ICS 33.040.40

YD

中华人民共和国通信行业标准

YD/T 1467-2006

IP 安全协议（IPSec）测试方法

Testing Methods of IP Security（IPSec）

2006-06-08 发布　　2006-10-01 实施

中华人民共和国信息产业部　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：

1.《IP安全协议体系结构》（MOD IETF RFC 2401）

2.《IP认证头（AH）》（MOD IETF RFC 2402）

3.《IP封装安全载荷（ESP）》（MOD IETF RFC 2406）

4.《IP安全协议（IPSec）技术要求》

5.《IP安全协议（IPSec）测试方法》

6.《IP安全协议（IPSec）穿越网络地址翻译（NAT）技术要求》

7.《因特网密钥交换协议（IKE v2）第1部分：技术要求》

8.《因特网密钥交换协议（IKE v2）第2部分：测试方法》

本标准与YD/T 1466-2006《IP安全协议（IPSec）技术要求》配套使用。

本标准由中国通信标准化协会提出并归口。

本标准起草单位：信息产业部电信研究院

中兴通讯股份有限公司

成都迈普产业集团有限公司

本标准主要起草人：魏　亮　袁　琦　何宝宏　许志军　彭志威　陈剑勇　范恒英

IP 安全协议（IPSec）测试方法

1 范围

本标准规定了 IPSec 的测试方法，包括 AH 和 ESP 功能测试和性能测试等。

本标准适用于支持 IPSec 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。

YD/T 1466-2006	IP 安全协议（IPSec）技术要求
IETF RFC 1321（1992）	MD5 消息摘要算法
IETF RFC 1828（1995）	使用 MD5 密钥的 IP 认证
IETF RFC 1829（1995）	ESP DES-CBC 转换
IETF RFC 2085（1997）	使用抗重播的 HMAC-MD5 IP 认证
IETF RFC 2104（1997）	HMAC：消息认证的密钥哈希
IETF RFC 2401（1998）	IP 安全架构
IETF RFC 2402（1998）	IP 认证头
IETF RFC 2403（1998）	ESP 和 AH 中 HMAC-MD5-96 的使用
IETF RFC 2404（1998）	ESP 和 AH 中 HMAC-SHA-1-96 的使用
IETF RFC 2405（1998）	带有显式 IV 的 ESP DES-CBC 密码算法
IETF RFC 2406（1998）	IP 封装安全载荷
IETF RFC 2407（1998）	对 ISAKMP 的因特网 IP 安全域解释
IETF RFC 2408（1998）	互联网安全联盟和密钥管理协议（ISAKMP）
IETF RFC 2410（1998）	IPSec 的空加密算法和使用
IETF RFC 2412（1998）	OAKLEY 密钥协议
IETF RFC 2451（1998）	ESP CBC 模式密码算法
IETF RFC 2857（2000）	ESP 和 AH 中 HMAC-RIPEMD-160-96 的使用
IETF RFC 3511（2003）	防火墙性能基准方法

3 缩略语

下列缩略语适用于本标准。

AH	Authentication Header	认证头
CBC	Copher Block Chaining	码块链
ESP	Encapsulating Security Payload	封装安全载荷
DES	Data Encryption Standard	数据加密标准
DUT	Device Under Tester	被测设备
HMAC	HASH MAC	散列 MAC

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
PMTU	Path Maximun Transmission Unit	路径最大传输单元
SA	Security Association	安全联盟
SAD	SA Database	数据库
SHA-1	Secure Hash Algorithm-1	安全散列算法-1
SPI	Security Parameter Index	安全参数索引
SPD	Security Policy Database	安全策略数据库
TCP	Transmission Control Protocol	传输控制协议
UDP	User Datagram Protocol	用户数据报协议

4 功能测试

4.1 AH 功能测试

4.1.1 AH：hmac-md5-96、传输模式

测试编号：1

测试项目：AH：hmac-md5-96、传输模式

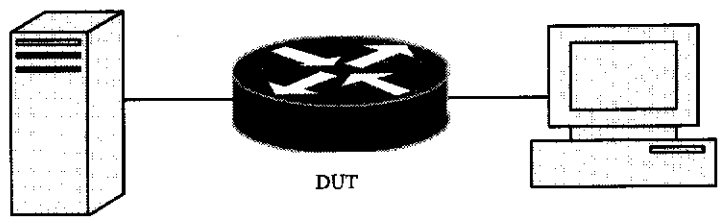
测试目的：验证 IPSec 实现 hmac-md5-96，传输模式的 AH 功能

测试依据：RFC 2402

测试仪表：协议仪真器

测试类型：必选

测试配置：



测试过程：

1）正确连接设备，DUT 为支持被测实现 IPSec 的设备，配置地址保持互通性。

2）配置 DUT 和协议仿真器的 IPSec，采用 AH：hmac-md5-96，传输模式。

3）配置 DUT 和协议仿真器采用源、目的地址作选择符。

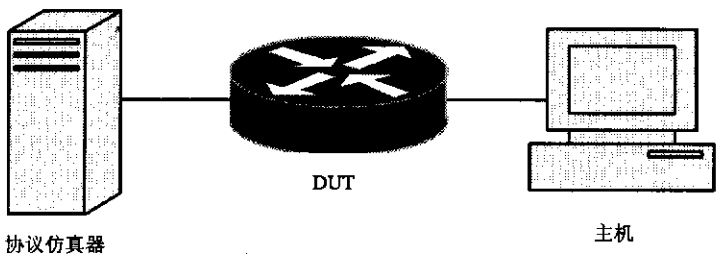
4）由协议仿真器向 DUT 发 Ping 包

预期结果：步骤 4）后 DUT 正确回应

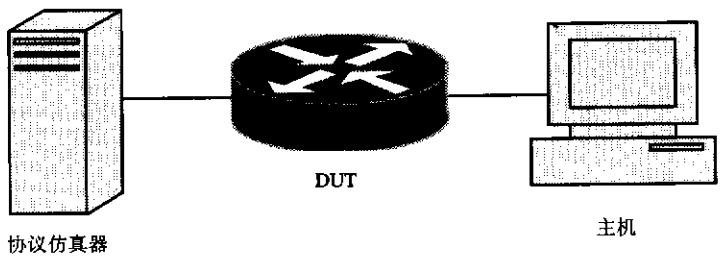
测试说明：

判定原则：测试结果必须与预期结果相符，否则不符合要求

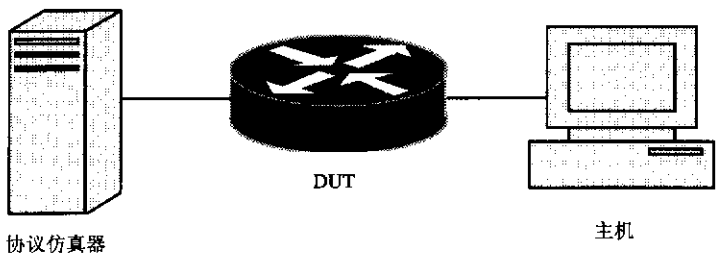
4.1.2 AH：hmac-md5-96、隧道模式

测试编号：2
测试项目：AH：hmac-md5-96、隧道模式
测试目的：验证 IPSec 实现 hmac-md5-96，隧道模式的 AH 功能
测试依据：RFC 2402
测试仪表：协议仿真设备
测试类型：必选
测试配置： 
测试过程： 1）正确连接设备，DUT 为支持被测实现 IPSec 的设备，配置地址保持互通性。 2）配置 DUT 和协议仿真器的 IPSec，采用 AH：hmac-md5-96、隧道模式。 3）配置 DUT 和协议仿真器采用源、目的地址作选择符。 4）由协议仿真器向主机发 Ping 包
预期结果：步骤 4）后主机正确回应
测试说明：
判定原则：测试结果必须与预期结果相符，否则不符合要求

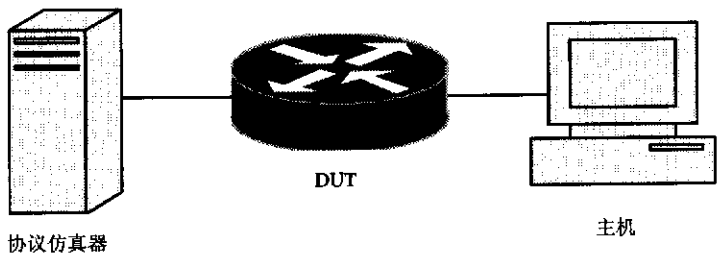
4.1.3 AH：hmac-sha-1-96、传输模式

测试编号：3
测试项目：AH：hmac-sha-1-96、传输模式
测试目的：验证 IPSec 实现 hmac- sha-1-96，传输模式的 AH 功能
测试依据：RFC 2402
测试仪表：协议仿真设备
测试类型：必选
测试配置： 
测试过程： 1）正确连接设备，DUT 为支持被测实现 IPSec 的设备，配置地址保持互通性。 2）配置 DUT 和协议仿真器的 IPSec，采用 hmac- sha-1-96，传输模式。 3）配置 DUT 和协议仿真器采用源、目的地址作选择符。 4）由协议仿真器向 DUT 发 Ping 包
预期结果：步骤 4）后 DUT 正确回应
测试说明：
判定原则：测试结果必须与预期结果相符，否则不符合要求

