IPsec VPN 原理与配置

Internet Protocol Security　Virtual Private Network ： IP 安全协议 虚拟专用网络

通讯点: 1.1.1.0/24 与 2.2.2.0/24

加密点: 202.100.1.1 与 61.128.1.1

注意：加密点不等于通讯点为Tunnel Mode

通讯点: 137.78.5.5 与 137.78.10.100

加密点: 137.78.5.5 与 137.78.10.100

注意：加密点等于通讯点为Transport Mode

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 VPN应用场景

- 企业分支可以通过IPSec VPN接入到企业总部网络。

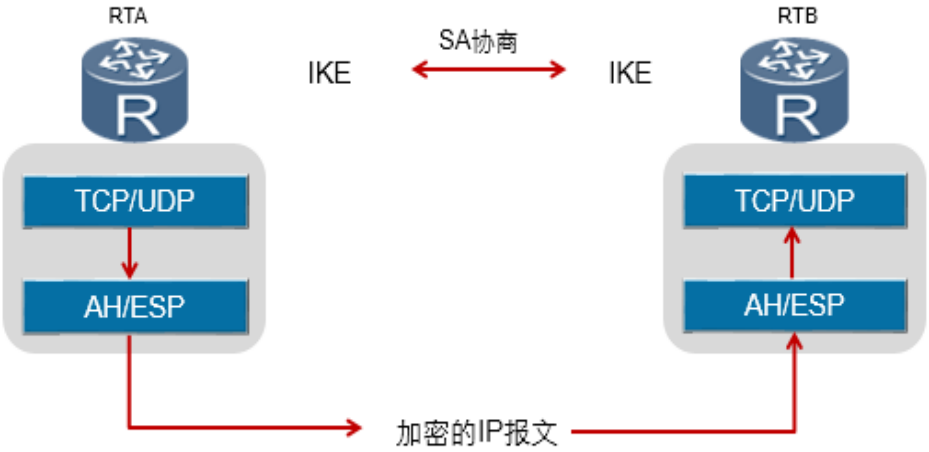
IPSec 是 IETF 定义的一个协议组。通信双方在 IP 层通过加密、完整性校验、数据源认证等方式，保证了 IP 数据报文在网络上传输的机密性、完整性和防重放。

- 机密性（Confidentiality）指对数据进行加密保护，用密文的形式传送数据。
- 完整性（Data integrity）指对接收的数据进行认证，以判定报文是否被篡改。

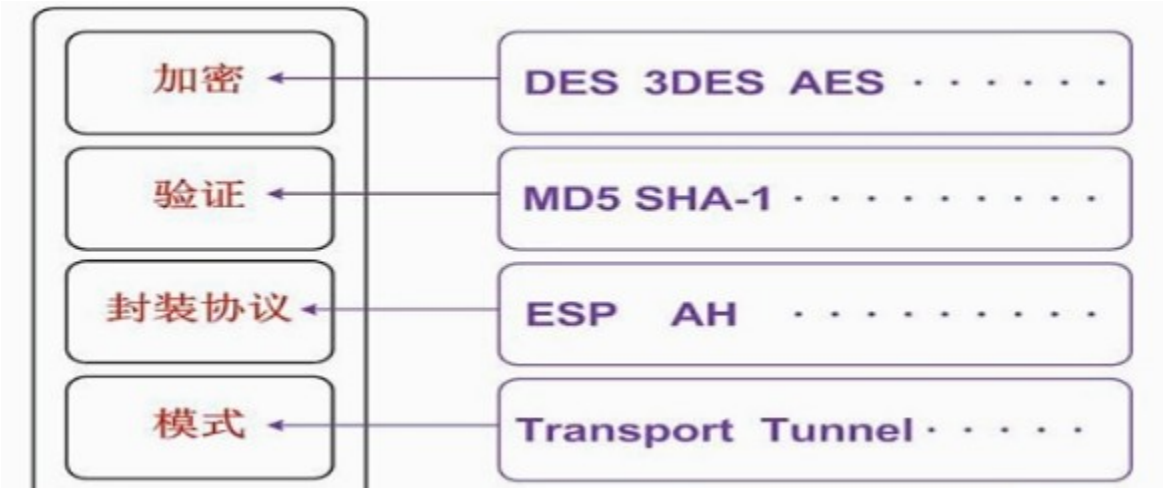
- 防重放（Anti-replay）指防止恶意用户通过重复发送捕获到的数据包所进行的攻击，即接收方会拒绝旧的或重复的数据包。

