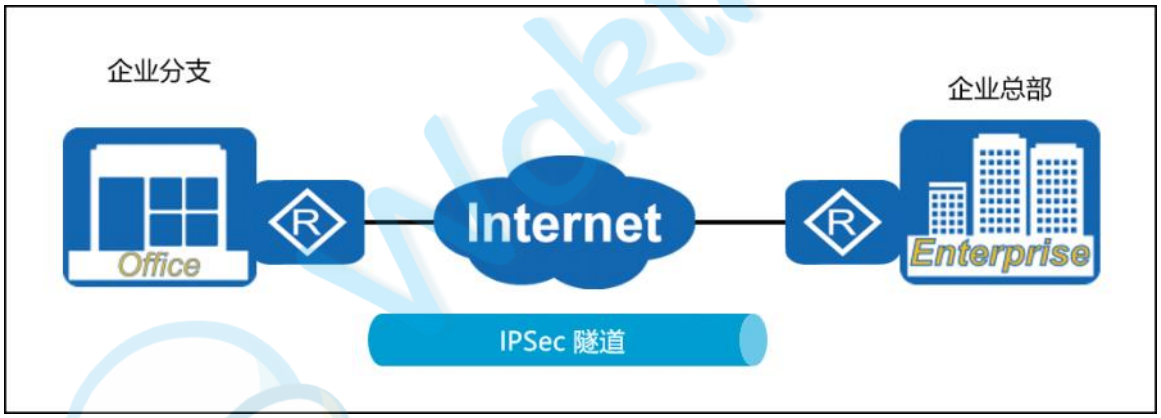
IPSec VPN

前言

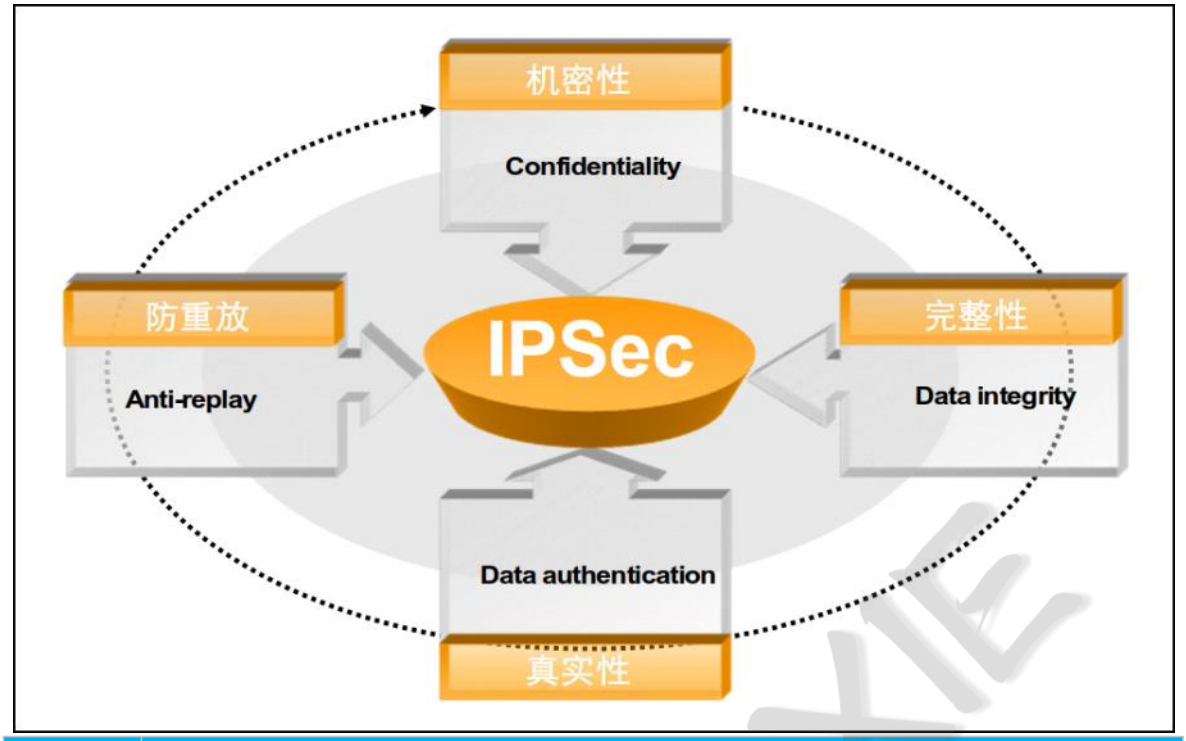
企业对网络安全性的需求日益提升，而传统的TCP/IP协议缺乏有效的安全认证和保密机制。IPSec（Internet Protocol Security）作为一种开放标准的安全框架结构，可以用来保证IP数据报文在网络上传输的机密性、完整性和防重放。

IPSec： Internet Protocol Security

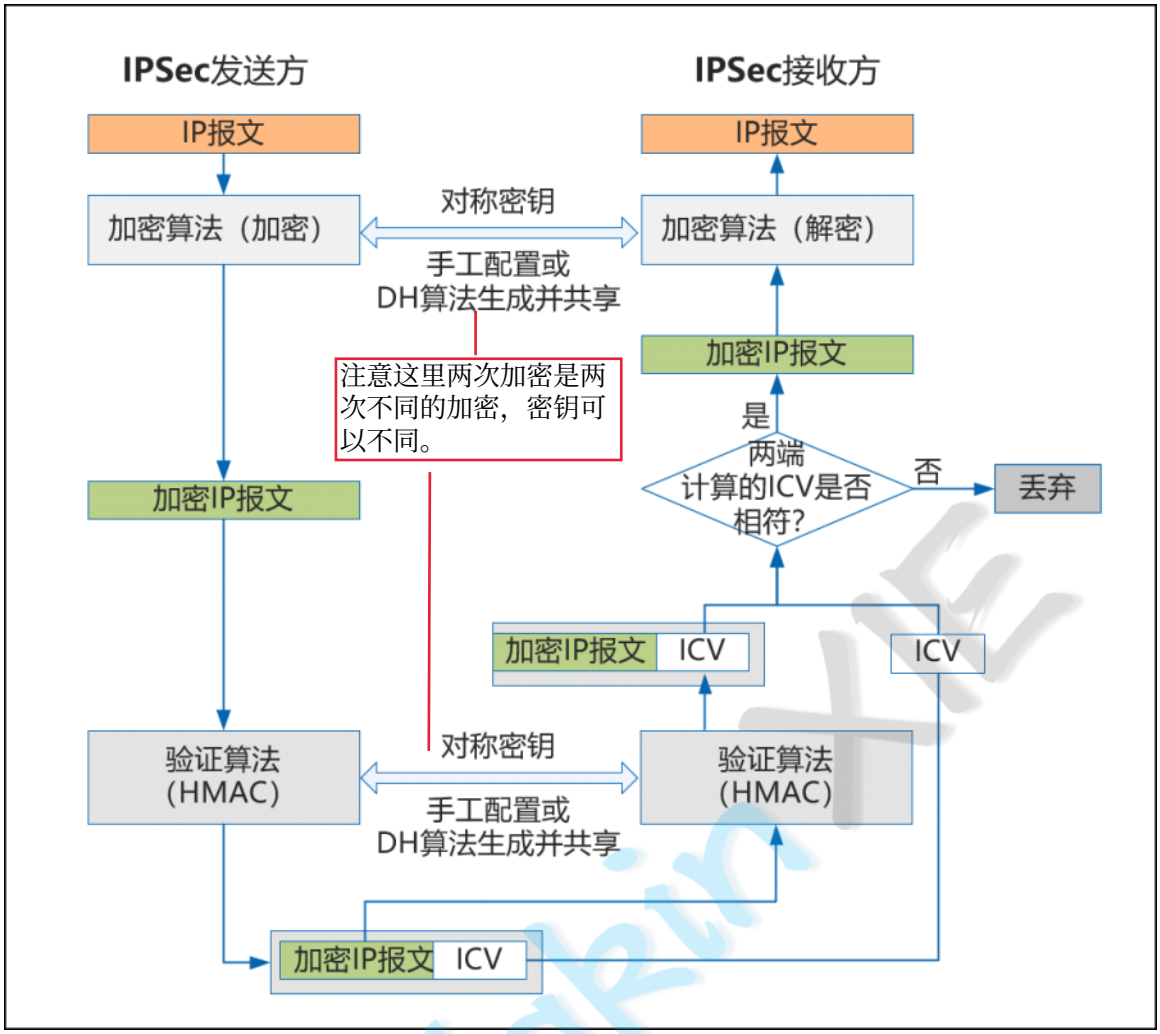
- 源于IPv6
- IETF制定的一套安全保密性能框架
- 建立在网络层的安全保障机制
- 引入多种加密算法、验证算法和密钥管理机制
- 也具有配置复杂、消耗运算资源较多、增加延迟、不支持组播等缺点
- IPSec VPN是利用IPSec隧道建立的VPN技术