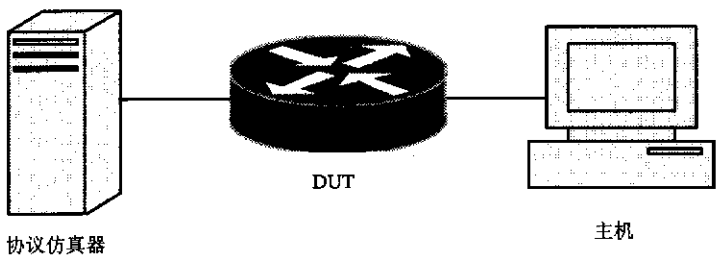
4.1.4 AH：hmac-sha-1-96、隧道模式

测试编号：4
测试项目：AH：hmac-sha-1-96、隧道模式
测试目的：验证 IPSec 实现 hmac-sha-196，隧道模式的 AH 功能
测试依据：RFC 2402
测试仪表：协议仿真设备
测试类型：必选
测试配置：： 
测试过程： 1）正确连接设备，DUT 为支持被测实现 IPSec 的设备，配置地址保持互通性。 2）配置 DUT 和协议仿真器的 IPSec，采用 hmac- sha-1-96、隧道模式。 3）配置 DUT 和协议仿真器采用源、目的地址作选择符。 4）由协议仿真器向主机发 Ping 包
预期结果：步骤 4）后主机正确回应
测试说明：
判定原则：测试结果必须与预期结果相符，否则不符合要求

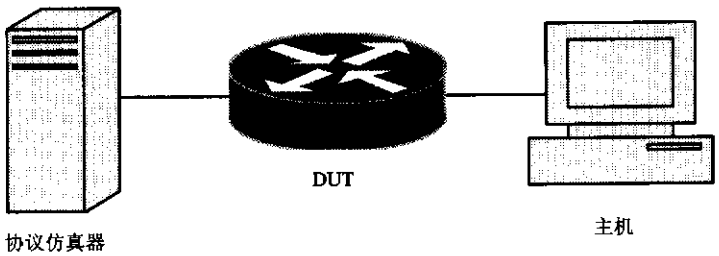
4.1.5 正确的 AH 报文处理

测试编号：5
测试项目：正确的 AH 报文处理
测试目的：验证 IPSec 处理正确的 AH 报文
测试依据：RFC 2402
测试仪表：协议仿真设备
测试类型：必选
测试配置： 
测试过程： 1）正确连接设备，DUT 为支持被测实现 IPSec 的设备，配置地址保持互通性。 2）配置 DUT 和协议仿真器的 IPSec，采用 AH：hmac-md5-96。 3）配置 DUT 和协议仿真器采用源、目的地址作选择符。 4）协议仿真器向被测设备发送正确的 AH 报文
预期结果：步骤 4）后被测设备接收 AH 报文，并交至上层处理
测试说明：
判定原则：测试结果必须与预期结果相符，否则不符合要求

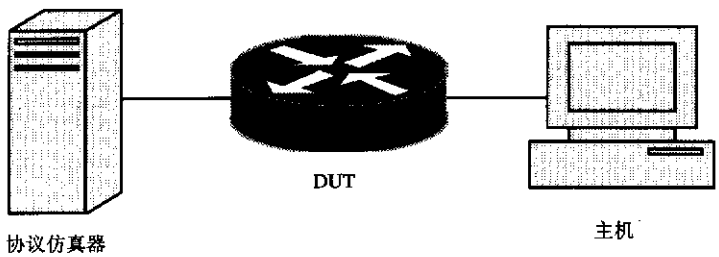
4.1.6 错误 ICV 字段的 AH 处理

测试编号：6
测试项目：错误 ICV 字段的 AH 处理
测试目的：验证 IPSec 丢弃错误 ICV 字段的 AH 报文
测试依据：RFC 2402
测试仪表：协议仿真设备
测试类型：必选
测试配置： 
测试过程： 1）正确连接设备，DUT 为支持被测实现 IPSec 的设备，配置地址保持互通性。 2）配置 DUT 和协议仿真器的 IPSec，采用 AH：hmac-md5-96。 3）配置 DUT 和协议仿真器采用源、目的地址作选择符。 4）协议仿真器向被测设备发送错误 ICV 字段的 AH 报文
预期结果：被测设备丢弃 AH 报文
测试说明：
判定原则：测试结果必须与预期结果相符，否则不符合要求

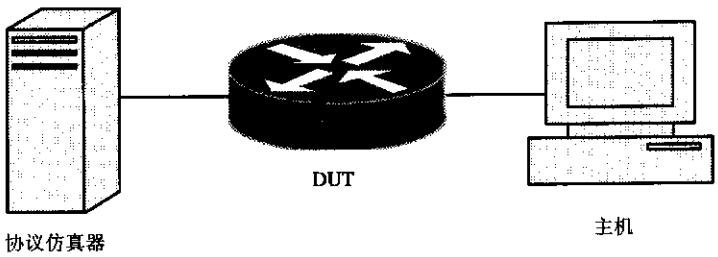
4.1.7 保留字段不为 0 的处理

测试编号：7
测试项目：保留字段不为 0 的处理
测试目的：验证 IPSec 丢弃保留字段不为 0 的 AH 报文
测试依据：RFC 2402
测试仪表：协议仿真设备
测试类型：必选
测试配置： 
测试过程： 1）正确连接设备，DUT 为支持被测实现 IPSec 的设备，配置地址保持互通性。 2）配置 DUT 和协议仿真器的 IPSec，采用 AH：hmac-md5-96。 3）配置 DUT 和协议仿真器采用源、目的地址作选择符。 4）协议仿真器向被测设备发送保留字段不为 0 的 AH 报文
预期结果：被测设备丢弃 AH 报文
测试说明：
判定原则：测试结果必须与预期结果相符，否则不符合要求

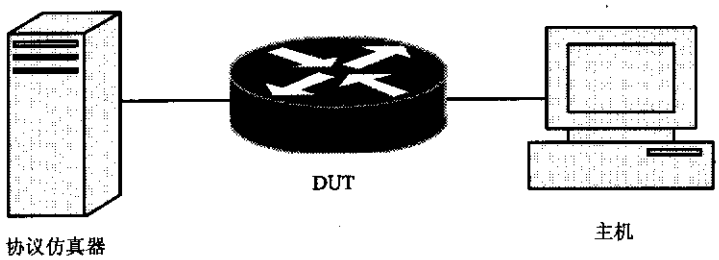
4.1.8 SPI 值不匹配的 AH 处理

测试编号：8
测试项目：SPI 值在 SAD 中不存在相应表项的 AH 处理
测试目的：验证 IPSec 丢弃 SPI 值在 SAD 中不存在相应表项的 AH 报文
测试依据：RFC 2402
测试仪表：协议仿真设备
测试类型：必选
测试配置： 
测试过程： 1）正确连接设备，DUT 为支持被测实现 IPSec 的设备，配置地址保持互通性。 2）配置 DUT 和协议仿真器的 IPSec，采用 AH：hmac-md5-96。 3）配置 DUT 和协议仿真器采用源、目的地址作选择符。 4）协议仿真器向被测设备发送 SPI 值在 SAD 中不存在相应表项的 AH 报文
预期结果：被测设备丢弃 AH 报文
测试说明：
判定原则：测试结果必须与预期结果相符，否则不符合要求

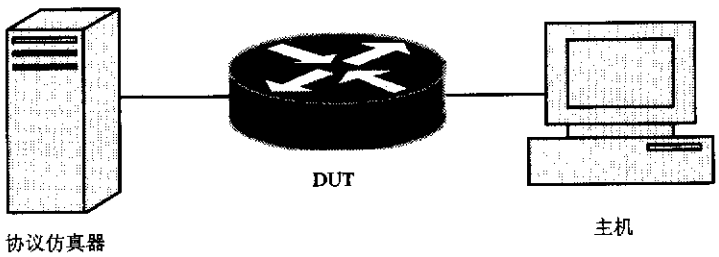
4.1.9 序列号为 0 的 AH 处理

测试编号：9
测试项目：序列号为 0 的 AH 处理
测试目的：验证 IPSec 丢弃序列号为 0 的 AH 报文
测试依据：RFC 2402
测试仪表：协议仿真设备
测试类型：必选
测试配置： 
测试过程： 1）正确连接设备，DUT 为支持被测实现 IPSec 的设备，配置地址保持互通性。 2）配置 DUT 和协议仿真器的 IPSec，采用 AH：hmac-md5-96。 3）配置 DUT 和协议仿真器采用源、目的地址作选择符。 4）协议仿真器向被测设备发送序列号为 0 的 AH 报文
预期结果：被测设备丢弃 AH 报文
测试说明：
判定原则：测试结果必须与预期结果相符，否则不符合要求