企业远程分支机构可以通过使用 IPSec VPN 建立安全传输通道，接入到企业总部网络。

IPSec架构

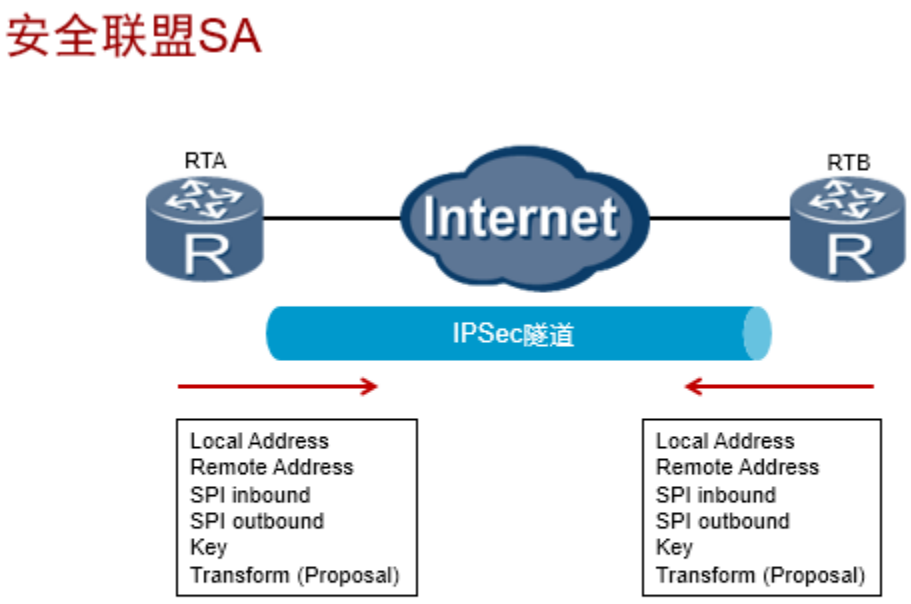


- IPSec不是一个单独的协议，它通过AH和ESP这两个安全协议来实现IP数据报的安全传送。
- IKE协议提供密钥协商，建立和维护安全联盟SA等服务。



IPSec VPN 体系结构主要由 AH（Authentication Header）、ESP（Encapsulating Security Payload）和 IKE（Internet Key Exchange）协议套件组成。

- AH 协议：主要提供的功能有数据源验证、数据完整性校验和防报文重放功能。然而，AH 并不加密所保护的数据报。
- ESP 协议：提供 AH 协议的所有功能外（但其数据完整性校验不包括 IP 头），还可提供对 IP 报文的加密功能。
- IKE 协议：用于自动协商 AH 和 ESP 所使用的密码算法。

