IPSec（Internet Protocol Security）作为开放标准的安全框架结构，可以保证IP数据报文在网络上传输的机密性、完整性和防重放。

IPSec架构

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 提供数据源验证、数据完整性校验和防报文重放功能，但是并不加密所保护的数据报
* ESP协议 除AH外的所有功能，且可以对IP报文进行加密
* IKE协议 用于自动协商AH和ESP所使用的密码算法

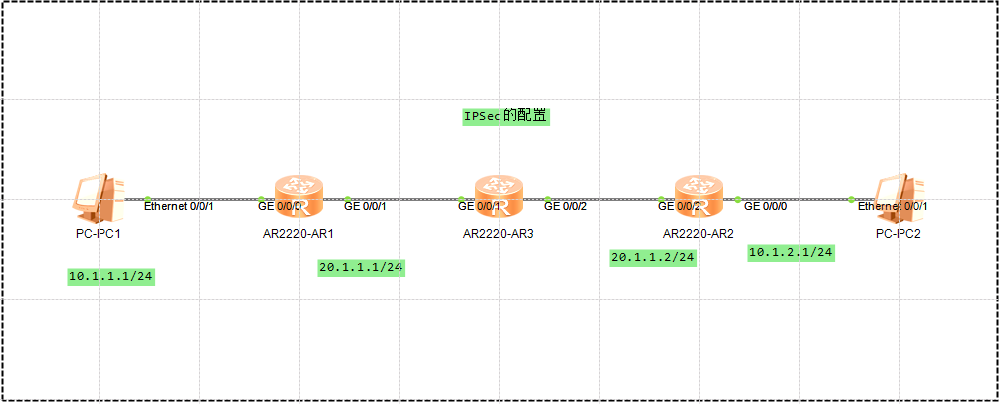
IPSec的传输模式

* 传输模式 AH或ESP报头位于IP报头和传输层报头之间
* 隧道模式 IPSec会生成一个新的IP报头，并封装在AH和ESP之前

配置网络可达🡪ACL识别兴趣流🡪创建安全倡议🡪创建安全策略🡪应用安全策略

IPSec的配置

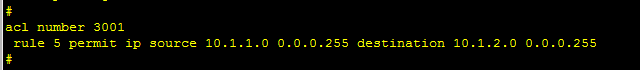
拓扑



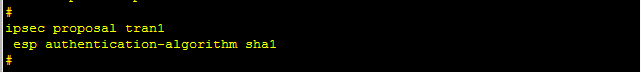
VPN的连接通过配置静态路由实现，所以先配置静态路由



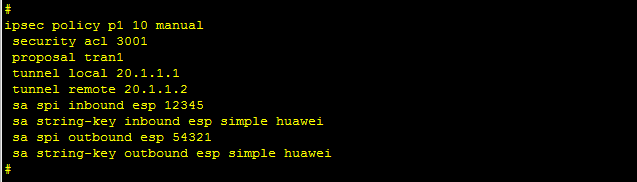
ACL的配置



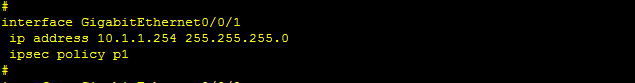
IPSec的提议配置



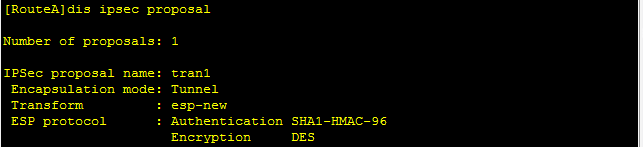
IPSec的策略配置



端口应用



IPSec的提议验证



IPSec的策略验证

