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。

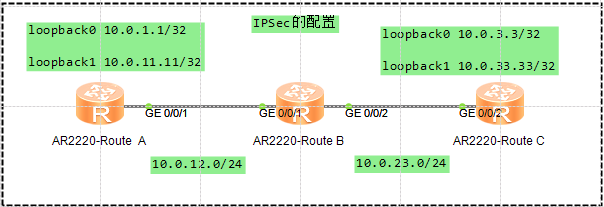
* AH协议 提供数据源验证、数据完整性校验和防报文重放功能，但是并不加密所保护的数据报
* ESP协议 除AH外的所有功能，且可以对IP报文进行加密
* IKE协议 用于自动协商AH和ESP所使用的密码算法

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



配置OSPF，网络连通

ACL的配置

[Route A]acl number 3001

[Route A-acl-adv-3001]rule permit ip source 10.0.1.0 0.0.0.255 destination 10.0.

3.0 0.0.0.255

[Route C]acl number 3001

[Route C-acl-adv-3001]rule permit ip source 10.0.3.0 0.0.0.255 destination 10.0.

1.0 0.0.0.255

IPSec的提议配置，隧道两端需使用相同的安全协议

[Route A]ipsec proposal tran1

[Route A-ipsec-proposal-tran1]esp authentication-algorithm sha1

[Route A-ipsec-proposal-tran1]esp encryption-algorithm 3des

[Route C]ipsec proposal tran1

[Route C-ipsec-proposal-tran1]esp authentication-algorithm sha1

[Route C-ipsec-proposal-tran1]esp encryption-algorithm 3des

IPSec的提议验证

<Route A>display ipsec proposal

Number of proposals: 1

IPSec proposal name: tran1

Encapsulation mode: Tunnel

Transform : esp-new

ESP protocol : Authentication SHA1-HMAC-96

Encryption 3DES

IPSec的策略配置

[Route A]ipsec policy p1 10 manual

[Route A-ipsec-policy-manual-p1-10]security acl 3001

[Route A-ipsec-policy-manual-p1-10]proposal tran1

[Route A-ipsec-policy-manual-p1-10]tunnel local 10.0.12.1

[Route A-ipsec-policy-manual-p1-10]tunnel remote 10.0.23.2

[Route A-ipsec-policy-manual-p1-10]sa spi outbound esp 54321

[Route A-ipsec-policy-manual-p1-10]sa spi inbound esp 12345

[Route A-ipsec-policy-manual-p1-10]sa string-key outbound esp simple huawei

[Route A-ipsec-policy-manual-p1-10]sa string-key inbound esp simple huawei

[Route C]ipsec policy p1 10 manual

[Route C-ipsec-policy-manual-p1-10]security acl 3001

[Route C-ipsec-policy-manual-p1-10]proposal tran1

[Route A-ipsec-policy-manual-p1-10]tunnel local 10.0.23.3

[Route A-ipsec-policy-manual-p1-10]tunnel remote 10.0.12.1

[Route A-ipsec-policy-manual-p1-10]sa spi outbound esp 12345

[Route A-ipsec-policy-manual-p1-10]sa spi inbound esp 54321

[Route A-ipsec-policy-manual-p1-10]sa string-key outbound esp simple huawei

[Route A-ipsec-policy-manual-p1-10]sa string-key inbound esp simple huawei

IPSec的策略验证

<Route A>display ipsec policy

===========================================

IPSec policy group: "p1"

Using interface: GigabitEthernet0/0/1

===========================================

Sequence number: 10

Security data flow: 3001

Tunnel local address: 10.0.12.1

Tunnel remote address: 10.0.23.2

Qos pre-classify: Disable

Proposal name:tran1

Inbound AH setting:

AH SPI:

AH string-key:

AH authentication hex key:

Inbound ESP setting:

ESP SPI: 12345 (0x3039)

ESP string-key: huawei

ESP encryption hex key:

ESP authentication hex key:

Outbound AH setting:

AH SPI:

AH string-key:

AH authentication hex key:

Outbound ESP setting:

ESP SPI: 54321 (0xd431)

ESP string-key: huawei

ESP encryption hex key:

ESP authentication hex key:

端口应用

[Route A]interface GigabitEthernet 0/0/1

[Route A-GigabitEthernet0/0/1]ipsec policy 1