VPN测试用例-IPsec

文档版本历史

文档版本号	编辑时间	编者	备注

适用性说明

参考文档	
适用版本	

1.功能说明：

支持 ESP 和 AH封装协议；
支持隧道模式和传输模式；
支持 Site to Site 、Remote Access 两种 VPN组网形式；
支持预共享密钥和 X.509 数字证书两种身份认证形式；
支持通过 IKE 自动完成 IPSec 安全联盟协商；
支持 DES、3DES、AES128/192/256 等多种加密算法；
支持 MD5、SHA-1 等多种哈希验证算法；
支持可以基于固定 IP 地址建立 IPSec 隧道，支持通过域名方式建立 IPSec 隧道；
支持 IPSec 报文的 UDP 封装模式，以保证 IPSec 能够穿越 NAT;
支持断线诊断 DPD 协议；

2.工作机制：

1）关键词：

IPsec（IP Security）：

是 IETF制定的三层隧道加密协议，它为 Internet 上传输的数据提供了高质量的、可互操作的、基于密码学的安全保证。它给出了应用于 IP 层上网络数据安全的一整套体系结构，包括网络认证协议 AH（Authentication Header，认证头）、ESP（Encapsulating Security Payload，封装安全载荷）、IKE（Internet Key Exchange，因特网密钥交换）和用于网络认证及加密的一些算法等。

AH协议：

可以同时提供数据完整性确认、数据来源确认、防重放等安全特性；AH常用摘要算法（单向 Hash 函数）MD5 和 SHA1实现该特性。

ESP协议：

提可以同时提供数据完整性确认、数据加密、防重放等安全特性；ESP 通常使用 DES、3DES、AES 等加密算法实现数据加密，使用 MD5 或 SHA1来实现数据完整性。ESP保护的是 IP 包的载荷，不包括 IP 头部，所以 ESP和 NAT是不冲突的。

SA（安全联盟）：

是两个 IPsec 实体（主机或者网关）之间经过协商建立起来的一种协定，包括采用的协议、算法、加密等。 SA是构成 IPsec 的基础。而建立 SA需要 2 个阶段：