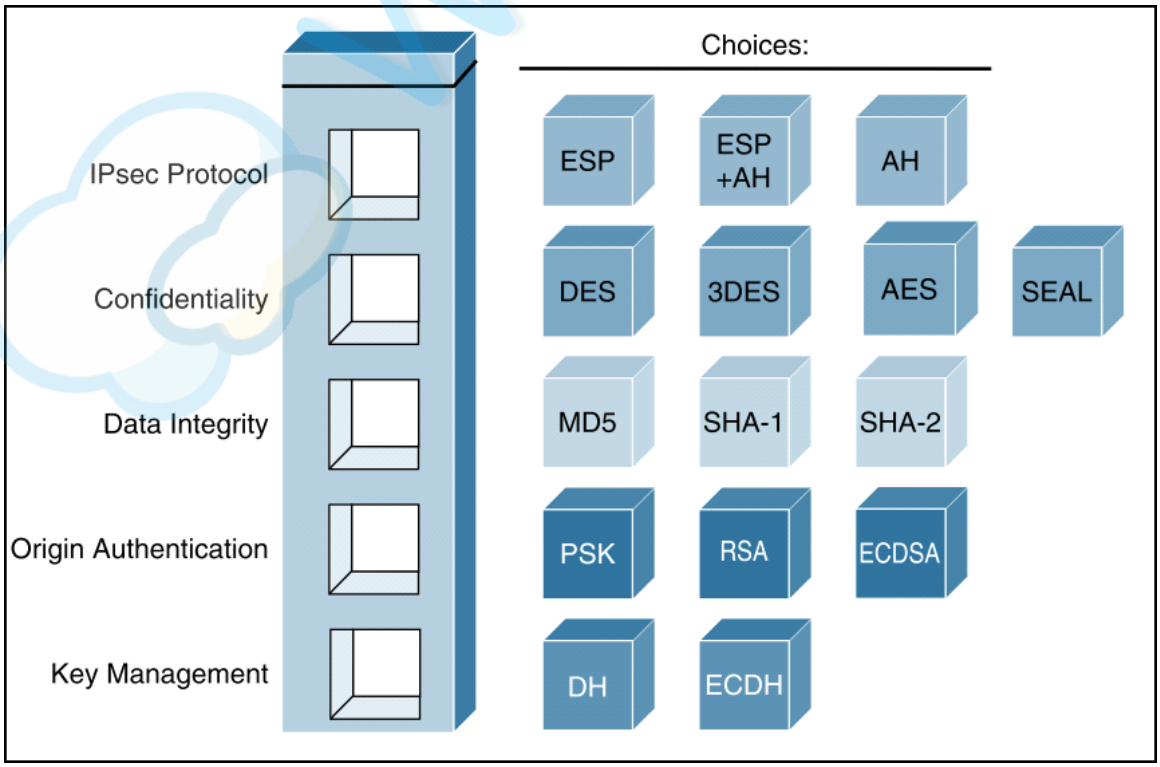
IPSec核心功能：



术语	备注
机密性	对数据进行加密，确保数据在传输过程中不被其它人员查看；
完整性	对接收到数据包进行完整性验证，以确保数据在传输过程中没有被篡改；
真实性	验证数据源，以保证数据来自真实的发送者（IP报文头内的源地址）；
抗重放	防止恶意用户通过重复发送捕获到的数据包所进行的攻击，即接收方会拒绝旧的或重复的数据包。



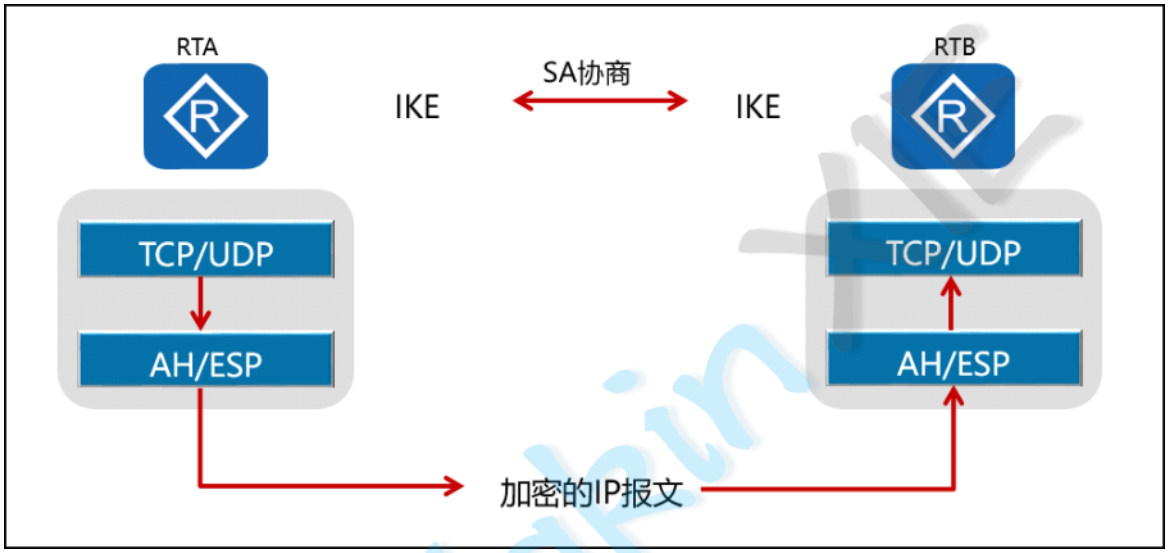
IPSec技术框架：



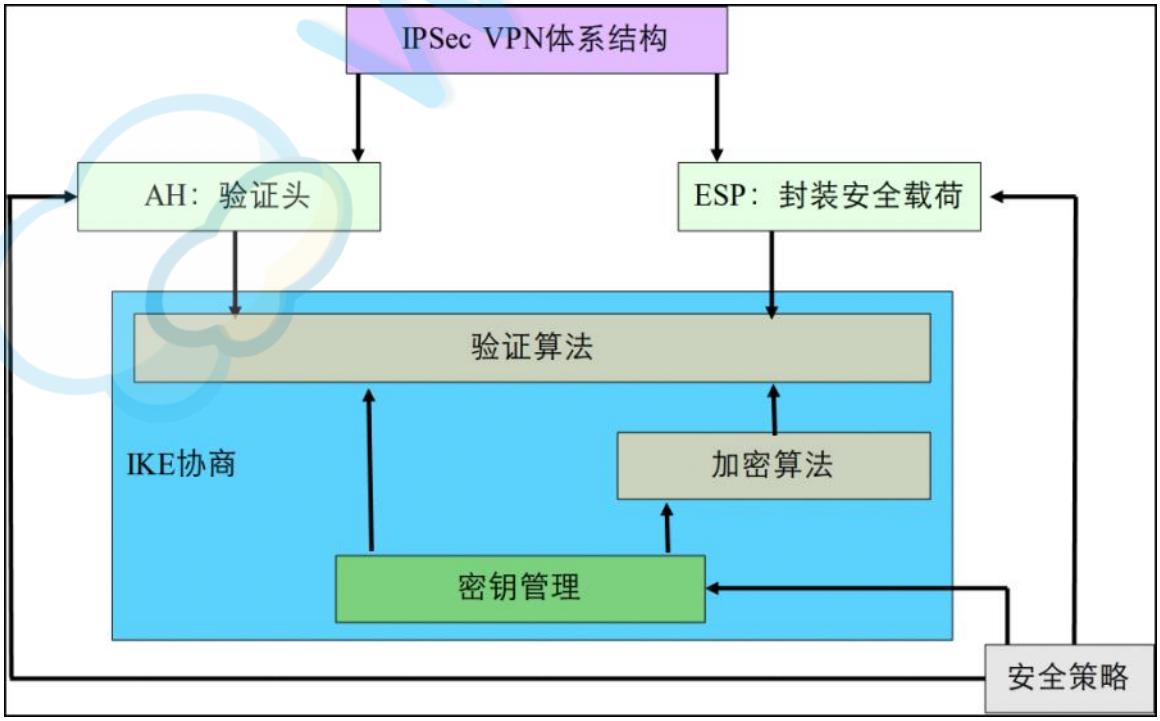
-

安全协议	ESP				AH			
加密	DES	3DES	AES	SM1/SM4				
验证	MD5	SHA1	SHA2	SM3	MD5	SHA1	SHA2	SM3
密钥交换	IKE（ISAKMP，DH）							

- 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SHA-1验证算法存在安全隐患，建议优先使用SHA-2或SM3算法。



- 通过AH和ESP这两个安全协议来实现IP数据报文的安全传送。
- IKE协议提供密钥协商，建立和维护安全联盟SA等服务。

- 

IPSec安全协议：

AH

- AH（Authentication Header）报文头验证协议，主要提供完整性、真实性、防重放功能；然而，AH并不加密数据报文（机密性）。IP协议号=51。