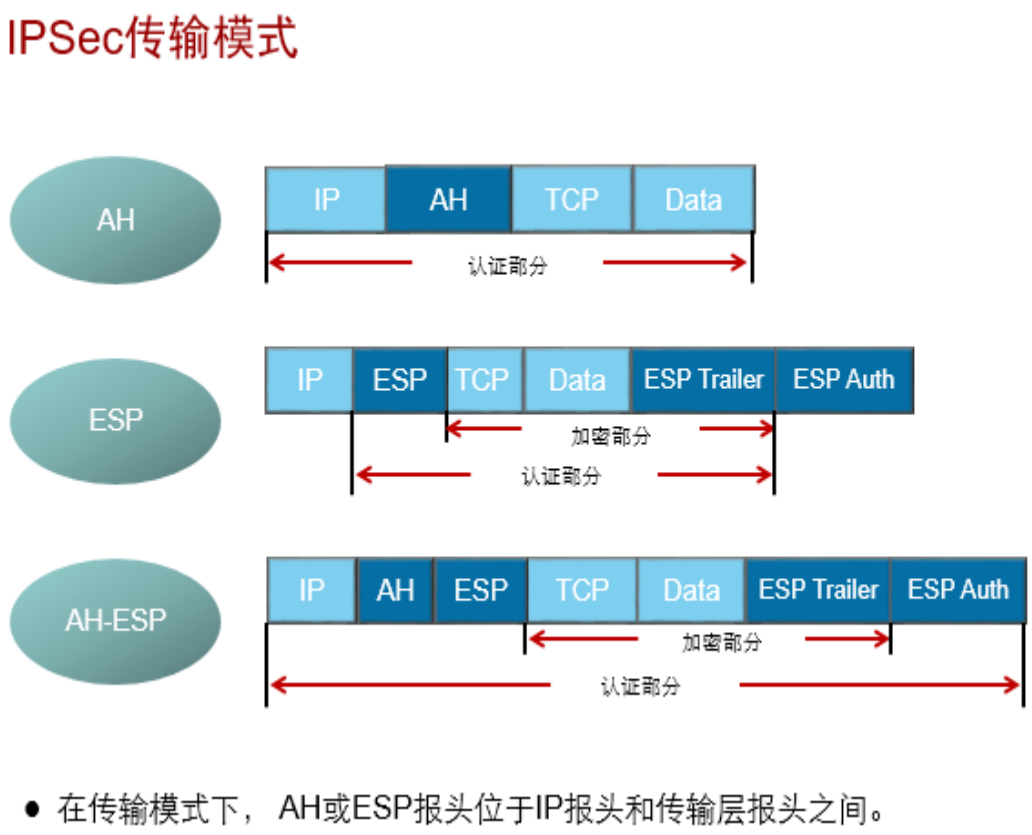


- 安全联盟定义了IPSec对等体间将使用的数据封装模式、认证和加密算法、密钥等参数。
- 安全联盟是单向的，两个对等体之间的双向通信，至少需要两个SA。

SA（Security Association）安全联盟定义了 IPSec 通信对等体间将使用的数据封装模式、认证和加密算法、秘钥等参数。SA 是单向的，两个对等体之间的双向通信，至少需要两个 SA。如果两个对等体希望同时使用 AH 和 ESP 安全协议来进行

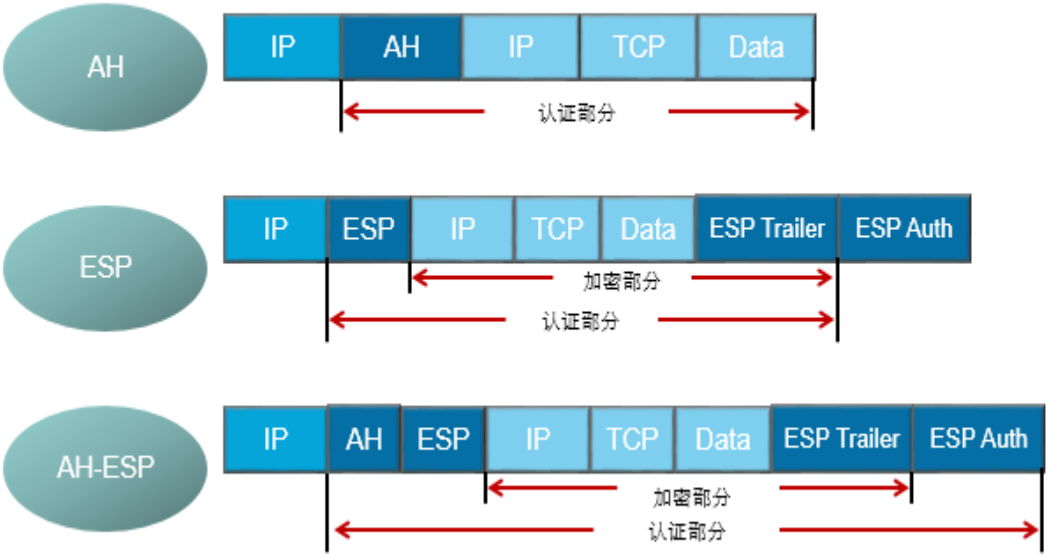
通信，则对等体针对每一种安全协议都需要协商一对 SA。
SA 由一个三元组来唯一标识，这个三元组包括安全参数索引 SPI（Security Parameter Index）、目的 IP 地址、安全协议（AH 或 ESP）。
建立 SA 的方式有以下两种：

