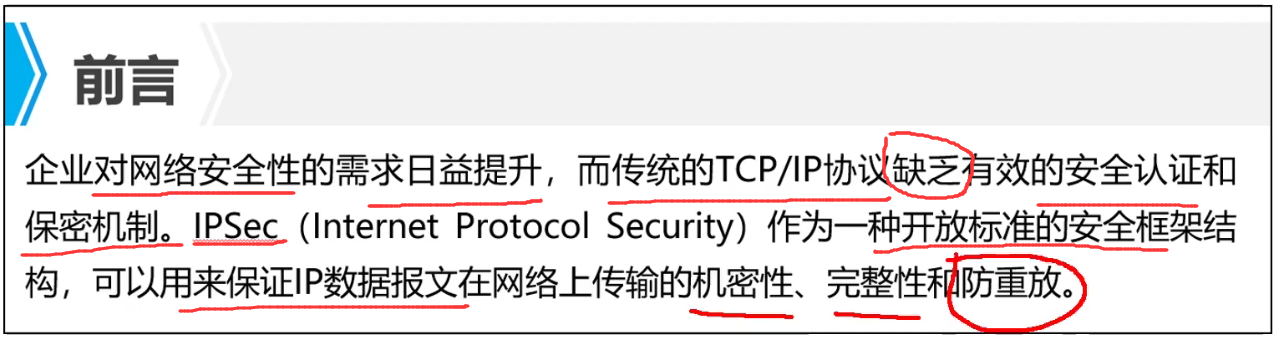
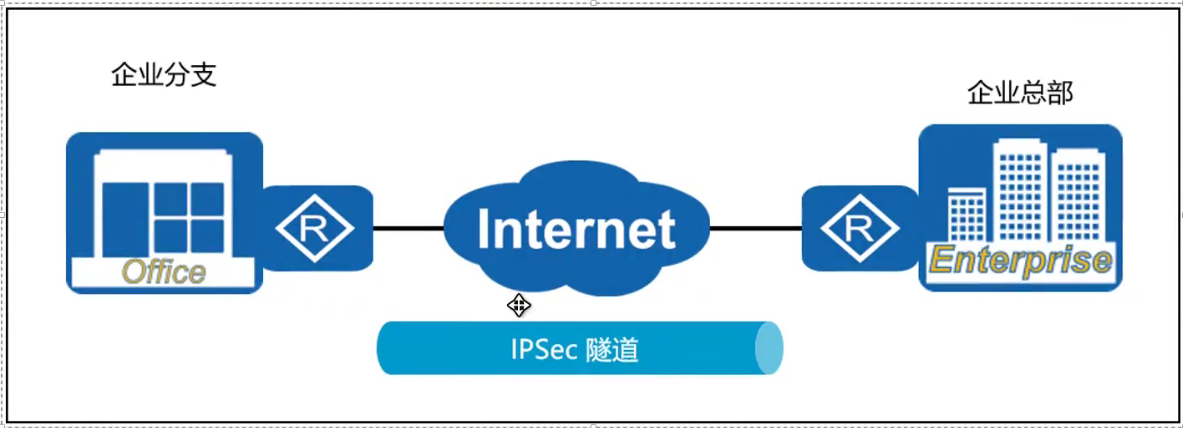
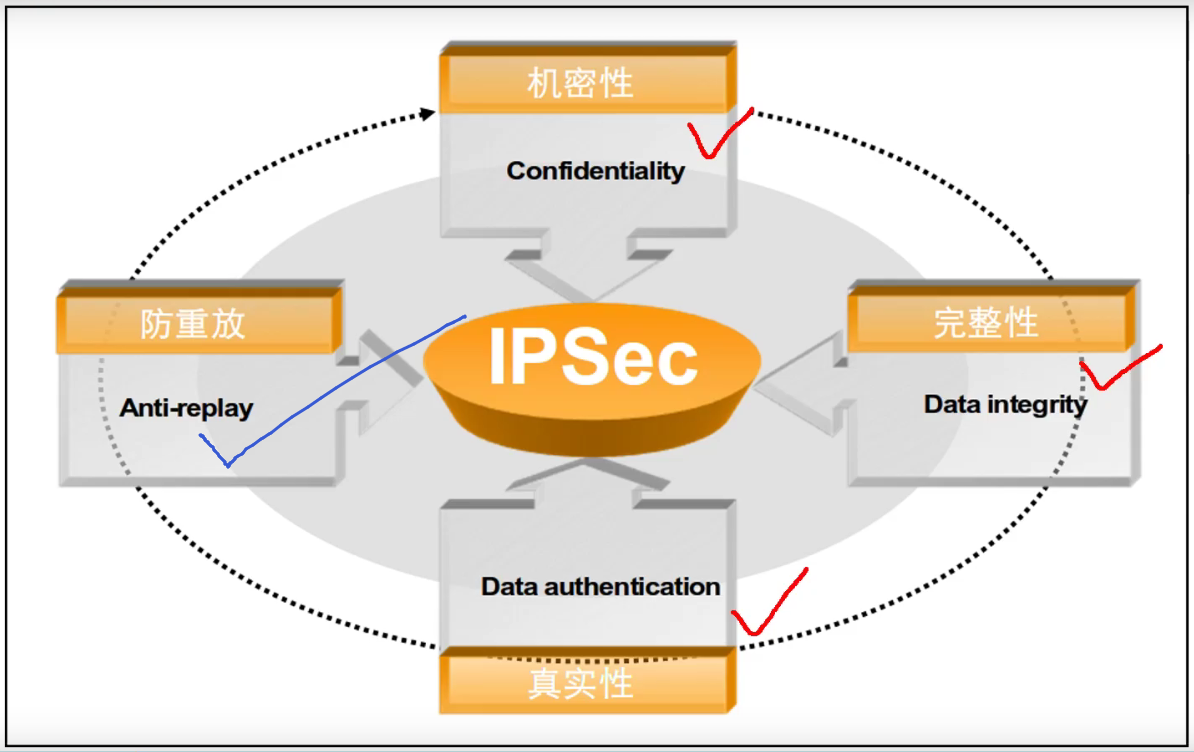
* 
* 随着网络安全需求的日益提升，而传统的TCP/IP协议缺乏有效的安全认证和保密机制（不加密，明文），所以我们要保证数据的安全性，因此IPsec就是一种开放的安全框架，可以用来保证IP数据报文在网络上传输的机密性，完整性和防重放。

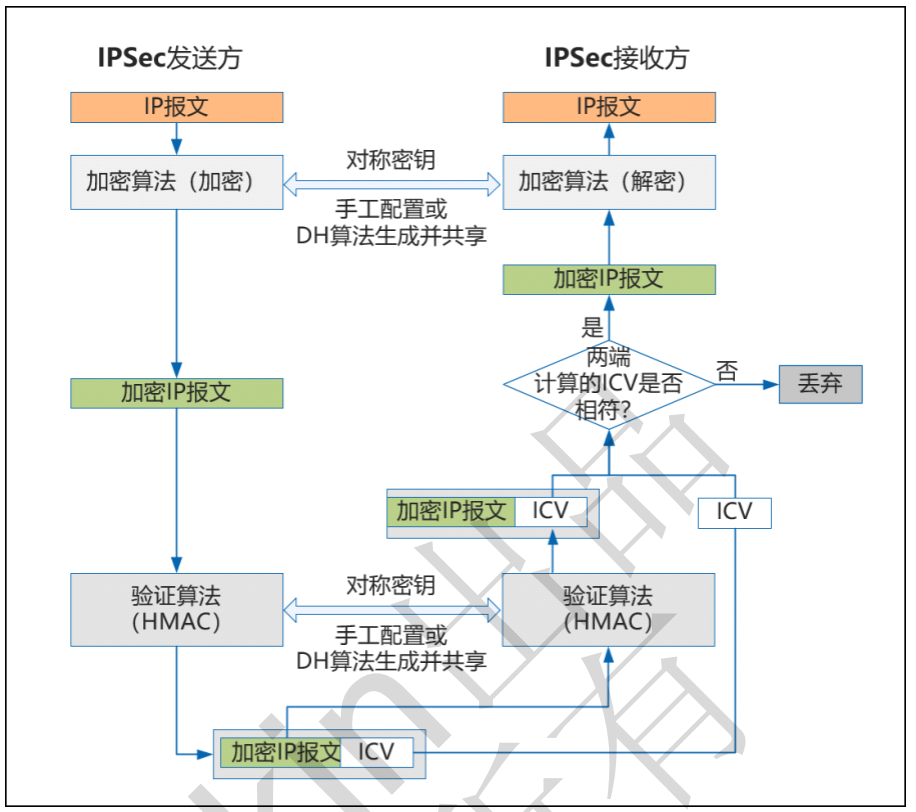
IPsec：Internet Protocol Security

* 源于IPv6
* IETF制定的一套安全保密性能框架
* 建立在网络层的安全保障机制
* 引入多种加密算法，验证算法和密钥管理机制
* 也具有配置复杂，消耗运算资源较多且增加延迟，不支持组播等缺点
* IPsecVPN是利用IPsec隧道建立的VPN技术（IPsec也是有隧道技术的，没有隧道根本不能成为一种合格的VPN技术）
* 