第一阶段，协商创建一个通信信道（ISAKMP SA），并对该信道进行认证，为双方进一步的 IKE 通信提供机密性、数据完整性以及数据源认证服务；

第二阶段，使用已建立的 ISAKMP SA 建立 IPsec SA。

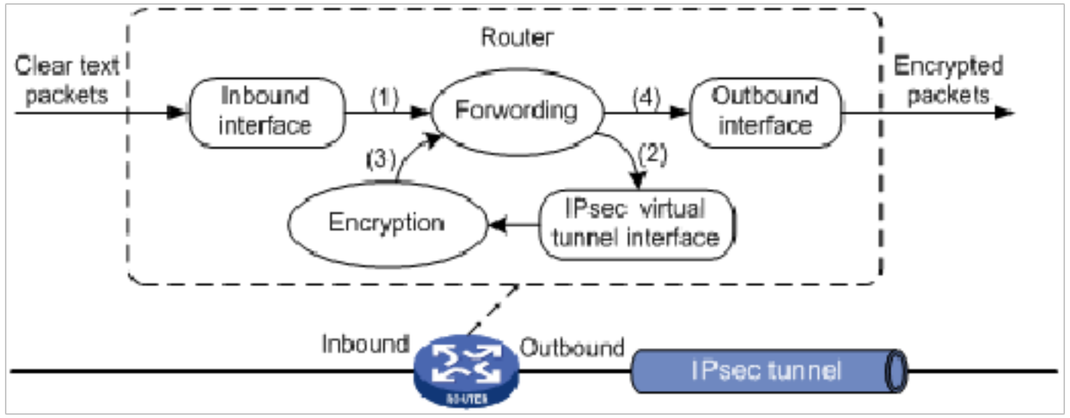
IKE（因特网密钥交换）：

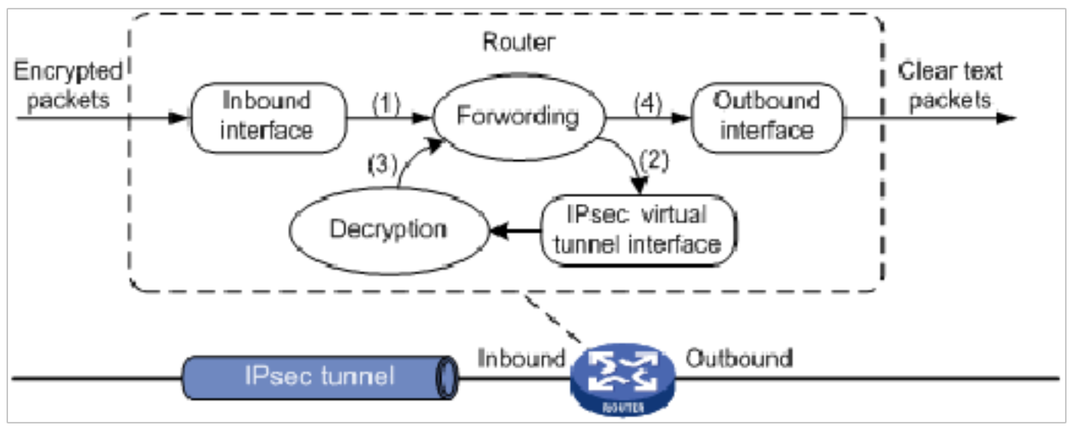
为 IPsec 提供了自动协商交换密钥、建立 SA 的服务，能够简化 IPsec 的使用和管理。IKE 是通过一系列数据的交换，最终计算出双方共享的密钥，并且即使第三者截获了双方用于计算密钥的所有交换数据，也不足以计算出真正的密钥。通过 IKE 建立隧道又分为两种模式：主模式（main）和野蛮模式（aggrmode，也叫快速模式）

应用场景：

在 IPsec 中，主要有两种应用场景，分别为 LAN-to-LAN 和 Remote（远程连接）。其中 LAN-to-LAN 需要隧道两端各有一个网关来进行连接，而 Remote 则是其中一端为 PC 端，通过 IPsec 软件来连接 VPN。

2）工作拓扑图：





3）工作过程：

（1）加封装过程：

A.Router1 将从入接口接收到的 IP 明文送到转发模块进行处理

B.转发模块依据路由查询结果，将 IP 明文发送到 IPsec 虚拟隧道接口进行加封装：原始 IP 报文被封装在一个新的 IP 报文中，新 IP 头中的源地址和目的地址分别为隧道接口的源地址和目的地址。

C.IPsec 虚拟隧道接口完成对 IP 明文的加封装处理后，将 IP 密文送到转发模块进行处理；

D.转发模块进行第二次路由查询后，将 IP 密文通过隧道接口的实际物理接口转发出去。

（2）解封装过程：

A.Router 将从入接口接收到的 IP 密文送到转发模块进行处理；

B.转发模块识别到此 IP 密文的目的地为本设备的隧道接口地址且 IP 协议号为 AH 或 ESP 时，会将 IP 密文送到相应的 IPsec 虚拟隧道接口进行解封装：将 IP 密文的外层 IP 头去掉，对内层 IP 报文进行解密处理。

