**Vpn（虚拟专用网）定义与类型**

常见：IPESC RGE /L2TP /SSL VPN /MPLS VPN

定义：VPN建立“保护”网络实体之间的通信

使用加密技术防止数据被窃听

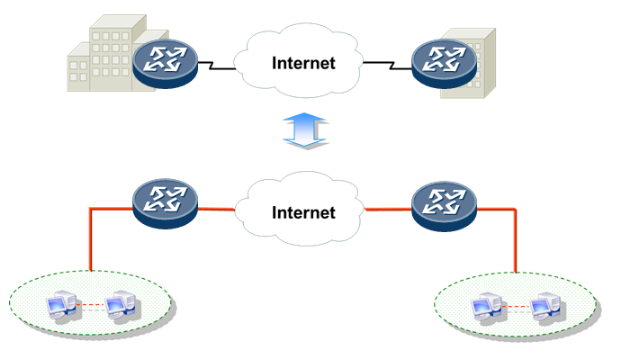
数据完整性验证防止数据被破坏、篡改

通过验证机制确认身份，防止冒充

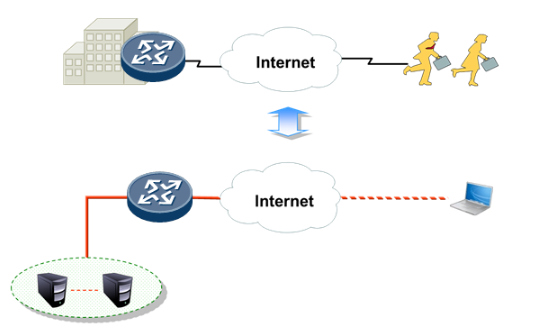


VPN类型

站点到站点VPN

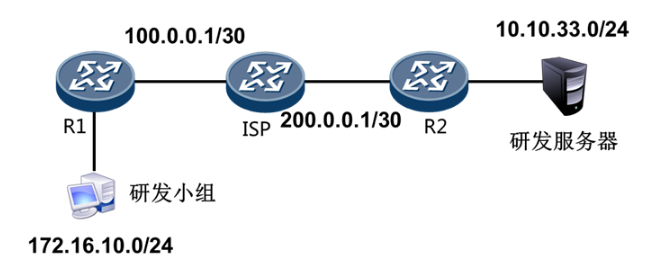


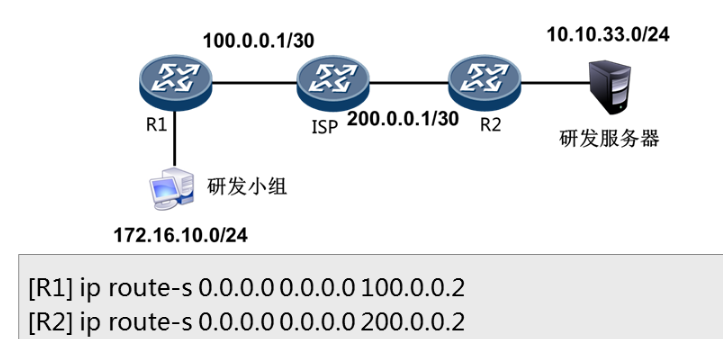
远程访问VPN



**VPN配置思路**

实例：研发小组可以通过VPN访问总公司研发服务器，但不能访问internet







阶段1：配置IKE（因特网密钥交换协议，作用：自动管理密钥）安全提议（算法集合）

阶段2：配置ACL

配置IPSec安全提议（算法集合）

配置IPSEC安全策略

在接口应用IPSEC安全策略

**阶段一原理与配置**

阶段一配置任务：

加密算法

认证算法

DH算法

预共享密钥

加密算法：防止数据被窃听

加密与解密

加密：明文数据“c”修改为密文数据“m”

解密：密文数据“m”修改为明文数据“c”