ESP

- ESP（Encapsulating Security Payload）封装安全载荷协议。除提供AH协议的所有功能外（但其完整性校验不包括IP头），还可提供对数据报文的加密功能。IP协议号=50。

安全特性	AH	ESP
协议号	51	50
数据完整性校验	支持	支持
数据源验证	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：

传输模式

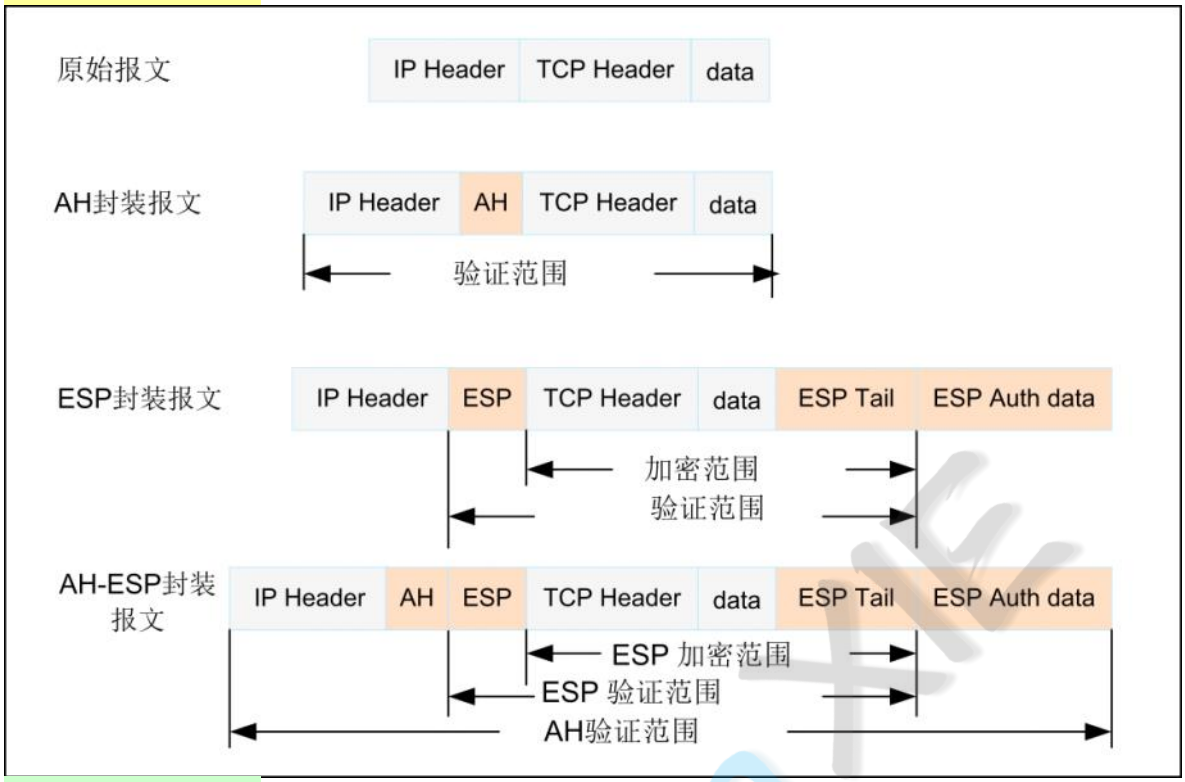
- 在传输模式（Transport Mode）下，IPSec头被插入到IP头之后但在所有传输层协议之前，或所有其他IPSec协议之前。

隧道模式

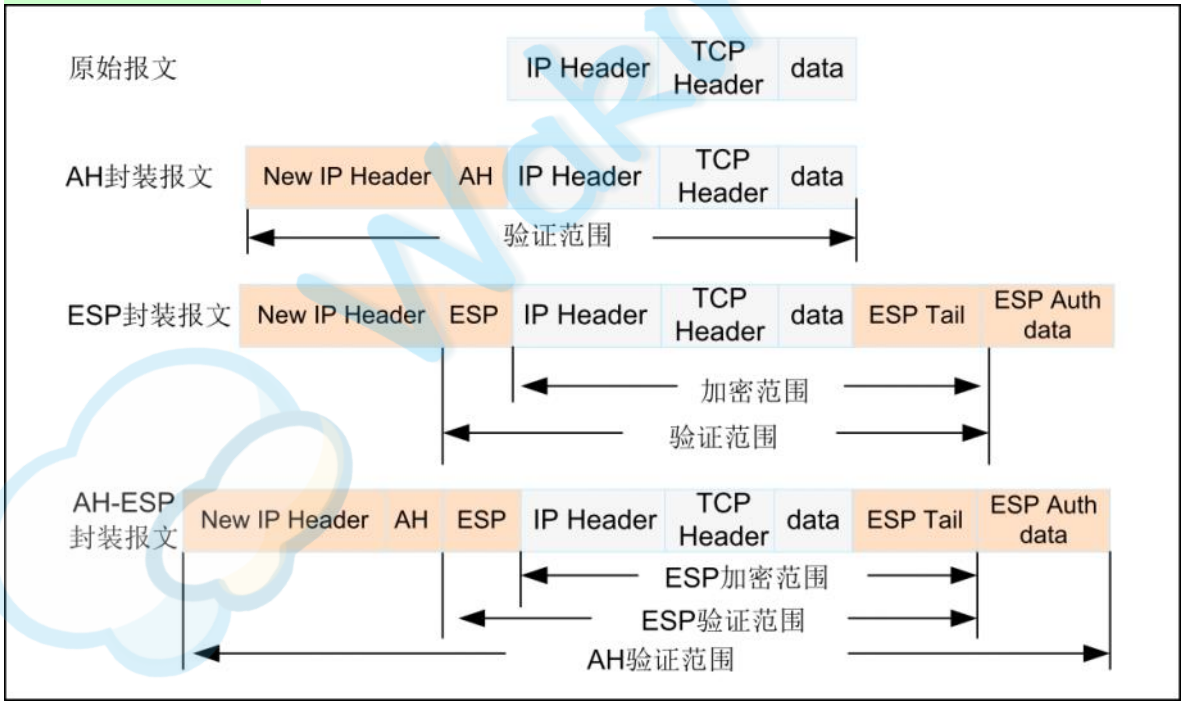
- 在隧道模式（Tunnel Mode）下，IPSec头插在原始IP头之前，另外生成一个新的报文头放到AH或ESP之前。

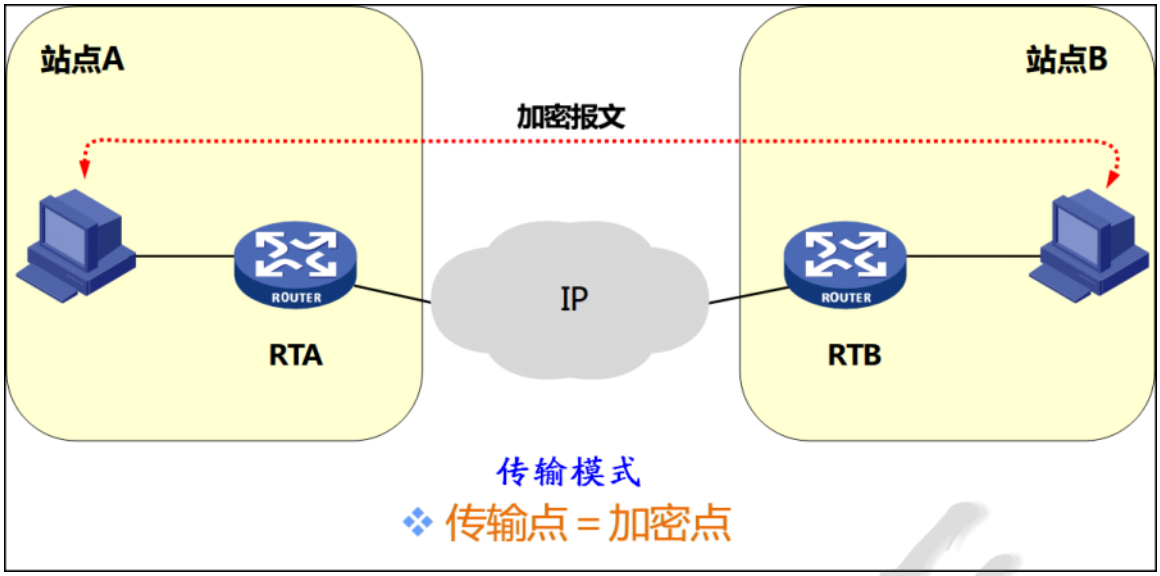
- 封装模式对比：
  - 安全性：
    - 隧道模式隐藏原IP头信息，安全性更好。
  - 性能：
    - 隧道模式有一个额外的IP头，隧道模式比传输模式占用更多带宽。

