**一、VPN技术**

概念：VPN（虚拟专用网），利用开放的公众IP/MPLS网络建立专用数据传输通道，将远程的分支机构、移动办公人员等连接起来。

原理：利用加密技术在公网中封装出一个数字通信的隧道。

实现VPN的关键技术：隧道技术、加密技术

根据层次进行VPN的分类（考点）

* **PPTP** vpn：工作在**二层**，要求三层网络是IP、单一隧道
* **L2TP** vpn：工作在二层，三层网络支持多种（ATM、帧中继等）、支持多隧道、隧道验证
* **MPLS** vpn：**2.5层**，多协议标记交换VPN（网规重点，企业常用）
* **IPsec vpn**：工作在三层
* GRE vpn：工作在三层，通用路由封装，支持多种网络层协议
* SSL vpn：在应用层

**二、IPsec VPN（思科时代常考）**

IPsec是一种开放标准的框架结构，特定的通信方之间在IP层通过加密和数据摘要（hash）等手段，来保证数据包在Internet网上传输时的**私密性、完整性和真实性**。

（大概就下面表格这个样子）

|  |  |  |
| --- | --- | --- |
| 新增加的IP头 | IPsec头 | 被封装的的原始IP包 |

**IPsec框架**

* **两个安全协议：**
  + **AH（认证头协议）：提供完整性和数据源认证功能，不提供机密性保护，不能做NAT。**
  + ESP（封装安全载荷）：AH+**机密性保护，**可以NAT。
* **密钥管理协议：**先用IKE SA建立隧道，再用IPsec SA对数据流进行保护。而密钥管理协议采用自动协商的机制，通过DH算法进行数据交换，计算出数据双方共享的密钥。

**两种模式**

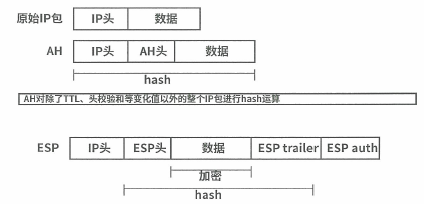
* **传输模式**：两个需要通信的计算机终端运行IPsec，对主机之间传输层的报文进行保护，进行数据传输的路由器不参与IPsec过程。

不改变原有的IP包头，通常用于主机与主机之间

**AH:**在**IP头和数据部**分之间插入一个AH头

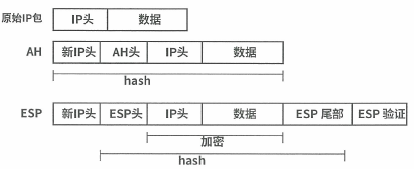
***AH对除了TTL、头校验和等变化值以外的整个IP包进行hash运算。***

**ESP**

****

**隧道模式（企业常用）：**常用于总部与分部之间。对整个数据包提供安全传输，主要通过在两个安全网关上运行IPSec。

增加新的IP头，通常用于私网与私网之间通过公网进行通信。



***注：做PAT的话会在新IP头前再封装一个UDP报文头，对内部不做改变。***

**IPSEC VPN（华为）工作流程**

1. **配置安全ACL：**配置哪些流量需要被保护
2. **配置安全提议：**配置IPsec的参数
3. **配置IKE：**预共享密钥，配置身份验证方法、加密算法等安全参数
4. **配置安全策略：**1和2做关联
5. **在接口应用安全策略**

**具体配置命令：**

**1、通过ACL定义需要保护的数据流**

[R1]acl 3000

[R1-acl-adv-3000]rule permit ip source **50.50.50.0 0.0.0.255** destination **60.60.60.0 0.0.0.255**

***//对端设备配置类似，只是源地址和目的地址交换***

**2、配置IPsec安全提议（封装模式、安全协议、加密算法和验证算法）**

[R1]ipsec proposal ***tran1****//起名，进入ipsec安全提议视图*

[R1-ipsec-proposa-tran1]encapsulation-mode ***tunnel***

***//配置工作在隧道模式下（可选传输模式transform）***

[R1-ipsec-proposa-tran1]transform **esp**

***//安全协议使用ESP（可选AH，默认ESP）***

[R1-ipsec-proposa-tran1]esp encryption-algorithm **3des**

***//对数据机密性保护采用3DES算法（可选DES、AES）***

[R1-ipsec-proposa-tran1] esp authentication-algorithm **sha1**

***//用SHA1哈希算法保证报文完整性（可选MD5）***

[R1-ipsec-proposa-tran1]quit

***//对端设备配置相同***

**3、配置IKE对等体**

[R1]ike peer ***peer1*** ***//命名***

[R1-ike-peer-peer1]pre-shared-key simple *Huawei*

***//配置预共享密钥（一般情况配置简要的密码认证）,两端网关设备的密码相同，则成为IKE对等体，成为安全网关***

[R1-ike-peer-peer1]remote-address **20.20.20.1**

***//指定对端IP***

[R1-ike-peer-peer1]quit

***//对端配置类似，指定对端IP的时候，指定30.30.30.1***

**还可以配置IKE提议（常见考法：作解释）：**

[R1]ike proposal {proposal-number}

***//数值越小，级别越高***

[R1-ike-proposal-10]encryption-algorithm {3des-cbc|aes-cbc[key-length]|des-cbc}

***//默认CBC模式的56位DES***

[R1-ike-proposal-10]authentication-mathod {pre-share|rsa-signature} ***//默认pre-share（预共享密钥）***

[R1-ike-proposal-10]authentication-algorithm {MD5|sha}

***//默认SHA-1验证算法***

[R1-ike-proposal-10]dh {group1（768位）| group2（1024位）| group3（1536位）| group4（2048位）}

***//进行密钥交换时候用的算法，默认group1***

[R1-ike-proposal-10]sa duration *seconds*

***//设置安全关联超时的时间，默认86400***

**如未作配置，则采用默认的IKE提议：DES、SHA-1、pre-Share、gourp1、86400**

**4、配置IPsec安全策略（并将1、2进行关联）**

[R1]ipsec policy ***csaimap*** 1 isakmp //给安全策略起名

[R1-ipsec-policy-isakmp-csaimap-1]proposal **tran1**

[R1-ipsec-policy-isakmp-csaimap-1]security **acl 3000**

[R1-ipsec-policy-isakmp-csaimap-1]ike-peer **peer1**

[R1-ipsec-policy-isakmp-csaimap-1]quit

***//对端设备配置一致***

**5、在接口上应用IPsec安全策略组**

[R1]interface **s0/0**

[R1-serial 0/0]ipsec policy **csaimap**

***//在隧道的起止点上应用***

***//对端设备配置基本类似，但注意对端地址需要修改***

***注意：考试中通常结合VPN原理来考，配置命令考法：解释或填空***

**三、策略路由（华为）**

**概念：**普通的路由根据路由表进行转发，策略路由根据规则对报文进行过滤和转发，是传统路由的一种有效加强。通常用在**负载均衡**的网络。

**优先级：**策略路由大于静态路由（60）和动态路由（看具体协议）

**作用：**例如访问联通的服务器用联通的数据线路，访问电信的服务器用电信的数据线路。

**要求看懂配置命令**