- 手工方式：安全联盟所需的全部信息都必须手工配置。手工方式建立安全联盟比较复杂，但优点是可以不依赖 IKE 而单独实现 IPSec 功能。当对等体设备数量较少时，或是在小型静态环境中，手工配置 SA 是可行的。
- IKE 动态协商方式：只需要通信对等体间配置好 IKE 协商参数，由 IKE 自动协商来创建和维护 SA。动态协商方式建立安全联盟相对简单些。对于中、大型的动态网络环境中，推荐使用 IKE 协商建立 SA。

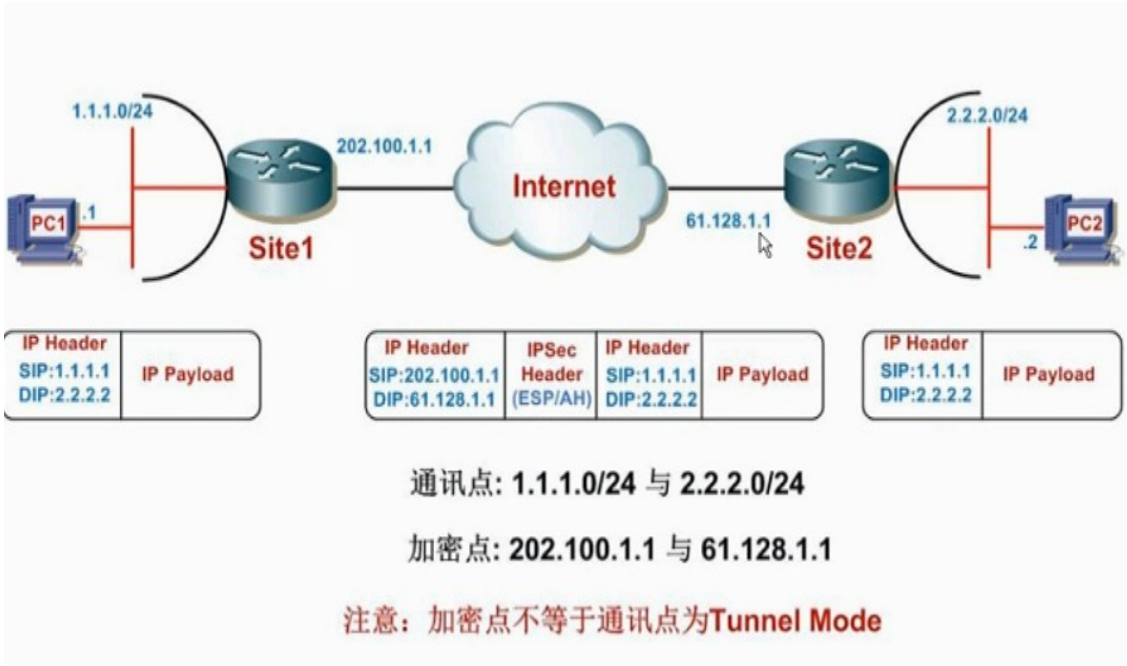


IPSec 协议有两种封装模式：传输模式和隧道模式。
传输模式中，在 IP 报文头和高层协议之间插入 AH 或 ESP 头。
传输模式中的 AH 或 ESP 主要对上层协议数据提供保护。
传输模式中的 AH：在 IP 头部之后插入 AH 头，对整个 IP 数据包进行完整性校验。
传输模式中的 ESP：在 IP 头部之后插入 ESP 头，在数据字段后插入尾部以及认证字段。对高层数据和 ESP 尾部进行加密，对 IP 数据包中的 ESP 报文头，高层数据和 ESP 尾部进行完整性校验。
传输模式中的 AH+ESP：在 IP 头部之后插入 AH 和 ESP 头，在数据字段后插入尾部以及认证字段。对高层数据和 ESP 尾部进行加密，对整个 IP 数据包进行完整性校验。