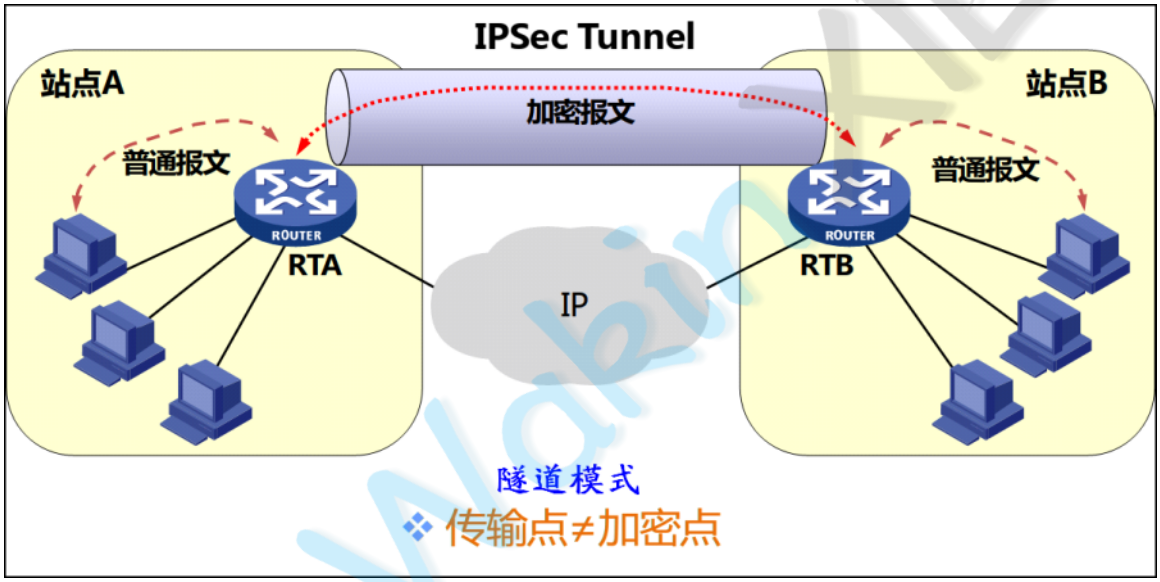
- **传输模式封装结构**:



- **隧道模式封装结构**:



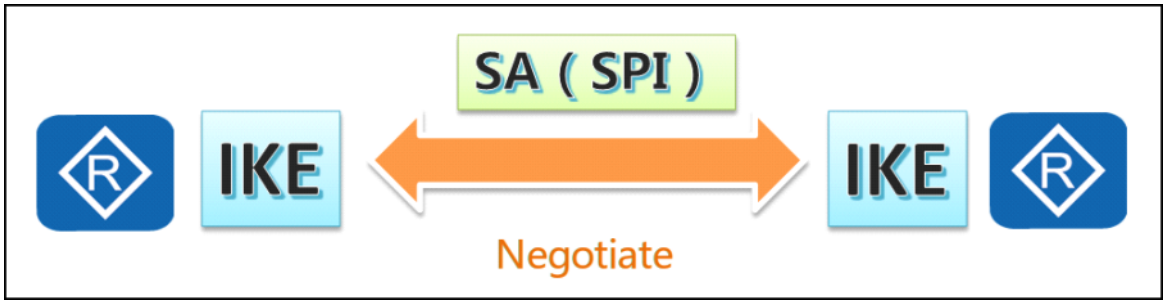
- 

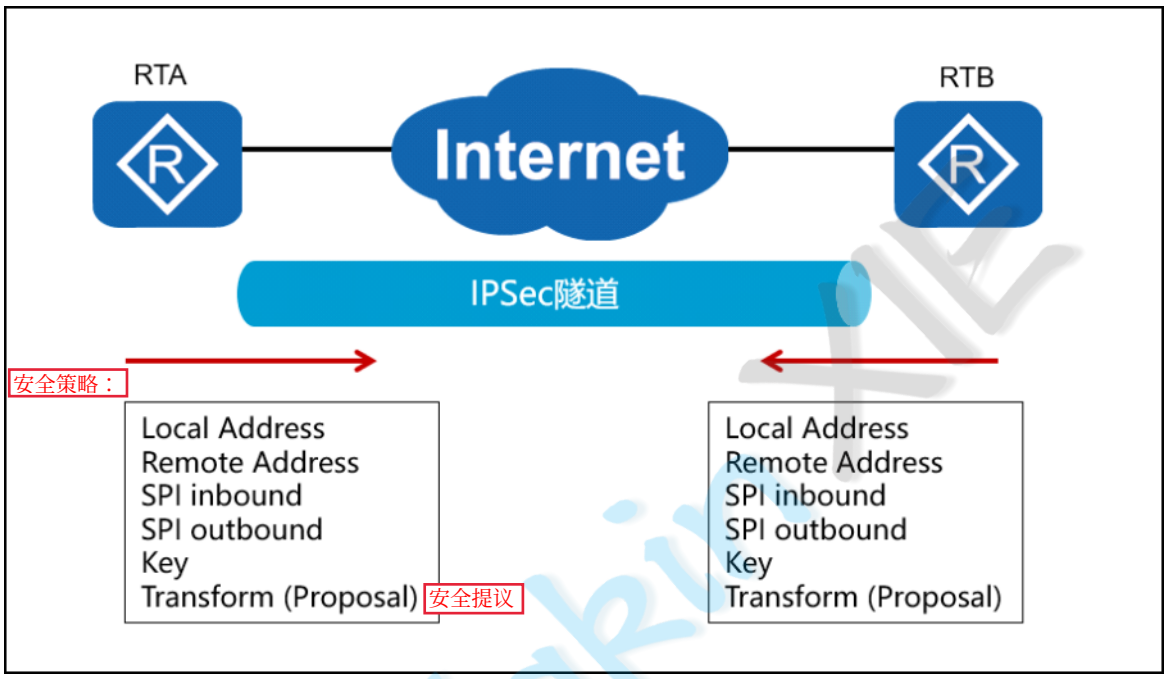
- 

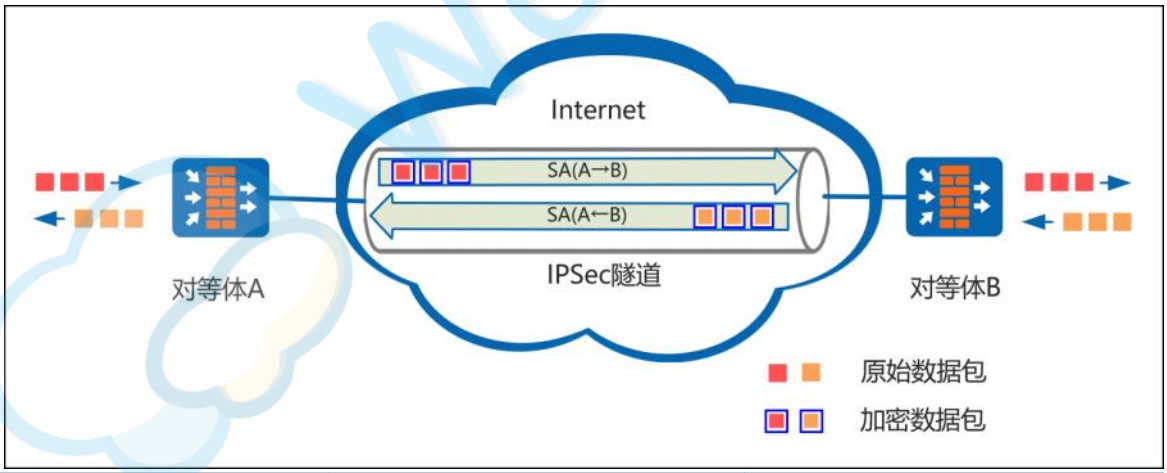
安全联盟：SA（Security Association）

- 顾名思义，通信双方结成盟友，相互信任亲密无间，即达成约定
- 由一个（SPI，IP目的地址，安全协议号）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
- 可以手工建立或通过IKE协商生成
- SPD（Security Policy Database）
- SAD（Security Association Database）

术语	备注
Negotiate	协商，两个节点要开始安全发送数据之前，必须完成的事情。
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。

