ICS 33.050
CCS M 30

团　体　标　准

T/TAF 219—2024

网络设备密码应用技术要求
入侵检测设备

Cryptography application technical requirement for network devices—
Intrusion detection devices

2024-02-23 发布　　2024-02-23 实施

电信终端产业协会　发布

目　　次

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。

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。

本文件由电信终端产业协会（TAF）提出并归口。

本文件起草单位：中国信息通信研究院、华为技术有限公司、中兴通讯股份有限公司、新华三技术有限公司、北京天融信网络安全技术有限公司、郑州信大捷安信息技术股份有限公司、启明星辰信息技术集团股份有限公司、博鼎实华(北京)技术有限公司。

本文件主要起草人：刘雅闻、张治兵、吴荣春、陈泽、陈鹏、周继华、王健，孙松儿、毕程、安高峰、韩思、管志遥、刘为华、刘献伦、陈萧宇、安锦程、刘向东。

引　　言

密码技术是网络安全的核心技术，是信息保护和网络信息体系建设的基础，是保障网络空间安全的关键技术。为推进《网络安全法》的落地实施，本文件提出入侵检测设备密码应用应满足的相关技术要求。

网络设备密码应用技术要求　入侵检测设备

1　范围

本文件规定了入侵检测设备在软件/固件安全、身份鉴别、访问控制、网络通信安全、数据安全、计算安全等方面的密码应用技术的技术要求。

本文件适用于在我国境内销售或提供的入侵检测设备（指包含网络入侵检测系统的硬件设备），也可为网络运营者采购入侵检测设备时提供依据，还适用于指导入侵检测设备的研发、测试等工作。

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 20275—2020　信息安全技术　网络入侵检测系统技术要求和测试评价方法

GB/T 25069—2022　信息安全技术　术语

GB/T 32915—2016　信息安全技术　二元序列随机性检测方法

GM/T 0005—2021　随机性检测规范

3　术语和定义

GB/T 25069—2022界定的以及下列术语和定义适用于本文件。

3.1

网络入侵检测系统　network-based instrusion detection system

是以网络上的数据包作为数据源，监听所保护网络节点的所有数据包并进行分析，从而发现异常行为的产品。

[来源：GB/T 20275—2021，5]

3.2

加密　encipherment/encryption

对数据进行密码变换以产生密文的过程。

3.3

解密　decipherment/decryption

对密文进行密码变换以产生数据的过程。

3.4

密钥　key

控制密码算法运算的关键信息或参数。

3.5

保密性 confidentiality

保证信息不被泄露给非授权的个人、进程等实体的性质。

3.6

数据完整性 data integrity

数据没有遭受以非授权方式所作的篡改或破坏的性质。

3.7

不可否认性 non-repudiation

证明一个已经发生的操作行为无法否认的性质。

3.8

重要数据 important data

主要指支持入侵检测设备自身运行管理所涉及的重要信息，主要包括身份鉴别信息、访问控制信息、配置信息、日志信息、升级数据、远程配置指令、告警信息、密钥等，具体参见附录A。

3.9

可信计算环境 trusted computing environment

基于硬件级隔离及安全启动机制，为确保安全敏感应用相关数据和代码的机密性、完整性、真实性和不可否认性目标构建的一种软件运行环境。

3.10

固件 firmware

写入EPROM（可擦写可编程只读存储器）或EEPROM(电可擦可编程只读存储器)中的程序。

4 缩略语

下列缩略语适用于本文件：

HTTPS：超文本传输安全协议（Hypertext Transfer Protocol Secure）

IPSec：互联网安全协议（Internet Protocol Security）

Netconf：网络配置协议（Network Configuration Protocol）

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

SSH：安全外壳协议（Secure Shell）

SSL：安全套接层（Secure Socket Layer）

VPN：虚拟专用网络(Virtual Private Network)

5 入侵检测设备密码应用技术要求

5.1 基本要求

入侵检测设备基本要求如下：

a) 应包含密钥产生、密钥存储、密钥使用、密钥更新等功能；
b) 应按照密钥更新周期要求更新密钥；
c) 应有安全措施防止密钥的泄露和替换；
d) 首次使用公钥前，应对证书有效性进行验证；
e) 涉及到使用随机数时，应符合GB/T 32915—2016，显著性水平参考GM/T 0005—2021；
f) 设备使用的密码技术（指本文件规定范围内的密码应用技术）应支持使用安全强度较高的密码算法，不宜使用安全强度弱的密码算法。