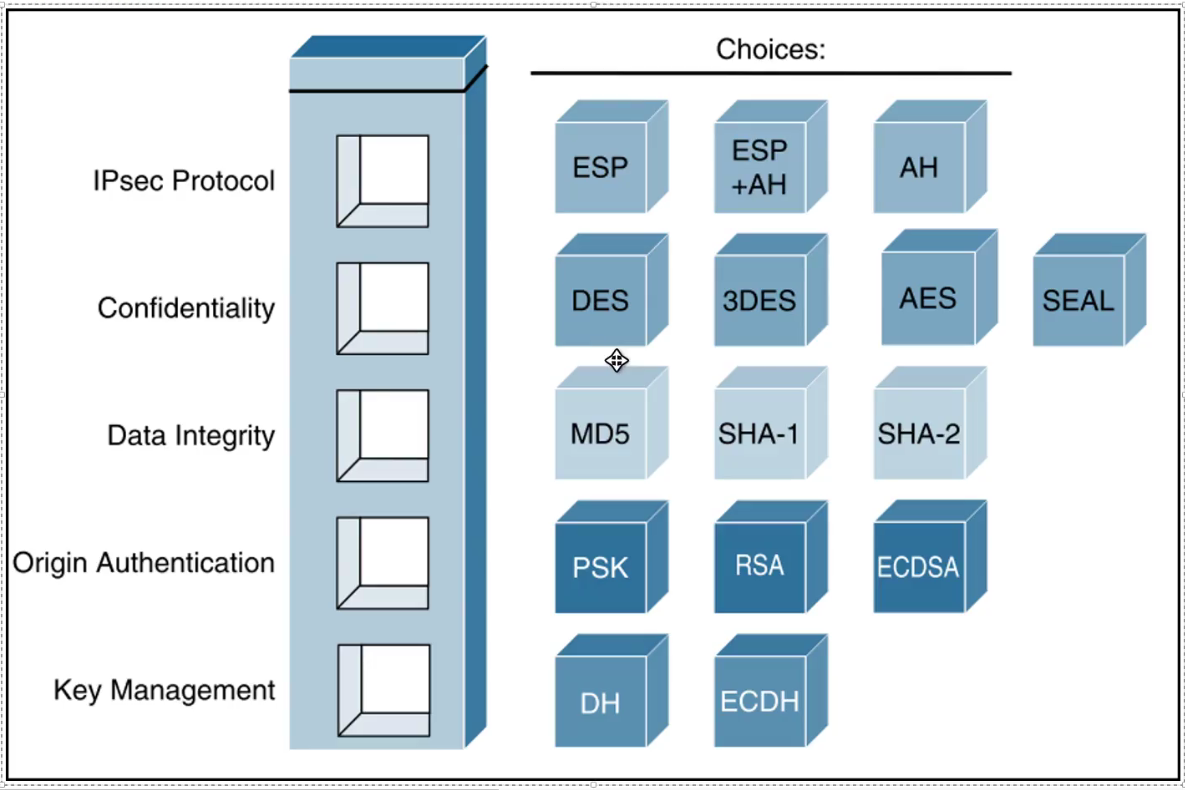
IPsec核心功能：

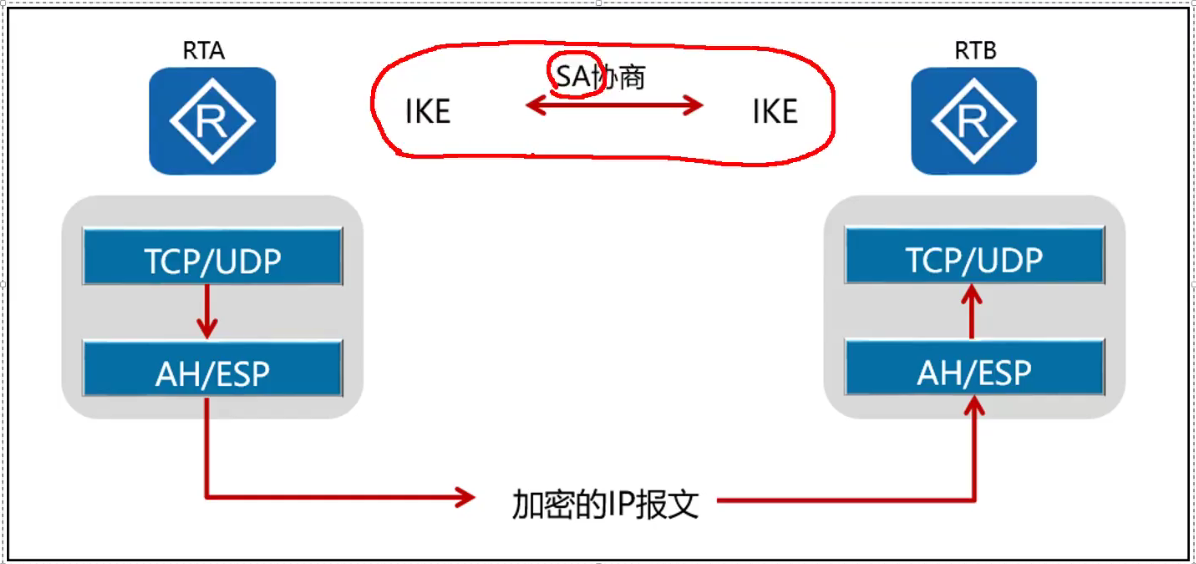
* 

|  |  |
| --- | --- |
| 术语 | 备注 |
| 机密性 | 对数据进行加密，确保在传输时不被泄露给非授权用户。 |
| 完整性 | 保障数据在传输时，不被非授权用户进行篡改。 |
| 真实性 | 验证数据源，以确保数据来自真实的发送者。（IP报文头部内的源地址）   在数通领域，并不牵扯到用证书来做验证，这里使用数据包的源地址就行。 |
| 防重放 | 防止恶意用户通过重复发送捕获到的数据包所进行攻击，即接收方会拒绝旧的或重复的数据包。 |

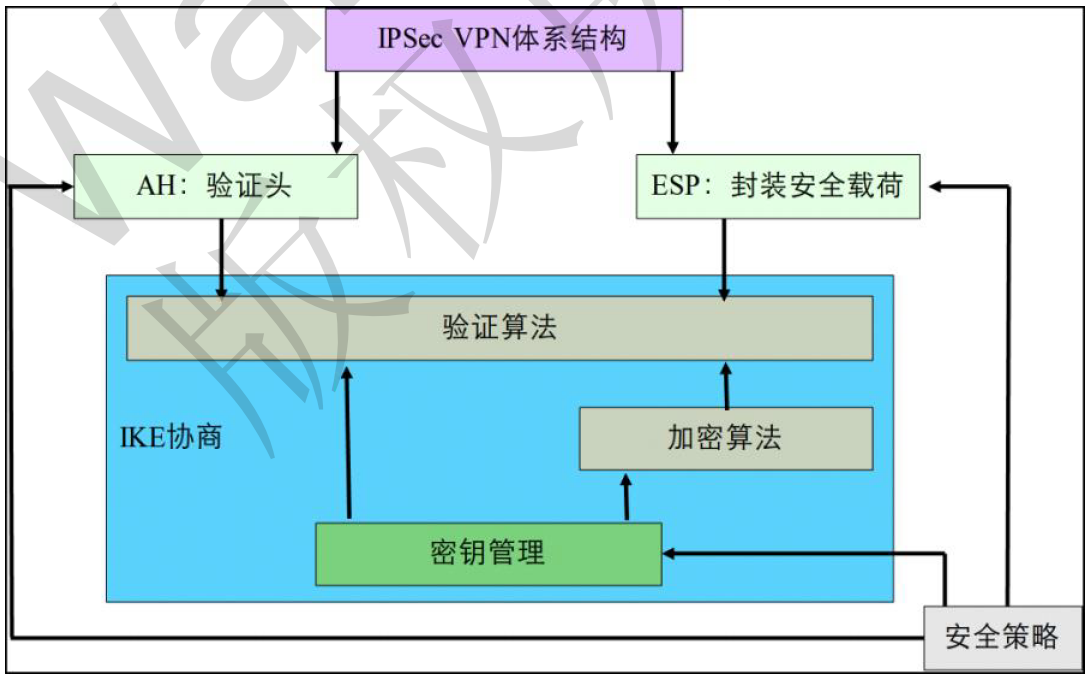
* IPsec在发送报文时会有哪些比较关键的步骤，以下图实例就是告诉我们是如何实现的
* 

