

ICS 35.110  
M 11

**YD**

# 中华人民共和国通信行业标准

YD/T 2392-2011

---

## IP 存储网络安全测试方法

Test methods of IP storage network security

2011-12-20 发布

2011-12-20 实施

---

中华人民共和国工业和信息化部 发布

## 目 次

前 言	II
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 概述	2
6 功能测试	4
6.1 iSCSI 安全功能测试	4
6.2 FCIP 安全功能测试	13
6.3 iFCP 安全功能测试	15
6.4 iSNS 安全功能测试	17
6.5 其他功能测试	27
7 性能测试	30
7.1 隧道数量测试	30
7.2 单隧道下设备吞吐量测试	31
7.3 多隧道下设备吞吐量测试	32
7.4 传输时延测试	33

## 前 言

本标准是通信存储安全系列标准之一，该系列标准预计发布如下：

- 《IP存储网络安全技术要求》
- 《IP存储网络安全测试方法》
- 《通信虚拟磁带库（VTL）安全技术要求》
- 《通信虚拟磁带库（VTL）安全测试方法》
- 《通信存储介质（SSD）加密安全技术要求》
- 《通信存储介质（SSD）加密安全测试方法》

随着灾备相关技术和业务的发展，还将制定后续相关标准。

本标准按照GB/T 1.1—2009给出的规则起草。

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：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。

本标准起草人：姚文斌、杨义先、王 枫、周丽凤。

# IP 存储网络安全测试方法

## 1 范围

本标准规定了利用IPsec为IP存储协议（包括iSCSI、FCIP、iFCP）以及因特网存储名称服务（iSNS）提供安全机制的测试方法，包括iSCSI、FCIP、iFCP和iSNS功能测试和性能测试等。

本标准适用于与IP存储网络有关设备。

## 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，仅所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。

YD/T 1467-2006 IP安全协议（IPSec）测试方法

YD/T 2391-2011 IP存储网络安全技术要求

IETF RFC 2401 IP安全安全架构(Security Architecture for IP)

IETF RFC 3720 因特网小型计算机系统接口（iSCSI）(Internet Small Computer Systems Interface (iSCSI))

IETF RFC 3821 基于IP的光纤信道协议（FCIP）(Fibre Channel Over TCP/IP (FCIP))

IETF RFC 4171 因特网存储名称服务（iSNS）(Internet Storage Name Service (iSNS))

IETF RFC 4172 因特网光纤信道协议（iFCP）(iFCP - A Protocol for Internet Fibre Channel Storage Networking)

IETF RFC 4306 因特网密钥交换协议（IKE）(Internet Key Exchange (IKEv2) Protocol)

## 3 术语和定义

下列术语和定义适用于本文件。

### 3.1

**因特网小型计算机系统接口 Internet Small Computer Systems Interface (iSCSI)**

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。

### 3.2

**因特网安全协议 Internet Protocol Security (IPSec)**

保护IP协议安全通信的标准，对传输途中的信息包进行加密或者防止遭到篡改的一种协议。

### 3.3

**安全远程密码 Secure Remote Password (SRP)**

一种安全的新型密码鉴别和密钥交换协议，提供客户端和服务端间的强相互认证。

### 3.4

**基于IP的光纤信道协议 Fiber Channel Over IP (FCIP)**

一种在TCP/IP上用管道技术实现光纤信道协议的机制，能够通过IP网络将各个孤立的光纤信道存储区域网络连接起来，从而形成一个统一的存储区域网络。

## 3.5

因特网光纤信道协议 Internet Fibre Channel Protocol (iFCP)

一种网关到网关的协议，为 TCP/IP 网络上的光纤设备提供光纤信道通信服务，可以实现端到端的 IP 连接。

## 3.6

启动器 Initiator

IP 存储网络中的服务器或工作站，发起对目标存储设备的事务。

## 3.7

目标器 Target

IP 存储网络中的存储设备。

## 3.8

因特网存储名称服务 Internet Storage Name Service (iSNS)

一种在 IP 网络中智能搜索存储设备的协议和机制，有助于在 TCP/IP 网络上自动发现、管理和配置光纤通道设备。

## 4 缩略语

下列缩略语适用于本文件。

AH	Authentication Header	认证头
CHAP	Challenge Handshake Authentication Protocol	挑战握手认证协议
DUT	Device Under Tester	被测设备
ESP	Encapsulating Security Payload	封装安全载荷
HMAC	HASH MAC	散列 MAC
IKE	Internet Key Exchange	因特网密钥交换
IP	Internet Protocol	互联网协议
IPSec	IP Security	IP 安全
MAC	Media Access Control	媒体接入控制
NAPT	Network Address Port Translation	网络地址端口转换
NAT	Network Address Translation	网络地址转换
SA	Security Association	安全联盟
SHA-1	Secure Hash Algorithm-1	安全散列算法-1
TCP	Transmission Control Protocol	传输控制协议
VPN	Virtual Private Network	虚拟专用网络

## 5 概述

本标准提供对 IP 存储协议（包括 iSCSI、FCIP、iSNS）以及因特网存储名称服务（iSNS）的安全功能测试，以及同等条件下的性能测试，包括：隧道数量测试、单隧道下设备吞吐量测试、多隧道下设备吞吐量测试、传输时延测试、丢包率测试。

表 1 给出了本标准具体测试项目的一览表。

表1 本标准具体的测试项目

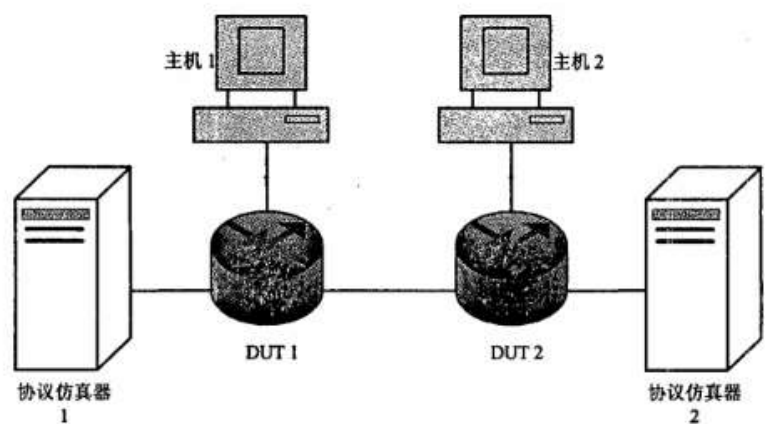
6 功能测试	6.1 iSCSI安全功能测试	6.1.1 CHAP认证	6.1.1.1 iSCSI协议: CHAP认证
			6.1.1.2 CHAP认证: 目标器验证启动器
			6.1.1.3 目标器、启动器使用相同CHAP认证密钥时的处理
			6.1.1.4 CHAP认证: 128bit的随机密钥加密方式
			6.1.1.5 CHAP认证: 不应重复使用相同的双向认证CHAP挑战
		6.1.2 SRP认证	6.1.2.1 iSCSI协议: SRP认证
			6.1.2.2 SRP认证: 常用SRP组, 附加SRP组
			6.1.2.3 SRP认证: 启动器与目标器必须支持高达1536bit的SRP组
		6.1.3 iSCSI安全: IPSec保护机制	
	6.2 FCIP安全功能测试	6.2.1	FCIP: 双向认证
		6.2.2	FCIP安全: IPSec安全机制
	6.3 iFCP安全功能测试	6.3.1	iFCP: 双向认证
		6.3.2	iFCP安全: IPSec安全机制
	6.4 iSNS安全功能测试	6.4.1	iSNS安全: IPSec重放保护机制
		6.4.2	iSNS安全: 服务器支持ESP隧道模式
		6.4.3	iSNS安全: 服务器支持ESP传输模式
		6.4.4	ESP: AES-XCBC-MAC认证、隧道模式
		6.4.5	ESP: AES-XCBC-MAC认证、传输模式
		6.4.6	iSNS: IKE认证
		6.4.7	iSNS: 预共享密钥认证
		6.4.8	iSNS: 数字签名证书的端认证
		6.4.9	iSNS: IKE主模式
		6.4.10	iSNS: IKE野蛮模式
	6.5 其他功能测试	6.5.1	IP存储网络安全机制: 完整性检查测试
		6.5.2	IP存储网络安全机制: SA功能测试
		6.5.3	IP存储网络安全机制: 兼容现有的安全机制
7 性能测试	7.1 隧道数量测试		
	7.2 单隧道下设备吞吐量测试		
	7.3 多隧道下设备吞吐量测试		
	7.4 传输时延测试		
	7.5 丢包率测试		