IPSec隧道模式



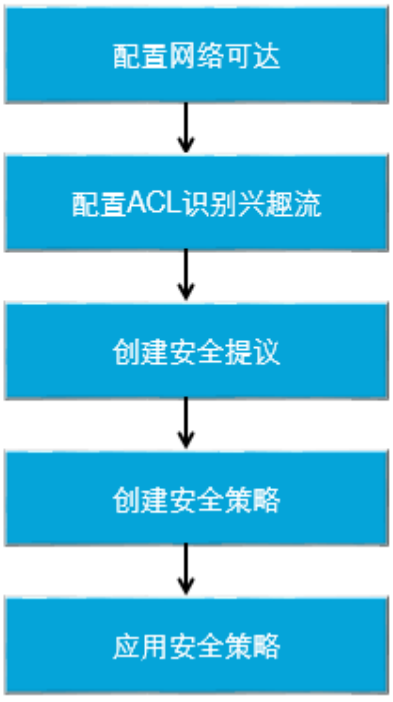
- 在隧道模式下，IPSec会另外生成一个新的IP报头，并封装在AH或ESP之前。



隧道模式中，AH 或 ESP 头封装在原始 IP 报文头之前，并另外生成一个新的 IP 头封装到 AH 或 ESP 之前。隧道模式可以

完全地对原始 IP 数据报进行认证和加密，而且，可以使用 IP Sec 对等体的 IP 地址来隐藏客户机的 IP 地址。
隧道模式中的 AH：对整个原始 IP 报文提供完整性检查和认证，认证功能优于 ESP。但 AH 不提供加密功能，所以通常和 ESP 联合使用。
隧道模式中的 ESP：对整个原始 IP 报文和 ESP 尾部进行加密，对 ESP 报文头，原始 IP 报文和 ESP 尾部进行完整性校验。
隧道模式中的 AH+ESP：对整个原始 IP 报文和 ESP 尾部进行加密，对除新 IP 头之外的整个 IP 数据包进行完整性校验。

IPSec VPN 配置步骤



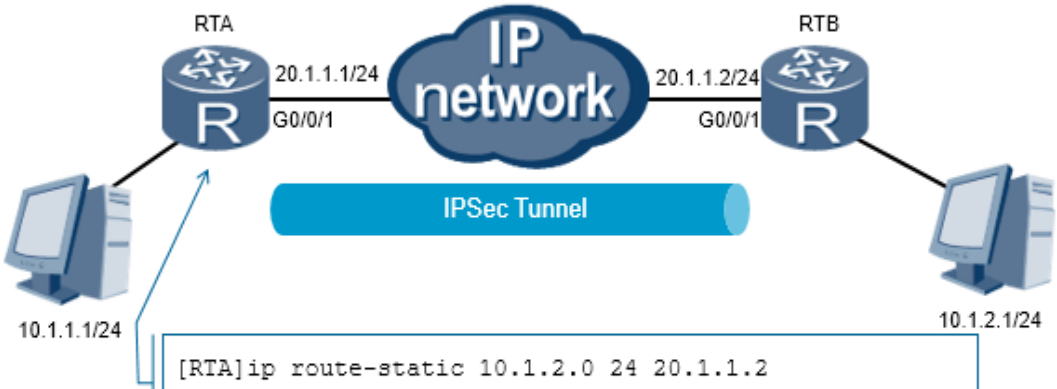
配置 IPSec VPN 的步骤如下：

- 首先需要检查报文发送方和接收方之间的网络层可达性，确保双方只有建立 IPSec VPN 隧道才能进行 IPSec 通信。
- 第二步是定义数据流。因为部分流量无需满足完整性和