IPsec技术框架：

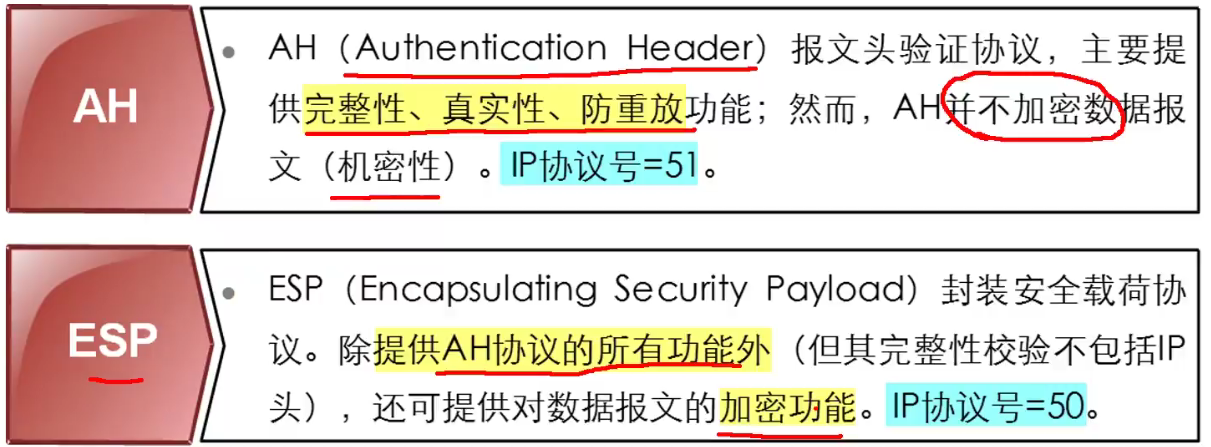
* 

* 
* DES和3DES加密算法存在安全隐患，建议优先使用AES,SM1或SM4算法。
* MD5和SHA1验证算法存在安全隐患，建议优先使用，SHA2或SM3算法。
* 还是要看两端设备支持那种算法，如果都支持，那么尽量使用更安全的算法。
* 
* 通过AH和ESP这两个安全协议来实现IP数据报文的安全传输。
* IKE协议提供密钥协商，建立和维护安全联盟SA等服务。
* IKE是一种协商的方法，或者标准，SA通俗的叫安全联盟，当协商完成就可以进行实际的封装和传递，这里使用的保护就是AH和ESP了。

这里推荐使用ESP，建议使用ESP，ESP有加密，AH没有加密但有其他特性。协商要保证安全有加密，传递数据要安全也有加密。

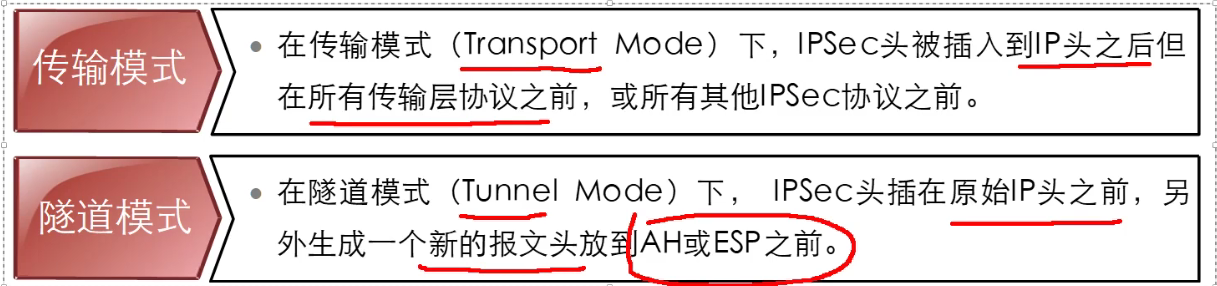
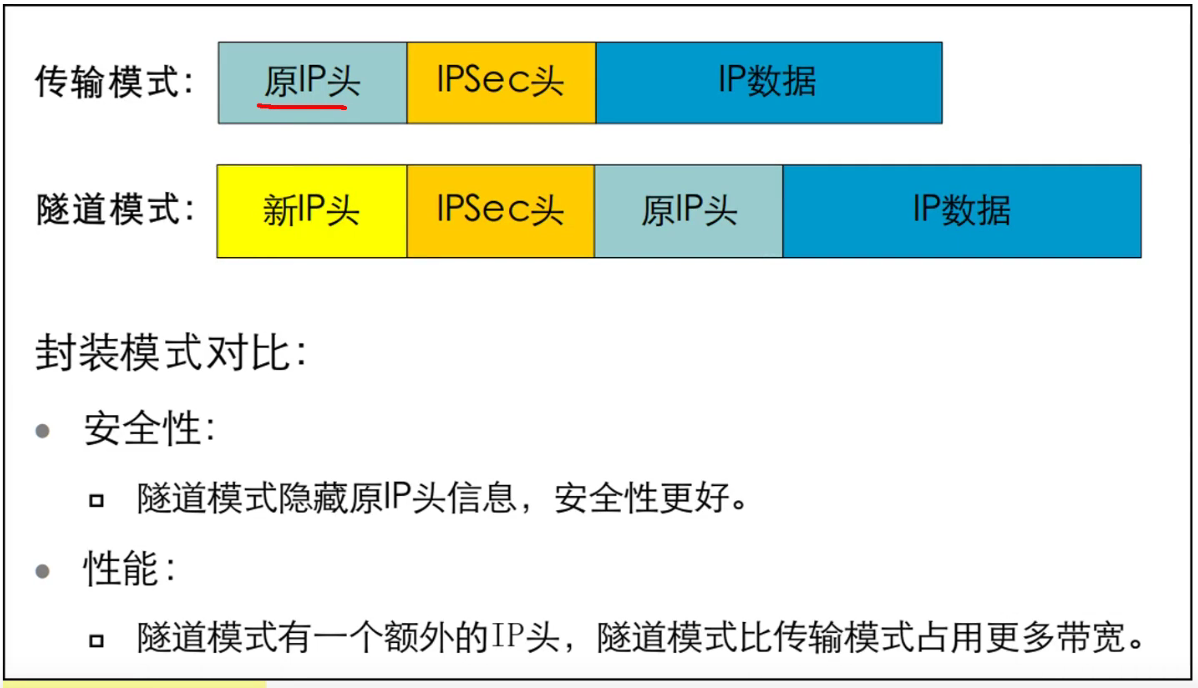
* 
* IKE协商：协商验证算法，加密算法。
* 密钥管理：算法要使用密钥，所以需要密钥管理技术，进行自动协商或者手动，然后分发。
* 数据包为什么要进行协商和加密验证，就是出于我们的安全策略。
* 策略包含了这些东西，最终这些都会关联到策略，然后再到接口进行调用，整套完成下来，会发现他是一个模块化的东西，如果要进行修改只需要修改对应的模块，至于实际的封装是AH和ESP。