## 6 功能测试

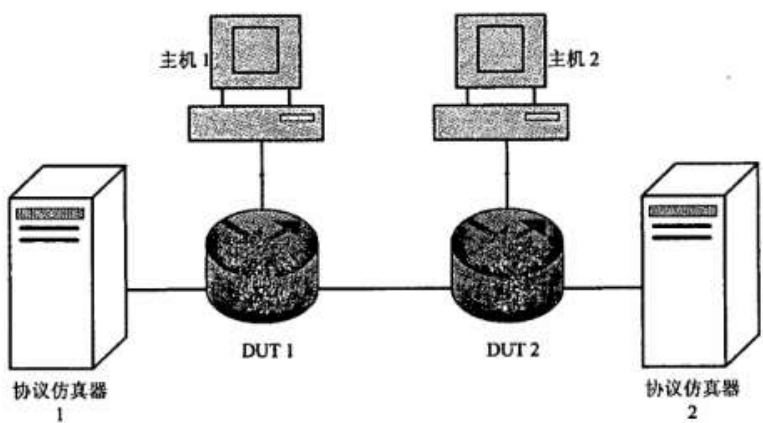
## 6.1 iSCSI 安全功能测试

## 6.1.1 CHAP 认证

## 6.1.1.1 iSCSI 协议：CHAP 认证

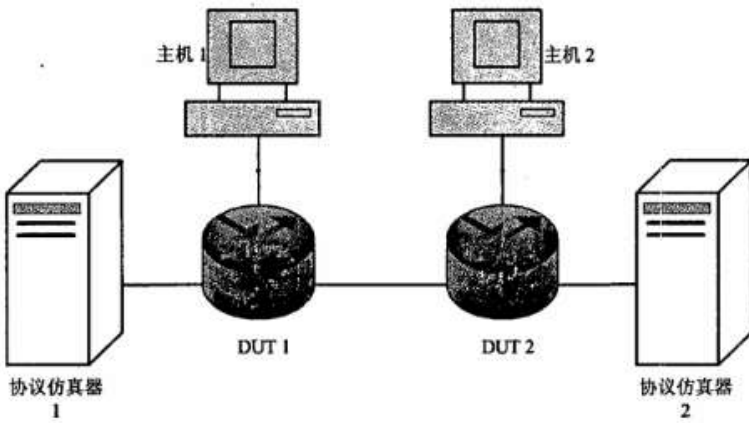
测试编号：1
测试项目：iSCSI协议：CHAP认证
测试目的：验证iSCSI协议支持CHAP认证
测试依据：IETF RFC 3720
测试仪表：协议仿真设备
测试类型：必选
<p>测试配置：</p>  <pre> graph LR     H1[主机1] --- DUT1((DUT 1))     H2[主机2] --- DUT2((DUT 2))     DUT1 --- DUT2     DUT1 --- PF1[协议仿真器 1]     DUT2 --- PF2[协议仿真器 2] </pre>
<p>测试过程：</p> <ol style="list-style-type: none"> <li>1) 正确连接设备，DUT为支持被测实现iSCSI的设备，其中DUT 1为启动器，DUT 2为目标器，配置地址保持互通性；</li> <li>2) 配置DUT和协议仿真器的iSCSI协议，采用：iSCSI协议，CHAP认证；</li> <li>3) 配置DUT和协议仿真器采用源、目的地址作为选择符；</li> <li>4) 分别由协议仿真器 1向DUT 1、协议仿真器 2向DUT 2发送Ping包</li> </ol>
预期结果：步骤4) 后DUT 1、DUT 2分别正确回应
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：无

## 6.1.1.2 CHAP 认证：目标器验证启动器

测试编号：2
测试项目：CHAP认证：目标器验证启动器
测试目的：测试当启动器认证失败时，目标器所做的处理
测试依据：IETF RFC 3720
测试仪表：协议仿真设备
测试类型：必选
测试配置：  <p>The diagram illustrates the test setup. On the left, a host labeled '主机1' is connected to a device labeled 'DUT 1'. Below 'DUT 1' is a box labeled '协议仿真器 1'. On the right, a host labeled '主机2' is connected to a device labeled 'DUT 2'. Below 'DUT 2' is a box labeled '协议仿真器 2'. A horizontal line connects 'DUT 1' and 'DUT 2', representing the network connection between the initiator and the target.</p>
测试过程： <ol style="list-style-type: none"> <li>1) 正确连接设备，DUT为支持被测实现iSCSI的设备，其中DUT 1为启动器，DUT 2为目标器，配置地址保持互通性；</li> <li>2) 配置DUT和协议仿真器的iSCSI协议，采用：iSCSI协议，CHAP认证；</li> <li>3) 配置DUT和协议仿真器采用源、目的地址作为选择符；</li> <li>4) 由启动器DUT 1向目标器DUT 2发起错误CHAP挑战，目标器DUT 2计算散列值并做比较验证操作</li> </ol>
预期结果：步骤4)后启动器DUT 1认证失败，目标器DUT 2不回送CHAP回应，同时关闭iSCSI的TCP连接
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：无



## 6.1.1.3 目标器、启动器使用相同 CHAP 认证密钥时的处理

测试编号: 3
测试项目: 启动器、目标器使用相同 CHAP 认证密钥时的处理
测试目的: 验证当启动器、目标器使用相同 CHAP 认证密钥时, 启动器认证失败
测试依据: IETF RFC 3720
测试仪表: 协议仿真设备
测试类型: 必选
测试配置:  <p>The diagram illustrates a test setup. At the top, there are two host icons labeled '主机 1' (Host 1) and '主机 2' (Host 2). Below them are two disk-like icons representing DUTs, labeled 'DUT 1' and 'DUT 2'. Host 1 is connected to DUT 1. Host 2 is connected to both DUT 1 and DUT 2. DUT 1 is connected to a server rack icon labeled '协议仿真器 1' (Protocol Emulator 1). DUT 2 is connected to a server rack icon labeled '协议仿真器 2' (Protocol Emulator 2).</p>
测试过程: <ol style="list-style-type: none"> <li>1) 正确连接设备, DUT 为支持被测实现 iSCSI 的设备, 其中 DUT 1 为启动器, DUT 2 为目标器, 配置地址保持互通性;</li> <li>2) 配置 DUT 和协议仿真器的 iSCSI 协议, 采用: iSCSI 协议, CHAP 认证, 启动器与目标器使用相同的 CHAP 认证密钥;</li> <li>3) 配置 DUT 和协议仿真器采用源、目的地址作为选择符;</li> <li>4) 由启动器 DUT 1 向目标器 DUT 2 发起 CHAP 挑战, 目标器 DUT 2 计算散列值并做比较验证操作</li> </ol>
预期结果: 步骤 4) 后启动器 DUT 1 认证失败, 目标器 DUT 2 不回送 CHAP 回应, 同时关闭 iSCSI 的 TCP 连接
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: 无

## 6.1.1.4 CHAP 认证: 128bit 的随机密钥加密方式

测试编号: 4

测试项目: CHAP 认证: 128bit 的随机密钥加密方式

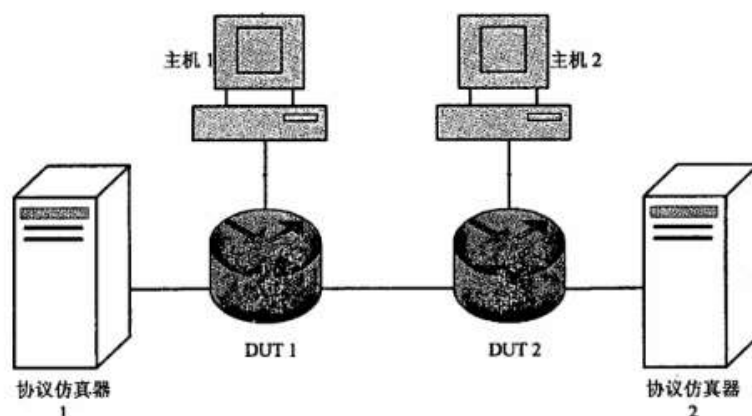
测试目的: 验证 CHAP 认证支持 128bit 的随机密钥加密方式

测试依据: IETF RFC 3720

测试仪表: 协议仿真设备

测试类型: 必选

测试配置:



测试过程:

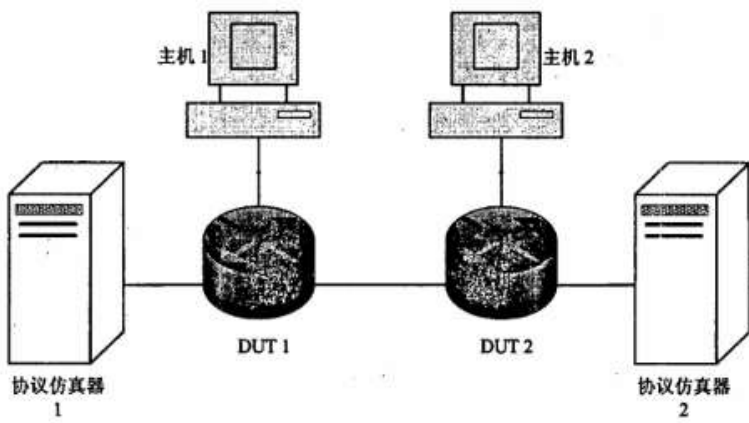
- 1) 正确连接设备, DUT 为支持被测实现 iSCSI 的设备, 其中 DUT 1 为启动器, DUT 2 为目标器, 配置地址保持互通性;
- 2) 配置 DUT 和协议仿真器的 iSCSI 协议, 采用: iSCSI 协议, CHAP 认证, 采用 128bit 的随机密钥加密方式;
- 3) 配置 DUT 和协议仿真器采用源、目的地址作为选择符;
- 4) 分别由协议仿真器 1 向 DUT 1、协议仿真器 2 向 DUT 2 发送 Ping 包

