

南昌大学软件学院

实验报告书

课程名： 网络安全技术

题目： IPsec VPN 配置配置实训

实验类别 【验证】

班级： 信息安全 193 班

学号： 8003119100

姓名： 丁俊

评语：

实验态度：认真（ ） 一般（ ） 较差（ ）
实验结果：正确（ ） 部分正确（ ） 错（ ）
实验理论：掌握（ ） 熟悉（ ） 了解（ ） 生疏（ ）
操作技能：较强（ ） 一般（ ） 较差（ ）
实验报告：较好（ ） 一般（ ） 较差（ ）

成绩： _____ 指导教师： 鄢志辉

一、实验目的

- 理解 IPSec VPN 的配置命令和防范
- 熟悉 Ipsec VPN 配置

二、实验设备及条件

- 运行 Windows 操作系统计算机一台
 - Cisco Packet Tracer 模拟软件
- 或
- Cisco 2811 路由器两台
 - 普通交换机一台
 - 运行 Windows 操作系统计算机三台
 - RJ-45 转 DB-9 反接线一根、RJ-45 双绞线若干
 - 超级终端应用程序

三、实验原理

什么是 IPSec VPN? IPSec VPN 即指采用 IPSec 协议来实现远程接入的一种 VPN 技术, IPSec 全称为 Internet Protocol Security, 是由 Internet Engineering Task Force (IETF) 定义的安全标准框架, 用以提供公用和专用网络的端对端加密和验证服务。IPsec 所具有的优点:

1、支持 IKE (Internet Key Exchange, 因特网密钥交换), 可实现密钥的自动协商功能, 减少了密钥协商的开销。可以通过 IKE 建立和维护安全关联 (Security Association, SA) 的服务, 简化了 IPsec 的使用和管理。

2、所有使用 IP 协议进行数据传输的应用系统和服务都可以使用 IPsec, 由于 IPSec 工作在 OSI 的第 3 层, 低于应用程序直接涉及的层级, 所以对于应用程序来讲, 利用 IPSec VPN 所建立起来的隧道是完全透明的, 无需修改既有的应用程序, 并且, 现有应用程序的安全解决方法也不会受到任何影响。

3、对数据的加密是以数据包为单位的, 而不是以整个数据流为单位, 这不仅灵活而且有助于进一步提高 IP 数据包的安全性, 可以有效防范网络攻击。

3.1 工作原理

IPsec 协议不是一个单独的协议, 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。其中, AH 协议和 ESP 协议用于提供安全服务, IKE 协议用于密钥交换。

IPsec 提供了两种安全机制：认证和加密。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篡改。加密机制通过对数据进行加密运算来保证数据的机密性，以防数据在传输过程中被窃听。IPsec 协议中的 AH 协议定义了认证的应用方法，提供数据源认证和完整性保证；ESP 协议定义了加密和可选认证的应用方法，提供数据可靠性保证。

AH 协议（IP 协议号为 51）提供数据源认证、数据完整性校验和防报文重放功能，它能保护通信免受篡改，但不能防止窃听，适合用于传输非机密数据。AH 的工作原理是在每一个数据包上添加一个身份验证报文头，此报文头插在标准 IP 包头后面，对数据提供完整性保护。可选的认证算法有 MD5（Message Digest）、SHA-1（Secure Hash Algorithm）等。MD5 算法的计算速度比 SHA-1 算法快，而 SHA-1 算法的安全强度比 MD5 算法高。

ESP 协议（IP 协议号为 50）提供加密、数据源认证、数据完整性校验和防报文重放功能。ESP 的工作原理是在每一个数据包的标准 IP 包头后面添加一个 ESP 报文头，并在数据包后面追加一个 ESP 尾。与 AH 协议不同的是，ESP 将需要保护的用户数据进行加密后再封装到 IP 包中，以保证数据的机密性。常见的加密算法有 DES、3DES、AES 等。同时，作为可选项，用户可以选择 MD5、SHA-1 算法保证报文的完整性和真实性。这三个加密算法的安全性由高到低依次是：AES、3DES、DES，安全性高的加密算法实现机制复杂，运算速度慢。对于普通的安全要求，DES 算法就可以满足需要。