4.1.10 序列号低于抗重播窗口左沿的 AH 处理

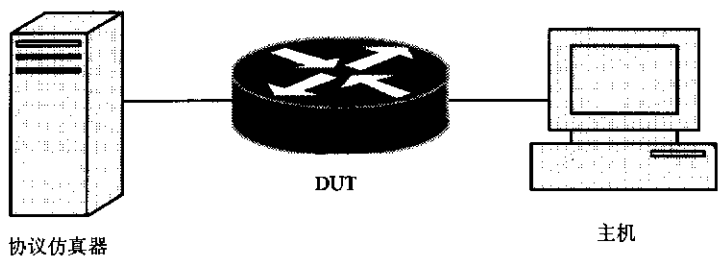
测试编号：10
测试项目：序列号低于抗重播窗口左沿的 AH 处理
测试目的：验证 IPSec 处理序列号低于抗重播窗口左沿的 AH 报文
测试依据：RFC 2402
测试仪表：协议仿真设备
测试类型：必选
测试配置： 
测试过程： 1）正确连接设备，DUT 为支持被测实现 IPSec 的设备，配置地址保持互通性。 2）配置 DUT 和协议仿真器的 IPSec，采用 AH：hmac-md5-96。 3）配置 DUT 和协议仿真器采用源、目的地址作选择符。 4）协议仿真器向被测设备发送序列号低于抗重播窗口左沿的 AH 报文
预期结果：被测设备丢弃 AH 报文
测试说明：
判定原则：测试结果必须与预期结果相符，否则不符合要求

4.1.11 序列号落在抗重播窗口内的 AH 处理

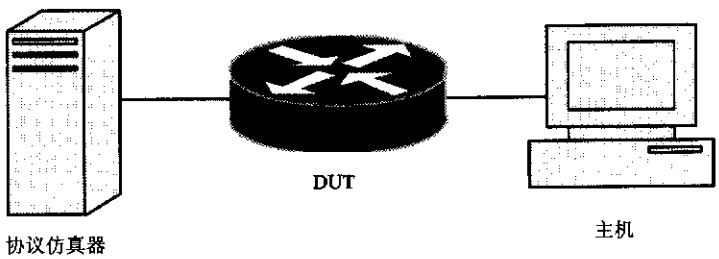
测试编号：11
测试项目：序列号落在抗重播窗口内的 AH 处理
测试目的：验证 IPSec 处理序列号落在抗重播窗口内的 AH 报文
测试依据：RFC 2402
测试仪表：协议仿真设备
测试类型：必选
测试配置： 
测试过程： 1）正确连接设备，DUT 为支持被测实现 IPSec 的设备，配置地址保持互通性。 2）配置 DUT 和协议仿真器的 IPSec，采用 AH：hmac-md5-96。 3）配置 DUT 和协议仿真器采用源、目的地址作选择符。 4）协议仿真器向被测设备发送序列号落在抗重播窗口内的 AH 报文
预期结果：被测设备接收 AH 报文
测试说明：
判定原则：测试结果必须与预期结果相符，否则不符合要求

4.2 ESP 功能测试

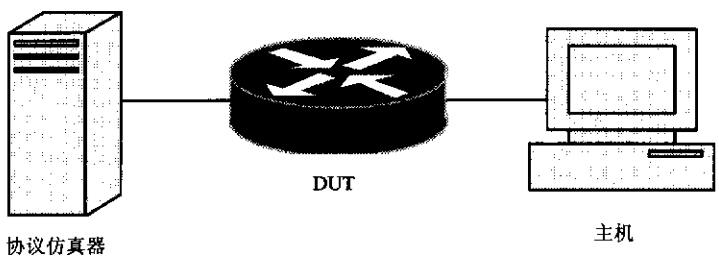
4.2.1 ESP：des-cbc、传输模式

测试编号：12
测试项目：ESP：des-cbc、传输模式
测试目的：验证 IPSec 实现 des-cbc，传输模式的 ESP 功能
测试依据：RFC 2406
测试仪表：协议仿真设备
测试类型：必选
测试配置： 
测试过程： 1）正确连接设备，DUT 为支持被测实现 IPSec 的设备，配置地址保持互通性。 2）配置 DUT 和协议仿真器的 IPSec，采用 ESP：des-cbc、传输模式。 3）配置 DUT 和协议仿真器采用源、目的地址作选择符。 4）由协议仿真器向 DUT 发 Ping 包。 5）配置 DUT 和协议仿真器的 IPSec，采用 ESP：des-cbc+hmac-md5-96、传输模式。 6）由协议仿真器向 DUT 发 Ping 包。 7）配置 DUT 和协议仿真器的 IPSec，采用 ESP：des-cbc+hmac-sha-1-96、传输模式。 8）由协议仿真器向 DUT 发 Ping 包
预期结果：步骤 4）、6）和 8）后 DUT 正确回应
测试说明：
判定原则：测试结果必须与预期结果相符，否则不符合要求

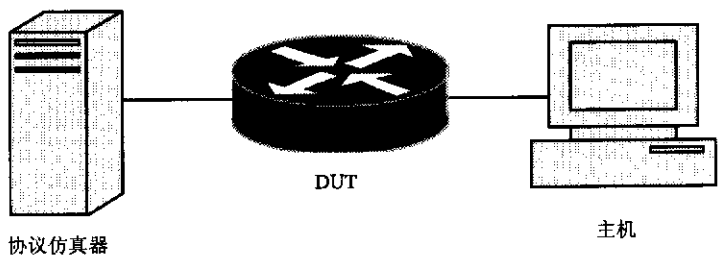
4.2.2 ESP：des-cbc、隧道模式

测试编号：13
测试项目：ESP：des-cbc，隧道模式
测试目的：验证 IPSec 具有 des-cbc，隧道模式的 ESP 功能
测试依据：RFC 2406
测试仪表：协议仿真设备
测试类型：必选
测试配置： 
测试过程： 1）正确连接设备，DUT 为支持被测实现 IPSec 的设备，配置地址保持互通性。 2）配置 DUT 和协议仿真器的 IPSec，采用 ESP：des-cbc、隧道模式。 3）配置 DUT 和协议仿真器采用源、目的地址作选择符。 4）由协议仿真器向主机发 Ping 包。 5）配置 DUT 和协议仿真器的 IPSec，采用 ESP：des-cbc+hmac-md5-96、隧道模式。 6）由协议仿真器向 DUT 发 Ping 包。 7）配置 DUT 和协议仿真器的 IPSec，采用 ESP：des-cbc+hmac-sha-1-96、隧道模式。 8）由协议仿真器向主机发 Ping 包
预期结果：步骤 4)、6）和 8）后主机正确回应
测试说明：
判定原则：测试结果必须与预期结果相符，否则不符合要求

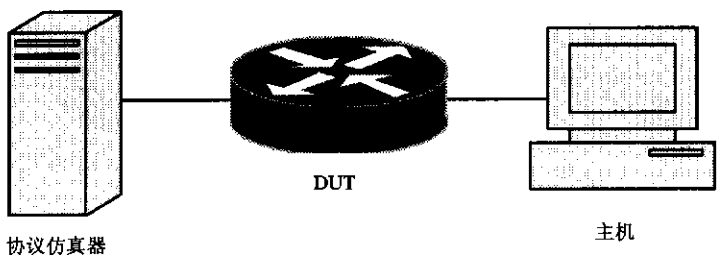
4.2.3 ESP：null、隧道模式

测试编号：14
测试项目：ESP：null、隧道模式
测试目的：验证 IPSec 实现 null，隧道模式的 ESP 功能
测试依据：RFC 2406
测试仪表：协议仿真设备
测试类型：必选
测试配置： 
测试过程： 1）正确连接设备，DUT 为支持被测实现 IPSec 的设备，配置地址保持互通性。 2）配置 DUT 和协议仿真器的 IPSec，采用 ESP：null+hmac_md5_96、隧道模式。 3）配置 DUT 和协议仿真器采用源、目的地址作选择符。 4）由协议仿真器向主机发 Ping 包。 5）配置 DUT 和协议仿真器的 IPSec，采用 ESP：null+hmac_sha_96、隧道模式。 6）由协议仿真器向主机发 Ping 包
预期结果：步骤 4)、6）后主机正确回应
测试说明：
判定原则：测试结果必须与预期结果相符，否则不符合要求