预期结果: 步骤 4) 后 DUT 1、DUT 2 分别正确回应

判定原则: 测试结果必须与预期结果相符, 否则不符合要求

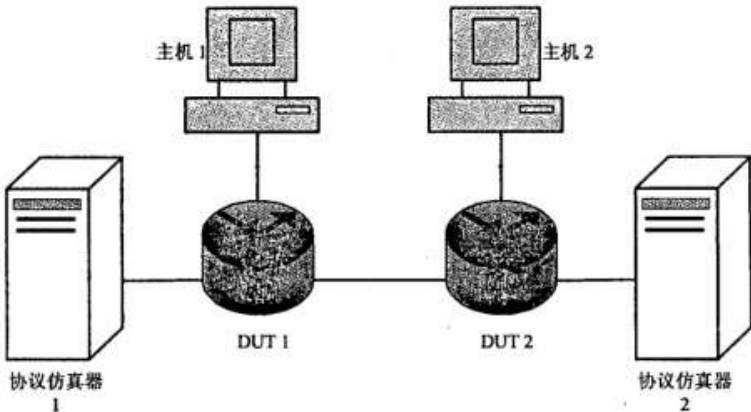
测试说明: 无

## 6.1.1.5 CHAP 认证：不应重复使用相同的双向认证 CHAP 挑战

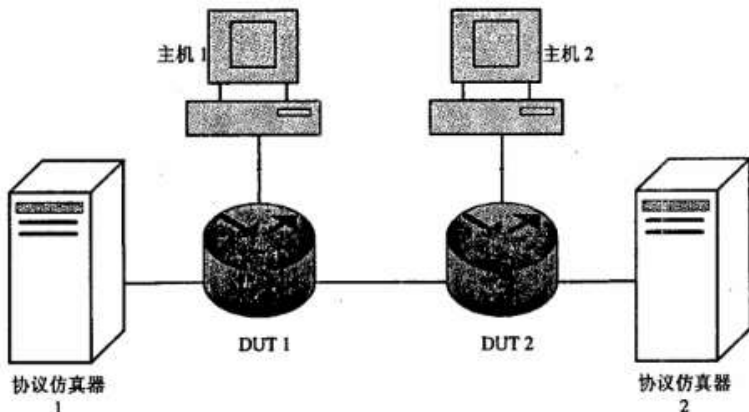
测试编号：5
测试项目：CHAP 认证：不应重复使用相同的双向认证 CHAP 挑战
测试目的：验证重复使用相同的双向认证 CHAP 挑战时所做的处理
测试依据：IETF RFC 3720
测试仪表：协议仿真设备
测试类型：必选
测试配置：  <p>The diagram illustrates a network setup for testing CHAP authentication. It features two hosts, labeled '主机 1' and '主机 2', each represented by a computer icon. Below each host is a corresponding DUT (Device Under Test), labeled 'DUT 1' and 'DUT 2', represented by a server icon. DUT 1 is connected to '协议仿真器 1' (Protocol Simulator 1), and DUT 2 is connected to '协议仿真器 2' (Protocol Simulator 2). The two DUTs are also connected to each other, forming a central link. The entire setup is enclosed in a rectangular box.</p>
测试过程： <ol style="list-style-type: none"> <li>1) 正确连接设备，DUT 为支持被测实现 iSCSI 的设备，其中 DUT 1 为启动器，DUT 2 为目标器，配置地址保持互通性；</li> <li>2) 配置 DUT 和协议仿真器的 iSCSI 协议，采用：iSCSI 协议，CHAP 认证，双向认证；</li> <li>3) 配置 DUT 和协议仿真器采用源、目的地址作为选择符；</li> <li>4) 由启动器 DUT 1 向目标器 DUT 2 发起重复的 CHAP 挑战</li> </ol>
预期结果：步骤 4) 后 iSCSI 的 TCP 连接断开
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：无

## 6.1.2 SRP 认证

## 6.1.2.1 iSCSI 协议: SRP 认证

测试编号: 6
测试项目: iSCSI 协议: SRP 认证
测试目的: 验证 iSCSI 协议支持 SRP 认证
测试依据: IETF RFC 3720
测试仪表: 协议仿真设备
测试类型: 可选
测试配置: 
测试过程: <ol style="list-style-type: none"> <li>1) 正确连接设备, DUT 为支持被测实现 iSCSI 的设备, 其中 DUT 1 为启动器, DUT 2 为目标器, 配置地址保持互通性;</li> <li>2) 配置 DUT 和协议仿真器的 iSCSI 协议, 采用: iSCSI 协议, SRP 认证;</li> <li>3) 配置 DUT 和协议仿真器采用源、目的地址作为选择符;</li> <li>4) 分别由协议仿真器 1 向 DUT 1、协议仿真器 2 向 DUT 2 发 Ping 包</li> </ol>
测试结果: 步骤 4) 后 DUT 1、DUT 2 分别正确回应
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: 无

## 6.1.2.2 SRP 认证: 常用 SRP 组, 附加 SRP 组

测试编号: 7
测试项目: SRP 认证: 常用 SRP 组, 附加 SRP 组
测试目的: 验证 SRP 认证应支持常用 SRP 组, 可以支持附加 SRP 组
测试依据: IETF RFC 3720
测试仪表: 协议仿真设备
测试类型: 可选
测试配置:  <p>The diagram illustrates a network setup for SRP authentication testing. It features two hosts, labeled '主机 1' (Host 1) and '主机 2' (Host 2), each connected to a corresponding DUT (Device Under Test), 'DUT 1' and 'DUT 2'. DUT 1 is connected to '协议仿真器 1' (Protocol Emulator 1) and DUT 2 is connected to '协议仿真器 2' (Protocol Emulator 2). Additionally, DUT 1 and DUT 2 are connected to each other, forming a central link between the two test environments.</p>
测试过程: <ol style="list-style-type: none"> <li>1) 正确连接设备, DUT 为支持被测实现 iSCSI 的设备, 其中 DUT 1 为启动器, DUT 2 为目标器, 配置地址保持互通性;</li> <li>2) 配置 DUT 和协议仿真器的 iSCSI 协议, 采用: iSCSI 协议, SRP 认证, 使用常用 SRP 组 (SRP-768, SRP-1024, SRP-1280, SRP-1536, SRP-2048);</li> <li>3) 配置 DUT 和协议仿真器采用源、目的地址作为选择符;</li> <li>4) 分别由协议仿真器 1 向 DUT 1、协议仿真器 2 向 DUT 2 发 Ping 包;</li> <li>5) 配置 DUT 和协议仿真器的 iSCSI 协议, 采用: iSCSI 协议, SRP 认证, 使用附加 SRP 组 (MODP-3072, MODP-4096, MODP-6144, MODP-8192);</li> <li>6) 分别由协议仿真器 1 向 DUT 1、协议仿真器 2 向 DUT 2 发 Ping 包</li> </ol>
预期结果: 步骤 4) 和 6) 后 DUT 1、DUT 2 分别正确回应
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: 无

## 6.1.2.3 SRP 认证: 启动器与目标器必须支持高达 1536bit 的 SRP 组

测试编号: 8

测试项目: SRP 认证: 启动器与目标器必须支持高达 1536bit 的 SRP 组

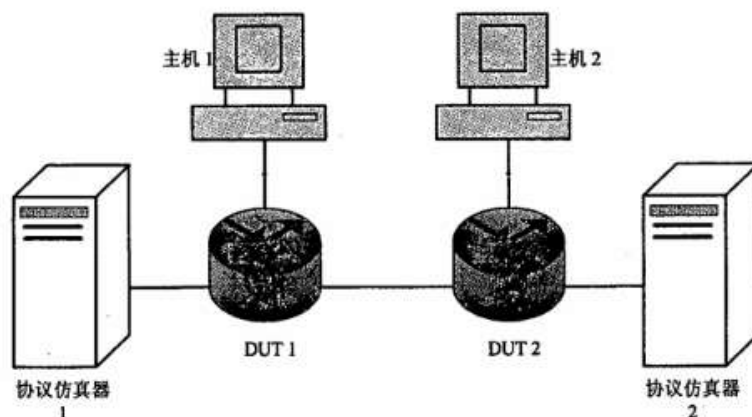
测试目的: 验证 SRP 认证中, 启动器、目标器必须支持高达 1536bit 的 SRP 组

测试依据: IETF RFC 3720

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 iSCSI 的设备, 其中 DUT 1 为启动器, DUT 2 为目标器, 配置地址保持互通性;
- 2) 配置 DUT 和协议仿真器的 iSCSI 协议, 采用: iSCSI 协议, SRP 认证, 使用 1536bit 的 SRP 组 (SRP-768, SRP-1024, SRP-1280, SRP-1536);
- 3) 配置 DUT 和协议仿真器采用源、目的地址作为选择符;
- 4) 分别由协议仿真器 1 向 DUT 1、协议仿真器 2 向 DUT 2 发 Ping 包

预期结果: 步骤 4) 后, DUT 1、DUT 2 分别正确回应

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: 无

## 6.1.3 iSCSI 安全: IPSec 保护机制

测试编号: 9
测试项目: iSCSI 安全: IPSec 保护机制
测试目的: 验证 iSCSI 与 IPSec 交互使用, 具有保障传输数据安全的功能
测试依据: IETF RFC 3720, YD/T 1467-2006
测试仪表: 协议仿真设备
测试类型: 必选
测试配置: <div style="text-align: center;"> <p>The diagram illustrates the test setup. It features two hosts, '主机 1' and '主机 2', each represented by a computer icon. '主机 1' is connected to 'DUT 1' (Device Under Test 1), and '主机 2' is connected to 'DUT 2' (Device Under Test 2). 'DUT 1' and 'DUT 2' are connected to each other via a central line. Additionally, 'DUT 1' is connected to '协议仿真器 1' (Protocol Simulator 1), and 'DUT 2' is connected to '协议仿真器 2' (Protocol Simulator 2). The protocol simulators are represented by server rack icons.</p> </div>
测试过程: <ol style="list-style-type: none"> <li>1) 正确连接设备, DUT 为支持被测实现 iSCSI、IPSec 的设备, 其中 DUT 1 为启动器, DUT 2 为目标器, 配置地址保持互通性;</li> <li>2) 按照 YD/T 1467-2006 4 功能测试相关规定测试</li> </ol>
预期结果: 步骤 2) 后, DUT 1、DUT 2 分别具备 IPSec 保护功能
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: 无

