# VPN的工作原理

VPN = 加密 + 隧道

二层隧道VPN

* L2TP
* PPTP
* L2F

三层隧道VPN

* GRE
* IPSEC

IPSec

* 隧道模式
* 传输模式

IPSec的安全协议

1. AH（Authentication Header）认证头协议

隧道中报文的数据源鉴别、数据的完整性保护、IP包进行认证防止攻击

1. ESP（Encapsulation Security Payload）封装安全载荷协议

数据的保密性、报文的认证和完整，相较AH增加加密功能

密钥管理协议

IKE（Internet Key Exchange）因特网密钥交换协议

# IPSec VPN的配置

1. 配置IKE的协商

启动IKE

Router(config)#crypto isakmp enable

建立和配置IKE协商策略

Router(config)#crypto isakmp policy 100

Router(config-isakmp)#authentication pre-share

Router(config-isakmp)#encryption 3des 加密算法

Router(config-isakmp)#hash md5 认证算法

Router(config-isakmp)#lifetime 60 SA活动时间

设置共享密钥和对端地址

Router(config)#crypto isakmp key cisco address 192.168.2.2

1. 配置IPSEC的协商

设置传输模式集

Router(config)#crypto ipsec transform-set tran1 esp-3des esp-md5-hmac

配置访问控制列表

1. 配置端口的应用

创建Crypto Maps

Router(config)#crypto map map1 100 ipsec-isakmp

配置Crypto Maps

Router(config-crypto-map)#match address 1

Router(config-crypto-map)#set peer 192.168.2.2

Router(config-crypto-map)#set transform-set tran1

应用Crypto Maps到端口

Router(config-if)#crypto map map1

1. 调试并排错

查看IKE策略

Router# show crypto isakmp policy

查看IPsce策略

Router# show crypto ipsec transform-set

查看SA信息

Router# show crypto ipsec sa

查看加密映射

Router# show crypto map