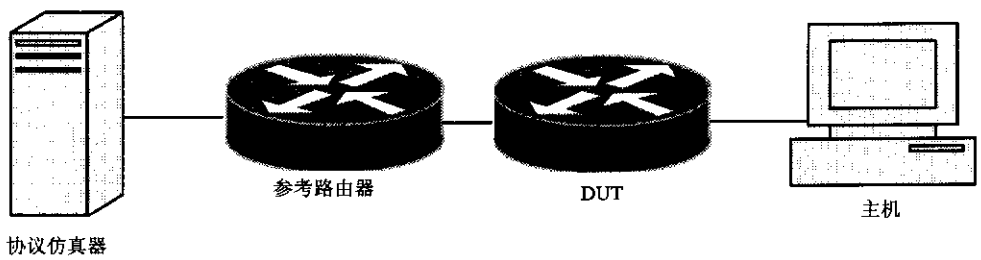
4.2.4 ESP：null、传输模式

测试编号：15
测试项目：ESP：null、传输模式
测试目的：验证 IPSec 具有 null，传输模式的 ESP 功能
测试依据：RFC 2406
测试仪表：协议仿真设备
测试类型：必选
测试配置： 
测试过程： 1）正确连接设备，DUT 为支持被测实现 IPSec 的设备，配置地址保持互通性。 2）配置 DUT 和协议仿真器的 IPSec，采用 ESP：null+hmac_md5_96、传输模式。 3）配置 DUT 和协议仿真器采用源、目的地址作选择符。 4）由协议仿真器向 DUT 发 Ping 包。 5）配置 DUT 和协议仿真器的 IPSec，采用 ESP：null+hmac_sha_96、传输模式。 6）由协议仿真器向 DUT 发 Ping 包
预期结果：步骤 4）、6）后 DUT 正确回应
测试说明：
判定原则：测试结果必须与预期结果相符，否则不符合要求

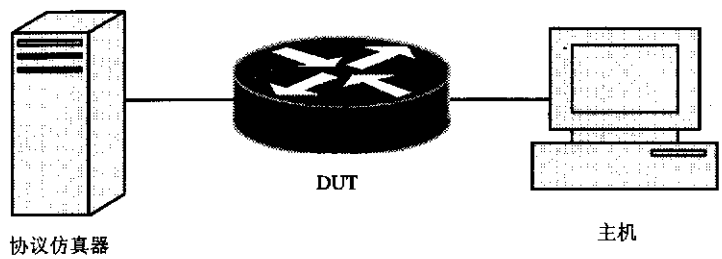
4.2.5 ESP：3des_cbc、传输模式

测试编号：16
测试项目：ESP：3des_cbc、传输模式
测试目的：验证 IPSec 具有 3des_cbc，传输模式的 ESP 功能
测试依据：RFC 2406
测试仪表：协议仿真设备
测试类型：必选
测试配置： 
测试过程： 1）正确连接设备，DUT 为支持被测实现 IPSec 的设备，配置地址保持互通性。 2）配置 DUT 和协议仿真器的 IPSec，采用 ESP：3des-cbc、传输模式。 3）配置 DUT 和协议仿真器采用源、目的地址作选择符。 4）由协议仿真器向 DUT 发 Ping 包。 5）配置 DUT 和协议仿真器的 IPSec，采用 ESP：3des-cbc+hmac-md5-96、传输模式。 6）由协议仿真器向 DUT 发 Ping 包。 7）配置 DUT 和协议仿真器的 IPSec，采用 ESP：3des-cbc+hmac-sha-1-96、传输模式。 8）由协议仿真器向 DUT 发 Ping 包
预期结果：步骤 4）、6）和 8）后 DUT 正确回应
测试说明：
判定原则：测试结果必须与预期结果相符，否则不符合要求

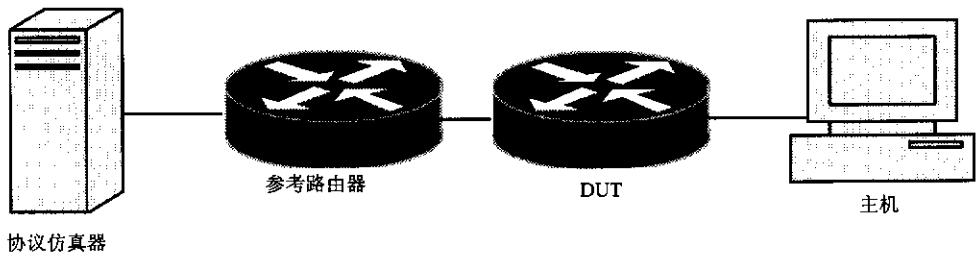
4.2.6 ESP：3des_cbc、隧道模式

测试编号：17
测试项目：ESP：3des_cbc、隧道模式
测试目的：验证 IPSec 具有 3des_cbc，隧道模式的 ESP 功能
测试依据：RFC 2406
测试仪表：协议仿真设备
测试类型：必选
测试配置： 
测试过程： 1）正确连接设备，DUT 为支持被测实现 IPSec 的设备，配置地址保持互通性。 2）配置 DUT 和协议仿真器的 IPSec，采用 ESP：3des-cbc、隧道模式。 3）配置 DUT 和协议仿真器采用源、目的地址作选择符。 4）由协议仿真器向主机发 Ping 包。 5）配置 DUT 和协议仿真器的 IPSec，采用 ESP：3des-cbc+hmac-md5-96、隧道模式。 6）由协议仿真器向主机发 Ping 包。 7）配置 DUT 和协议仿真器的 IPSec，采用 ESP：3des-cbc+hmac-sha-1-96、隧道模式。 8）由协议仿真器向主机发 Ping 包
预期结果：步骤 4）、6）和 8）后主机正确回应
测试说明：
判定原则：测试结果必须与预期结果相符，否则不符合要求

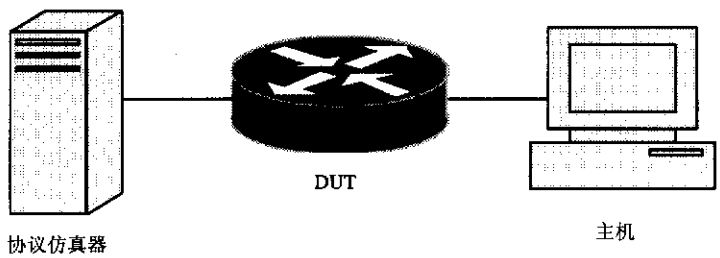
4.2.7 ESP：AES、传输模式

测试编号：18
测试项目：ESP：AES、传输模式
测试目的：验证 IPSec 具有 AES，传输模式的 ESP 功能
测试依据：RFC 2406
测试仪表：协议仿真设备
测试类型：可选
测试配置： 
测试过程： 1）正确连接设备，DUT 为支持被测实现 IPSec 的设备，配置地址保持互通性。 2）配置 DUT 和协议仿真器的 IPSec，采用 ESP：AES、传输模式。 3）配置 DUT 和协议仿真器采用源、目的地址作选择符。 4）由协议仿真器向 DUT 发 Ping 包。 5）配置 DUT 和协议仿真器的 IPSec，采用 ESP：AES+hmac-md5-96、传输模式。 6）由协议仿真器向 DUT 发 Ping 包。 7）配置 DUT 和协议仿真器的 IPSec，采用 ESP：AES+hmac-sha-1-96、传输模式。 8）由协议仿真器向 DUT 发 Ping 包
预期结果：步骤 4）、6）和 8）后 DUT 正确回应
测试说明：
判定原则：测试结果必须与预期结果相符，否则不符合要求

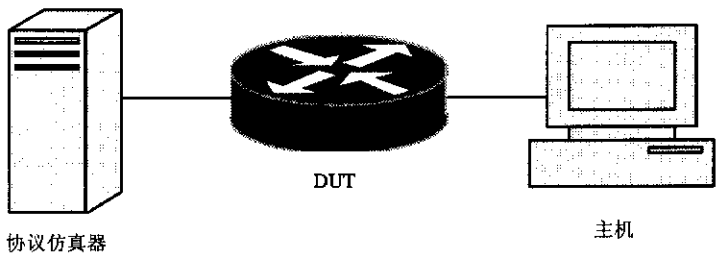
4.2.8 ESP：AES、隧道模式

测试编号：19
测试项目：ESP：AES、隧道模式
测试目的：验证 IPSec 具有 AES，隧道模式的 ESP 功能
测试依据：RFC 2406
测试仪表：协议仿真设备
测试类型：可选
测试配置： 
测试过程： 1）正确连接设备，DUT 为支持被测实现 IPSec 的设备，配置地址保持互通性。 2）配置 DUT 和协议仿真器的 IPSec，采用 ESP：AES、隧道模式。 3）配置 DUT 和协议仿真器采用源、目的地址作选择符。 4）由协议仿真器向主机发 Ping 包。 5）配置 DUT 和协议仿真器的 IPSec，采用 ESP：AES+hmac-md5-96、隧道模式。 6）由协议仿真器向主机发 Ping 包。 7）配置 DUT 和协议仿真器的 IPSec，采用 ESP：AES+hmac-sha-1-96、隧道模式。 8）由协议仿真器向主机发 Ping 包
预期结果：步骤 4)、6）和 8）后主机正确回应
测试说明：
判定原则：测试结果必须与预期结果相符，否则不符合要求

