ICS 35.020
L 80

中华人民共和国国家标准

GB/T 28456—2012

IPsec 协议应用测试规范

Testing specification for applications of IPsec protocol

2012-06-29 发布　　2012-10-01 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

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:信息工程大学信息工程学院。

本标准主要起草人:曾勇军、王清贤、颜学雄、武东英、朱俊虎、尹美娟。

引　言

IPsec是目前广泛使用的网络安全协议，相关产品种类较多。尽管各厂家均声称支持IPsec协议，但由于协议理解上的不同，造成产品在实现方式、完成的功能、提供的安全服务上存在差异。此外目前缺少规范的评估和检测手段，难以确定IPsec协议应用与协议标准的符合程度，难以给出产品准确的评价和分类，这不利于IPsec协议的推广和使用。为进一步规范IPsec协议的开发、评估和使用，有必要对IPsec协议的测试标准进行研究和制定。

本标准为IPsec协议应用的测试标准，依据IPsec协议相关RFC标准制定。

本标准根据IPsec协议的工作模式，从功能、性能、健壮性和互操作性等方面组织测试内容并设计测试步骤。本标准给出的测试步骤，旨在规范测试基本步骤和关键要点，测试人员可在此基础上选择相关的辅助工具，产生具体的测试用例并进行测试。

IPsec 协议应用测试规范

1 范围

本标准对 IPsec 协议应用的测试内容及测试步骤进行了规范。

本标准适用于 IPsec 协议应用的开发单位、第三方授权测试认证机构、用户等对 IPsec 协议应用测试时参考使用。

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 5271.8—2001 信息技术 词汇 第 8 部分：安全

GB/T 17178.1—1997 信息技术 开放系统互连 一致性测试方法和框架 第 1 部分：基本概念

3 术语和定义

GB/T 5271.8—2001 界定的以及下列术语和定义适用于本文件。

3.1

IP 安全协议 IP security

一套用于保护 IP 通信的安全协议。它是 IPv4 的一个可选协议系列，也是 IPv6 的组成部分之一，是一个网络层协议。它提供了认证和加密两种安全机制：认证机制使 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在传输过程中是否遭到篡改；加密机制通过对数据进行编码来保证数据的保密性，防止数据在传输过程中遭到截获而失密。

3.2

IPsec 协议应用 application of the IPsec protocol

按照 IPsec 协议标准实现的产品或功能模块。

3.3

安全关联 security association

两个通信实体经协商建立起来的一种协定，它描述了实体如何利用安全服务来进行安全的通信。安全关联包括了执行各种网络安全服务所需要的信息。

3.4

互联网安全关联与密钥管理协议 internet security association and key management protocol

定义了建立、协商、修改和删除安全关联的过程和报文格式，并定义了交换密钥产生和认证数据的载荷格式。这些格式为传输密钥和认证信息提供了一致的框架。

3.5

载荷 payload

ISAKMP 通信双方交换信息的传输形式，是构造 ISAKMP 消息的基本单位。

3.6

认证头 authentication header

属于 IPsec 的一种协议，用于提供 IP 数据报的数据完整性、数据源认证以及抗重放攻击服务的功能。