- 

- 

- 

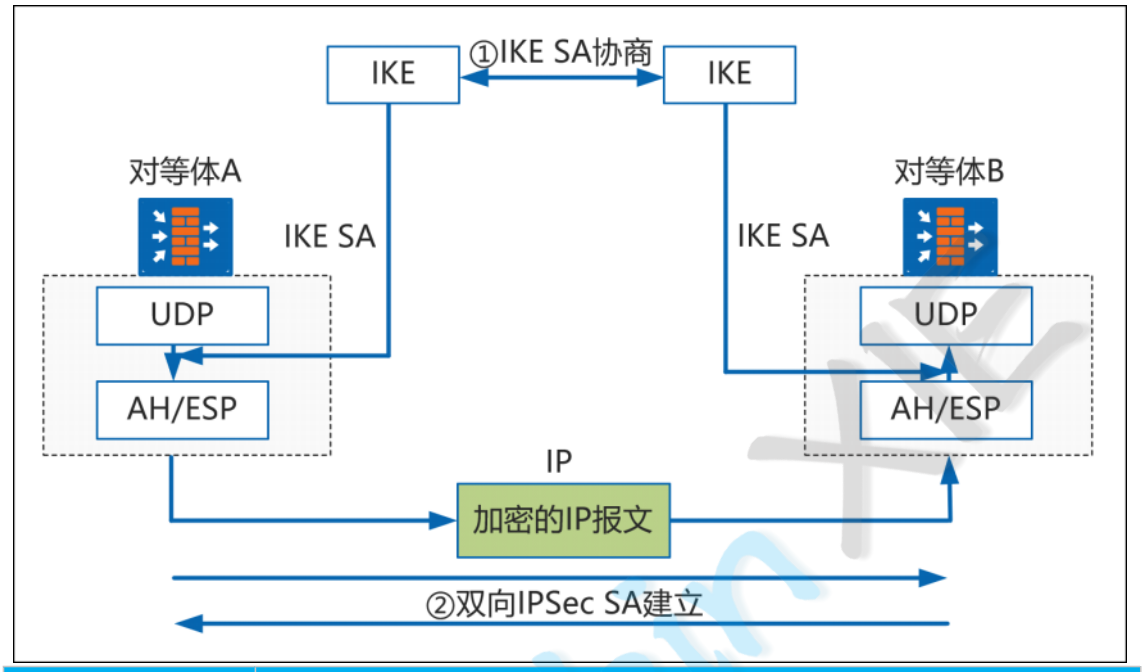
对比项	手工建立	IKE协商
密钥生成	手工配置	DH算法
密钥刷新	手动刷新	动态刷新
生存周期	永久	可配置
适用环境	设备数量少，小型网络	中大型网络

IKE： Internet Key Exchange，因特网密钥交换

- 建立在ISAKMP（Internet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地分发密钥，验证身份
- 定时更新SA和密钥，实现完善的前向安全性

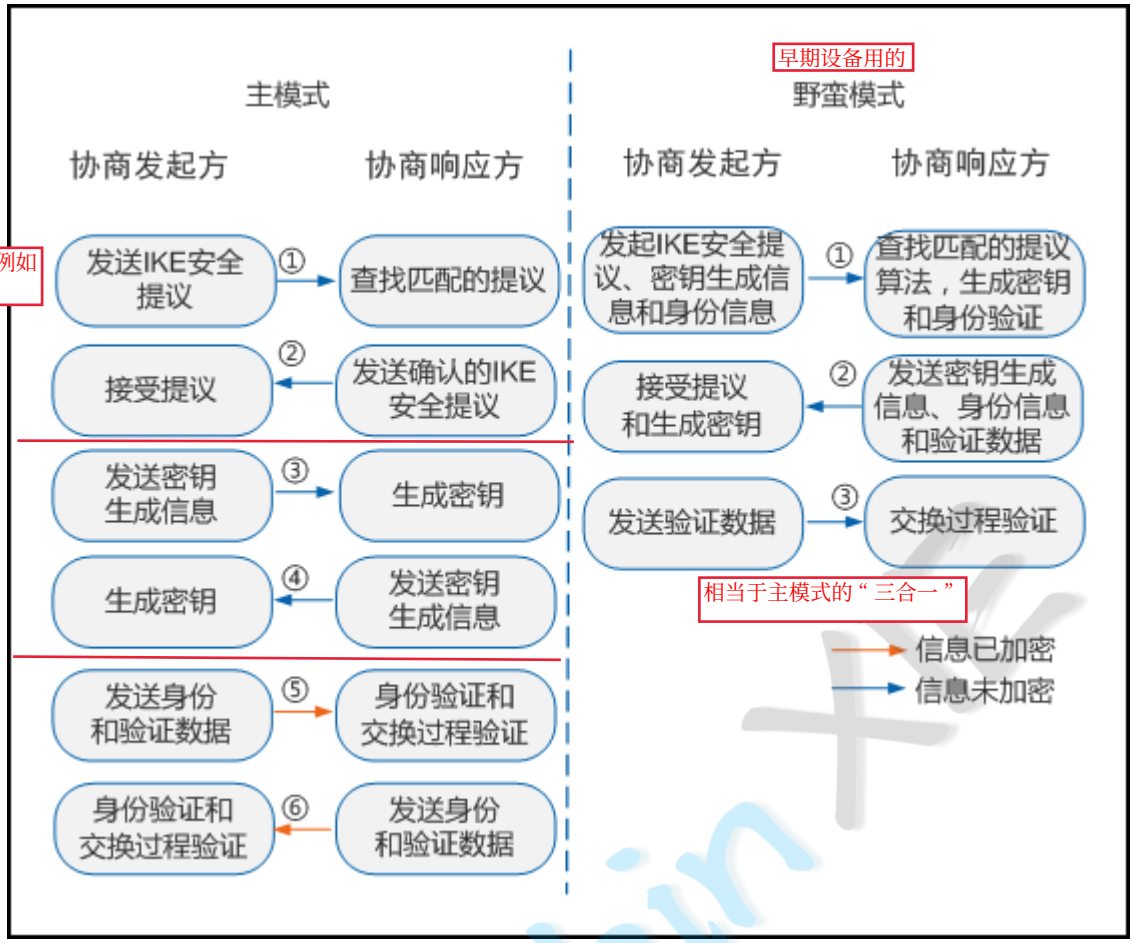
Perfect Forward Security，当私钥被泄漏后，必然会导致之前的数据被破解，但可以保证未来的数据安全（本质是会额外做一次密钥交换）经典的例子就是 445 的心脏滴血漏洞，会泄漏私钥，由于没有向前保密的特性，导致危害很大

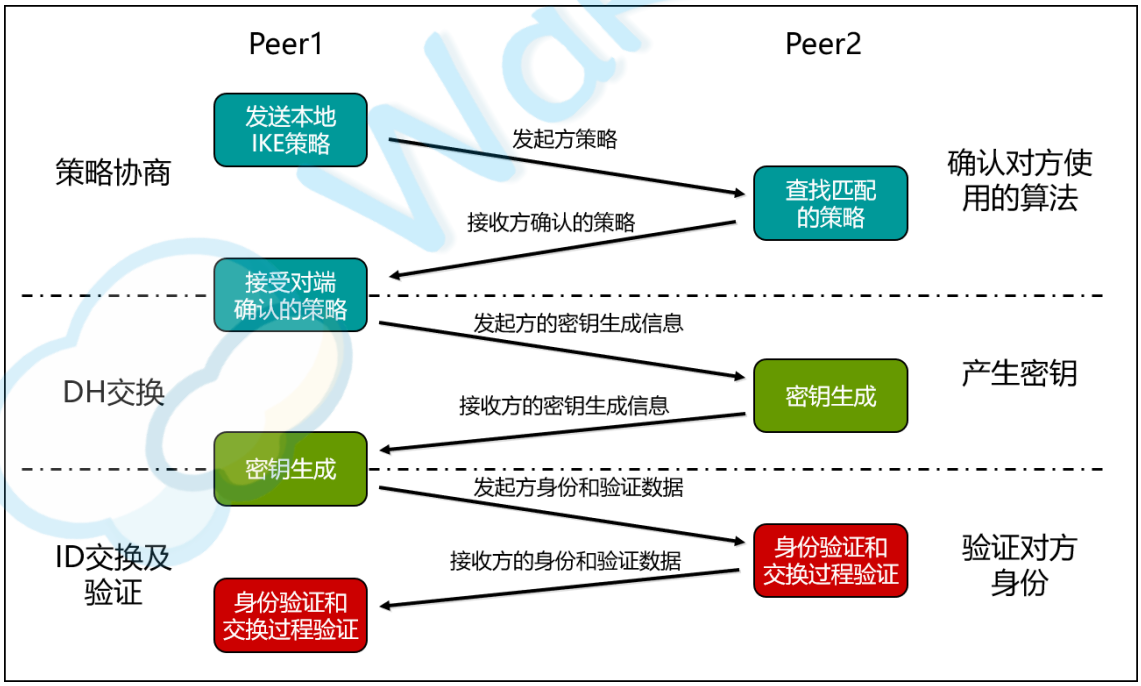
- 允许IPSec提供抗重播服务
- 简化IPSec的使用和管理，大大简化了IPSec的配置和维护工作
- 