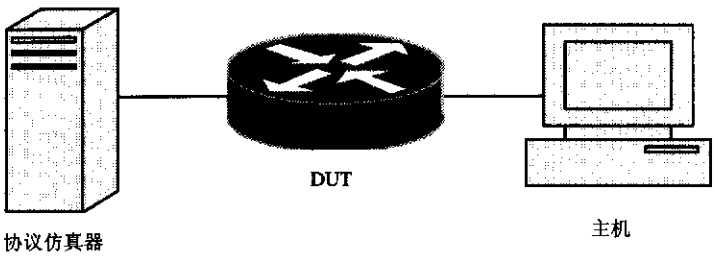
4.2.9 正确的 ESP 报文处理

测试编号：20
测试项目：正确的 ESP 报文处理
测试目的：验证 IPSec 处理正确的 ESP 报文
测试依据：RFC 2406
测试仪表：协议仿真设备
测试类型：必选
测试配置： 
测试过程： 1）正确连接设备，DUT 为支持被测实现 IPSec 的设备，配置地址保持互通性。 2）配置 DUT 和协议仿真器的 IPSec，采用 ESP：3des_cbc。 3）配置 DUT 和协议仿真器采用源、目的地址作选择符。 4）协议仿真器向被测设备发送正确的 ESP 报文
预期结果：步骤 4）后被测设备接收 ESP 报文，并交至上层处理
测试说明：
判定原则：测试结果必须与预期结果相符，否则不符合要求

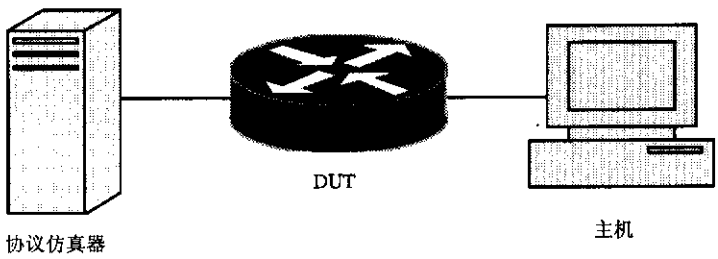
4.2.10 填充项长度和下一个头字段不以 4 字节靠齐的 ESP 处理

测试编号：21
测试项目：填充项长度和下一个头字段不以 4 字节靠齐的 ESP 处理
测试目的：验证 IPSec 丢弃填充项长度和下一个头字段不以 4 字节靠齐的 ESP 报文
测试依据：RFC 2406
测试仪表：协议仿真设备
测试类型：必选
测试配置： 
测试过程： 1）正确连接设备，DUT 为支持被测实现 IPSec 的设备，配置地址保持互通性。 2）配置 DUT 和协议仿真器的 IPSec，采用 ESP：3des_cbc。 3）配置 DUT 和协议仿真器采用源、目的地址作选择符。 4）协议仿真器向被测设备发送填充长度和下一个头字段不以 4 字节靠齐的 ESP 报文
预期结果：被测设备丢弃 ESP 报文
测试说明：
判定原则：测试结果必须与预期结果相符，否则不符合要求

4.2.11 认证字段未正确计算的 ESP 处理

测试编号：22
测试项目：认证字段未正确计算的 ESP 处理
测试目的：验证 IPSec 丢弃认证字段未正确计算的 ESP 处理
测试依据：RFC 2406
测试仪表：协议仿真设备
测试类型：必选
测试配置： 
测试过程： 1）正确连接设备，DUT 为支持被测实现 IPSec 的设备，配置地址保持互通性。 2）配置 DUT 和协议仿真器的 IPSec，采用 ESP：3des_cbc。 3）配置 DUT 和协议仿真器采用源、目的地址作选择符。 4）协议仿真器向被测设备发送认证字段未正确计算的 ESP 报文
预期结果：被测设备丢弃 ESP 报文
测试说明：
判定原则：测试结果必须与预期结果相符，否则不符合要求

4.2.12 SPI 字段在 0~255 之间的 ESP 处理

测试编号：23
测试项目：SPI 字段在 0~255 之间的 ESP 处理
测试目的：验证 IPSec 丢弃 SPI 字段在 0~255 之间的 ESP 报文
测试依据：RFC 2406
测试仪表：协议仿真设备
测试类型：必选
测试配置： 
测试过程： 1）正确连接设备，DUT 为支持被测实现 IPSec 的设备，配置地址保持互通性。 2）配置 DUT 和协议仿真器的 IPSec，采用 ESP：3des_cbc。 3）配置 DUT 和协议仿真器采用源、目的地址作选择符。 4）协议仿真器向被测设备发送 SPI 字段在 0~255 之间的 ESP 报文
预期结果：被测设备丢弃 ESP 报文
测试说明：
判定原则：测试结果必须与预期结果相符，否则不符合要求

4.2.13 载荷长度为 0 的 ESP 处理

测试编号：24

测试项目：载荷长度为 0 的 ESP 处理

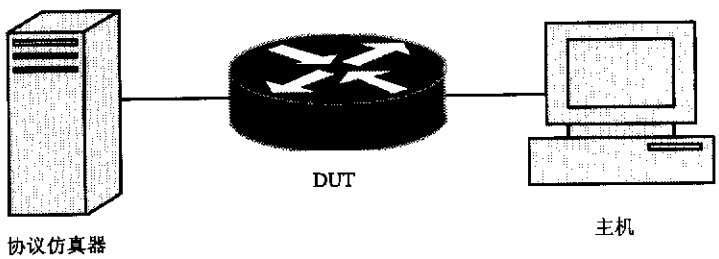
测试目的：验证 IPSec 丢弃载荷长度为 0 的 ESP 报文

测试依据：RFC 2406

测试仪表：协议仿真设备

测试类型：必选

测试配置：



测试过程：

1）正确连接设备，DUT 为支持被测实现 IPSec 的设备，配置地址保持互通性。

2）配置 DUT 和协议仿真器的 IPSec，采用 ESP：3des_cbc。

3）配置 DUT 和协议仿真器采用源、目的地址作选择符。

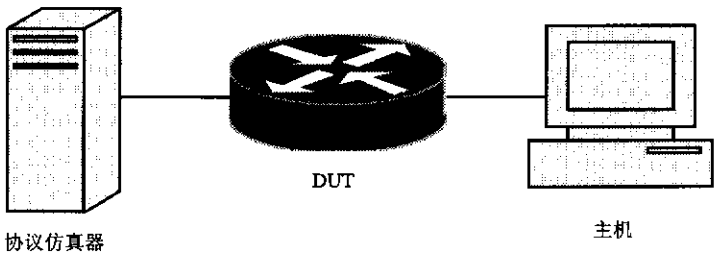
4）协议仿真器向被测设备发送载荷长度为 0 的 ESP 报文

预期结果：被测设备丢弃 ESP 报文

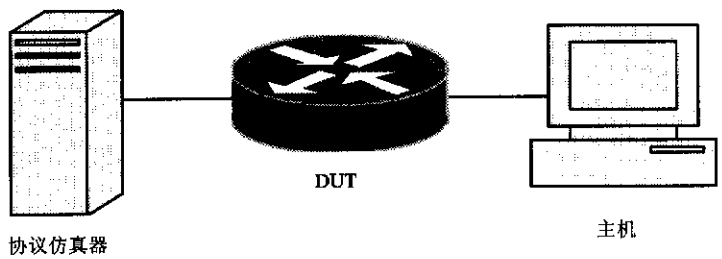
测试说明：

判定原则：测试结果必须与预期结果相符，否则不符合要求

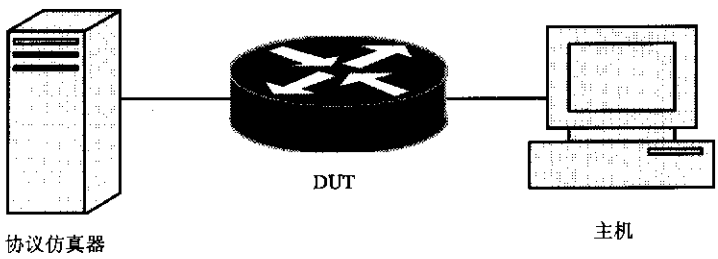
4.2.14 序列号为 0 的 ESP 处理

测试编号：25
测试项目：序列号为 0 的 ESP 处理
测试目的：验证 IPSec 丢弃序列号为 0 的 ESP 报文
测试依据：RFC 2406
测试仪表：协议仿真设备
测试类型：必选
测试配置： 
测试过程： 1）正确连接设备，DUT 为支持被测实现 IPSec 的设备，配置地址保持互通性。 2）配置 DUT 和协议仿真器的 IPSec，采用 ESP：3des_cbc。 3）配置 DUT 和协议仿真器采用源、目的地址作选择符。 4）协议仿真器向被测设备发送序列号为 0 的 ESP 报文
预期结果：被测设备丢弃 ESP 报文
测试说明：
判定原则：测试结果必须与预期结果相符，否则不符合要求

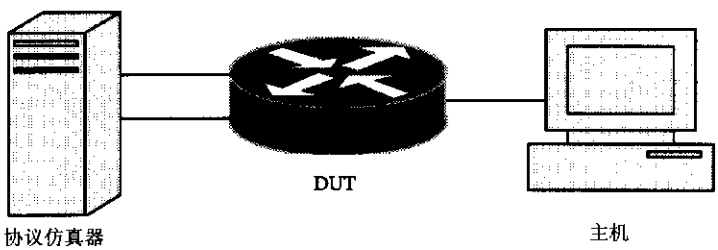
4.2.15 填充长度不在 0～255 范围的 ESP 处理

测试编号：26
测试项目：填充长度不在 0～255 范围的 ESP 处理
测试目的：验证 IPSec 丢弃填充长度不在 0～255 范围的 ESP 报文
测试依据：RFC 2406
测试仪表：协议仿真设备
测试类型：必选
测试配置： 
测试过程： 1）正确连接设备，DUT 为支持被测实现 IPSec 的设备，配置地址保持互通性。 2）配置 DUT 和协议仿真器的 IPSec，采用 ESP：3des_cbc。 3）配置 DUT 和协议仿真器采用源、目的地址作选择符。 4）协议仿真器向被测设备发送填充长度为 256 的 ESP 报文
预期结果：被测设备丢弃 ESP 报文
测试说明：
判定原则：测试结果必须与预期结果相符，否则不符合要求