5.2 软件/固件安全

入侵检测设备软件/固件安全要求如下：

a) 升级时，应使用密码技术保证软件/固件升级包的完整性与来源真实性；
b) 可使用密码技术保证软件/固件保密性；
c) 可使用密码技术来保证软件/固件完整性；
d) 可使用密码技术保证软件/固件抵御常见的攻击，如反编译、重打包等；
e) 启动时，可使用密码技术保证软件/固件的完整性。

5.3 身份鉴别

入侵检测设备身份鉴别要求如下：

a) 应使用密码技术对访问入侵检测设备的终端、软件或用户进行身份鉴别，必要时使用密码技术进行双向身份鉴别；
b) 应支持使用密码技术保证身份鉴别信息传输过程中的保密性；
c) 应支持使用密码技术保证身份鉴别信息存储过程中的保密性；
d) 可使用密码技术保证身份鉴别信息传输过程中的完整性；
e) 可使用密码技术保证身份鉴别信息存储过程中的完整性；
f) 可使用密码技术来抵御常见的重放攻击，如伪随机数等。

5.4 访问控制

入侵检测设备访问控制要求如下：

a) 可使用密码技术实现访问控制功能，如数字证书等；
b) 可使用密码技术保证访问控制信息的完整性。

5.5 网络通信安全

入侵检测设备网络通信安全要求如下：

a) 远程管理时，应支持使用密码技术建立可信信道/可信路径；
    1) 在支持web管理时，应支持HTTPS，并避免使用安全强度弱的密码算法与加密模式；
    2) 在支持SSH管理时，应支持SSHv2，并避免使用安全强度弱的密码算法与加密模式；
    3) 在支持SNMP管理时，应支持SNMPv3，应使用authPriv（SNMPv3的一种安全级别，既认证又加密）模式；
    4) 在支持Netconf管理时，安全传输层应避免使用安全强度弱的密码算法与加密模式。
b) 在使用IPSec VPN或SSL VPN时，应避免使用安全强度弱的密码算法与加密模式；
c) 应使用密码技术保证路由协议认证功能的安全；

d) 可使用通信数据加密再传输的方式保证信息不被泄露。

5.6 数据安全

入侵检测设备数据安全要求如下：

a) 应使用密码技术保证远程配置指令在传输过程中的保密性与完整性，如接受集中管理平台管理或与其他安全设备联动时下发的安全策略等；
b) 应使用密码技术保证告警信息在传输过程中的完整性，如向集中管理平台上报的安全事件、故障告警等；
c) 可使用密码技术保证配置信息、日志信息等重要数据在传输过程中的保密性和完整性；
d) 可使用密码技术保证配置信息、日志信息等重要数据在存储过程中的保密性和完整性；
e) 可使用密码技术保证设备抵御常见的攻击，防止密钥等重要数据泄露，如计时攻击等。

5.7 计算安全

入侵检测设备计算安全要求如下：

a) 可使用可信计算技术建立可信计算环境；
b) 可使用密码技术对重要可执行程序进行完整性保护，并对其来源进行真实性验证。

附 录 A
（资料性）
重要数据说明

表 A.1 中列举了入侵检测设备涉及的重要数据。重要数据包括但不限于身份鉴别信息、访问控制信息、配置信息、日志信息、升级数据、远程配置指令、密钥等。

表A.1 入侵检测设备涉及的重要数据示例

序号	重要数据类型	备注
1	访问控制信息	系统访问控制策略、重要信息敏感资源标记等
2	身份鉴别信息	如用户口令、生物特征等
3	配置信息	系统启动时对程序进行配置的信息，如服务端口、数据库连接信息、线程池信息等
4	远程配置指令	远程配置安全策略等
5	升级数据	特征库、规则文件、系统/软件升级包等
6	告警信息	设备故障信息、安全事件告警信息等
7	日志信息	系统操作审计日志、访问日志、系统安全日志等
8	密钥	私钥、对称密钥等

参 考 文 献

[1] GB/T 39786—2021 信息安全技术 信息系统密码应用基本要求
[2] GB/T 37092—2018 信息安全技术 密码模块安全要求
[3] GB/T 22239—2019 信息安全技术 网络安全等级保护基本要求
[4] GB/T 20275—2020 信息安全技术 网络入侵检测系统技术要求和测试评价方法
[5] GB/T 32915—2016 信息安全技术 二元序列随机性检测方法
[6] GM/T 0005—2021 随机性检测规范

电信终端产业协会团体标准

网络设备密码应用技术要求　入侵检测设备

T/TAF 219—2024

*

电信终端产业协会印发
地址：北京市西城区新街口外大街 28 号
电话：010-82052809
电子版发行网址：www.taf.org.cn