



# 中华人民共和国国家标准

GB/T 33131—2016

---

## 信息安全技术 基于 IPsec 的 IP 存储 网络安全技术要求

Information security technology—Specification for IP storage network  
security based on IPsec

2016-10-13 发布

2017-05-01 实施

---

中华人民共和国国家质量监督检验检疫总局  
中国国家标准化管理委员会 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 缩略语 .....	2
5 基于 IPsec 的 IP 存储网络安全 .....	3
5.1 总体要求 .....	3
5.2 IPsec/IKE 应用要求 .....	3
5.2.1 IPsec 应用要求 .....	3
5.2.2 IKE 应用要求 .....	3
5.2.3 IKE 安全策略配置 .....	4
5.2.4 IPsec 安全检查 .....	4
5.2.5 IKE 及应用层鉴别 .....	4
6 基于 IPsec 的 iSCSI 安全 .....	5
6.1 iSCSI 实施 IPsec 保护 .....	5
6.2 IKE 与 iSCSI 的关系 .....	5
6.3 运用 IPsec 保护 iSCSI 会话创建 .....	5
6.4 运用 IPsec 保护 iSCSI 会话关闭 .....	5
6.5 运用 IPsec 进行 iSCSI 错误处理 .....	6
7 基于 IPsec 的 FCIP 安全 .....	6
7.1 FCIP 实施 IPsec 保护 .....	6
7.2 运用 IPsec 保护 FCIP 安全 .....	6
8 基于 IPsec 的 iFCP 安全 .....	6
8.1 iFCP 实施 IPsec 保护 .....	6
8.2 运用 IPsec 保护 iFCP 安全 .....	7
9 基于 IPsec 的 iSNS 安全 .....	7
9.1 iSNS 实施 IPsec 保护 .....	7
9.2 运用 IPsec 保护 iSNS 安全 .....	7
附录 A (资料性附录) IP 存储网络 .....	9

## 前 言

本标准按照 GB/T 1.1—2009 给出的规则起草。

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这些专利的责任。

本标准由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本标准起草单位:北京邮电大学、工业和信息化部电信研究院、华为技术有限公司、北京天地方元科技有限公司。

本标准起草人:刘建毅、王枫、张茹、姚文斌、肖达、伍淳华、杨义先、雷鸣涛。

# 信息安全技术 基于 IPsec 的 IP 存储 网络安全技术要求

## 1 范围

本标准规定了利用 IPsec 保护 IP 存储网络安全的技术要求,主要涉及了 iSCSI、iFCP、FCIP 等协议和因特网存储名称服务(iSNS)。

本标准适用于 IP 存储网络安全设备的研制、生产和测试。

## 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。

GM/T 0005 随机性检测规范

GM/T 0009 SM2 算法使用规范

GM/T 0022 IPsec VPN 网关技术规范

IETF RFC3723 基于 IP 的安全块存储协议(Securing block storage protocols over IP)

## 3 术语和定义

下列术语和定义适用于本文件。

### 3.1

**存储区域网络 storage area network**

一种用在服务器和存储设备之间的、专用的、高性能的网络体系。

### 3.2

**IP 存储网络 storage area network over IP**

一种在 IP 以太网上架构的存储区域网络。

### 3.3

**小型计算机系统接口 small computer system interface**

一种用于计算机和外部设备之间的通用接口标准,采用客户-服务器架构。

### 3.4

**因特网小型计算机系统接口 internet small computer systems interface**

一种在 TCP/IP 上传输数据块的标准,用来建立和管理 IP 存储设备、主机和客户机等之间的相互连接,并创建存储区域网络。

### 3.5

**因特网安全协议 internet protocol security**

保护 IP 协议安全通信的标准,提供了鉴别和加密两种安全机制;鉴别机制使 IP 通信的数据接收方能够确认数据发送方的真实身份以及数据是否遭到篡改;加密机制保证数据的保密性,防止数据在传输过程中遭到截获而失密。