4.2.16 序列号低于抗重播窗口左沿的 ESP 处理

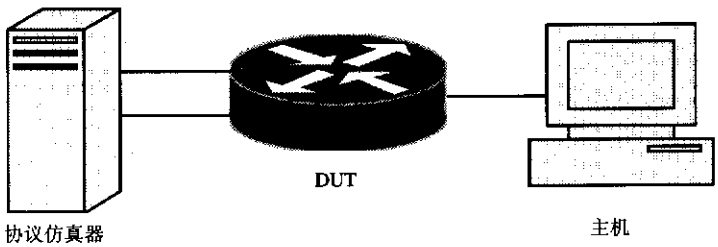
测试编号：27
测试项目：序列号低于抗重播窗口左沿的 ESP 处理
测试目的：验证 IPSec 丢弃序列号低于抗重播窗口左沿的 ESP 报文
测试依据：RFC 2406
测试仪表：协议仿真设备
测试类型：必选
测试配置： 
测试过程： 1）正确连接设备，DUT 为支持被测实现 IPSec 的设备，配置地址保持互通性。 2）配置 DUT 和协议仿真器的 IPSec，采用 ESP：3des_cbc。 3）配置 DUT 和协议仿真器采用源、目的地址作选择符。 4）协议仿真器向被测设备发送 ESP 头中序列号低于抗重播窗口左沿的 ESP 报文
预期结果：被测设备丢弃 ESP 报文
测试说明：
判定原则：测试结果必须与预期结果相符，否则不符合要求

4.2.17 序列号落在抗重播窗口内的 ESP 处理

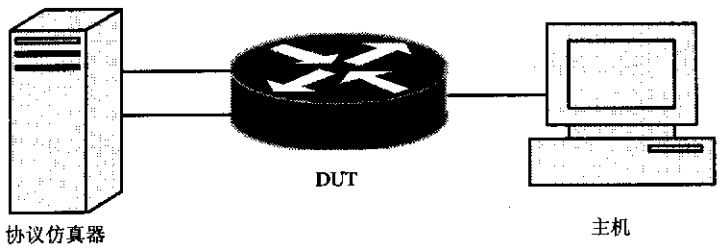
测试编号：28
测试项目：序列号落在抗重播窗口内的 ESP 处理
测试目的：验证 IPSec 丢弃序列号落在抗重播窗口内的 ESP 报文
测试依据：RFC 2406
测试仪表：协议仿真设备
测试类型：必选
测试配置： 
测试过程： 1）正确连接设备，DUT 为支持被测实现 IPSec 的设备，配置地址保持互通性。 2）配置 DUT 和协议仿真器的 IPSec，采用 ESP：3des_cbc。 3）配置 DUT 和协议仿真器采用源、目的地址作选择符。 4）协议仿真器向被测设备发送 ESP 头中序列号落在抗重播窗口内的 ESP 报文
预期结果：被测设备接收 ESP 报文
测试说明：
判定原则：测试结果必须与预期结果相符，否则不符合要求

4.3 SA 测试

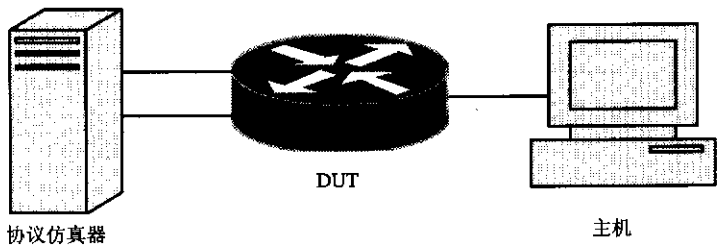
4.3.1 SPD 策略设置为应用 IPSec 的测试

测试编号：29
测试项目：SPD 策略设置为应用 IPSec 的测试
测试目的：验证 IPSec 正确处理 SPD 策略设置为应用 IPSec 的数据包
测试依据：RFC 2401
测试仪表：协议仿真设备
测试类型：必选
测试配置： 
测试过程： 1）正确连接设备，配置地址保持互通性。 2）配置 DUT 和协议仿真器的 IPSec。 3）配置 DUT 和协议仿真器采用源、目的地址作选择符，配置 DUT 的 SPD 策略为应用 IPSec。 4）协议仿真器的一个端口发送数据包
预期结果：协议仿真器的另一个端口观察应用 IPSec 的数据包
测试说明：
判定原则：测试结果必须与预期结果相符，否则不符合要求

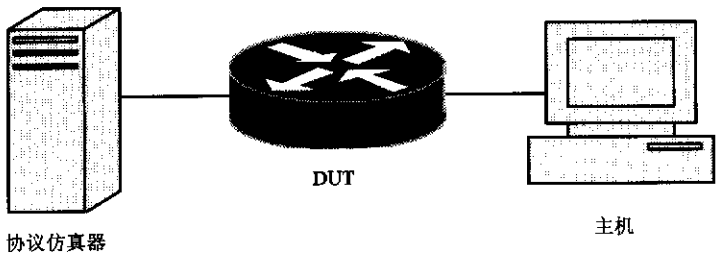
4.3.2 SPD 策略设置为丢弃的测试

测试编号：30
测试项目：SPD 策略设置为丢弃的测试
测试目的：验证 IPSec 正确处理 SPD 策略设置为丢弃的数据包
测试依据：RFC 2401
测试仪表：协议仿真设备
测试类型：可选
测试配置： 
测试过程： 1） 正确连接设备，配置地址保持互通性。 2） 配置 DUT 和协议仿真器的 IPSec。 3） 配置 DUT 和协议仿真器采用源、目的地址作选择符，配置 DUT 的 SPD 策略为丢弃。 4） 协议仿真器的一个端口发送数据包
预期结果：协议仿真器的另一个端口观察未接收到数据包
测试说明：
判定原则：测试结果必须与预期结果相符，否则不符合要求

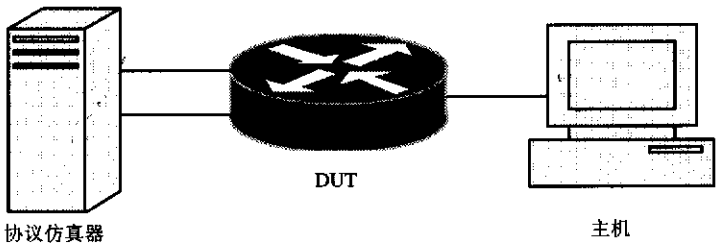
4.3.3 SPD 策略设置为绕过 IPSec 的测试

测试编号：31
测试项目：SPD 策略设置为绕过 IPSec 的测试
测试目的：验证 IPSec 正确处理 SPD 策略设置为绕过 IPSec 的数据包
测试依据：RFC 2401
测试仪表：协议仿真设备
测试类型：必选
测试配置： 
测试过程： 1）正确连接设备，配置地址保持互通性。 2）配置 DUT 和协议仿真器的 IPSec。 3）配置 DUT 和协议仿真器采用源、目的地址作选择符，配置 DUT 的 SPD 策略为绕过 IPSec。 4）协议仿真器的一个端口发送数据包
预期结果：协议仿真器的另一个端口观察发现了未应用 IPSec 的数据包
测试说明：
判定原则：测试结果必须与预期结果相符，否则不符合要求

4.3.4 SA 生存期测试

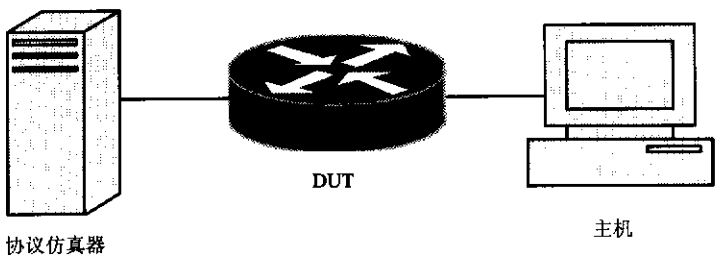
测试编号：32
测试项目：SA 生存期测试
测试目的：验证 IPSec 在 SA 的有效生存期内转发包
测试依据：RFC 2401
测试仪表：协议仿真设备
测试类型：必选
测试配置： 
测试过程： 1）正确连接设备，DUT 为支持被测实现 IPSec 的设备，配置地址保持互通性。 2）配置 DUT 和协议仿真器的 IPSec。 3）配置 DUT 和协议仿真器手工建立 SA，采用源、目的地址作选择符。 4）按持续时间方式配置 SA 的生存期为 10s。 5）在 DUT 观察 SAD 字段的生存期。 6）由协议仿真器向主机发送 Ping 包。 7）等待 10s 后，由协议仿真器向主机发送 Ping 包。 8）按字节方式配置 SA 的生存期为 1k。 9）由协议仿真器向主机发送超过一定流量的 Ping 包
预期结果：步骤 6）后，正确回应；步骤 7）后，无回应；步骤 9）后，当 Ping 包的流量小于 1k 时，正确回应，当 Ping 包的流量大于 1k 时无回应
测试说明：
判定原则：测试结果必须与预期结果相符，否则不符合要求