C.IPsec 虚拟隧道接口完成对 IP 密文的解封装处理之后，将 IP 明文重新送回转发模块处理；

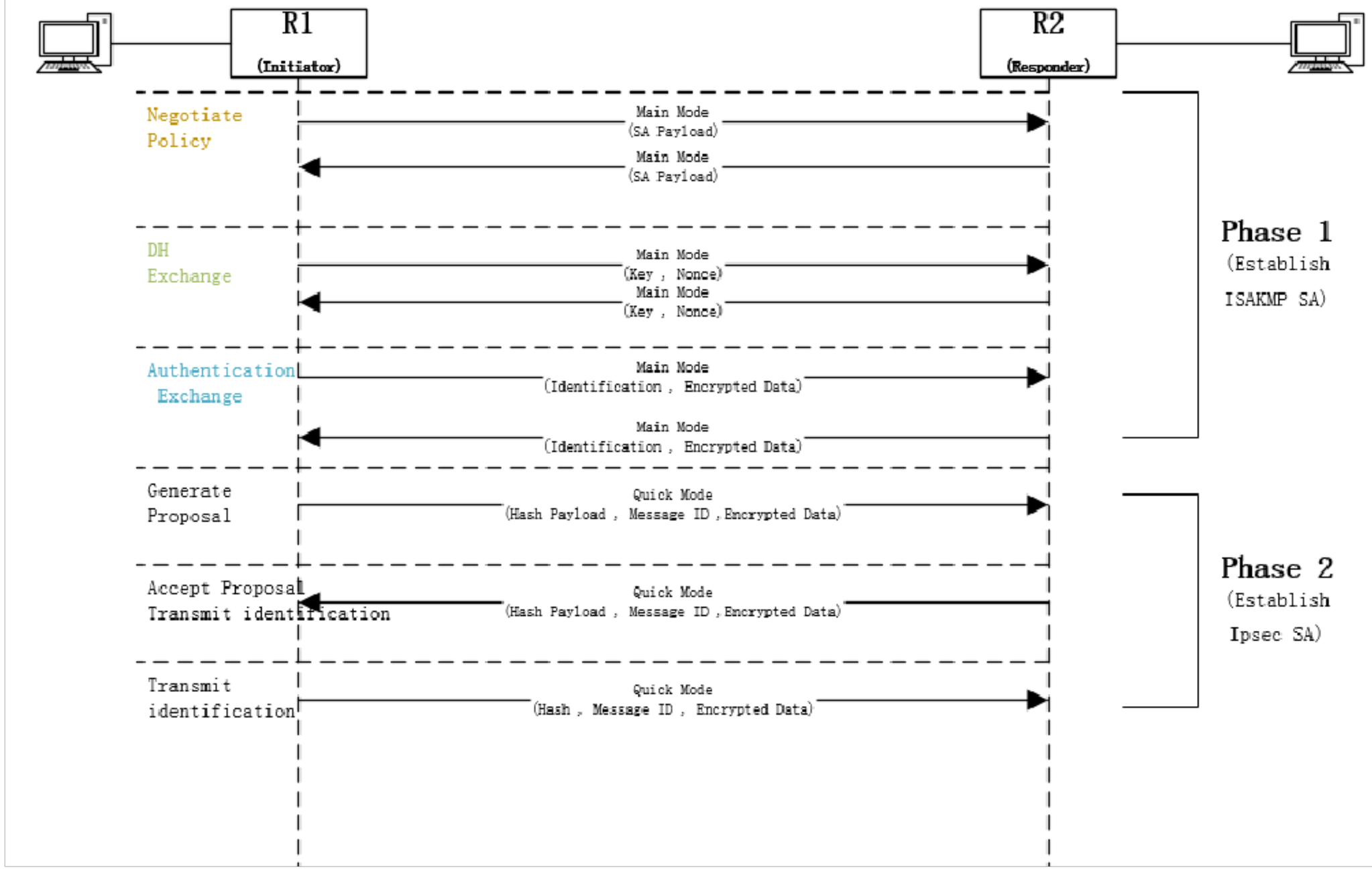
D.转发模块进行第二次路由查询后，将 IP 明文从隧道的实际物理接口转发出去。

4）IPsec 报文格式及发送：

（1）报文格式：

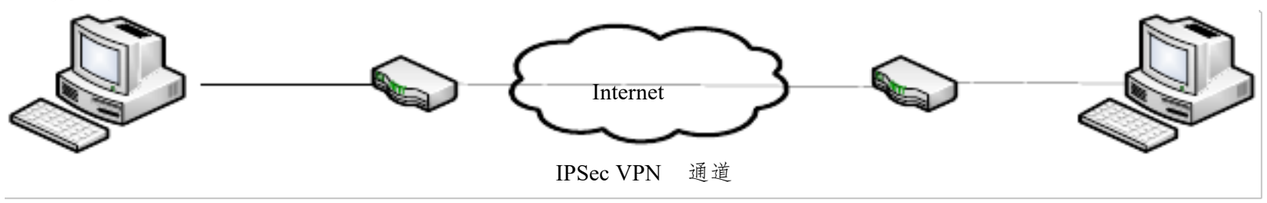
Mode / Protocol	Transport	Tunnel
AH	IP AH Data	IP AH IP Data
ESP	IP ESP Data ESP-T	IP ESP IP Data ESP-T
AH-ESP	IP AH ESP Data ESP-T	IP AH ESP IP Data ESP-T