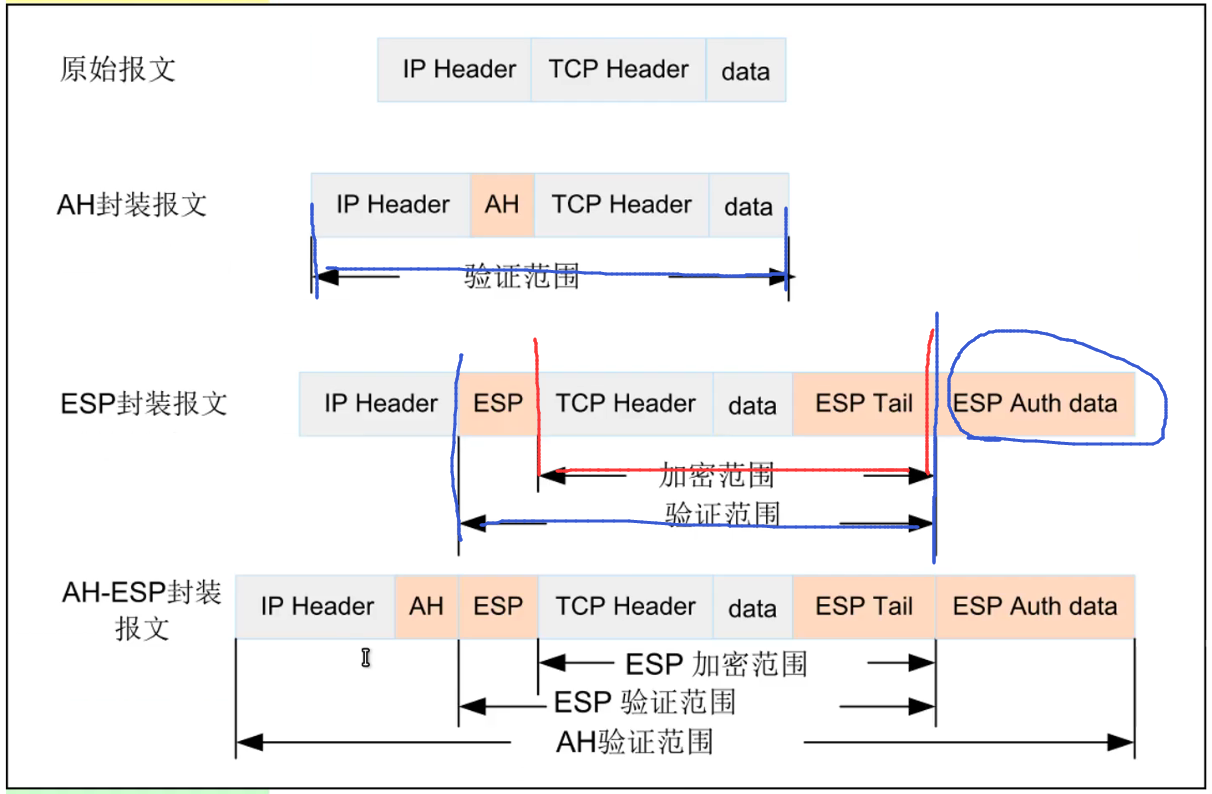
IPsec安全协议：

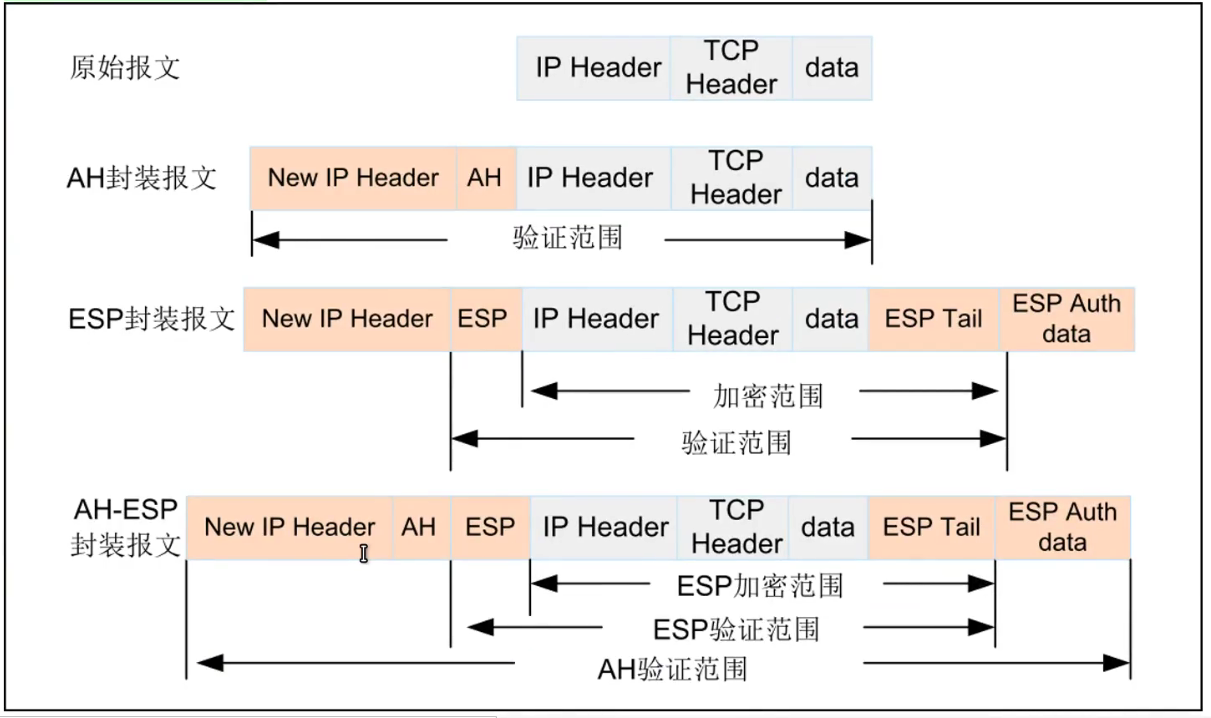
* 
* AH：报文头验证协议，提供完整性，真实性，防重放等特性，但是AH并不进行数据加密，协议号为51。
* ESP：封装安全载荷协议，提供完整性，真实性，防重放，且提供数据加密，但是校验不包括IP报头，协议号为50.

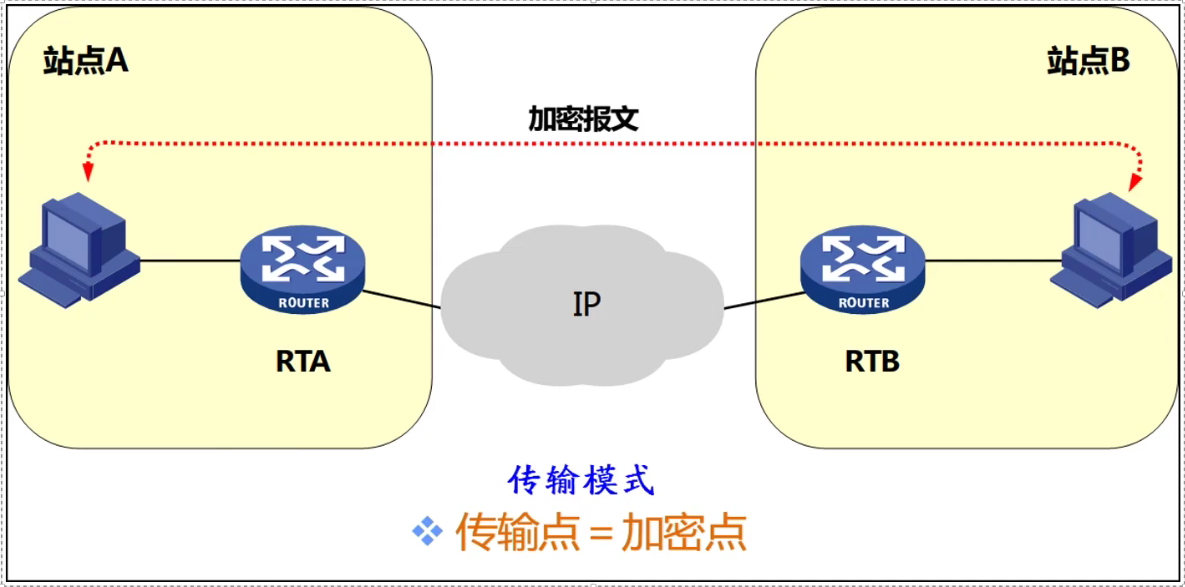
|  |  |  |
| --- | --- | --- |
| 安全特性 | AH | ESP |
| 协议号 | 51 | 50 |
| 数据完整性校验 | 支持 | 支持 |
| 数据加密 | 不支持 | 支持 |
| 防报文重放攻击 | 支持 | 支持 |
| NAT穿越 | 不支持 | 支持 |