加密算法分类

对称（加密解密用同一个密钥）：

加密算法：DES（数据加密标准）

3DES（三重加密算法）

AES（高级加密标准）比较多

非对称（加密解密用的不是用一个密钥：公钥加密、私钥解密）

加密算法：RSA（使用三位数学家名字首字母来命名）

优势：安全：私钥永远不会被其他设备得到

缺点：计算过程复杂：它的计算效率要比对称加密算法低的多（大约要慢1500倍）

认证算法：保证数据完整性（校验文件）

哈希（HASH）

MD5：信息-摘要算法，创建了一个128为（16字节）的签名，很多协议都使用该算法做验证，执行速度快，但安全性相比SHA稍微差点

SHA：安全散列算法，已成为美国国家标准，它可以产生160位的签名（20字节的长度），为了更加安全，已经开发了SHA-256和SHA-512等。

DH算法

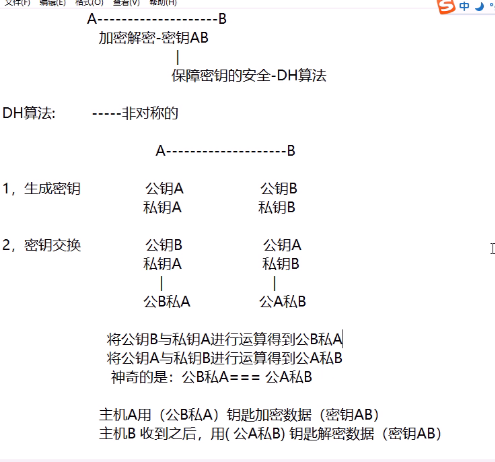
一般用来实现IPSec中的internet密钥交换

DH算法将对称加密和非对称加密算法结合在一起

DH算法支持可变的密钥长度（DH组长度来显示）

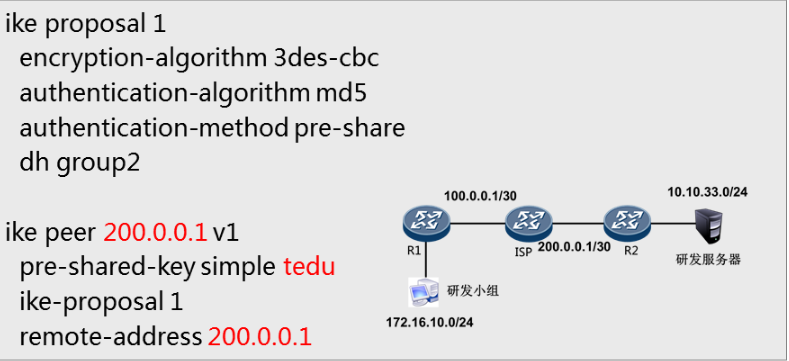
其中DH组1为768，DH组2为1024，DH组5为1536，DH组14为1024