（2）报文发送


R1
(Initiator)
R2
(Responder)
Negotiate
Policy
Main Mode
(SA Payload)
Main Mode
(SA Payload)
DH
Exchange
Main Mode
(Key , Nonce)
Main Mode
(Key , Nonce)
Authentication
Exchange
Main Mode
(Identification , Encrypted Data)
Main Mode
(Identification , Encrypted Data)
Generate
Proposal
Quick Mode
(Hash Payload , Message ID , Encrypted Data)
Accept Proposal
Transmit identification
Quick Mode
(Hash Payload , Message ID , Encrypted Data)
Transmit
identification
Quick Mode
(Hash , Message ID , Encrypted Data)
Phase 1
(Establish
ISAKMP SA)
Phase 2
(Establish
Ipsec SA)

3.网络拓扑图：

隧道模式：



传输模式：

4.测试用例：

1）LAN-to-LAN应用场景：

服务端和客户端都有安全网关

编号	测试标题	前置条件	执行步骤	预期结果	实际结果	测试结论
	IP 地址格式验证	1.能正常进入网关配置界面 2.其它各项参数配置正确	1.在本地地址栏输入正确的 IP 地址格式：192.168.78.140，点击保存 2.在本地地址栏输入错误的 IP 地址格式：192.168.78，点击保存 3.对对端地址、本地子网和远程子网进行如上的配置并保存	步骤 1： 保存成功 步骤 2： 保存失败，提示地址格式错误 步骤 3： 分别同步骤 1 和步骤 2 所对应的结果		

	交换模式验证	1.客户端和服务端都能正常进入网关配置界面 2.其它各项参数配置正确 3.PC1 端网关设为 send，PC2 端网关设为 receive 。 4.PC1 到 PC2 网络连接正常，可正常访问 5.封装模式选择 Tunnel	1.客户端和服务端都设置 main 交换模式，使能 IPsec 2.PC1pingPC2 并抓包 3.客户端和服务端都设置 aggrmode 交换模式，使能 IPsec 4.PC1pingPC2 并抓包	步骤 2： PC1 可 ping 通 PC2 且第一阶段的建立通过 6 次报文才完成 步骤 4： PC1 可 ping 通 PC2，第一阶段的建立通过 3 次报文就完成		
	加密算法的验证	1.客户端和服务端都能正常进入网关配置界面 2.其它各项参数配置正确 3.PC1 端网关设为 send，PC2 端网关设为 receive 。 4.PC1 到 PC2 网络连接正常，可正常访问 5.封装模式选择 Tunnel	1.将两端的第一阶段加密算法都采用 DES 加密，使能 IPsec，让 PC1pingPC2 2.将两端的第一阶段加密算法都采用 3DES 加密，使能 IPsec，让 PC1pingPC2 3.将两端的第一阶段加密算法都采用 AES128 加密，使能 IPsec，让 PC1pingPC2 4.将两端的第一阶段加密算法都采用 AES192 加密，使能 IPsec，让 PC1pingPC2 5.将两端的第一阶段加密算法都采用 AES256 加密，使能 IPsec，让 PC1pingPC2 6.第二阶段采用 ESP 协议后，对加密算	步骤 1： PC1 可 ping 通 PC2 步骤 2： PC1 可 ping 通 PC2 步骤 3： PC1 可 ping 通 PC2 步骤 4： PC1 可 ping 通 PC2 步骤 5： PC1 可 ping 通 PC2 步骤 6： PC1 可 ping 通 PC2		