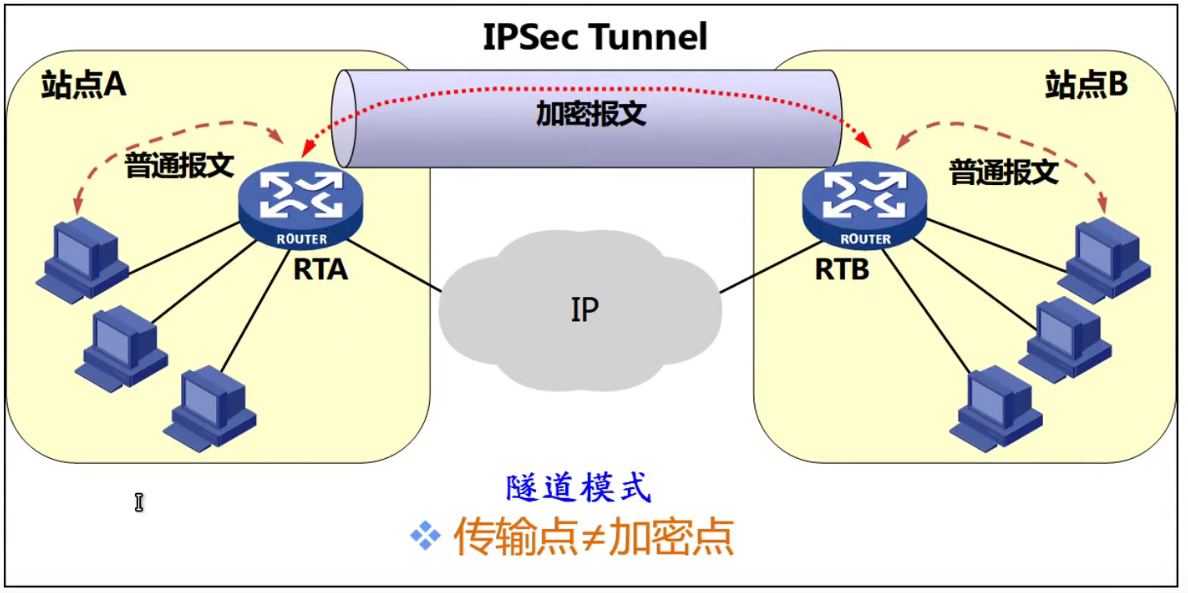
IPsec封装模式：两种模式，四种数据报文格式。

* 
* 传输模式和隧道模式是对立的，隧道是加新报头，传输是不加。
* 传输模式：在原始IP报头后面加入IPsec报头（ESP或AH报头）。
* 隧道模式：在原始IP报头前面加入IPsec报头（ESP或AH报头），另外再生成一个新IP报头放到IPsec报头前面。
* 安全性：隧道模式隐藏原IP报头，安全性更高。
* 性能：隧道模式有一个新的IP报头，所以传输模式比隧道模式更占用带宽。
* 

* 传输模式封装结构
* AH：整个IP层往后都会做验证。
* ESP：ESP头部和尾部做验证，加密除ESP字段外到ESP尾部数据。注：为什么不加密IP头部，加密了设备无法读取到数据。
* 

* 隧道模式封装结构
* 

* 两个设备直接做的数据协商和加密，没有新的IP报头，负责发送数据同时也负责加密和验证。
* 

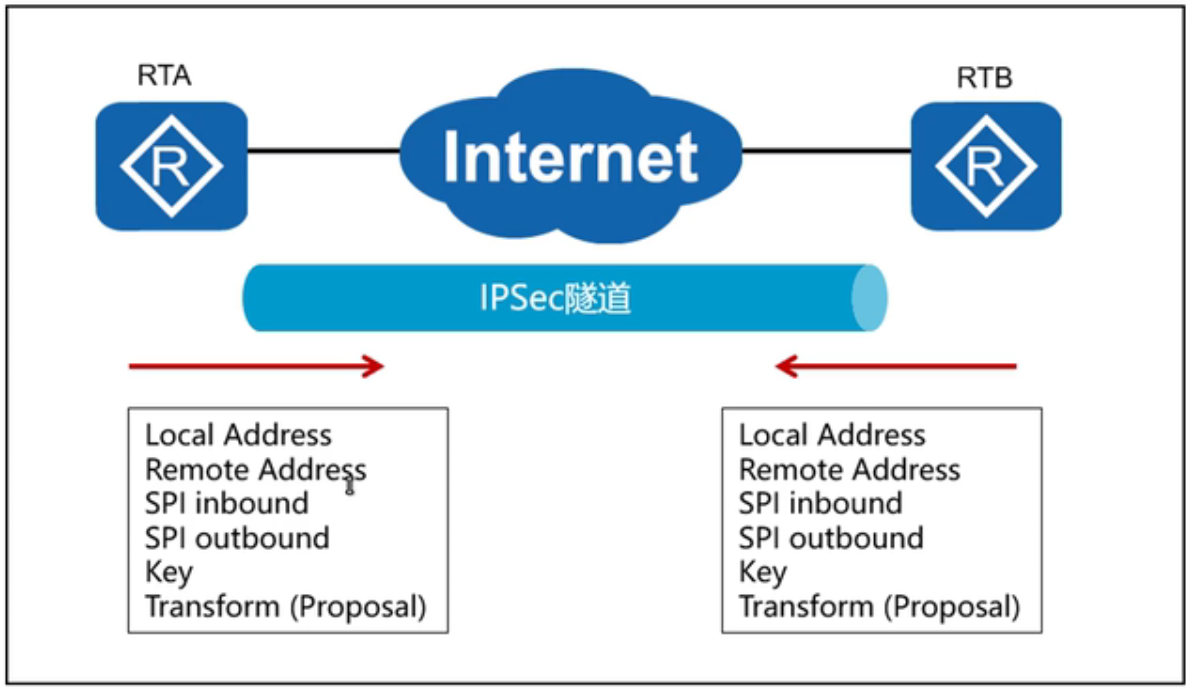
* 传输点不是加密点，也就是说出口设备进行协商和加密，实际传输数据是其他设备。
* 

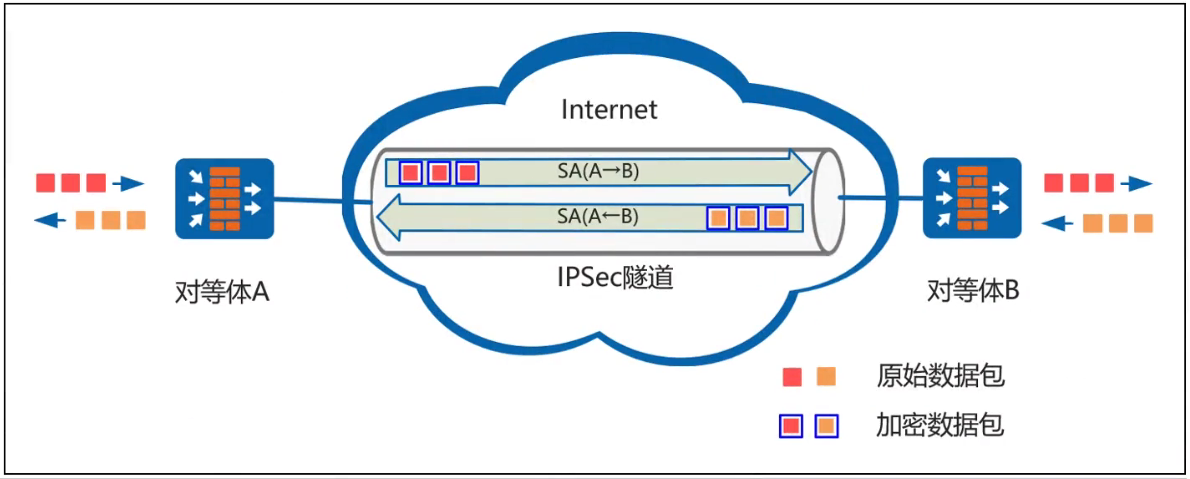
安全联盟：SA (Security Association)