4.3.5 选择符测试

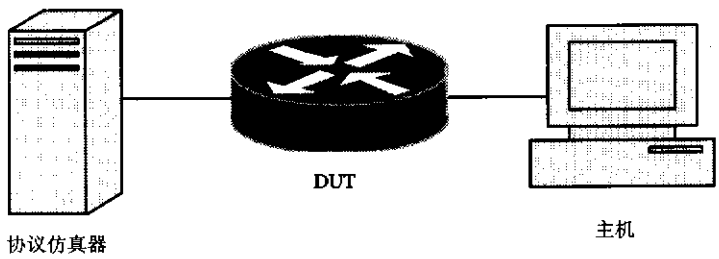
测试编号：33
测试项目：选择符测试
测试目的：验证 IPSec 根据配置的不同选择符转发数据包
测试依据：RFC 2401
测试仪表：协议仿真设备
测试类型：可选
测试配置： 
测试过程： 1）正确连接设备，DUT 为支持被测实现 IPSec 的设备，配置地址保持互通性。 2）配置 DUT 和协议仿真器的 IPSec。 3）配置 DUT 和协议仿真器采用源、目的地址作选择符，由协议仿真器向 DUT 发 Ping 包。 4）配置源、目的端口作选择符，由协议仿真器的一个端口发送 UDP 包。 5）配置上层协议作选择符，由协议仿真器的一个端口发送 UDP 包
预期结果：步骤 3）后协议仿真器正确回应；步骤 4）、5）后协议仿真器的另一个端口收到所发的包
测试说明：
判定原则：测试结果必须与预期结果相符，否则不符合要求

4.4 其他功能测试

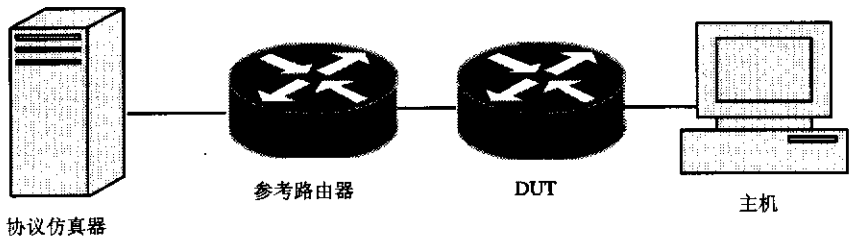
4.4.1 AH ESP 嵌套功能测试

测试编号：34
测试项目：ESP AH 嵌套模式
测试目的：验证 IPSec 的 ESP AH 嵌套模式功能
测试依据：RFC 2401
测试仪表：协议仿真设备
测试类型：可选
测试配置： 
测试过程： 1）正确连接设备，DUT 为支持被测实现 IPSec 的设备，配置地址保持互通性。 2）配置 DUT 和协议仿真器的 IPSec，采用 AH 与 ESP 嵌套的隧道模式，先进行 ESP 隧道封装，在新的 IP 头和 ESP 之间再增加 AH 头，不再添加新的 IP 头。 3）配置 DUT 和协议仿真器采用源、目的地址作选择符。 4）由协议仿真器向主机发 Ping 包。 5）配置 DUT 和协议仿真器的 IPSec，采用 AH 与 ESP 嵌套的传输模式，先进行 ESP 封装，在原 IP 头和 ESP 之间再增加 AH 头。 6）重复步骤 3）和 4）
预期结果：步骤 4）和 6）后协议主机正确回应
测试说明：
判定原则：测试结果必须与预期结果相符，否则不符合要求

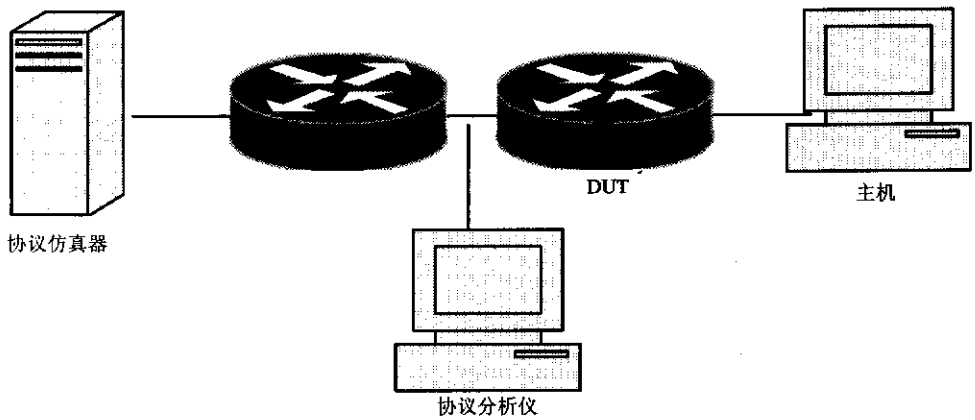
4.4.2 隧道模式 COS 复制测试

测试编号：35
测试项目：隧道模式 COS 字段复制测试
测试目的：验证 IPSec 在隧道模式下复制 COS 字段
测试依据：RFC 2401
测试仪表：协议仿真设备
测试类型：必选
测试配置： 
测试过程： 1）正确连接设备，DUT 为支持被测实现 IPSec 的设备，配置地址保持互通性。 2）配置 DUT 和协议仿真器的 IPSec，使用隧道模式。 3）配置 DUT 和协议仿真器采用源、目的地址作选择符。 4）由协议仿真器向主机发 Ping 包。 5）在发送的 Ping 包上设置优先级。 6）在设备上通过 Debug 查看数据包
预期结果：在 6）步骤中隧道外层 COS 值等于内层所设置 COS
测试说明：
判定原则：测试结果必须与预期结果相符，否则不符合要求

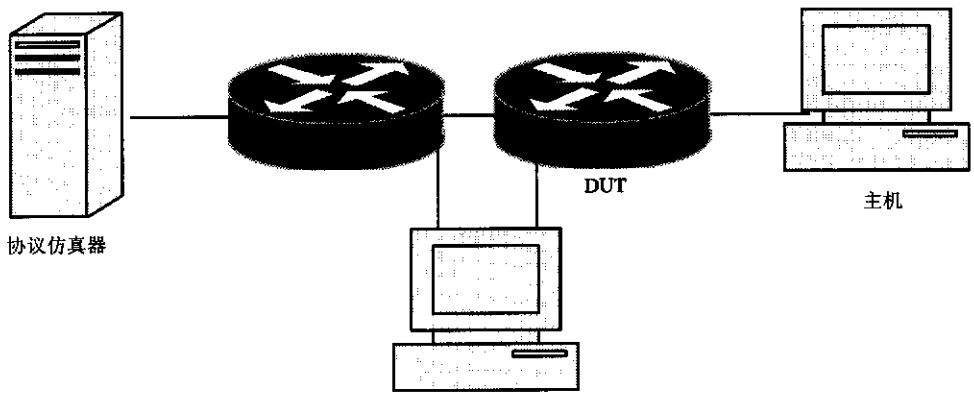
4.4.3 分段重组测试

测试编号：36
测试项目：分段重组测试
测试目的：验证 IPSec 的分段重组功能
测试依据：RFC 2401
测试仪表：协议仿真设备
测试类型：必选
测试配置： 
测试过程： 1）正确连接设备，DUT 为支持被测实现 IPSec 的设备，配置地址保持互通性。 2）配置 DUT 的 MTU 为 1500，配置协议仿真器和参考设备的 MTU 为 576。 3）配置 DUT 和协议仿真器的 IPSec。 4）配置 DUT 和协议仿真器采用源、目的地址作选择符。 5）由主机向协议仿真器发 Ping 包。 5）配置 DUT 的 MTU 为 1200，配置协议仿真器和参考设备的 MTU 为 800。重复步骤 3）~5）
预期结果：步骤 5）和 6）后 Ping 包在 DUT 端重组，并正确回应
测试说明：
测试结果：
判定原则：测试结果必须与预期结果相符，否则不符合要求