			法同样进行如上的操作验证			
	验证算法的验证	1.客户端和服务端都能正常进入网关配置界面 2.其它各项参数配置正确 3.PC1 端网关设为 send，PC2 端网关设为 receive 。 4.PC1 到 PC2 网络连接正常，可正常访问	1.将两端的第一阶段验证算法都采用 MD5，使能 IPsec，让 PC1pingPC2 2.将两端的第一阶段验证算法都采用 SHA1，使能 IPsec，让 PC1pingPC2 3.第二阶段采用 AH 协议后，对验证算法同样进行如上的操作验证 4. .第二阶段采用 ESP 协议后，对验证算法同样进行如上的操作验证	步骤 1： PC1 可 ping 通 PC2 步骤 2： PC1 可 ping 通 PC2 步骤 3： PC1 可 ping 通 PC2 步骤 4： PC1 可 ping 通 PC2		
	协议类型的验证	1.客户端和服务端都能正常进入网关配置界面 2.其它各项参数配置正确 3.PC1 端网关设为 send，PC2 端网关设为 receive 。 4.PC1 到 PC2 网络连接正常，可正常访问 5.封装模式选择 Tunnel	1.将两端的协议类型都采用 ESP 协议，使能 IPsec，PC1pingPC2 2.将两端的协议类型都采用 AH 协议，使能 IPsec，PC1pingPC2	步骤 1： PC1 可 ping 通 PC2 步骤 2： PC1 可 ping 通 PC2		
	本端子网验证	1.客户端和服务端都能正常进入网关配置界面 2.其它各项参数配置正确	1. 在客户端设置本地子网为 192.168.1.1 子网掩码为 255.255.255.128 2.在客户端在连接 PC3 后再连接上	步骤 2： PC4 无法 ping 通 PC2 步骤 3： PC4 可以 ping 通 PC2		

		send，PC2 端网关设为 receive 。 4.PC1 到 PC2 网络连接正常，可正常访问 5.封装模式选择 Tunnel	PC4，让 PC4pingPC2 3.断开 PC3 的连接，重连 PC4，使能 IPsec，让 PC4pingPC2			
	对端子网验证	1.客户端和服务端都能正常进入网关配置界面 2.其它各项参数配置正确 3.PC1 端网关设为 send，PC2 端网关设为 receive 。 4.PC1 到 PC2 网络连接正常，可正常访问 5.封装模式选择 Tunnel	1.在本端端设置正确的对端子网为 192.168.1.1 子网掩码为 255.255.255.128 2.设置正确的本端子网范围 3.PC1pingPC2 4.在本端设置与对端不相符的对端子网 192.168.2.1，子网掩码为 255.255.255.128 5.PC1pingPC2	步骤 3： PC1 可 ping 通 PC2 步骤 5: 步骤 1 不可 ping 通 PC2		
	子网超出范围（包括超出 LAN 口子网范围以及网段与 LAN 口网段不一致）	1.客户端和服务端都能正常进入网关配置界面 2.其它各项参数配置正确 3.PC1 端网关设为 send，PC2 端网关设为 receive 。 4.PC1 到 PC2 网络	1.在客户端设置网关 IP 为 192.168.78.140,LAN 口 IP 为 192.168.1.1，地址池为 192.168.1.10-192.168.1.100 2.设置本地子网为 192.168.1.1,子网掩码为 255.255.255.128，使能 IPsec，让 PC1pingPC2 3.设置本地子网为 192.168.3.1,子网掩	步骤 2： PC1 无法 ping 通 PC2 步骤 3： PC1 无法 ping 通 PC2 步骤 4： PC1 无法 ping 通 PC2		

		访问 5.封装模式选择 Tunnel	码 255.255.255.255，使能 IPsec，让 PC1pingPC2 4.对远程子网进行同样的操作。			
	两端交换模式不一致	1.客户端和服务端都能正常进入网关配置界面 2.其它各项参数配置正确 3.PC1 端网关设为 send，PC2 端网关设为 receive 。 4.PC1 到 PC2 网络连接正常，可正常访问 5.封装模式选择 Tunnel	1.一端设置交换模式为 main，另一端设置交换模式为 aggrmode ，使能 IPsec 2.查看连接状态并让 PC1pingPC2	步骤 2： 可以联通，但是 PC1 无法 ping 通 PC2		
	两端交换方向都设置相同	1.客户端和服务端都能正常进入网关配置界面 2.其它各项参数配置正确 3.PC1 到 PC2 网络连接正常，可正常访问 4.封装模式选择 Tunnel	1.将两端交换方向都设置成 Receive，使能 IPsec 2.让 PC1pingPC2 3.将两端交换方向都设置成 Send，使能 IPsec 4.让 PC1pingPC2	步骤 2： PC1 无法 ping 通 PC2 步骤 4： PC1 无法 ping 通 PC2		
	共享密钥不一致	1.客户端和服务端都能正常进入网关配置界面	1.将一端的密钥设置为 12345，另一端的密钥设置成 54321，使能 IPsec 2.让 PC1pingPC2	步骤 2： PC1 无法 ping 通 PC2		