* 顾名思义，通信双方结成盟友，相互信任，即达成约定。
* SA由一个（SPI，IP目的地址，安全协议号（AH，ESP））三元组唯一标识。
* 决定了对报文进行何种处理：模式，协议，算法，密钥。生存周期等。
* 每个IPsec SA都是单向的。
* SA可以手工建立或者IKE协商生成。
* SPD（Security Policy Database）安全策略数据库
* SAD（Security Association Datebase）安全联盟数据库

|  |  |
| --- | --- |
| 术语 | 备注 |
| Negotiate | 协商，两个节点要开始安全发送数据之前，必须要做的事情。（动态协商） |
| SA | Security Association 安全联盟，协商的结果，类似合约书。 |
| SPI | Security Parameter index 安全参数索引，SA内包含，用于区分多个SA。 |
| IKE | Internet Key Exchange 因特网密钥交换，SA协商的方法和标准。 |

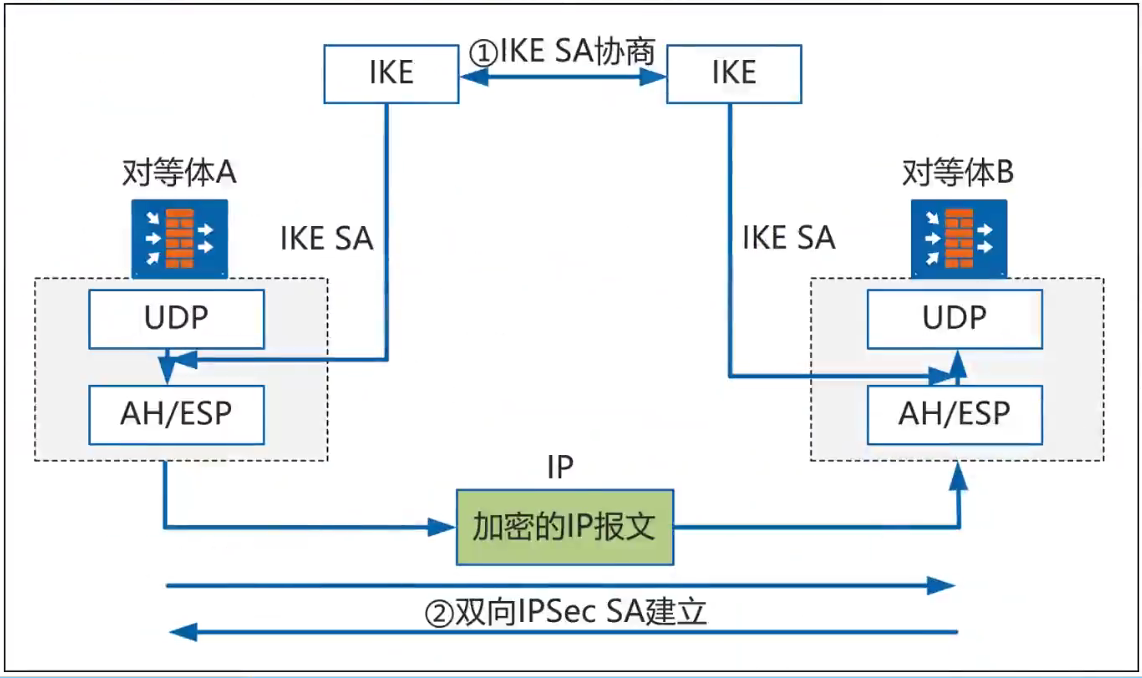
* 两端设备先进行协商， 协商完毕后会有SA，SA包含了SPI，IKE和IPsec参数，协商的方法是使用IKE或者手动。
* 

* 

* 

|  |  |  |
| --- | --- | --- |
| 对比项 | 手工建立 | IKE协商 |
| 密钥生成 | 手工配置 | DH算法 |
| 密钥刷新 | 手工配置 | 动态刷新 |
| 生成周期 | 永久 | 可配置 |
| 适用环境 | 小型网络环境 | 中大型网络环境 |

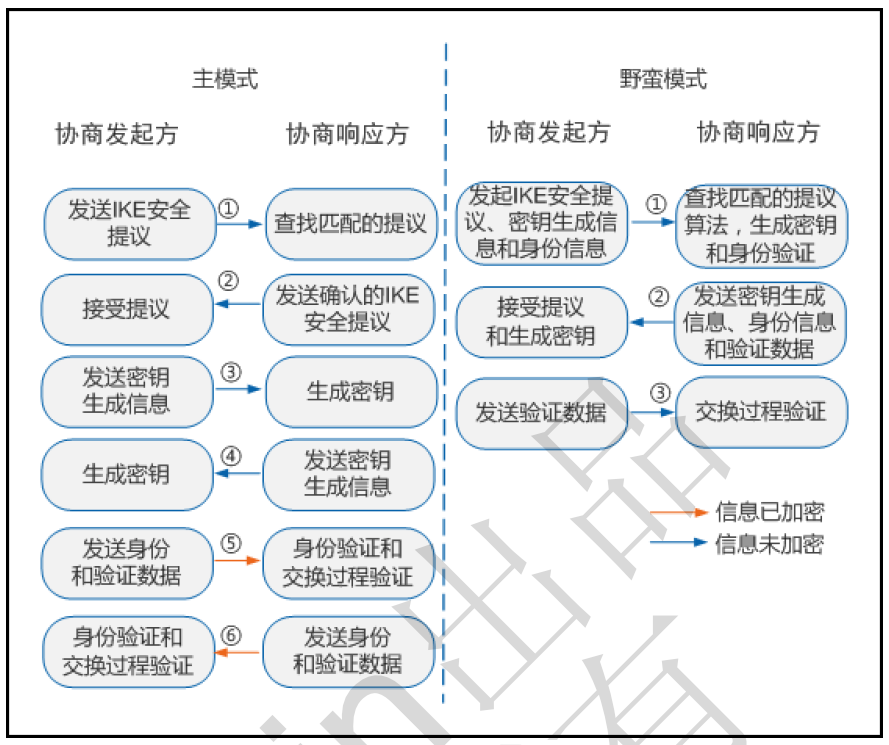
IKE：Intelnet Key Exchange，因特网密钥交换

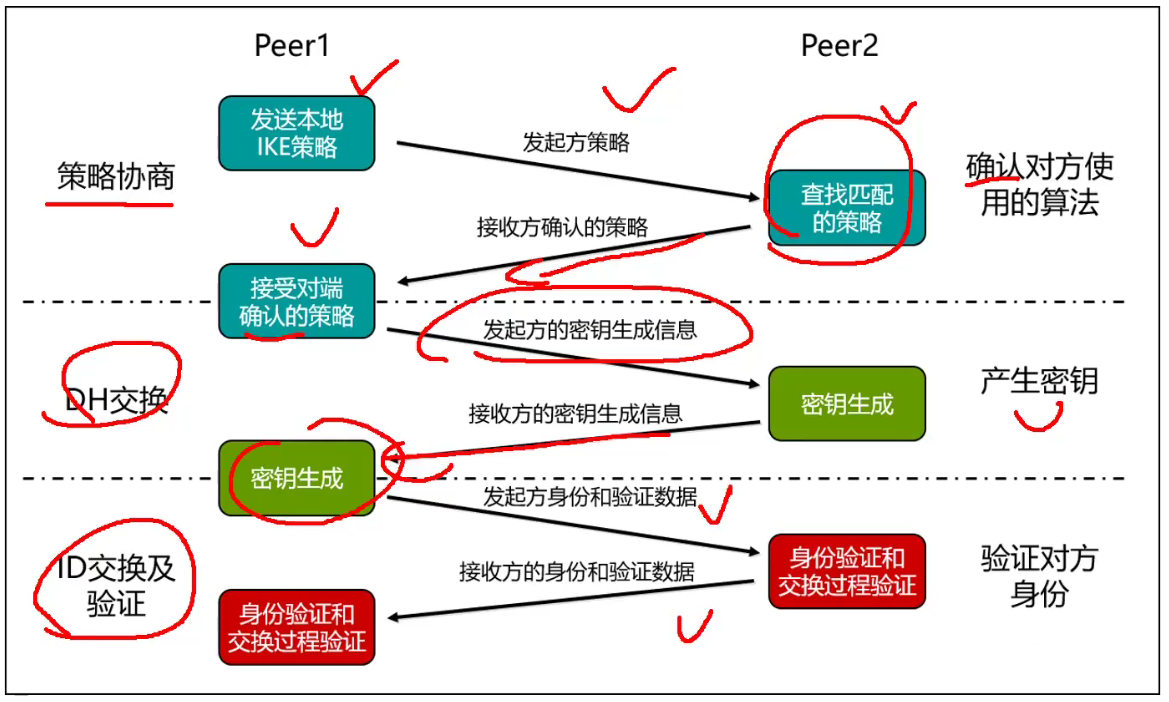
* 建立在ISAKMP（Intelnet安全联盟和密钥管理协议）定义的框架上。
* 基于UDP（端口号500）的应用层协议，可为数据加密提供所需的密钥。
* 使用DH算法，在不安全的网络上安全的分发密钥，验证身份。
* 定时更新SA和密钥，实现完善的前向安全性（PFS）。
* 允许IPsec提供防重放服务（加入随机数）。
* 简化IPsec的使用和管理，大大简化了IPsec的配置和维护工作。
* 
* IPsec会有两次SA协商，IKE SA协商主要是保证数据通道，通道里面传输加密数据使用IPsecSA来进行协商。
* IKE有分版本v1和v2，模式分主模式和野蛮模式。
* 首先会有IKE的协商，先有IKE协商出来的SA，然后再协商IPsecSA出来。这个过程有两个阶段。