## 6.2 FCIP 安全功能测试

## 6.2.1 FCIP: 双向认证

测试编号: 10

测试项目: FCIP: 双向认证

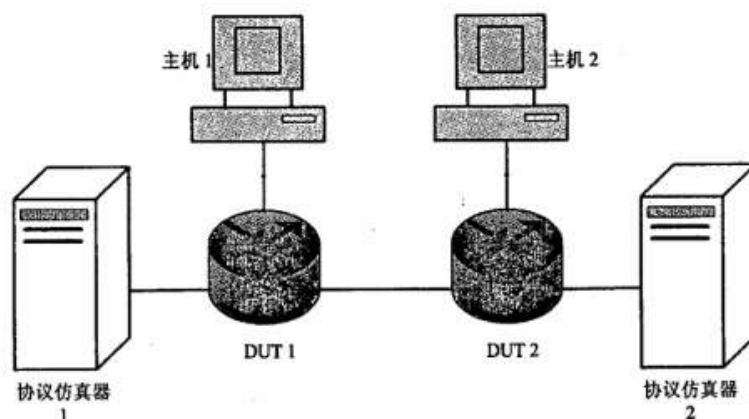
测试目的: 验证 FCIP 协议应支持双向认证

测试依据: IETF RFC 3821

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 FCIP 的设备, 其中 DUT 1 为启动器, DUT 2 为目标器, 配置地址保持互通性;
- 2) 配置 DUT 和协议仿真器的 FCIP 协议, 采用: FCIP 协议, 双向认证;
- 3) 配置 DUT 和协议仿真器采用源、目的地址作为选择符;
- 4) 分别由协议仿真器 1 向 DUT 1、协议仿真器 2 向 DUT 2 发 Ping 包

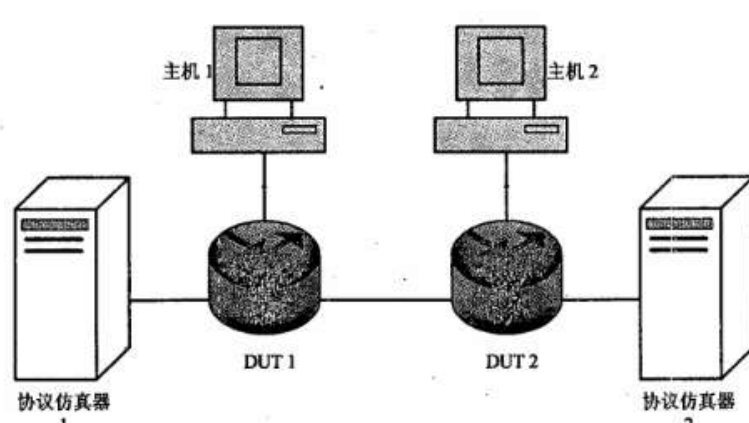
预期结果: 步骤 4) 后, DUT 1、DUT 2 分别正确回应

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: 无

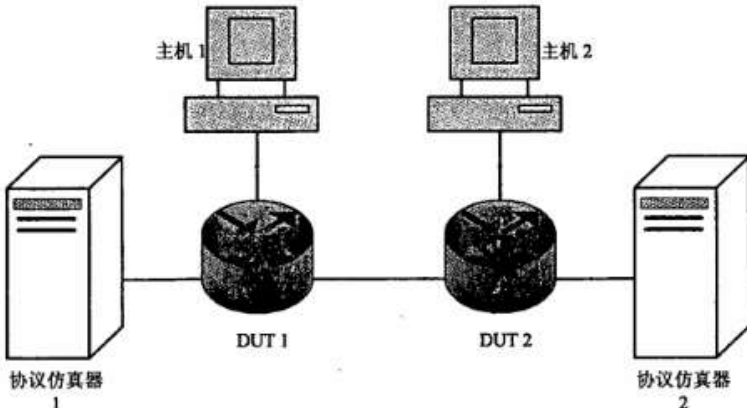


## 6.2.2 FCIP 安全: IPSec 安全机制

测试编号: 11
测试项目: FCIP 安全: IPSec 保护机制
测试目的: 验证 FCIP 与 IPSec 交互使用, 具有保障传输数据安全的功能
测试依据: IETF RFC 3821, YD/T 1467-2006
测试仪表: 协议仿真设备
测试类型: 必选
测试配置:  <p>The diagram illustrates the test configuration. It shows two hosts, 主机 1 and 主机 2, connected to two devices, DUT 1 and DUT 2. DUT 1 is connected to 主机 1 and 主机 2. DUT 2 is connected to 主机 2 and 协议仿真器 2. 协议仿真器 1 is connected to DUT 1. 协议仿真器 2 is connected to DUT 2.</p>
测试过程: <ol style="list-style-type: none"> <li>1) 正确连接设备, DUT 为支持被测实现 FCIP、IPSec 的设备, 其中 DUT 1 为启动器, DUT 2 为目标器, 配置地址保持互通性;</li> <li>2) 按照 YD/T 1467-2006 4 功能测试相关规定测试</li> </ol>
预期结果: 步骤 2) 后, DUT 1、DUT 2 分别具备 IPSec 保护功能
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: 无

## 6.3 iFCP 安全功能测试

## 6.3.1 iFCP: 双向认证

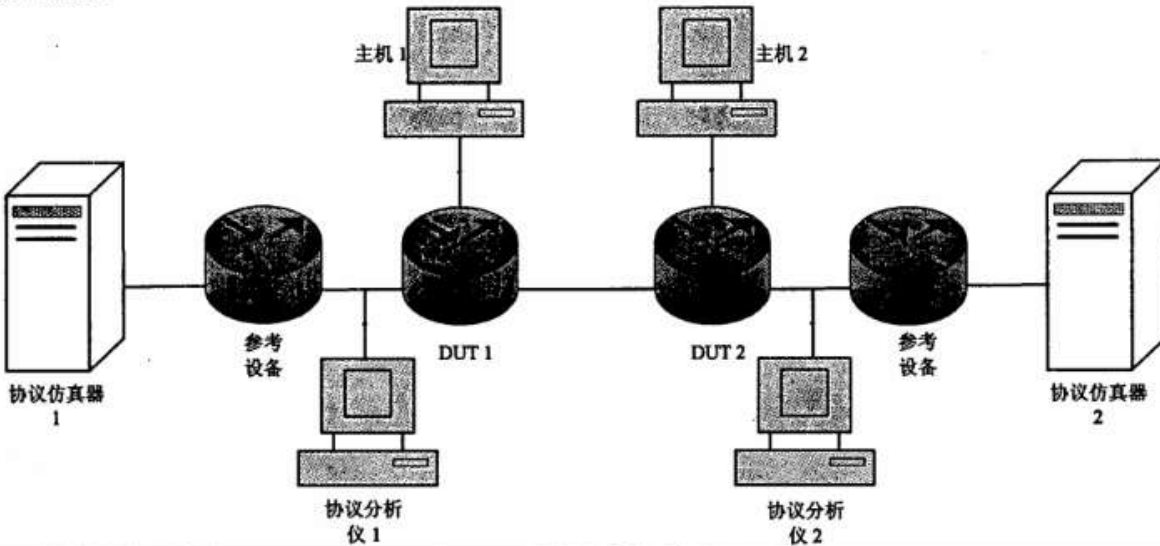
测试编号: 12
测试项目: iFCP: 双向认证
测试目的: 验证 iFCP 协议应支持双向认证
测试依据: IETF RFC 4172
测试仪表: 协议仿真设备
测试类型: 必选
测试配置: 
测试过程: <ol style="list-style-type: none"> <li>1) 正确连接设备, DUT 为支持被测实现 iFCP 的设备, 其中 DUT 1 为启动器, DUT 2 为目标器, 配置地址保持互通性;</li> <li>2) 配置 DUT 和协议仿真器的 iFCP 协议, 采用: iFCP 协议, 双向认证;</li> <li>3) 配置 DUT 和协议仿真器采用源、目的地址作为选择符;</li> <li>4) 分别由协议仿真器 1 向 DUT 1、协议仿真器 2 向 DUT 2 发 Ping 包</li> </ol>
预期结果: 步骤 4) 后, DUT 1、DUT 2 分别正确回应
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: 无