在实际进行 IP 通信时，可以根据实际安全需求同时使用这两种协议或选择使用其中的一种。AH 和 ESP 都可以提供认证服务，不过，AH 提供的认证服务要强于 ESP。同时使用 AH 和 ESP 时，设备支持的 AH 和 ESP 联合使用的方式为：先对报文进行 ESP 封装，再对报文进行 AH 封装，封装之后的报文从内到外依次是原始 IP 报文、ESP 头、AH 头和外部 IP 头。IPsec 有如下两种工作模式：

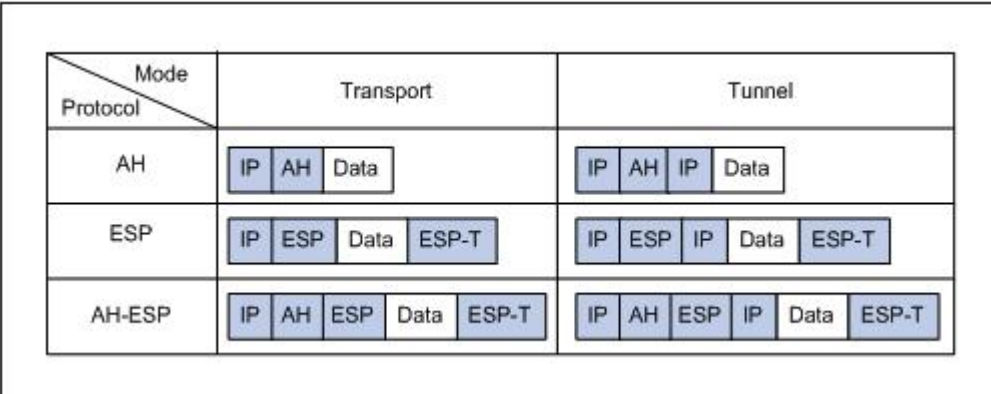


图 1 IPsec VPN 模式

tunnel 和 transport 模式下的数据封装形式，data 为传输层数据

(1) 隧道 (tunnel) 模式：用户的整个 IP 数据包被用来计算 AH 或 ESP 头，AH 或 ESP 头以及 ESP 加密的用户数据被封装在一个新的 IP 数据包中。通常，隧道模式应用在两个安全网关之间的通讯。

(2) 传输 (transport) 模式：只是传输层数据被用来计算 AH 或 ESP 头，AH 或 ESP 头以及 ESP 加密的用户数据被放置在原 IP 包头后面。通常，传输模式应用在两台主机之间的通讯，或一台主机和一个安全网关之间的通讯。

四、实验步骤

使用网络仿真软件 Cisco Packet Tracer 模拟图 2 网络（或者，用双绞线和串行线连接 2 台路由器、1 台交换机、3 台主机设置路由器、主机的 IP 地址和子网掩码。本次实训在思科模拟器上和实际物理环境中都能配通。