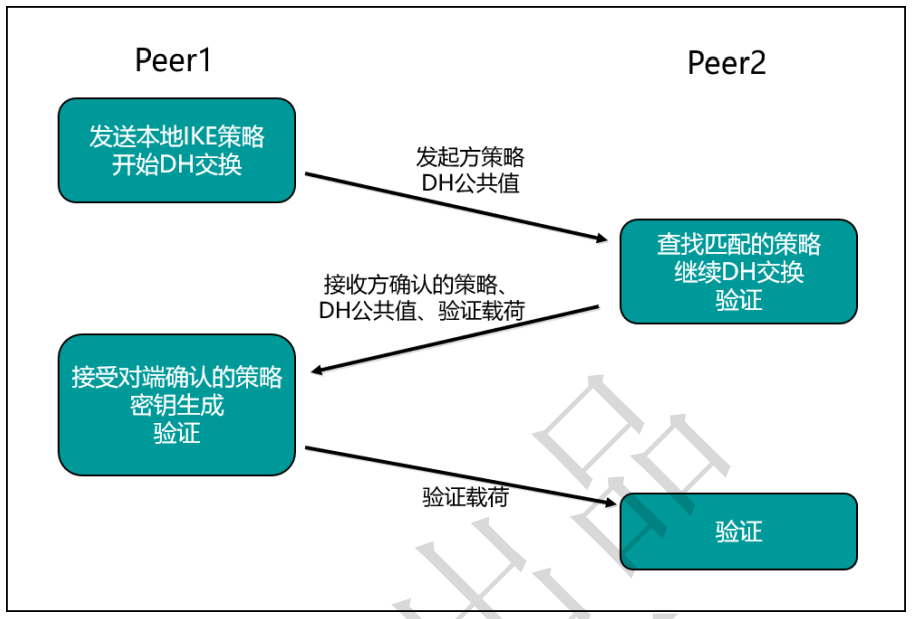
|  |  |
| --- | --- |
| 阶段 | 备注 |
| 阶段 1  Phase 1 | 在网络上建立一个IKE SA ,为阶段2协商通过保护  分主模式（Main mode）和野蛮模式（Affressive mode） |
| 阶段2  Phase 2 | 在阶段1 IKE SA 的保护下完成IPsec SA的协商  快速模式（Quick mode） |

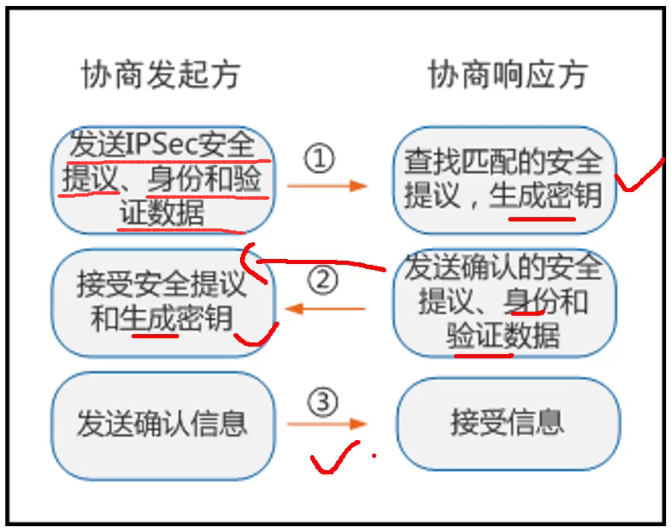
* 两端之间建立一个IKE SA完成身份验证和密钥信息交换后，在IKE SA的保护下，

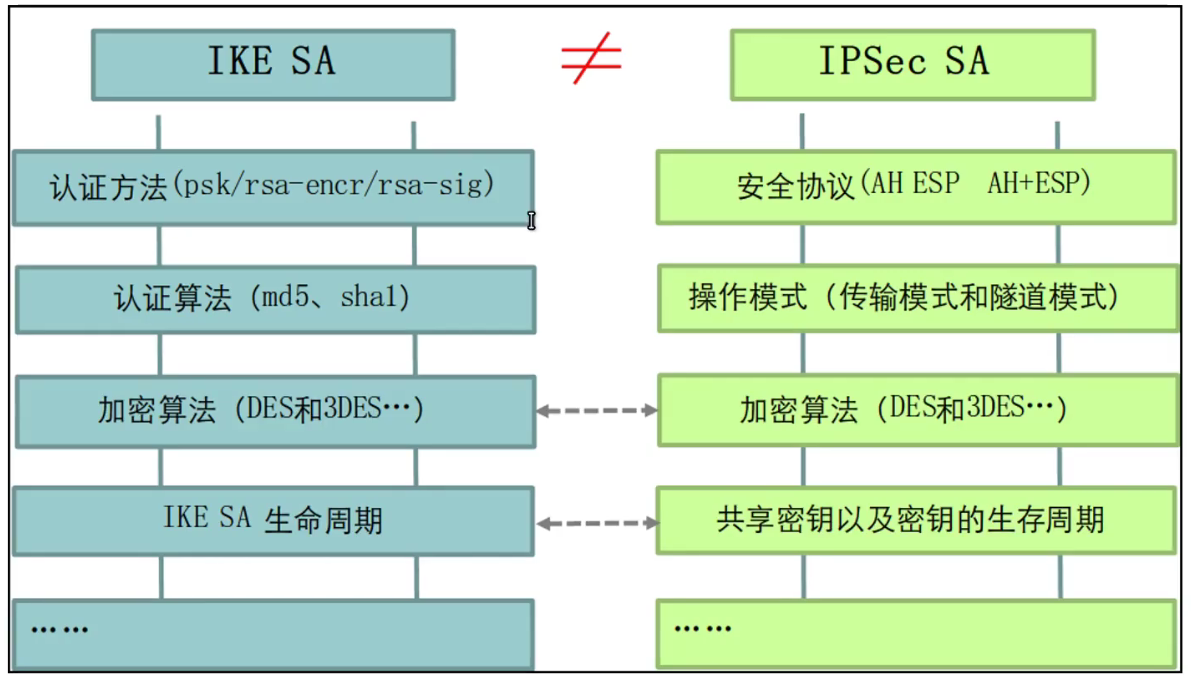
根据配置的AH/ESP安全协议等参数协商出一对IPsecSA。

* IKE协商模式
* 主模式：6个数据包，3个阶段（安全提议，生成密钥，验证身份（加密））
* 野蛮模式：3个数据包，1个阶段（三个阶段合并为一个，然后验证）
* 