## 6.3.2 iFCP 安全: IPsec 安全机制

测试编号: 13
测试项目: iFCP 安全: IPsec 保护机制
测试目的: 验证 iFCP 与 IPsec 交互使用, 具有保障传输数据安全的功能
测试依据: IETF RFC 4172, YD/T 1467-2006
测试仪表: 协议仿真设备
测试类型: 必选
测试配置: <div style="text-align: center;"> <pre> graph LR     subgraph Hosts         H1[主机 1]         H2[主机 2]     end     subgraph DUTs         DUT1[DUT 1]         DUT2[DUT 2]     end     subgraph Simulators         S1[协议仿真器 1]         S2[协议仿真器 2]     end     H1 --- DUT1     H2 --- DUT2     DUT1 --- DUT2     DUT1 --- S1     DUT2 --- S2           </pre> </div>
测试过程: <ol style="list-style-type: none"> <li>1) 正确连接设备, DUT 为支持被测实现 iFCP、IPsec 的设备, 其中 DUT 1 为启动器, DUT 2 为目标器, 配置地址保持互通性;</li> <li>2) 按照 YD/T 1467-2006 4 功能测试相关规定测试</li> </ol>
预期结果: 步骤 2) 后, DUT 1、DUT 2 分别具备 IPsec 保护功能
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: 无

## 6.4 iSNS 安全功能测试

## 6.4.1 iSNS 安全: IPSec 重放保护机制

测试编号: 14
测试项目: iSNS 安全: IPSec 重放保护机制
测试目的: 验证 iSNS 实现的安全机制支持 IPSec 的重放保护机制
测试依据: IETF RFC 4171, YD/T 1467-2006
测试仪表: 协议仿真设备
测试类型: 必选
测试配置: 
测试过程: <ol style="list-style-type: none"> <li>1) 正确连接设备, DUT 为支持被测实现 iSNS、IPSec 的设备, 其中 DUT 1 为客户端, DUT 2 为服务器端, 配置地址保持互通性;</li> <li>2) 按照 YD/T 1467-2006 4.4.4 抗重播攻击测试规定的方法测试</li> </ol>
预期结果: 步骤 2) 后, 协议仿真器 1、协议仿真器 2 均无法收到返回的 Ping 包
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: 无

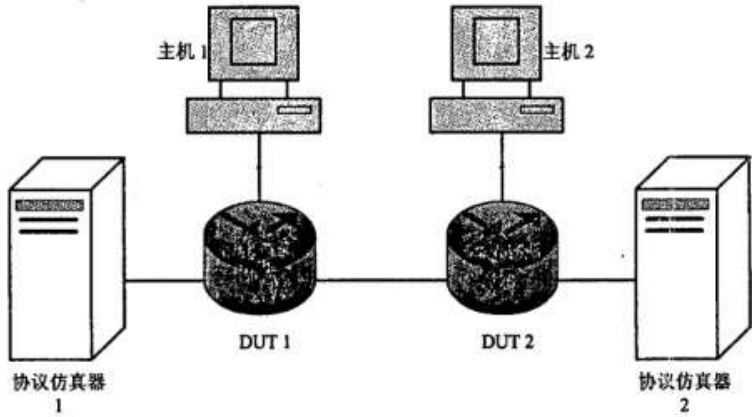
## 6.4.2 iSNS 安全：服务器支持 ESP 隧道模式

测试编号：15
测试项目：iSNS 安全：服务器支持 ESP 隧道模式
测试目的：验证 iSNS 实现的安全机制中，iSNS 服务器支持 ESP 隧道模式
测试依据：IETF RFC 4171，YD/T 1467-2006
测试仪表：协议仿真设备
测试类型：必选
测试配置： <div style="text-align: center;"> <pre> graph LR     H1[主机 1] --- DUT1[DUT 1]     H2[主机 2] --- DUT1     H2 --- DUT2[DUT 2]     DUT1 --- DUT2     DUT1 --- PF1[协议仿真器 1]     DUT2 --- PF2[协议仿真器 2]           </pre> </div>
测试过程： <ol style="list-style-type: none"> <li>1) 正确连接设备，DUT 为支持被测实现 iSNS、IPSec 的设备，其中 DUT 1 为客户端，DUT 2 为服务器端，配置地址保持互通性；</li> <li>2) 只针对 DUT 2 进行测试，按照 YD/T 1467-2006 4 功能测试中相关 ESP 隧道模式规定的方法测试</li> </ol>
预期结果：步骤 2) 后，iSNS 服务器端 DUT 2 具备 IPSec：ESP 隧道模式功能
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：无

## 6.4.3 iSNS 安全：服务器支持 ESP 传输模式

测试编号：16
测试项目：iSNS 安全：服务器支持 ESP 传输模式
测试目的：验证 iSNS 实现的安全机制中，iSNS 服务器支持 ESP 传输模式
测试依据：IETF RFC 4171，YD/T 1467-2006
测试仪表：协议仿真设备
测试类型：可选
测试配置： <pre> graph LR     subgraph Hosts         H1[主机 1]         H2[主机 2]     end     subgraph DUTs         DUT1[DUT 1]         DUT2[DUT 2]     end     subgraph Simulators         S1[协议仿真器 1]         S2[协议仿真器 2]     end     H1 --- DUT1     H2 --- DUT2     DUT1 --- DUT2     DUT1 --- S1     DUT2 --- S2   </pre>
测试过程： <ol style="list-style-type: none"> <li>1) 正确连接设备，DUT 为支持被测实现 iSNS、IPSec 的设备，其中 DUT 1 为客户端，DUT 2 为服务器端，配置地址保持互通性；</li> <li>2) 只针对 DUT 2 进行测试，按照 YD/T 1467-2006 4 功能测试中相关 ESP 隧道模式规定的方法测试</li> </ol>
预期结果：步骤 2) 后，iSNS 服务器端 DUT 2 具备 IPSec：ESP 传输模式功能
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：无

## 6.4.4 ESP: AES-XCBC-MAC 认证、隧道模式

测试编号: 17
测试项目: ESP: AES-XCBC-MAC 认证、隧道模式
测试目的: 验证 iSNS 安全机制具有 AES-XCBC-MAC 认证、隧道模式的 ESP 功能
测试依据: IETF RFC 4171
测试仪表: 协议仿真设备
测试类型: 必选
测试配置: 
测试过程: <ol style="list-style-type: none"> <li>1) 正确连接设备, DUT 为支持被测实现 iSNS、IPSec 的设备, 其中 DUT 1 为客户端, DUT 2 为服务器端, 配置地址保持互通性;</li> <li>2) 配置 DUT 和协议仿真器的 iSNS 和 IPSec, 采用: iSNS, IPSec, ESP: AES-XCBC-MAC 认证、隧道模式;</li> <li>3) 配置 DUT 和协议仿真器采用源、目的地址作为选择符;</li> <li>4) 分别由协议仿真器 1 向主机 1、协议仿真器 2 向主机 2 发 Ping 包;</li> <li>5) 配置 DUT 和协议仿真器的 iSNS 和 IPSec, 采用: iSNS, IPSec, ESP: AES-XCBC-MAC 认证+HMAC-MD5-96 隧道模式;</li> <li>6) 分别由协议仿真器 1 向主机 1、协议仿真器 2 向主机 2 发 Ping 包;</li> <li>7) 配置 DUT 和协议仿真器的 iSNS 和 IPSec, 采用: iSNS, IPSec, ESP: AES-XCBC-MAC 认证+HMAC-SHA-1-96、隧道模式;</li> <li>8) 分别由协议仿真器 1 向主机 1、协议仿真器 2 向主机 2 发 Ping 包</li> </ol>
预期结果: 步骤 4)、6)、8) 后, 主机 1、主机 2 分别正确回应
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: 无

## 6.4.5 ESP: AES-XCBC-MAC 认证、传输模式

测试编号: 18

测试项目: ESP: AES-XCBC-MAC 认证、传输模式

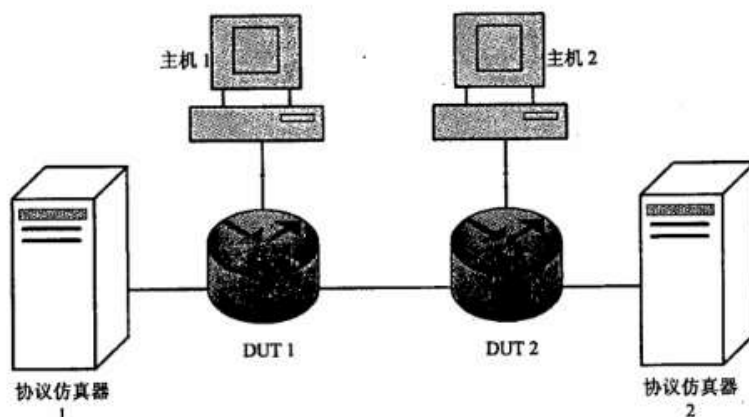
测试目的: 验证 iSNS 安全机制具有 AES-XCBC-MAC 认证、传输模式的 ESP 功能

测试依据: IETF RFC 4171

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 iSNS、IPSec 的设备, 其中 DUT 1 为客户端, DUT 2 为服务器端, 配置地址保持互通性;
- 2) 配置 DUT 和协议仿真器的 iSNS 和 IPSec, 采用: iSNS, IPSec, ESP: AES-XCBC-MAC 认证、传输模式;
- 3) 配置 DUT 和协议仿真器采用源、目的地址作为选择符;
- 4) 分别由协议仿真器 1 向 DUT 1、协议仿真器 2 向 DUT 2 发 Ping 包;
- 5) 配置 DUT 和协议仿真器的 iSNS 和 IPSec, 采用: iSNS, IPSec, ESP: AES-XCBC-MAC 认证+HMAC-MD5-96、传输模式;
- 6) 分别由协议仿真器 1 向 DUT 1、协议仿真器 2 向 DUT 2 发 Ping 包;
- 7) 配置 DUT 和协议仿真器的 iSNS 和 IPSec, 采用: iSNS, IPSec, ESP: AES-XCBC-MAC 认证+HMAC-SHA-1-96、传输模式;
- 8) 分别由协议仿真器 1 向 DUT 1、协议仿真器 2 向 DUT 2 发 Ping 包