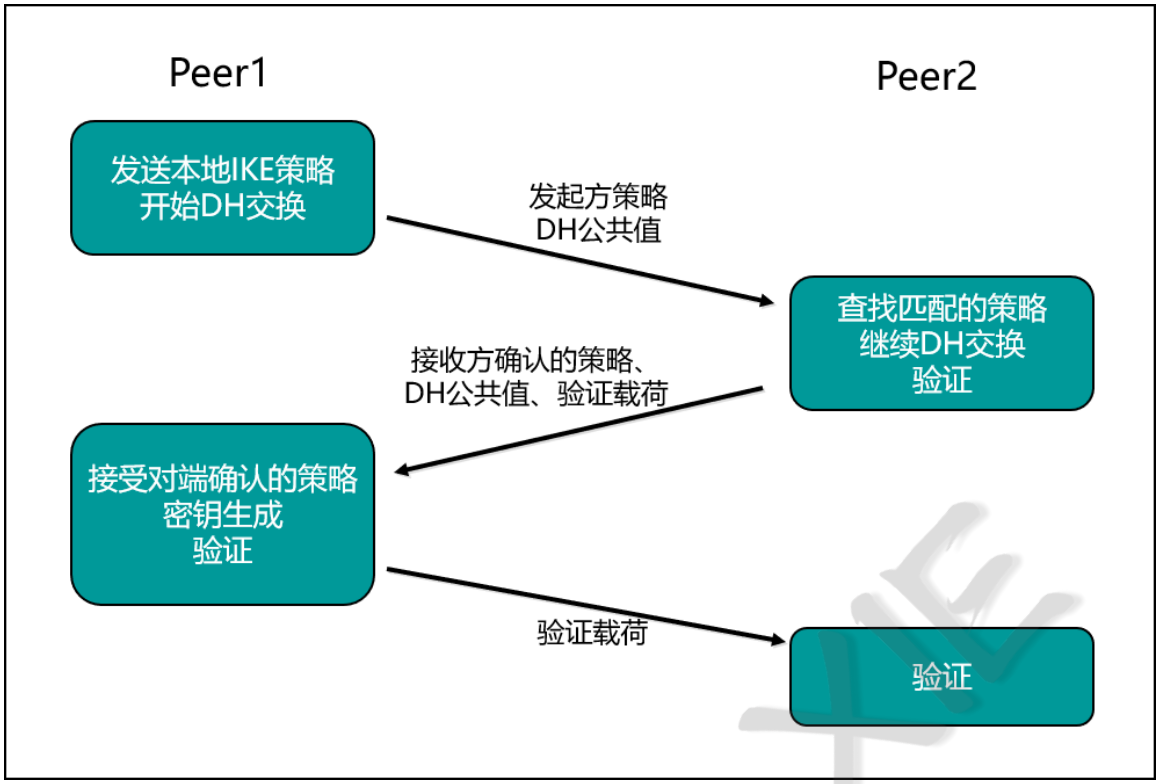
阶段	备注
阶段1 **Phase 1**	在网络上建立一个 IKE SA，为阶段2协商提供保护 分主模式（Main Mode）和野蛮模式（Aggressive Mode）
阶段2 **Phase 2**	在阶段1建立的IKE SA的保护下完成 IPSec SA 的协商 快速模式（Quick Mode）

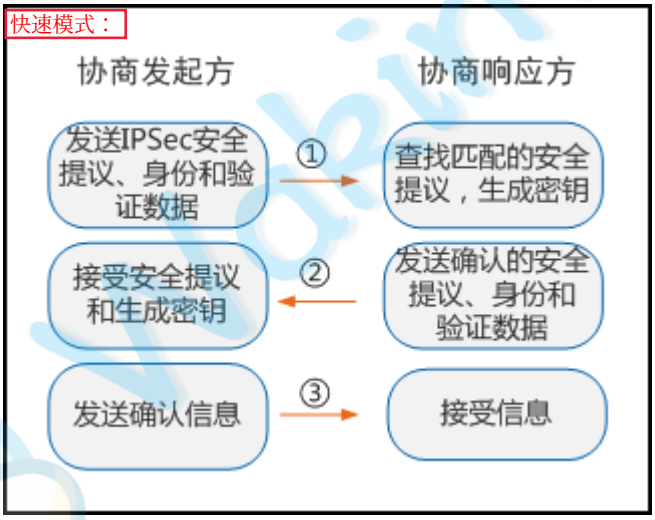
- 对等体之间建立一个IKE SA完成身份验证和密钥信息交换后，在IKE SA的保护下，根据配置的AH/ESP安全协议等参数协商出一对IPSec SA。

