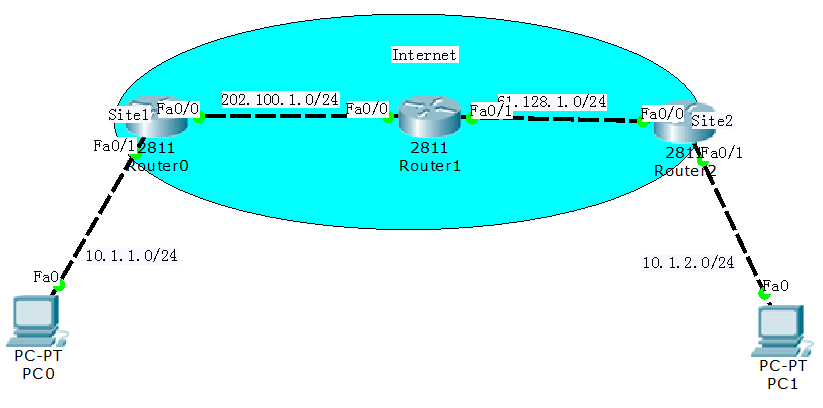
IPSec VPN



实验目的 ：建立IPSec VPN，实现PC间的安全通信

**Site1**:

crypto isakmp policy 100 /第一阶段策略Policy

encr 3des /加密方式

hash md5 /散列算法

authentication pre-share /认证方式

group 2 /DH组

!

crypto isakmp key cisco address 61.128.1.1 /第一阶段密钥、以及指向对端加密点

crypto ipsec transform-set myset esp-3des esp-sha-hmac /第二阶段定义转换级

access-list 100 permit icmp host 10.1.1.1 host 10.1.2.1 /设置感兴趣流

crypto map wuyi 10 ipsec-isakmp /定义map，注意ID，通过isakmp通信

set peer 61.128.1.1 /指向对端加密点

set transform-set myset /调用转换级

match address 100 /匹配感兴趣流

!

interface FastEthernet0/0

ip address 202.100.1.1 255.255.255.0

crypto map wuyi /在加密点的接口激活VPN（也就是公网IP）

!

**Site2**:

crypto isakmp policy 100 /第一阶段策略Policy

encr 3des /加密方式

hash md5 /散列算法

authentication pre-share /认证方式

group 2 /DH组

!

crypto isakmp key cisco address 202.100.1.1 /第一阶段密钥、以及指向对端加密点

crypto ipsec transform-set myset esp-3des esp-sha-hmac /第二阶段定义转换级

access-list 100 permit icmp host 10.1.2.1 host 10.1.1.1 /设置感兴趣流

crypto map wuyi 10 ipsec-isakmp /定义map，注意ID，通过isakmp通信

set peer 202.100.1.1 /指向对端加密点

set transform-set myset /调用转换级

match address 100 /匹配感兴趣流

!

interface FastEthernet0/0

ip address 61.128.1.1 255.255.255.0

crypto map wuyi /在加密点的接口激活VPN（也就是公网IP）

!

**查看：**

Site1#show crypto isakmp sa

IPv4 Crypto ISAKMP SA

dst src state conn-id slot status

61.128.1.1 202.100.1.1 QM\_IDLE 1037 0 ACTIVE

Site1#show crypto ipsec sa

interface: FastEthernet0/0

Crypto map tag: wuyi, local addr 202.100.1.1

protected vrf: (none)

local ident (addr/mask/prot/port): (10.1.1.1/255.255.255.255/1/0)

remote ident (addr/mask/prot/port): (10.1.2.1/255.255.255.255/1/0)

current\_peer 61.128.1.1 port 500

PERMIT, flags={origin\_is\_acl,}

#pkts encaps: 7, #pkts encrypt: 7, #pkts digest: 0

#pkts decaps: 6, #pkts decrypt: 6, #pkts verify: 0

#pkts compressed: 0, #pkts decompressed: 0

#pkts not compressed: 0, #pkts compr. failed: 0

#pkts not decompressed: 0, #pkts decompress failed: 0

#send errors 1, #recv errors 0

……