预期结果: 步骤 4)、6)、8) 后, DUT 1、DUT 2 分别正确回应

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: 无



## 6.4.6 iSNS: IKE 认证

测试编号: 19
测试项目: iSNS: IKE 认证
测试目的: 验证 iSNS 支持 IKE 认证
测试依据: IETF RFC 4306
测试仪表: 协议仿真设备
测试类型: 必选
测试配置: <div style="text-align: center;"> <pre> graph LR     H1[主机 1] --- DUT1[DUT 1]     H2[主机 2] --- DUT1     H2 --- DUT2[DUT 2]     DUT1 --- DUT2     DUT1 --- PF1[协议仿真器 1]     DUT2 --- PF2[协议仿真器 2]           </pre> </div>
测试过程: <ol style="list-style-type: none"> <li>1) 正确连接设备, DUT 为支持被测实现 iSNS、IPSec 的设备, 其中 DUT 1 为客户端, DUT 2 为服务器端, 配置地址保持互通性;</li> <li>2) 配置 DUT 和协议仿真器的 iSNS 与 IPSec, 采用: iSNS 协议、IPSec、IKE 认证;</li> <li>3) 配置 DUT 和协议仿真器采用源、目的地址作为选择符;</li> <li>4) 分别由协议仿真器 1 向 DUT 1、协议仿真器 2 向 DUT 2 发 Ping 包</li> </ol>
预期结果: 步骤 4) 后, DUT 1、DUT 2 分别正确回应
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: 无

## 6.4.7 iSNS: 预共享密钥认证

测试编号: 20

测试项目: iSNS: 预共享密钥认证

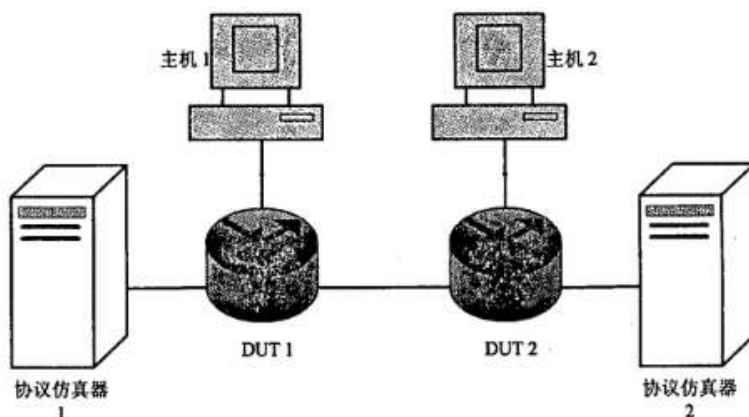
测试目的: 验证 iSNS 实现的安全机制支持预共享密钥认证

测试依据: IETF RFC 4171

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 iSNS、IPSec 的设备, 其中 DUT 1 为客户端, DUT 2 为服务器端, 配置地址保持互通性;
- 2) 配置 DUT 和协议仿真器的 iSNS 与 IPSec, 采用: iSNS 协议、IPSec、预共享密钥认证;
- 3) 配置 DUT 和协议仿真器采用源、目的地址作为选择符;
- 4) 分别由协议仿真器 1 向 DUT 1、协议仿真器 2 向 DUT 2 发 Ping 包

预期结果: 步骤 4) 后, DUT 1、DUT 2 分别正确回应

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: 无

## 6.4.8 iSNS: 数字签名证书的端认证

测试编号: 21

测试项目: iSNS: 数字签名证书的端认证

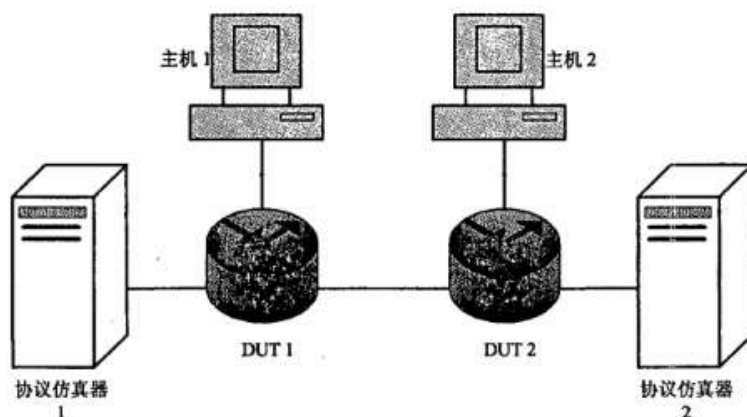
测试目的: 验证 iSNS 实现的安全机制可支持数字签名证书的端认证

测试依据: IETF RFC 4171

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 iSNS、IPSec 的设备, 其中 DUT 1 为客户端, DUT 2 为服务器端, 配置地址保持互通性;
- 2) 配置 DUT 和协议仿真器的 iSNS 与 IPSec, 采用: iSNS 协议、IPSec、数字签名证书的端认证;
- 3) 配置 DUT 和协议仿真器采用源、目的地址作为选择符;
- 4) 分别由协议仿真器 1 向 DUT 1、协议仿真器 2 向 DUT 2 发 Ping 包

预期结果: 步骤 4) 后, DUT 1、DUT 2 分别正确回应

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: 无

## 6.4.9 iSNS: IKE 主模式

测试编号: 22

测试项目: iSNS: IKE 主模式

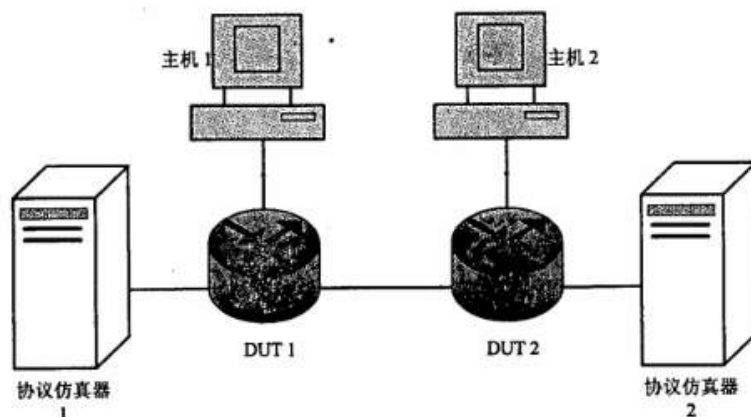
测试目的: 验证 iSNS 实现的安全机制支持 IKE 主模式

测试依据: IETF RFC 4306

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 iSNS、IPSec 的设备, 其中 DUT 1 为客户端, DUT 2 为服务器端, 配置地址保持互通性;
- 2) 配置 DUT 和协议仿真器的 iSNS 与 IPSec, 采用: iSNS 协议、IPSec、IKE 主模式;
- 3) 配置 DUT 和协议仿真器采用源、目的地址作为选择符;
- 4) 分别由协议仿真器 1 向 DUT 1、协议仿真器 2 向 DUT 2 发 Ping 包

预期结果: 步骤 4), DUT 1、DUT 2 分别正确回应

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: 无

## 6.4.10 iSNS: IKE 野蛮模式

测试编号: 23
测试项目: iSNS: IKE 野蛮模式
测试目的: 验证 iSNS 实现的安全机制支持 IKE 野蛮模式
测试依据: IETF RFC 4306
测试仪表: 协议仿真设备
测试类型: 必选
测试配置: <div style="text-align: center;"> <pre> graph LR     subgraph Hosts         H1[主机 1]         H2[主机 2]     end     subgraph DUTs         DUT1[DUT 1]         DUT2[DUT 2]     end     subgraph Simulators         S1[协议仿真器 1]         S2[协议仿真器 2]     end     H1 --- DUT1     H2 --- DUT2     DUT1 --- DUT2     DUT1 --- S1     DUT2 --- S2           </pre> </div>
测试过程: <ol style="list-style-type: none"> <li>1) 正确连接设备, DUT 为支持被测实现 iSNS、IPSec 的设备, 其中 DUT 1 为客户端, DUT 2 为服务器端, 配置地址保持互通性;</li> <li>2) 配置 DUT 和协议仿真器的 iSNS 与 IPSec, 采用: iSNS 协议、IPSec、IKE 野蛮模式;</li> <li>3) 配置 DUT 和协议仿真器采用源、目的地址作为选择符;</li> <li>4) 分别由协议仿真器 1 向 DUT 1、协议仿真器 2 向 DUT 2 发 Ping 包</li> </ol>
预期结果: 步骤 4), DUT 1、DUT 2 分别正确回应
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: 无