机密性要求，所以需要对流量进行过滤，选择出需要进行 IPSec 处理的兴趣流。可以通过配置 ACL 来定义和区分不同的数据流。

- 第三步是配置 IPSec 安全提议。IPSec 提议定义了保护数据流所用的安全协议、认证算法、加密算法和封装模式。安全协议包括 AH 和 ESP，两者可以单独使用或一起使用。AH 支持 MD5 和 SHA-1 认证算法；ESP 支持两种认证算法（MD5 和 SHA-1）和三种加密算法（DES、3DES 和 AES）。为了能够正常传输数据流，安全隧道两端的对等体必须使用相同的安全协议、认证算法、加密算法和封装模式。如果要在两个安全网关之间建立 IPSec 隧道，建议将 IPSec 封装模式设置为隧道模式，以便隐藏通信使用的实际源 IP 地址和目的 IP 地址。
- 第四步是配置 IPSec 安全策略。IPSec 策略中会应用 IPSec 提议中定义的安全协议、认证算法、加密算法和封装模式。每一个 IPSec 安全策略都使用唯一的名称和序号来标识。IPSec 策略可分成两类：手工建立 SA 的策略和 IKE 协商建立 SA 的策略。
- 第五步是在一个接口上应用 IPSec 安全策略。

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 tran1
[RTA-ipsec-proposal-tran1]esp authentication-algorithm
sha1
```

本示例中的 IPSec VPN 连接是通过配置静态路由建立的，下一跳指向 RTB。需要配置两个方向的静态路由确保双向通信可达。建立一条高级 ACL，用于确定哪些感兴趣流需要通过 IPSec VPN 隧道。高级 ACL 能够依据特定参数过滤流量，继而对流量执行丢弃、通过或保护操作。

执行 **ipsec proposal** 命令，可以创建 IPSec 提议并进入 IPSec 提议视图。配置 IPSec 策略时，必须引用 IPSec 提议来指定 IPSec 隧道两端使用的安全协议、加密算法、认证算法和封装模式。缺省情况下，使用 **ipsec proposal** 命令创建的 IPSec 提议采用 ESP 协议、MD5 认证算法和隧道封装模式。在 IPSec 提议视图下执行下列命令可以修改这些参数。

执行 **transform [ah | ah-esp | esp]**命令，可以重新配置隧道采用的安全协议。

执行 **encapsulation-mode {transport | tunnel }**命令，可以配置

报文的封装模式。
执行 **esp authentication-algorithm [md5 | sha1 | sha2-256 | sha2-384 | sha2-512]**命令，可以配置 ESP 协议使用的认证算法。
执行 **esp encryption-algorithm [des | 3des | aes-128 | aes-192 | aes-256]**命令，可以配置 ESP 加密算法。
执行 **ah authentication-algorithm [md5 | sha1 | sha2-256 | sha2-384 | sha2-512]**命令，可以配置 AH 协议使用的认证算法。

配置验证