密钥的有效长度越长，安全性也就越强，同时CPU占用率也越高。



预共享密钥：防止冒充，进行身份确认，类似于暗号

配置命令



**阶段二原理与配置**

配置任务

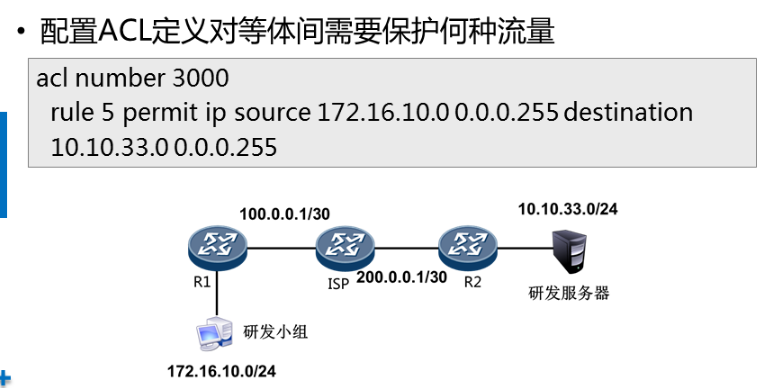
配置ACL ---哪些数据可以传输

配置IPSec安全提议 ---数据加密

配置IPSec安全策略 ---上两个调用

在接口应用IPSec安全策略 ---

定义保护流量



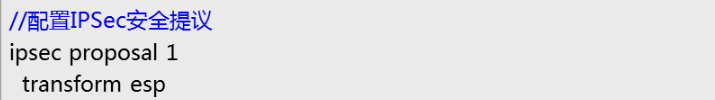
定义安全协议

AH（认证头协议）：数据验证，对整个IP数据包

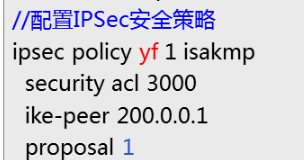
ESP（封装安全负载荷协议）

-ESP对用户数据实现加密功能

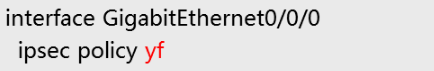
-ESP只对IP数据的有效载荷进行验证，不包括外部的IP包头



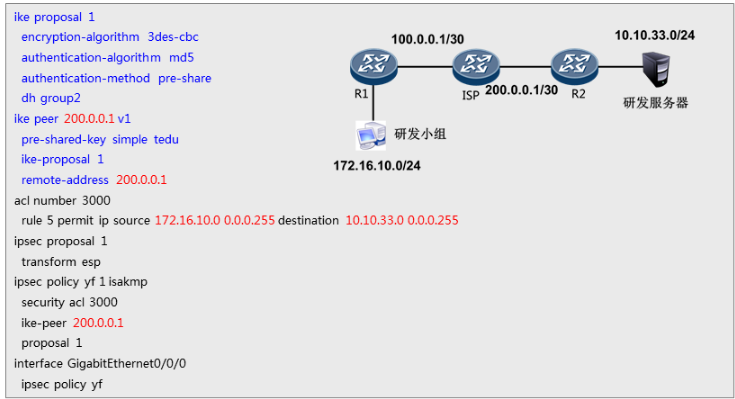
配置安全策略

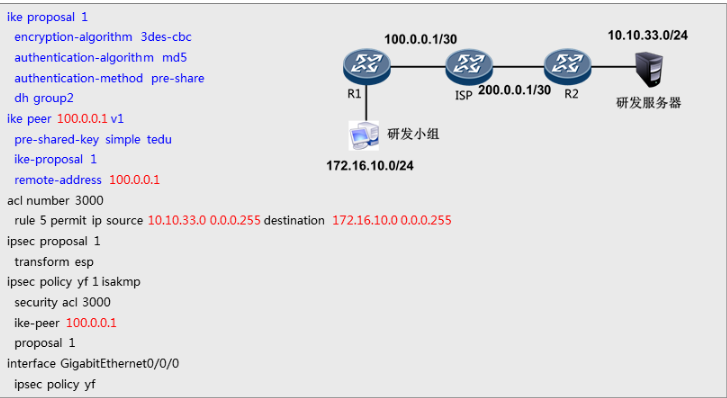