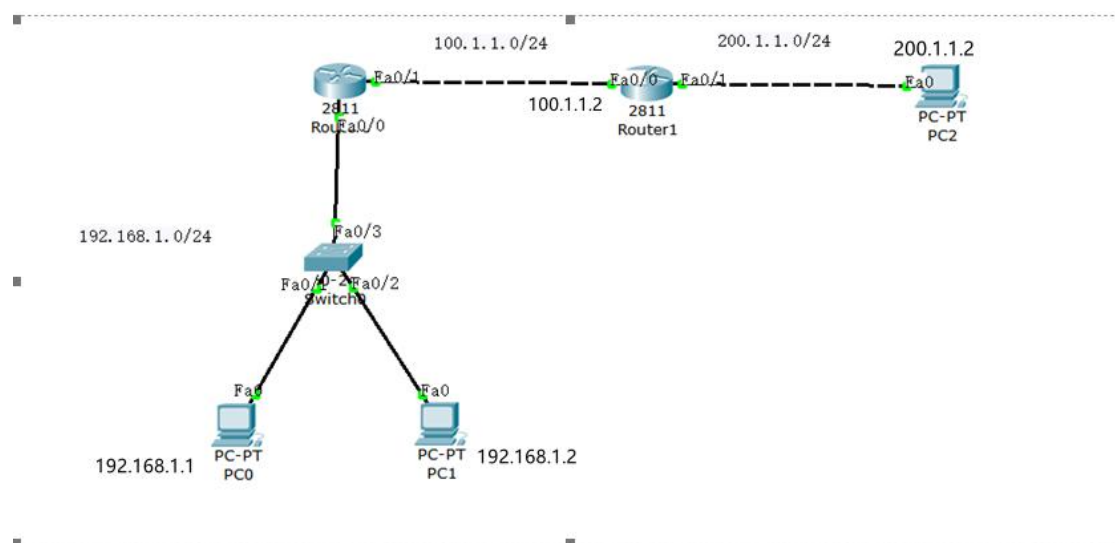


图 2 网络结构

配置 Route0:

```
Router(config)#cry
Router(config)#crypto isa
Router(config)#crypto isakmp enable
Router(config)#crypto isakmp p
Router(config)#crypto isakmp policy 100
Router(config-isakmp)#auth
Router(config-isakmp)#authentication pre-
Router(config-isakmp)#authentication pre-share
Router(config-isakmp)#encr
Router(config-isakmp)#encryption des
Router(config-isakmp)#group 1
Router(config-isakmp)#hash md
Router(config-isakmp)#hash md5
Router(config-isakmp)#lifetime 86400
Router(config-isakmp)#crypto isakmp key ciscoll22 address 100.1.1.2
Router(config)#cryp
Router(config)#crypto ipsec ipe
Router(config)#crypto ipsec ip
Router(config)#crypto ipsec ips
Router(config)#crypto ipsec tra
Router(config)#crypto ipsec transform-set abc es
Router(config)#crypto ipsec transform-set abc esp
Router(config)#crypto ipsec transform-set abc esp-des esp-md5-hmac
Router(config)#cr
Router(config)#crypto ip
Router(config)#crypto ipsec security-association lifetime 86400
% Invalid input detected at '^' marker.

Router(config)#acce
Router(config)#access-list 110 permit tcp 192.168.1.0 0.0.0.255 200.1.1.0 0.0.0.
255
Router(config)#access-list 110 permit tcp 200.1.1.0 0.0.0.255 192.168.1.0 0.0.0.
255
Router(config)#crpto
Router(config)#crpto map mymap 100 ipsec
Router(config)#crpto map mymap 100 ipsec-
Router(config)#crpto map mymap 100 ipsec-isakmp
```

Route1 的配置也和上图差不多。

```
Router(config)#cry
Router(config)#crypto isa
Router(config)#crypto isakmp enable
Router(config)#crypto isakmp p
Router(config)#crypto isakmp policy 100
Router(config-isakmp)#auth
Router(config-isakmp)#authentication pre-
Router(config-isakmp)#authentication pre-share
Router(config-isakmp)#encr
Router(config-isakmp)#encryption des
Router(config-isakmp)#group 1
Router(config-isakmp)#hash md
Router(config-isakmp)#hash md5
Router(config-isakmp)#lifetime 86400
Router(config-isakmp)#crypto isakmp key ciscoll22 address 100.1.1.2
Router(config)#cryp
Router(config)#crypto ipsec ipe
Router(config)#crypto ipsec ip
Router(config)#crypto ipsec ips
Router(config)#crypto ipsec tra
Router(config)#crypto ipsec transform-set abc es
Router(config)#crypto ipsec transform-set abc esp
Router(config)#crypto ipsec transform-set abc esp-des esp-md5-hmac
Router(config)#cr
Router(config)#crypto ip
Router(config)#crypto ipsec security-association lifetime 86400
% Invalid input detected at '^' marker.

Router(config)#acce
Router(config)#access-list 110 permit tcp 192.168.1.0 0.0.0.255 200.1.1.0 0.0.0.
255
Router(config)#access-list 110 permit tcp 200.1.1.0 0.0.0.255 192.168.1.0 0.0.0.
255
Router(config)#crpto
Router(config)#crpto map mymap 100 ipsec
Router(config)#crpto map mymap 100 ipsec-
Router(config)#crpto map mymap 100 ipsec-isakmp
```