4.4.4 抗重播攻击测试

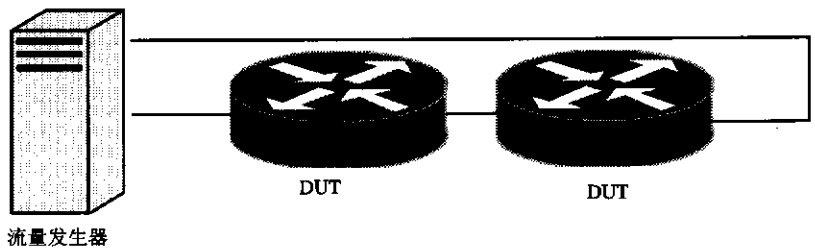
测试编号：37
测试项目：抗重播攻击测试
测试目的：验证 IPSec 的抗重播攻击功能
测试依据：RFC 2401
测试仪表：协议仿真设备
测试类型：必选
测试配置： 
测试过程： 1）正确连接设备，DUT 为支持被测实现 IPSec 的设备，配置地址保持互通性。 2）配置 DUT 和协议仿真器的 IPSec 使用 AH。 3）配置 DUT 和协议仿真器采用源、目的地址作选择符。 4）从协议仿真器发送 Ping 包。 5）在协议分析仪监视设备与 DUT 间的通信，将 Ping 包存储。 6）重播所存储的 Ping 包。 7）配置 DUT 和协议仿真器的 IPSec 使用 ESP，重复步骤 3）~6）
预期结果：步骤 6）、7）后协议仿真器无法收到返回的 Ping 包
测试说明：
判定原则：测试结果必须与预期结果相符，否则不符合要求

4.4.5 完整性检查测试

测试编号：38
测试项目：完整性检查测试
测试目的：验证 IPSec 的完整性检查功能
测试依据：RFC 2401
测试仪表：协议仿真设备
测试类型：必选
测试配置： 
测试过程： 1）正确连接设备，DUT 为支持被测实现 IPSec 的设备，配置地址保持互通性。 2）配置 DUT 和协议仿真器的 IPSec 使用 AH。 3）配置 DUT 和协议仿真器采用源、目的地址作选择符。 4）配置协议分析仪为桥接方式工作。 5）从协议仿真器发送 Ping 包。 6）在协议分析仪监视设备与 DUT 间的通信，将 PING 包内容修改后发送。 7）配置 DUT 和协议仿真器的 IPSec 使用 ESP，重复 3）~6）步骤
预期结果：步骤 6)、7）后协议仿真器无法收到返回的 Ping 包
测试说明：
判定原则：测试结果必须与预期结果相符，否则不符合要求

5 性能测试

5.1 隧道数量测试

测试编号：39
测试项目：设备建立隧道的数量极限
测试目的：测试设备建立隧道的数量极限
测试依据：RFC 2401
测试仪表：协议仿真设备
测试类型：必选
测试配置： 
测试过程： 1）正确连接设备，DUT 为支持被测实现 IPSec 的设备，配置地址保持互通性。 2）配置 DUT 的 IPSec。 3）配置 DUT 采用源、目的地址作选择符，从 DUT 到 DUT 建立隧道。 4）从流量发生器发出不同源地址的包。 5）观察隧道建立数量
预期结果：待定
判定原则：测试结果必须与预期结果相符，否则不符合要求

5.2 单隧道下设备吞吐量测试

测试编号：40

测试项目：测试设备在 IPSec 单隧道下的吞吐量

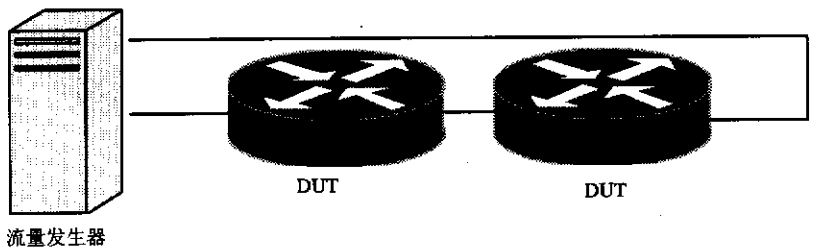
测试目的：测试设备在 IPSec 单隧道下的吞吐量

测试依据：RFC 2401

测试仪表：协议仿真设备

测试类型：必选

测试配置：



测试过程：

1）正确连接设备，DUT 为支持被测实现 IPSec 的设备，配置地址保持互通性。

2）配置 DUT 的 IPSec。

3）配置 DUT 采用源、目的地址作选择符，从 DUT 到 DUT 建立一个隧道。

4）从流量发生器发送不同大小帧的 IP 测试包，测出各种帧大小的丢包率。 帧大小为 64、128、256、512、1024、1280、1518。

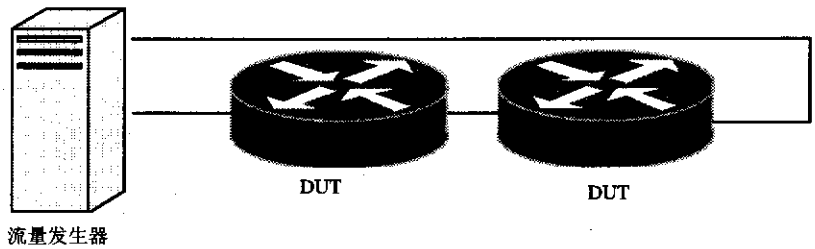
5）测试吞吐量

预期结果：待定

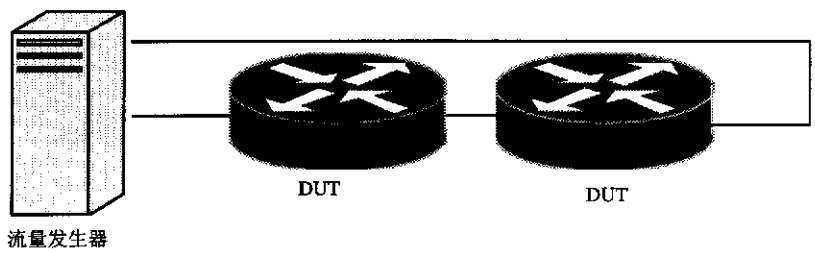
判定原则：测试结果必须与预期结果相符，否则不符合要求

测试说明：测试结果与测试过程中使用的算法有关

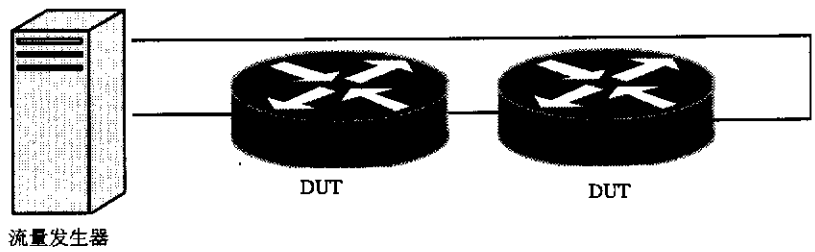
5.3 多隧道下设备吞吐量测试

测试编号：41
测试项目：测试设备在 IPSec 多隧道下的吞吐量
测试目的：测试设备在 IPSec 多隧道下的吞吐量
测试依据：RFC 2401
测试仪表：协议仿真设备
测试类型：必选
测试配置： 
测试过程： 1）正确连接设备，DUT 为支持被测实现 IPSec 的设备，配置地址保持互通性。 2）配置 DUT 的 IPSec。 3）配置 DUT 采用源、目的地址作选择符，从 DUT 到 DUT 建立 256（暂定）个隧道。 4）从流量发生器发送不同大小帧的 IP 测试包，测出各种帧大小的丢包率。 帧大小为 64、128、256、512、1024、1280、1518。 5）测试吞吐量
预期结果：待定
判定原则：测试结果必须与预期结果相符，否则不符合要求
测试说明：测试结果与测试过程中使用的算法有关

5.4 传输时延测试

测试编号：42
测试项目：测试设备在 IPSec 隧道上的传输时延
测试目的：测试设备在 IPSec 隧道上的传输时延
测试依据：RFC 2401
测试仪表：协议仿真设备
测试类型：必选
测试配置： 
测试过程： 1）正确连接设备，DUT 为支持被测实现 IPSec 的设备，配置地址保持互通性。 2）配置 DUT 的 IPSec。 3）配置 DUT 采用源、目的地址作选择符，从 DUT 到 DUT 建立隧道。 5）从流量发生器从流量发生器发送不同大小帧的 IP 测试包，测出各种帧大小的丢包率。 帧大小为 64、128、256、512、1024、1280、518。 6）读取时延
预期结果：待定
判定原则：测试结果必须与预期结果相符，否则不符合要求
测试说明：测试结果与测试过程中使用的算法有关

5.5 丢包率测试

测试编号：43
测试项目：测试设备在 IPSec 隧道上的丢包率
测试目的：测试设备在 IPSec 隧道上的丢包率
测试依据：RFC 2401
测试仪表：协议仿真设备
测试类型：必选
测试配置： 
测试过程： 1）正确连接设备，DUT 为支持被测实现 IPSec 的设备，配置地址保持互通性。 2）配置 DUT 的 IPSec。 3）配置 DUT 采用源、目的地址作选择符，从 DUT 到 DUT 建立隧道。 4）从流量发生器从流量发生器发送不同大小帧的 IP 测试包，测出各种帧大小的丢包率。 帧大小为 64、128、256、512、1024、1280、1518。 5）读取丢包率
预期结果：待定
判定原则：测试结果必须与预期结果相符，否则不符合要求
测试说明：测试结果与测试过程中使用的算法有关