范
- [6] GB/T 43844—2024 IPv6地址分配和编码规则 接口标识符
- [7] GA/T 1542—2019 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
- [8] 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
- [9] GA/T 1558—2019 信息安全技术 基于IPv6的高性能网络脆弱性扫描产品安全技术要求
- [10] GA/T 1728—2020 信息安全技术 基于IPv6的高性能网络入侵监测系统产品安全技术要求
- [11] YD/T 1341—2005 IPv6基本协议-IPv6协议
- [12] YD/T 1343—2005 IPv6邻居发现协议-基于IPv6的邻居发现协议
- [13] YD/T 1344—2005 IPv6地址结构协议-IPv6无状态地址自动配置
- [14] YD/T 2169—2010 IPv6技术要求-IPv6路径最大传输单元发现协议
- [15] YD/T 4267—2023 IP网络切片总体架构与技术要求
- [16] RFC 2766 Network Address Translation-Protocol Translation (NAT-PT)
- [17] RFC 3715:IPsec-Network Address Translation (NAT)Compatibility Requirements
- [18] RFC 4301:Security Architecture for the Internet Protocol
- [19] RFC 4303:IP Encapsulating Security Payload (ESP)

中华人民共和国公共安全
行业标准
信息安全技术 网络安全等级保护
基本要求 第8部分:IPv6网络安全
扩展要求

GA/T 1390.8—2025

*

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)

网址 www.spc.net.cn

总编室:(010)68533533 发行中心:(010)51780238

读者服务部:(010)68523946

中国标准出版社秦皇岛印刷厂印刷

各地新华书店经销

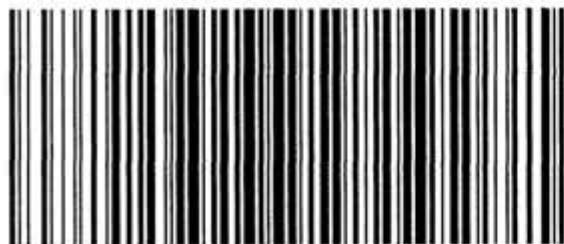
*

开本 880×1230 1/16 印张 1 字数 21 千字
2025 年 12 月第 1 版 2025 年 12 月第 1 次印刷

*

书号: 155066 • 2-39570 定价 31.00 元

如有印装差错 由本社发行中心调换
版权专有 侵权必究
举报电话:(010)68510107



GA/T 1390.8-2025