## 6.5 其他功能测试

## 6.5.1 IP 存储网络安全机制：完整性检查测试

测试编号：24

测试项目：IP 存储网络安全机制：完整性检查测试

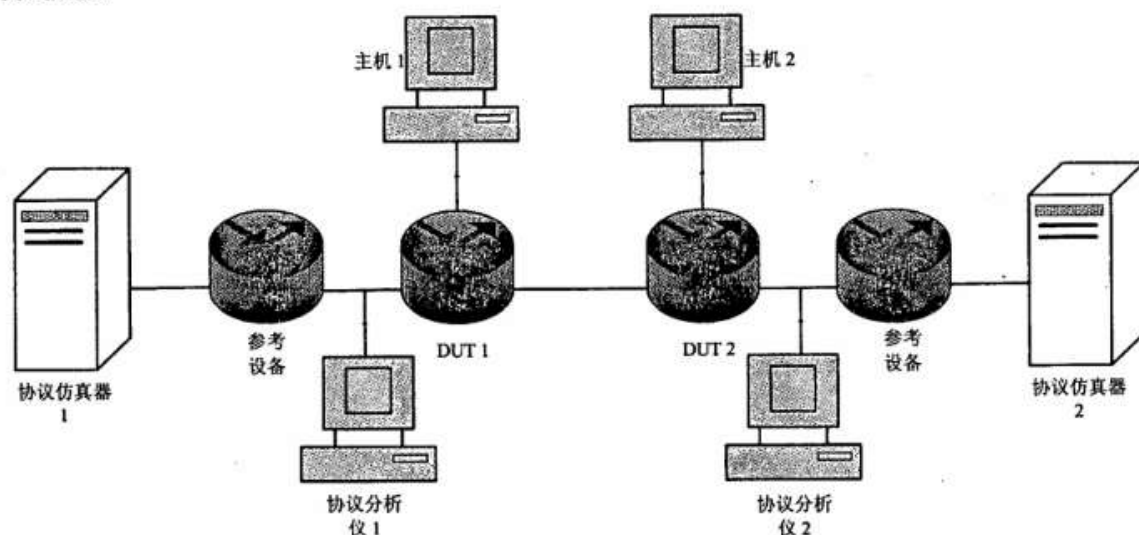
测试目的：验证 IP 存储网络安全机制具有完整性检查功能

测试依据：YD/T 1467-2006

测试仪表：协议仿真设备

测试类型：必选

测试配置：



测试过程：

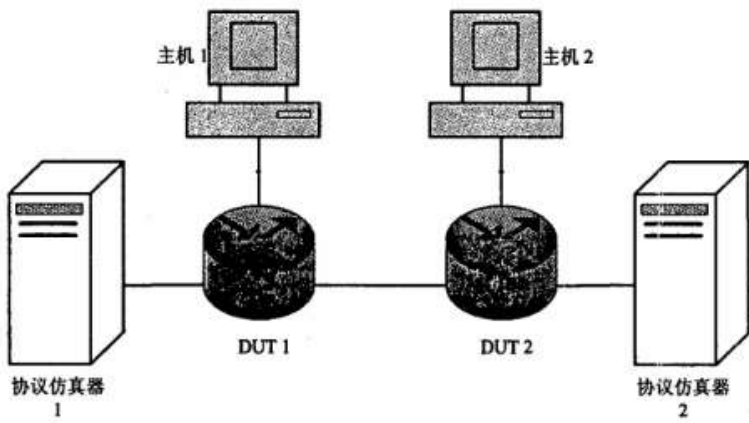
- 1) 正确连接设备，DUT 为支持被测实现 iSCSI、FCIP、iFCP、iSNS、IPSec 的设备，其中 DUT 1 为客户端（或者为启动器），DUT 2 为服务器端（或者为目标器），配置地址保持互通性；
- 2) 配置 DUT 和协议仿真器的 IP 存储网络安全协议为 iSCSI；
- 3) 配置 DUT 和协议仿真器的 IPSec，使用 AH；
- 4) 配置 DUT 和协议仿真器采用源、目的地址作为选择符；
- 5) 配置协议分析仪为桥接方式工作；
- 6) 从协议仿真器发送 ping 包；
- 7) 在协议分析仪监视参考设备和 DUT 间的通信，将 ping 包修改后发送；
- 8) 配置 DUT 和协议仿真器的 IPSec，使用 ESP，重复步骤 4) ~7)；
- 9) 配置 DUT 和协议仿真器的 IP 存储网络安全协议为 FCIP，重复步骤 3) ~8)；
- 10) 配置 DUT 和协议仿真器的 IP 存储网络安全协议为 iFCP，重复步骤 3) ~8)；
- 11) 配置 DUT 和协议仿真器的 IP 存储网络安全协议为 iSNS，重复步骤 3) ~8)；

预期结果：步骤 7) ~11) 后，协议仿真器 1、协议仿真器 2 均无法收到返回的 Ping 包

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：无

## 6.5.2 IP 存储网络安全机制: SA 功能测试

测试编号: 25
测试项目: IP 存储网络安全机制: SA 功能测试
测试目的: 验证 IP 存储网络安全机制中实现 SA 功能
测试依据: YD/T 1467-2006
测试仪表: 协议仿真设备
测试类型: 必选
测试配置: 
测试过程: <ol style="list-style-type: none"> <li>1) 正确连接设备, DUT 为支持被测实现 iSCSI、FCIP、iFCP、iSNS、IPSec 的设备, 其中 DUT 1 为客户端 (或者为启动器), DUT 2 为服务器端 (或者为目标器), 配置地址保持互通性;</li> <li>2) 配置 DUT 和协议仿真器的 IP 存储网络安全协议为 iSCSI;</li> <li>3) 配置 DUT 和协议仿真器的 IPSec;</li> <li>4) 按照 YD/T 1467-2006 中 4.3 SA 测试规定的方法测试;</li> <li>5) 配置 DUT 和协议仿真器的 IP 存储网络安全协议为 FCIP, 重复步骤 3) ~4);</li> <li>6) 配置 DUT 和协议仿真器的 IP 存储网络安全协议为 iFCP, 重复步骤 3) ~4);</li> <li>7) 配置 DUT 和协议仿真器的 IP 存储网络安全协议为 iSNS, 重复步骤 3) ~4)</li> </ol>
预期结果: 测试结果与 YD/T 1467-2006 中 4.3 SA 测试预期结果相符
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: 无

## 6.5.3 IP 存储网络安全机制：兼容现有的安全机制

测试编号：26

测试项目：IP 存储网络安全机制：兼容现有的安全机制

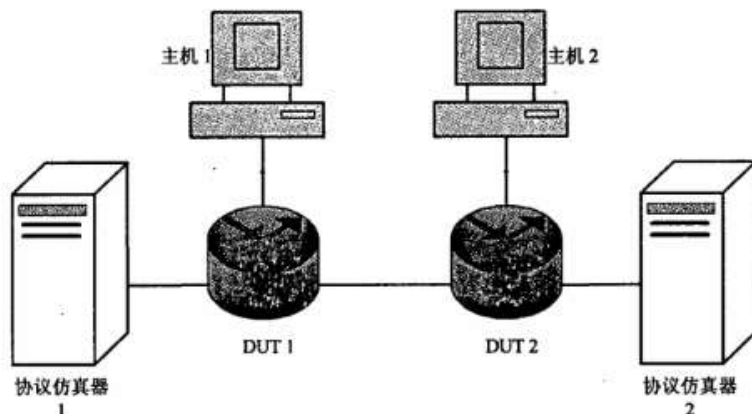
测试目的：验证 IP 存储网络兼容现有的安全机制，如防火墙、NAT、NAPT、VPN 等服务

测试依据：RFC3273，YD/T 1467-2006

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 iSCSI、FCIP、iFCP、iSNS、IPSec 的设备，其中 DUT 1 为客户端（或者为启动器），DUT 2 为服务器端（或者为目标器），配置地址保持互通性；
- 2) 配置 DUT 和协议仿真器的 IP 存储网络安全协议为 iSCSI；
- 3) 配置 DUT 和协议仿真器的 IPSec，配置其他安全机制，如防火墙、NAT、NAPT、VPN 等服务；
- 4) 配置 DUT 和协议仿真器采用源、目的地址作为选择符；
- 5) 分别由协议仿真器 1 向 DUT 1、协议仿真器 2 向 DUT 2 发 Ping 包；
- 6) 配置 DUT 和协议仿真器的 IP 存储网络安全协议为 FCIP，重复步骤 3) ~5)；
- 7) 配置 DUT 和协议仿真器的 IP 存储网络安全协议为 iFCP，重复步骤 3) ~5)；
- 8) 配置 DUT 和协议仿真器的 IP 存储网络安全协议为 iSNS，重复步骤 3) ~5)