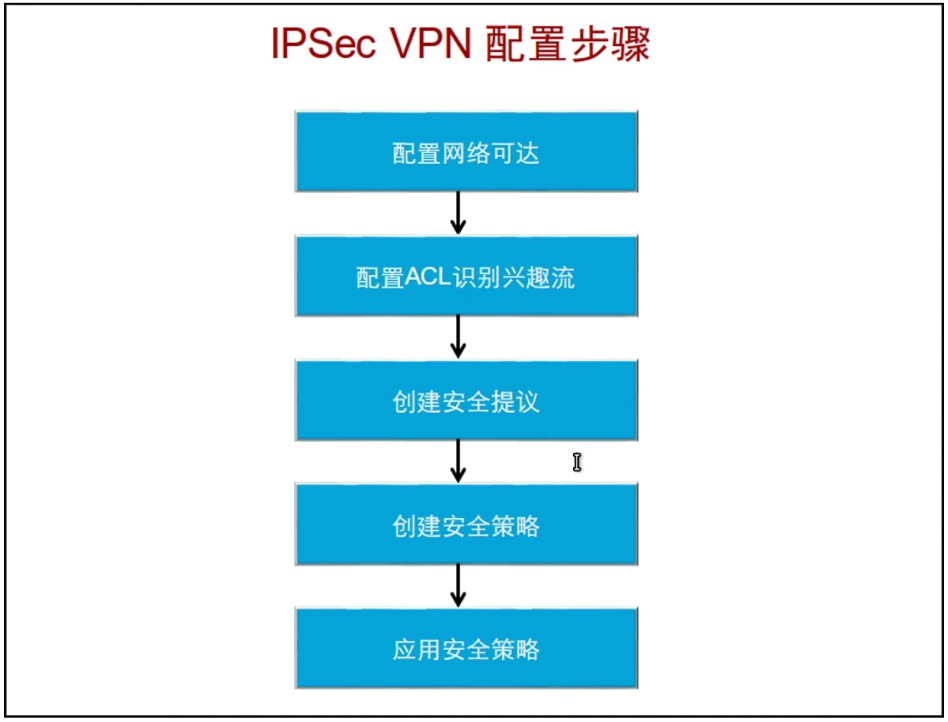
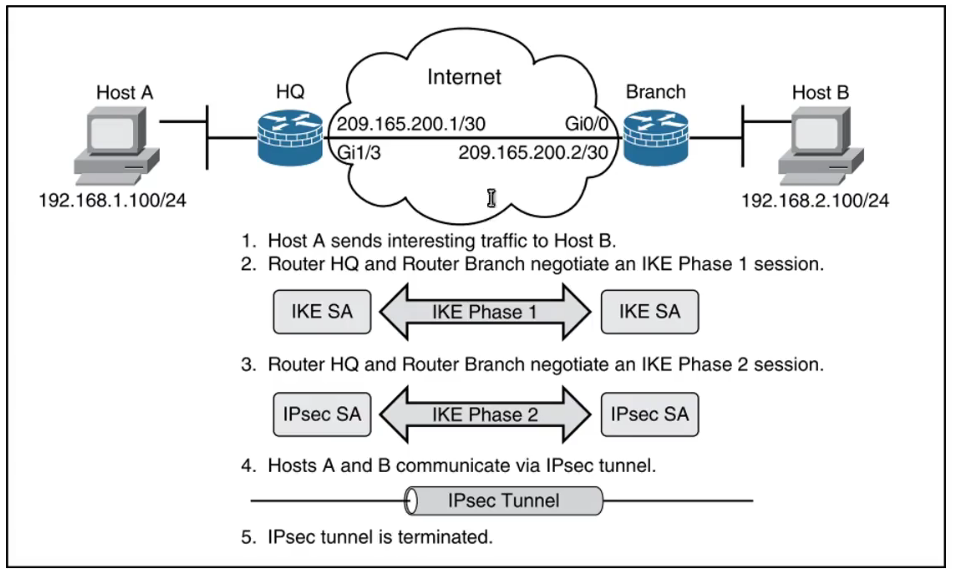
* 

* 

* IPsecSA协商：
* 快速模式：3个数据包（全部加密）发送IPsec安全提议，身份和数据验证，互相交换，然后验证。
* 

* 总结
* IKE SA和IPsec SA是两种不同的SA。
* IKE SA：认证算法，加密算法，认证方法（预共享密钥/证书），生命周期
* IPsec SA：安全协议(ESP/AH)，模式（传输/隧道），加密算法，生命周期
* 

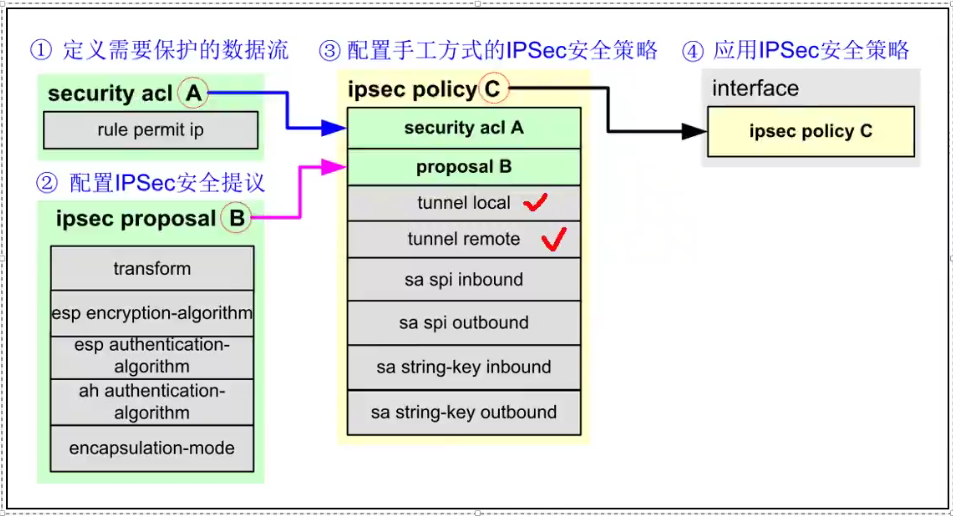
IPSecVPN配置：

* 
* IPsec流程图
* 配置好以下拓扑，从a发送到b的感兴趣流，会从出口hq和branch进行协商sa，协商有两个阶段，IKE SA和IPsec SA，交换安全策略信息后，建立SA，完成IPsec隧道。
* 

|  |  |
| --- | --- |
| 命令 | 备注 |
| Ipsec proposal x | 创建IPsec安全提议 x=提议名称 |
| Encapsulation tunnel/transport | 配置封装模式 隧道/传输 |
| Transform esp/ah/esp-ah | 配置隧道协议 esp/ah/esp-ah |
| Esp encryption-algorithm x | 配置esp协议使用加密算法 x=算法 |
| Esp/an authentication-algorithm x | 配置esp/ah协议使用认证算法 x=算法 |
| Dis ipsec proposal / name x | 查看IPsec安全提议状态配置 |
|  | IPsec安全提议 |
| Ipsec policy x id manual | 创建IPsec策略 x=策略名称 id=序列号 manual=手动 |
| Security acl x | 配置引用的acl |
| Proposal x | 配置引用的安全提议 |
| Tunnel local x | 配置隧道口源地址 |
| Tunnel remote x | 配置隧道口目的地址 |
| Sa spi inbound/outbound esp/ah x | 配置SA的spi 出入双方都需要对应 x=spi |
| Sa string-key inbound/outbound esp/ah cipher x | 配置SA的key 出入双方都需要对应 x=密钥 |
| Dis ipsec policy /name x | 查看ipsec策略状态配置 |
|  | IPsec手动安全策略 |
| Ike proposal x | 创建ike安全提议 x=序列号 |
| authentication-method pre-share/rsa-signature/digital-envelope | 配置认证方式 psk/证书/数字信封 |
| authentication-algorithm x | 配置认证算法 x=算法 |
| encryption-algorithm x | 配置加密算法 x算法 |
| Dh group x | 配置dh组  x=组 |
| Sa duration x | 配置sa超时时间 |
| Dis ike proposal  /number x | 查看ike安全提议信息 x=序列号 |
|  | IKE安全提议 |
| Ike peer x v1/v2 | 创建ike对等体  版本v1/v2 |
| Exchange-mode main/aggressive | 配置对等体模式 模式/主模式/野蛮 |
| Pre-shared-key cipher x | 配置psk密钥 |
| Ike proposal x | 配置引用ike安全提议 |
| local-address x | 配置对等体 源地址 |
| Remote-address x | 配置对等体 目的地址 |
|  | IKE对等体 |
| IPSec policy x id isakmp | 创建IPSec策略 isakmp=自动 |
| Proposal x | 配置引用IPSec安全提议 |
| Ike-peer x | 配置引用ike对等体 |
| Security x | 配置引用acl |
|  | ike协商安全策略 |
| Dis ipsec statistics esp/an | 查看接口流量统计 |
| Dis ike/ipsec sa /brief/duration | 查看sa安全联盟 b=简明信息 dur=生存时间 |
|  | 查看IPSec/ike sa |

* 手动设置sa没有时间限制。
* sa两端之间生存时间不一致，按照小的计算。
* 需要走IPsecVPN隧道的流量需要在NAT中做排除，没有排除等同流量往公网走，那么就出问题了。

IPsec协商配置流程图：

* 
* 