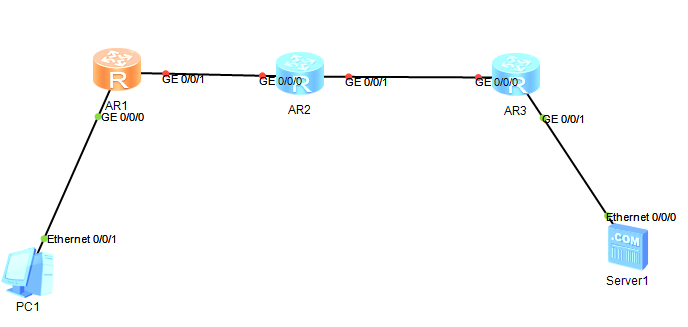
在接口上应用安全策略

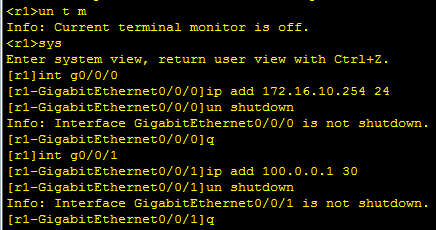


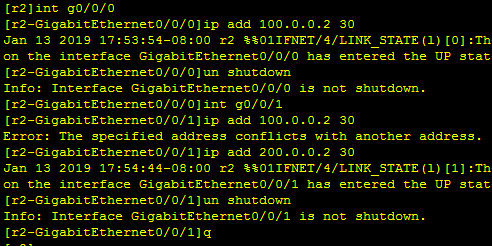
VPN配置命令模板

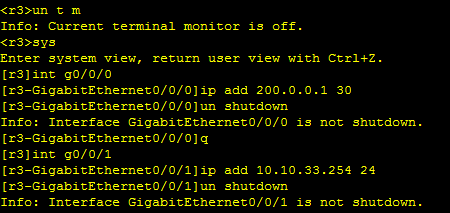








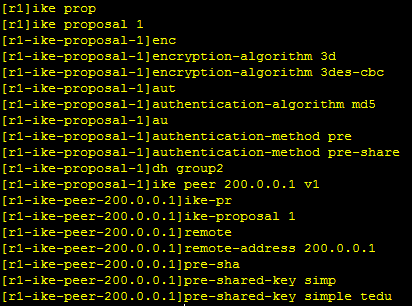




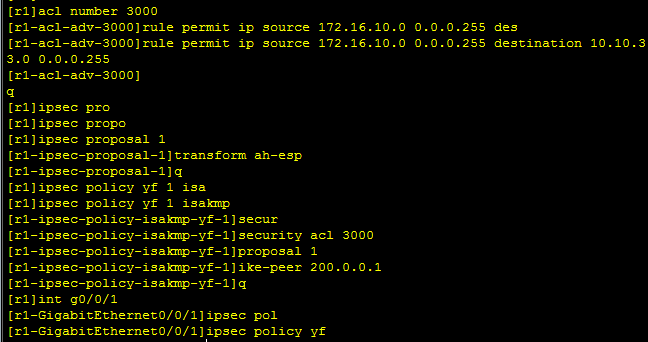




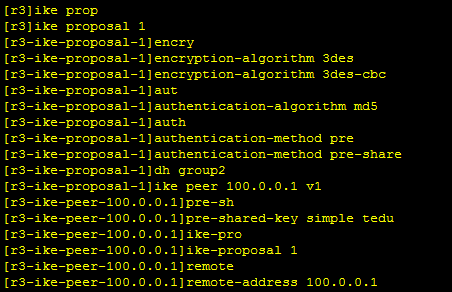
r1阶段一



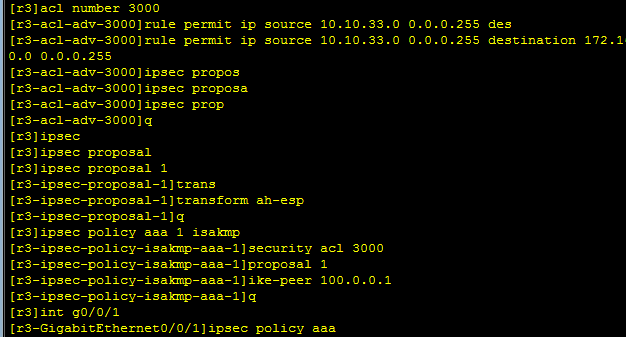
r1阶段二



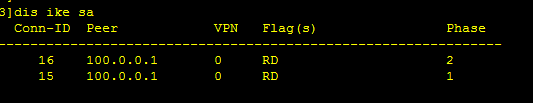
r3阶段一

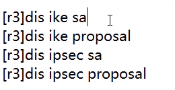


r3阶段二









定义隧道模式：IP包被保护、封装概念