```
[RTA]display ipsec proposal
 Number of proposals: 1
 IPSec proposal name: tran1
 Encapsulation mode: Tunnel
 Transform          : esp-new
 ESP protocol       : Authentication SHA1-HMAC-96
                      Encryption     DES
```

- IPSec VPN对等体配置的安全提议参数必须一致。

执行 **display ipsec proposal [name <proposal-name>]**命令，可以查看 IPSec 提议中配置的参数。
Number of proposals 字段显示的是已创建的 IPSec 提议的个数。
IPSec proposal name 字段显示的是已创建 IPSec 提议的名称。
Encapsulation mode 字段显示的指定提议当前使用的封装模式，其值可以为传输模式或隧道模式。

Transform 字段显示的是 IPSec 所采用的安全协议，其值可以是 AH、ESP 或 AH-ESP。
ESP protocol 字段显示的是安全协议所使用的认证和加密算法。

IPSec VPN 配置

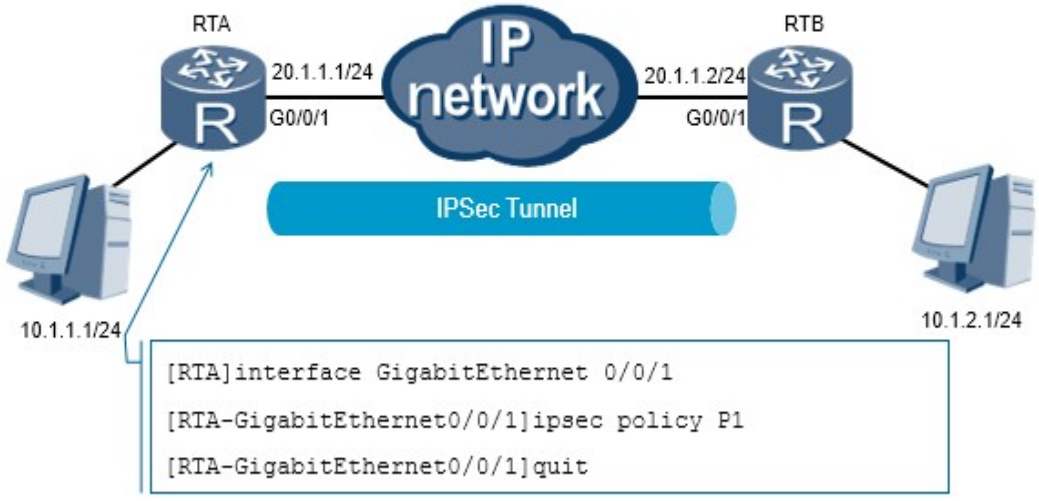
```
[RTA]ipsec  policy P1 10 manual
[RTA-ipsec-policy-manual-P1-10]security acl 3001
[RTA-ipsec-policy-manual-P1-10]proposal tran1
[RTA-ipsec-policy-manual-P1-10]tunnel remote 20.1.1.2
[RTA-ipsec-policy-manual-P1-10]tunnel local 20.1.1.1
[RTA-ipsec-policy-manual-P1-10]sa spi outbound esp 54321
[RTA-ipsec-policy-manual-P1-10]sa 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 policy *policy-name seq-number* 命令用来创建一条 IPSec 策略，并进入 IPSec 策略视图。安全策略是由 *policy-name* 和 *seq-number* 共同来确定的，多个具有相同 *policy-name* 的安全策略组成一个安全策略组。在一个安全策略组中最多可以设置 16 条安全策略，而 *seq-number* 越小的安全策略，优先级越高。在一个接口上应用了一个安全策略组，实际上是同时应用了安全策略组中所有的安全策略，这样能够对不同的数据流采用不同的安全策略进行保护。
IPSec 策略除了指定策略的名称和序号外，还需要指定 SA 的建立方式。如果使用的是 IKE 协商，需要执行 **ipsec-policy-template** 命令配置指定参数。如果使用的是手工建立方式，所

有参数都需要手工配置。本示例采用的是手工建立方式。
security acl *acl-number* 命令用来指定 IPSec 策略所引用的访问控制列表。
proposal *proposal-name* 命令用来指定 IPSec 策略所引用的提议。
tunnel local { *ip-address* | *binding-interface* }命令用来配置安全隧道的本端地址。
tunnel remote *ip-address* 命令用来设置安全隧道的对端地址。
sa spi { **inbound** | **outbound** } { **ah** | **esp** } *spi-number* 命令用来设置安全联盟的安全参数索引 SPI。在配置安全联盟时，入方向和出方向安全联盟的安全参数索引都必须设置，并且本端的入方向安全联盟的 SPI 值必须和对端的出方向安全联盟的 SPI 值相同，而本端的出方向安全联盟的 SPI 值必须和对端的入方向安全联盟的 SPI 值相同。

IPSec VPN配置



ipsec policy *policy-name* 命令用来在接口上应用指定的安全策略组。手工方式配置的安全策略只能应用到一个接口。

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:tran1
...
```

执行 **display ipsec policy [brief | name** *policy-name* [*seq-number*]]命令，可以查看指定 IPSec 策略或所有 IPSec 策略。命令的显示信息中包括：策略名称、策略序号、提议名称、ACL、隧道的本端地址和隧道的远端地址等。

配置验证

```
……
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:
……
```

执行 **display ipsec policy** 命令，还可以查看出方向和入方向 SA 相关的参数。

总结

- 安全联盟的作用是什么?
- IPSec VPN将会对过滤后的感兴趣数据流如何操作?

- SA（Security Association）安全联盟定义了 IPSec 通信对等体间将使用的数据封装模式、认证和加密算法、密钥等参数。
- 经过 IPSec 过滤后的感兴趣数据流将会通过 SA 协商的各种参数进行处理并封装，之后通过 IPSec 隧道转发。