预期结果：步骤 5) ~8) 后，DUT 1、DUT 2 分别正确回应

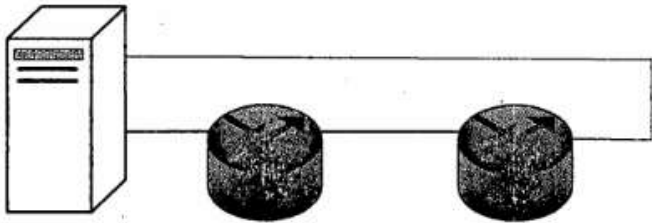
判定原则：测试结果必须与预期结果相符，否则不符合要求

测试说明：无

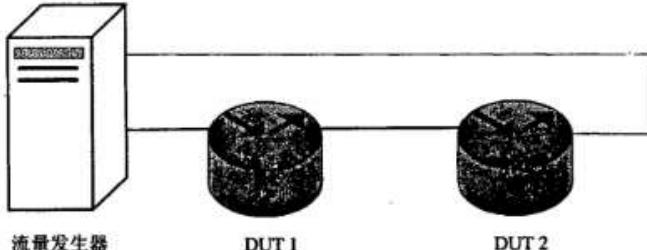


## 7 性能测试

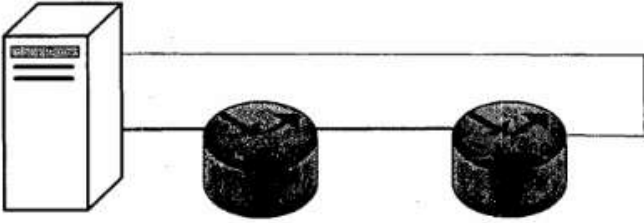
## 7.1 隧道数量测试

测试编号: 27
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: IETF RFC 2401, YD/T 1467-2006
测试仪表: 协议仿真设备
测试类型: 必选
测试配置: <div style="text-align: center;">  <p>流量发生器      DUT 1      DUT 2</p> </div>
测试过程: <ol style="list-style-type: none"> <li>1) 正确连接设备, DUT 为支持被测实现 iSCSI、FCIP、iFCP、iSNS、IPSec 的设备, 其中 DUT 1 为客户端 (或者为启动器), DUT 2 为服务器端 (或者为目标器), 配置地址保持互通性;</li> <li>2) 配置 DUT 的 IPSec, IP 安全存储网络协议使用 iSCSI;</li> <li>3) 配置 DUT 采用源、目的地址作为选择符, 从 DUT 1 到 DUT 2 建立隧道;</li> <li>4) 从流量发生器发出不同源地址的包;</li> <li>5) 观察隧道建立数量;</li> <li>6) 配置 DUT 的 IPSec, IP 安全存储网络协议使用 FCIP, 重复步骤 3) ~5);</li> <li>7) 配置 DUT 的 IPSec, IP 安全存储网络协议使用 iFCP, 重复步骤 3) ~5);</li> <li>8) 配置 DUT 的 IPSec, IP 安全存储网络协议使用 iSNS, 重复步骤 3) ~5)</li> </ol>
判定原则: 不做判定
测试说明: 无

## 7.2 单隧道下设备吞吐量测试

测试编号: 28
测试项目: 测试 IP 存储网络安全中, 设备在 IPSec 单隧道下的吞吐量
测试目的: 测试 IP 存储网络安全中, 设备在 IPSec 单隧道下的吞吐量
测试依据: IETF RFC 2401, YD/T 1467-2006
测试仪表: 协议仿真设备
测试类型: 必选
测试配置: <div style="text-align: center;">  <p>流量发生器      DUT 1      DUT 2</p> </div>
测试过程: <ol style="list-style-type: none"> <li>1) 正确连接设备, DUT 为支持被测实现 iSCSI、FCIP、iFCP、iSNS、IPSec 的设备, 其中 DUT 1 为客户端 (或者为启动器), DUT 2 为服务器端 (或者为目标器), 配置地址保持互通性;</li> <li>2) 配置 DUT 的 IPSec, IP 安全存储网络协议使用 iSCSI;</li> <li>3) 配置 DUT 采用源、目的地址作为选择符, 从 DUT 1 到 DUT 2 建立一个隧道;</li> <li>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;</li> <li>5) 测试吞吐量;</li> <li>6) 配置 DUT 的 IPSec, IP 安全存储网络协议使用 FCIP, 重复步骤 3) ~5);</li> <li>7) 配置 DUT 的 IPSec, IP 安全存储网络协议使用 iFCP, 重复步骤 3) ~5);</li> <li>8) 配置 DUT 的 IPSec, IP 安全存储网络协议使用 iSNS, 重复步骤 3) ~5)</li> </ol>
判定原则: 不做判定
测试说明: 测试结果与测试过程中使用的算法有关

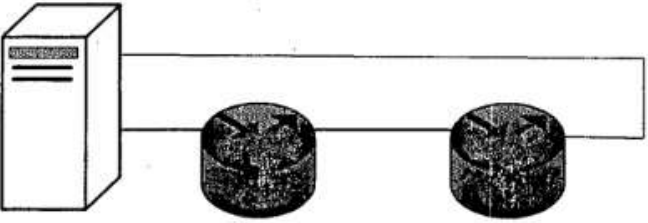
## 7.3 多隧道下设备吞吐量测试

测试编号: 29
测试项目: 测试 IP 存储网络安全中, 设备在 IPSec 多隧道下的吞吐量
测试目的: 测试 IP 存储网络安全中, 设备在 IPSec 多隧道下的吞吐量
测试依据: IETF RFC 2401, YD/T 1467-2006
测试仪表: 协议仿真设备
测试类型: 必选
测试配置: <div style="text-align: center;">  <p>流量发生器      DUT 1      DUT 2</p> </div>
测试过程: <ol style="list-style-type: none"> <li>1) 正确连接设备, DUT 为支持被测实现 iSCSI、FCIP、iFCP、iSNS、IPSec 的设备, 其中 DUT 1 为客户端 (或者为启动器), DUT 2 为服务器端 (或者为目标器), 配置地址保持互通性;</li> <li>2) 配置 DUT 的 IPSec, IP 安全存储网络协议使用 iSCSI;</li> <li>3) 配置 DUT 采用源、目的地址作为选择符, 从 DUT 1 到 DUT 2 建立 256 (暂定) 个隧道;</li> <li>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;</li> <li>5) 测试吞吐量;</li> <li>6) 配置 DUT 的 IPSec, IP 安全存储网络协议使用 FCIP, 重复步骤 3) ~5);</li> <li>7) 配置 DUT 的 IPSec, IP 安全存储网络协议使用 iFCP, 重复步骤 3) ~5);</li> <li>8) 配置 DUT 的 IPSec, IP 安全存储网络协议使用 iSNS, 重复步骤 3) ~5)</li> </ol>
判定原则: 不做判定
测试说明: 测试结果与测试过程中使用的算法有关

## 7.4 传输时延测试

测试编号: 30
测试项目: 测试 IP 存储网络安全中, 设备在 IPSec 隧道上的传输时延
测试目的: 测试 IP 存储网络安全中, 设备在 IPSec 隧道上的传输时延
测试依据: IETF RFC 2401, YD/T 1467-2006
测试仪表: 协议仿真设备
测试类型: 必选
测试配置: <div style="text-align: center; margin-top: 20px;">  <p>流量发生器      DUT 1      DUT 2</p> </div>
测试过程: <ol style="list-style-type: none"> <li>1) 正确连接设备, DUT 为支持被测实现 iSCSI、FCIP、iFCP、iSNS、IPSec 的设备, 其中 DUT 1 为客户端 (或者为启动器), DUT 2 为服务器端 (或者为目标器), 配置地址保持互通性;</li> <li>2) 配置 DUT 的 IPSec, IP 安全存储网络协议使用 iSCSI;</li> <li>3) 配置 DUT 采用源、目的地址作为选择符, 从 DUT 1 到 DUT 2 建立隧道;</li> <li>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;</li> <li>5) 读取时延;</li> <li>6) 配置 DUT 的 IPSec, IP 安全存储网络协议使用 FCIP, 重复步骤 3) ~5);</li> <li>7) 配置 DUT 的 IPSec, IP 安全存储网络协议使用 iFCP, 重复步骤 3) ~5);</li> <li>8) 配置 DUT 的 IPSec, IP 安全存储网络协议使用 iSNS, 重复步骤 3) ~5)</li> </ol>
判定原则: 不做判定
测试说明: 测试结果与测试过程中使用的算法有关

## 7.5 丢包率测试

测试编号: 31
测试项目: 测试 IP 存储网络安全中, 设备在 IPSec 隧道上的丢包率
测试目的: 测试 IP 存储网络安全中, 设备在 IPSec 隧道上的丢包率
测试依据: IETF RFC 2401, YD/T 1467-2006
测试仪表: 协议仿真设备
测试类型: 必选
测试配置: <div style="text-align: center; margin-top: 20px;">  <p>流量发生器          DUT 1          DUT 2</p> </div>
测试过程: <ol style="list-style-type: none"> <li>1) 正确连接设备, DUT 为支持被测实现 iSCSI、FCIP、iFCP、iSNS、IPSec 的设备, 其中 DUT 1 为客户端 (或者为启动器), DUT 2 为服务器端 (或者为目标器), 配置地址保持互通性;</li> <li>2) 配置 DUT 的 IPSec, IP 安全存储网络协议使用 iSCSI;</li> <li>3) 配置 DUT 采用源、目的地址作为选择符, 从 DUT 1 到 DUT 2 建立隧道;</li> <li>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;</li> <li>5) 读取丢包率;</li> <li>6) 配置 DUT 的 IPSec, IP 安全存储网络协议使用 FCIP, 重复步骤 3) ~5);</li> <li>7) 配置 DUT 的 IPSec, IP 安全存储网络协议使用 iFCP, 重复步骤 3) ~5);</li> <li>8) 配置 DUT 的 IPSec, IP 安全存储网络协议使用 iSNS, 重复步骤 3) ~5)</li> </ol>
判定原则: 不做判断
测试说明: 测试结果与测试过程中使用的算法有关

中 华 人 民 共 和 国  
通 信 行 业 标 准  
IP 存储网络安全测试方法  
YD/T 2392-2011

\*

人民邮电出版社出版发行  
北京市崇文区夕照寺街 14 号 A 座  
邮政编码: 100061  
宝隆元(北京)印刷技术有限公司印刷  
版权所有 不得翻印

\*

开本: 880×1230 1/16 2012 年 1 月第 1 版  
印张: 2.5 2012 年 1 月北京第 1 次印刷  
字数: 68 千字

ISBN 978 - 7 - 115 - 2453/ 12 - 31

定价: 25 元

本书如有印装质量问题, 请与本社联系 电话: (010)67114922