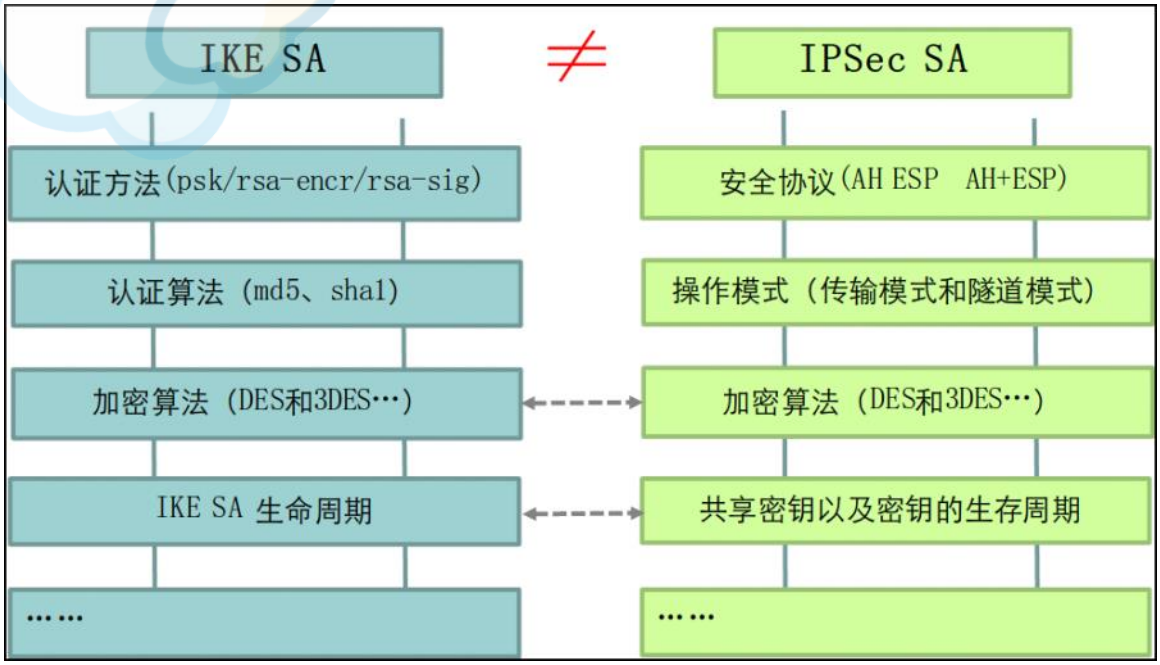
提议包含一些参数，例如加密的方式等。

- 

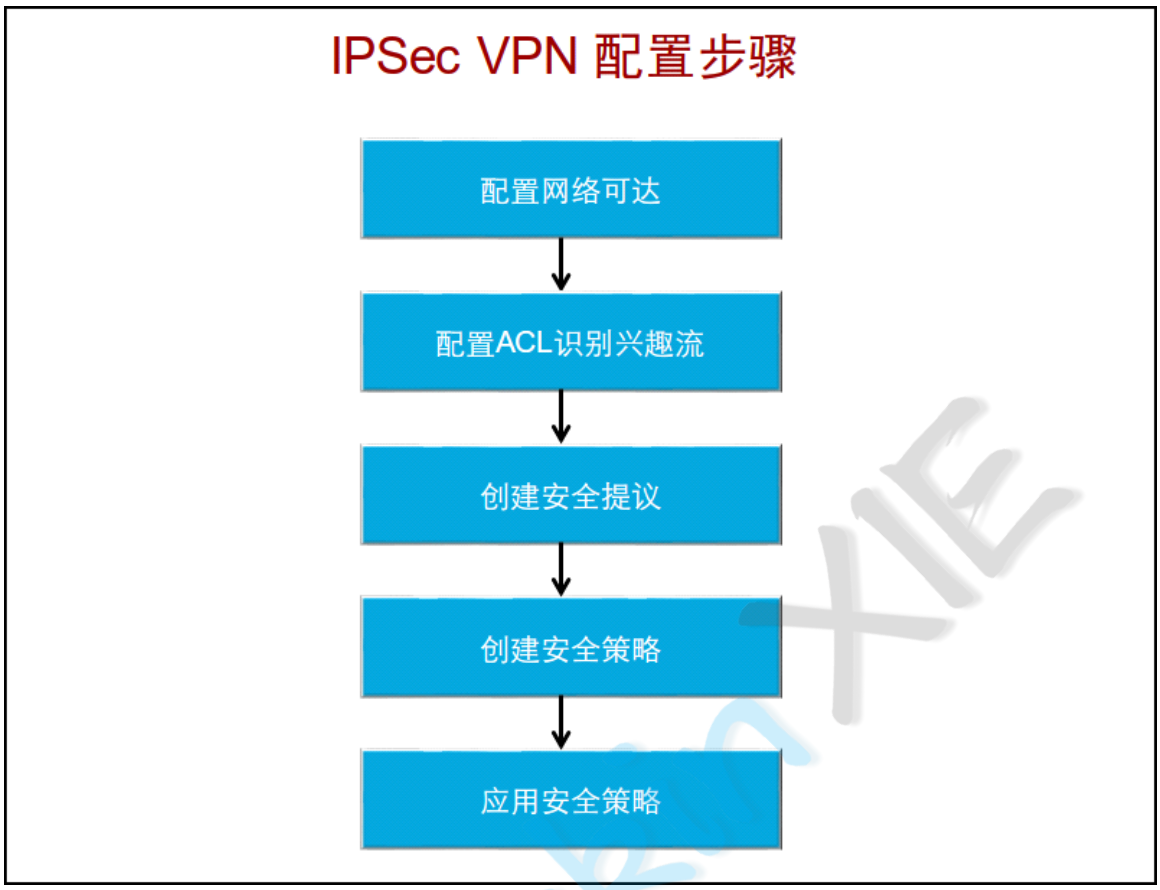
- 

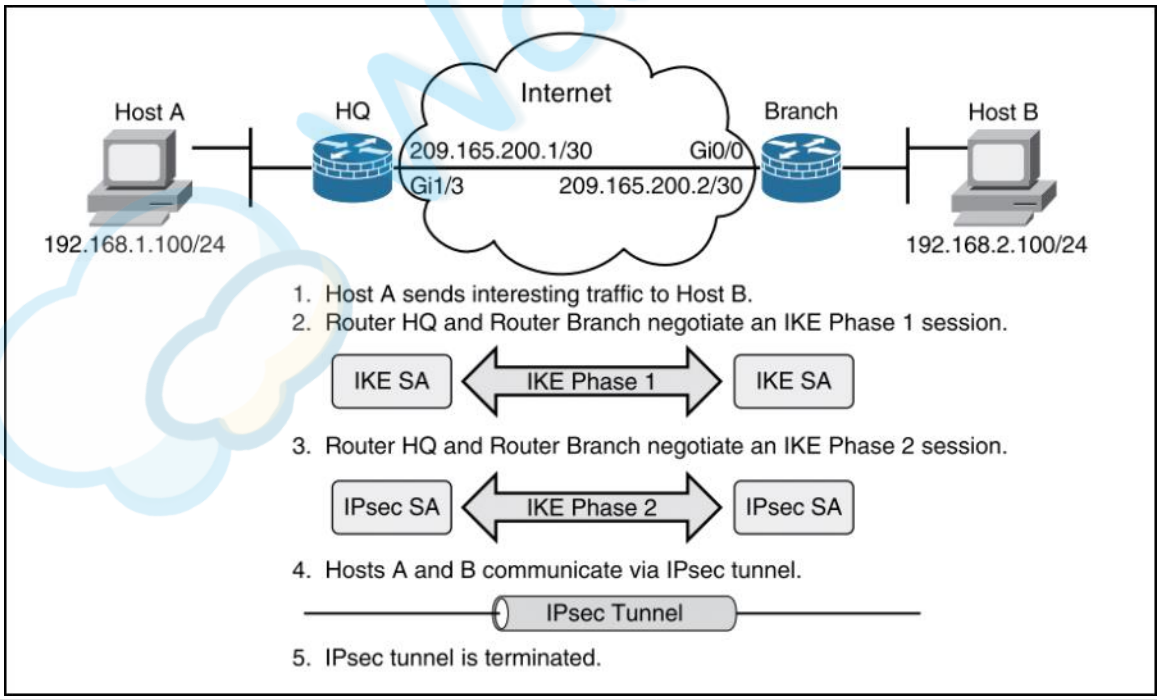
- 

- 

- 

IPSec VPN配置：

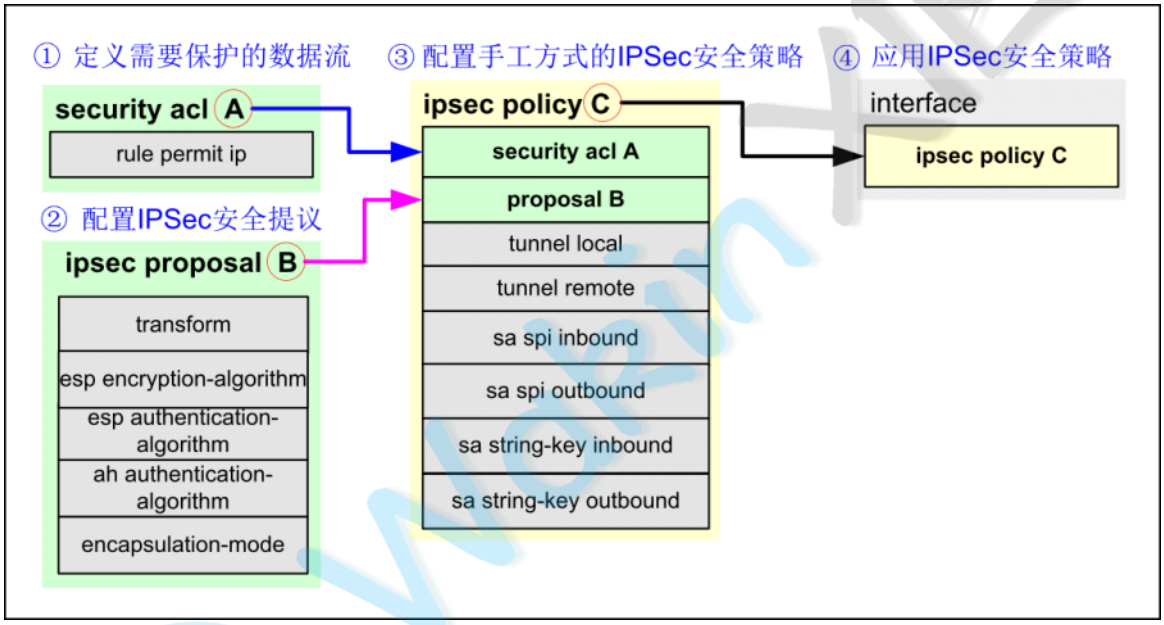
- 

- 

命令	备注
ipsec proposal shanghai	创建并配置IPSec提议。
encapsulation-mode tunnel	配置报文的封装模式。
transform esp	配置隧道采用的安全协议。

esp authentication-algorithm sha2-256	配置ESP协议使用的认证算法。
esp encryption-algorithm aes-128	配置ESP加密算法。
display ipsec proposal	验证IPSec提议配置。
↑↑↑↑↑↑↑↑↑↑↑↑↑↑↑↑↑↑↑↑↑↑↑↑↑↑↑↑↑↑↑↑↑↑	**老司机分界线，IPSec安全提议。**
ipsec policy P1 10 manual	创建并配置IPSec策略（手动）。
security acl 3000	配置引用的ACL。
proposal shanghai	配置引用的提议。
tunnel local 12.0.0.2	配置安全隧道的本端地址。
tunnel remote 13.0.0.3	配置安全隧道的对端地址。
sa spi inbound/outbound esp 12345	配置SA的SPI。 入方向和出方向都必须设置，并且双方的必须相互对应。
sa string-key inbound/outbound esp cipher wakin	配置SA的认证密钥。 入方向和出方向都必须设置，并且双方的必须相互对应。
display ipsec policy	验证IPSec手动策略配置。
↑↑↑↑↑↑↑↑↑↑↑↑↑↑↑↑↑↑↑↑↑↑↑↑↑↑↑↑↑↑↑↑↑↑	**老司机分界线，手动安全策略。**
ike proposal 10	创建并配置IKE提议。
authentication-method pre-share	配置身份认证方式。
authentication-algorithm sha2-256	配置数据认证算法。
encryption-algorithm aes-cbc-256	配置加密算法。
dh group14	配置密钥交换算法。
display ike proposal	验证IKE提议。
↑↑↑↑↑↑↑↑↑↑↑↑↑↑↑↑↑↑↑↑↑↑↑↑↑↑↑↑↑↑↑↑↑↑	**老司机分界线，IKE安全提议。**
ike peer shanghai v1	创建并配置IKE对等体。
exchange-mode main/aggressive	配置模式。
pre-shared-key cipher huawei	配置PSK。
ike-proposal 10	配置引用的IKE提议。
local-address 12.0.0.1	配置本地IP地址。
remote-address 23.0.0.3	配置对端IP地址。
↑↑↑↑↑↑↑↑↑↑↑↑↑↑↑↑↑↑↑↑↑↑↑↑↑↑↑↑↑↑↑↑↑↑	**老司机分界线，IKE对等体。**

ipsec policy P2 10 isakmp	创建并配置IPSec策略（自动）。
security acl 3000	配置引用的ACL。
proposal shanghai	配置引用的IPSec提议。
ike-peer shanghai	配置引用的IKE对等体。
↑↑↑↑↑↑↑↑↑↑↑↑↑↑↑↑↑↑↑↑↑↑↑↑↑↑↑↑↑↑↑↑↑↑↑↑↑↑	**老司机分界线，自动安全策略。**
ipsec policy P1/P2 配在公网接口上	在接口上应用指定的安全策略组。
display ike/ipsec sa	验证安全联盟。
↑↑↑↑↑↑↑↑↑↑↑↑↑↑↑↑↑↑↑↑↑↑↑↑↑↑↑↑↑↑↑↑↑↑↑↑↑↑	**老司机分界线，调用安全策略。**

