ICS 33.040.40
M 33

中华人民共和国国家标准

GB/T 21643—2008

IP 认证头(AH)

IP Authentication Header

(IETF RFC 2402:1998,MOD)

2008-04-10 发布　　2008-11-01 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

本标准是IP安全协议(IPSec)系列标准之一,该系列标准的名称及结构预计如下:

——国家标准《IP安全协议体系结构》(IETF RFC 2401:1998,MOD)[1)]

——GB/T 21643—2008《IP认证头(AH)》(IETF RFC 2402:1998,MOD)

——国家标准《IP封装安全载荷(ESP)》(IETF RFC 2406:1998,MOD)[1)]

——YD/T 1466—2006《IP安全协议(IPSec)技术要求》

——YD/T 1467—2006《IP安全协议(IPSec)测试方法》

——YD/T 1468—2006《IP安全协议(IPSec)穿越网络地址翻译(NAT)技术要求》

——行业标准(YD)《因特网密钥交换协议(IKE v2) 第1部分:技术要求》[1)]

——行业标准(YD)《因特网密钥交换协议(IKE v2) 第2部分:测试方法》[1)]

本标准修改采用IETF RFC 2402:1998《IP认证头(AH)》,与之相比的主要区别是:

——删除了RFC 2402中第4章、第6章、第7章和附录A的内容。

——将RFC 2402中第1章、第2章、第3章和第5章的内容作为本标准的第4章、第5章、第6章和第7章。

——根据GB/T 1系列标准的要求,增加了本标准的第1章、第2章和第3章的内容。

本标准由中华人民共和国信息产业部提出。

本标准由中国通信标准化协会归口。

本标准起草单位:信息产业部电信研究院。

本标准主要起草人:袁琦、何宝宏。

1) 待发布。

IP 认证头(AH)

1 范围

本标准规定了 AH 协议的技术要求，包括 AH 协议头格式、AH 协议处理、一致性要求等。

本标准适用于支持 AH 协议的数据设备。

2 规范性引用文件

下列文件中的条款通过本标准的引用而成为本标准的条款。凡是注日期的引用文件，其随后所有的修改单(不包括勘误的内容)或修订版均不适用于本标准，然而，鼓励根据本标准达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件，其最新版本适用于本标准。

IETF RFC 2401:1998 IP 安全协议体系结构

IETF RFC 2406:1998 IP 封装安全载荷(ESP)

IETF RFC 1883:1995 IPv6 协议

IETF RFC 2403:1998 ESP 和 AH 中使用 MD5-96 的 HMAC 算法

IETF RFC 2404:1998 ESP 和 AH 中使用 SHA-1-96 的 HMAC 算法

3 缩略语

下列缩略语适用于本标准。

AH	Authentication Header	认证头
DES	Data Encryption Standard	数据加密标准
ESP	Encapsulating Security Payload	封装安全载荷
HMAC	HASH MAC	散列 MAC
IANA	Internet Assigned Numbers Authority	互联网地址分配机构
ICMP	Internet Control Message Protocol	互联网控制消息协议
ICV	Integrity Check Value	完整性校验值
IPSec	IP Security	IP 安全
IP	Internet Protocol	互联网协议
MD5	Message Digest 5	消息摘要 5
SA	Security Association	安全联盟
SHA-1	Secure Hash Algorithm-1	安全散列算法-1
SPI	Security Parameter Index	安全参数索引
TCP	Transmission Control Protocol	传输控制协议
TOS	Type of Service	服务类型
UDP	User Datagram Protocol	用户数据报协议

4 概述

AH 为 IP 包提供无连接完整性、数据来源认证和抗重播保护。抗重播保护是可选的，由接收者决定是否使用。当建立安全联盟时，要求发送者增加序列号以用于抗重播保护，只有当接收者检查了序列号，服务才是有效的。

AH 尽可能地为 IP 头和上层协议提供认证。一些 IP 头字段在传输时会改变，当 IP 包到达接收者