实验：

既然设置了 ipsec，那么应该可以 ping 通：

```
PC>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Request timed out.
Request timed out.
Reply from 192.168.1.1: bytes=32 time=0ms TTL=126
Reply from 192.168.1.1: bytes=32 time=0ms TTL=126

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 2, Lost = 2 (50% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

PC>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

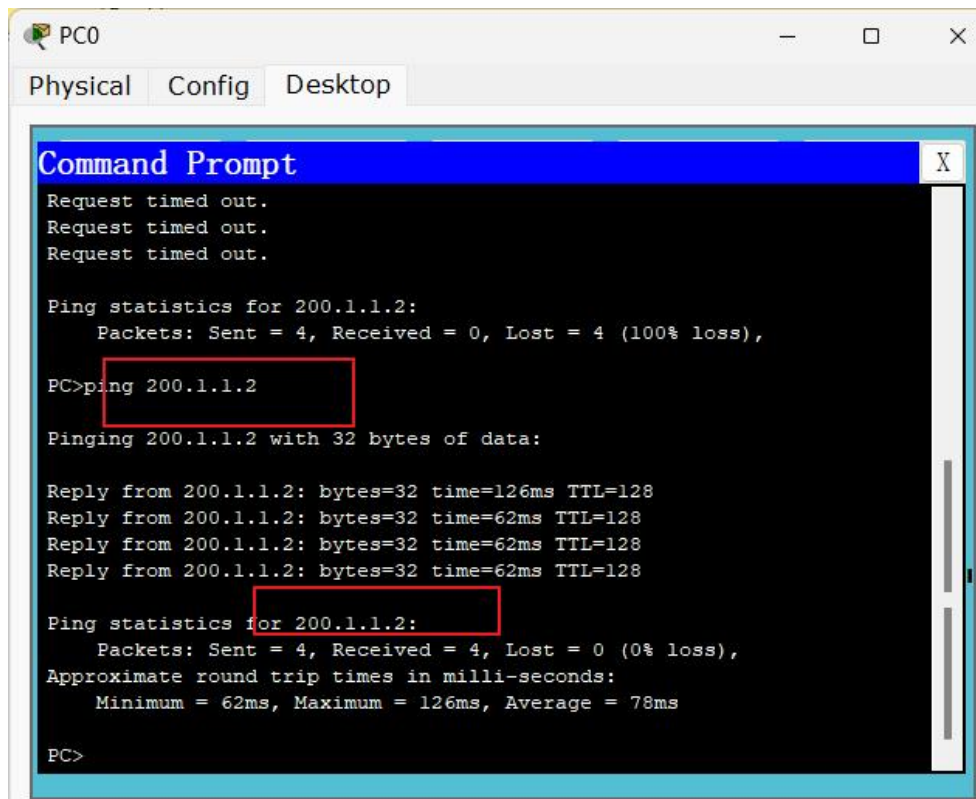
Request timed out.
Reply from 192.168.1.2: bytes=32 time=1ms TTL=126
Reply from 192.168.1.2: bytes=32 time=0ms TTL=126
Reply from 192.168.1.2: bytes=32 time=0ms TTL=126

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

PC>
```

如图，pc2 可以 ping 通 pc0 和 pc1.

pc0 或 pc1 也可以 ping 通 pc2



The screenshot shows a window titled "PC0" with tabs for "Physical", "Config", and "Desktop". The "Desktop" tab is active, displaying a "Command Prompt" window. The command prompt shows the execution of a ping command to 200.1.1.2. The output indicates that the ping was successful, with 4 packets sent and 4 received, resulting in 0% loss. The round trip times are listed as Minimum = 62ms, Maximum = 126ms, and Average = 78ms. Two red boxes highlight the command "PC>ping 200.1.1.2" and the "Ping statistics for 200.1.1.2:" section of the output.

```
PC0
Physical Config Desktop
Command Prompt
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 200.1.1.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

PC>ping 200.1.1.2

Pinging 200.1.1.2 with 32 bytes of data:

Reply from 200.1.1.2: bytes=32 time=126ms TTL=128
Reply from 200.1.1.2: bytes=32 time=62ms TTL=128
Reply from 200.1.1.2: bytes=32 time=62ms TTL=128
Reply from 200.1.1.2: bytes=32 time=62ms TTL=128

Ping statistics for 200.1.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 62ms, Maximum = 126ms, Average = 78ms

PC>
```