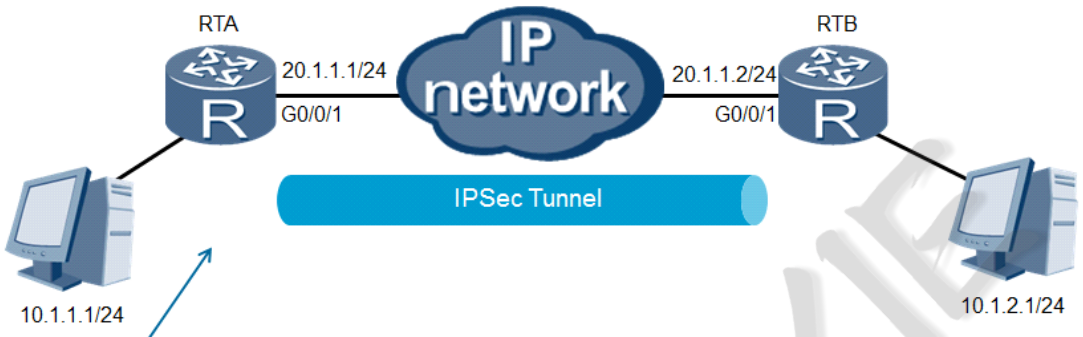
- 

配置项	天地会总舵	天地会分舵
ACL	acl number 3000 注意这里配的是私网地址 rule 5 permit ip source 192.168.0.0 0.0.0.255 destination 172.16.0.0 0.0.0.255	acl number 3000 rule 5 permit ip source 172.16.0.0 0.0.0.255 destination 192.168.0.0 0.0.0.255
IPSec 安全提议	ipsec proposal pro1 transform esp encapsulation-mode tunnel esp authentication-algorithm sha1 esp encryption-algorithm aes	ipsec proposal pro1 transform esp encapsulation-mode tunnel esp authentication-algorithm sha1 esp encryption-algorithm aes
IPSec 安全策略	ipsec policy policy1 1 manual security acl 3000 proposal pro1 tunnel local 1.1.1.1 tunnel remote 2.2.2.2 隧道两端配公网地址，即添加新的公网 IP 头 sa spi inbound esp 54321 sa spi outbound esp 12345 sa string-key inbound esp huawei@123 sa string-key outbound esp huawei@456	ipsec policy policy1 1 manual security acl 3000 proposal pro1 tunnel local 2.2.2.2 tunnel remote 1.1.1.1 sa spi inbound esp 12345 sa spi outbound esp 54321 sa string-key inbound esp huawei@456 sa string-key outbound esp huawei@123
应用 IPSec 安全策略	interface GigabitEthernet0/0/1 ip address 1.1.1.1 255.255.255.0	interface GigabitEthernet0/0/0 ip address 2.2.2.2 255.255.255.0

	sa string-key outbound esp huawei@456	sa string-key outbound esp huawei@123
应用 IPSec 安全策略	**interface GigabitEthernet0/0/1** ip address 1.1.1.1 255.255.255.0 ipsec policy policy1	**interface GigabitEthernet0/0/0** ip address 2.2.2.2 255.255.255.0 ipsec policy policy1

需要注意的是，配置了 NAT，而且 ACL 配置的是内网 IP 之后，进入隧道之前，源地址就会从私网地址经过 NAT 转换成公网地址，此时就不会走隧道（不和 ACL 匹配），因此要在 NAT 的 ACL 中将要走 VPN 的流量排除。
rule den ip so 源内网地址 子网掩码 des 目标地址 子网掩码
然后其他的流量都做转换：
rule per ip

IPSec VPN 配置




```
[RTA]ip route-static 10.1.2.0 24 20.1.1.2
[RTA]acl number 3001
[RTA-acl-adv-3001]rule 5 permit ip source 10.1.1.0
0.0.0.255 destination 10.1.2.0 0.0.0.255
[RTA]ipsec proposal shanghai
```

配置验证

```
[RTA]display ipsec proposal
 Number of proposals: 1
 IPSec proposal name: shanghai
 Encapsulation mode: Tunnel
 Transform          : esp-new
 ESP protocol       : Authentication MD5-HMAC-96
                      Encryption     DES
```

- IPSec VPN对等体配置的安全提议参数必须一致。

IPSec VPN 配置

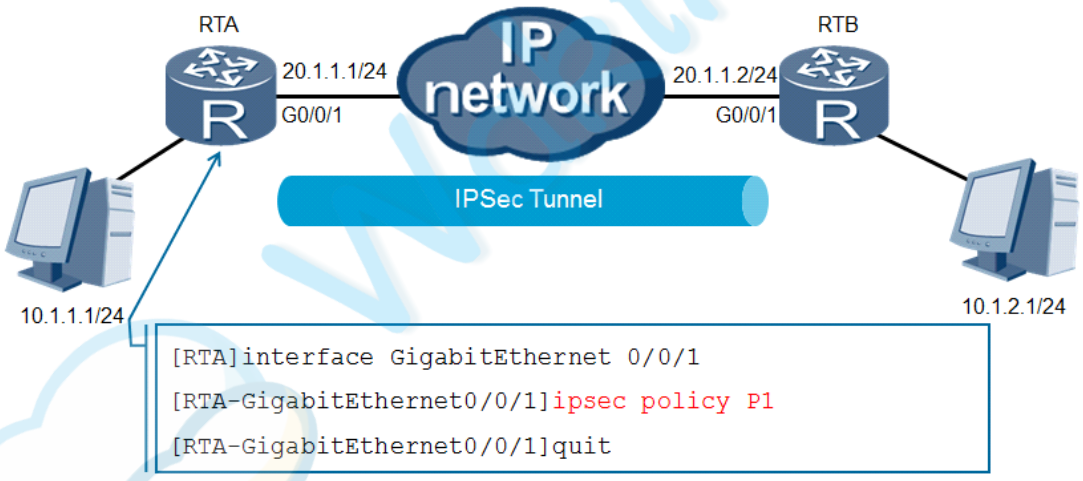
```
[RTA]ipsec  policy P1 10 manual
[RTA-ipsec-policy-manual-P1-10]security acl 3001
[RTA-ipsec-policy-manual-P1-10]proposal tran1
[RTA-ipsec-policy-manual-P1-10]tunnel remote 20.1.1.2
```

IPSec VPN 配置

```
[RTA]ipsec  policy P1 10 manual
[RTA-ipsec-policy-manual-P1-10]security acl 3001
[RTA-ipsec-policy-manual-P1-10]proposal tran1
[RTA-ipsec-policy-manual-P1-10]tunnel remote 20.1.1.2
[RTA-ipsec-policy-manual-P1-10]tunnel local 20.1.1.1
[RTA-ipsec-policy-manual-P1-10]sa spi outbound esp 54321
[RTA-ipsec-policy-manual-P1-10]sa spi inbound esp 12345
[RTA-ipsec-policy-manual-P1-10]sa string-key outbound esp simple huawei
[RTA-ipsec-policy-manual-P1-10]sa string-key inbound esp simple huawei
```

- 安全策略将要保护的数据流和安全提议进行绑定。

IPSec VPN配置




```
[RTA]interface GigabitEthernet 0/0/1
[RTA-GigabitEthernet0/0/1]ipsec policy P1
[RTA-GigabitEthernet0/0/1]quit
```

配置验证

```
[RTA]display ipsec policy
==============================================
IPSec policy group: "P1"
Using interface: GigabitEthernet 0/0/1
==============================================
    Sequence number: 10
    Security data flow: 3001
    Tunnel local  address: 20.1.1.1
    Tunnel remote address: 20.1.1.2
    Qos pre-classify: Disable
    Proposal name:shanghai
...
```

```
……
Inbound ESP setting:
      ESP SPI: 12345 (0x3039)
      ESP string-key: huawei
      ESP encryption hex key:
      ESP authentication hex key:
   Outbound ESP setting:
      ESP SPI: 54321 (0xd431)
      ESP string-key: huawei
      ESP encryption hex key:
      ESP authentication hex key:
……
```