自制IPsec vpn配置实验

实验需求

R1、R2间tunnel建立私网；

Vpn网关间配置ipsec实现数据加密；

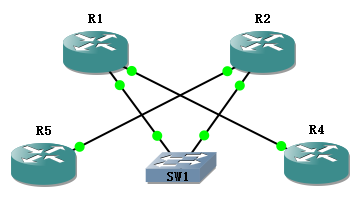
使用tunnel模式下的ESP包头封装；

使用3des加密算法，md5摘要算法；

设置NAT旁路绕行流量；

利用HSRP实现链路备份；

一。基础配置+tunnel+ospf配置



R1：

interface Tunnel12

ip address 192.168.12.1 255.255.255.0

ip ospf 1 area 0

tunnel source 12.12.12.1

tunnel destination 12.12.12.2

!

interface Ethernet0/0

ip address 12.12.12.1 255.255.255.0

half-duplex

no shutdown

!

interface Ethernet0/1

ip address 14.14.14.1 255.255.255.0

half-duplex

no shutdown

!

router ospf 1

router-id 1.1.1.1

log-adjacency-changes

network 14.14.14.1 0.0.0.0 area 0

!

R2：

interface Tunnel12

ip address 192.168.12.2 255.255.255.0

ip ospf 1 area 0

tunnel source 12.12.12.2

tunnel destination 12.12.12.1

!

interface Ethernet0/0

ip address 12.12.12.2 255.255.255.0

half-duplex

no shutdown

!

interface Ethernet0/1

ip address 25.25.25.2 255.255.255.0

half-duplex

no shutdown

!

router ospf 1

router-id 2.2.2.2

log-adjacency-changes

network 25.25.25.2 0.0.0.0 area 0

!

R4:

interface Loopback0

ip address 4.4.4.4 255.255.255.0

!

interface Ethernet0/1

ip address 14.14.14.4 255.255.255.0

half-duplex

no shutdown

router ospf 1

router-id 4.4.4.4

log-adjacency-changes

network 4.4.4.4 0.0.0.0 area 0

network 14.14.14.4 0.0.0.0 area 0

!

R5:

interface Loopback0

ip address 5.5.5.5 255.255.255.0

!

interface Ethernet0/1

ip address 25.25.25.5 255.255.255.0

half-duplex

no shutdown

router ospf 1

router-id 5.5.5.5

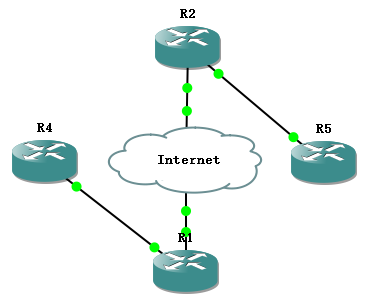
log-adjacency-changes

network 5.5.5.5 0.0.0.0 area 0

network 25.25.25.5 0.0.0.0 area 0

!

二。配置ipsec vpn



三。

R1：

Router(config)#crypto isakmp enable

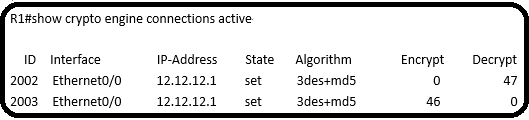
Router(config)#crypto isakmp policy 1   
Router(config-isakmp)#group 1   
Router(config-isakmp)#hash md5 （设置密钥认证使用的算法）  
Router(config-isakmp)#authentication pre-share （使用预先设置的密钥）  
Router(config-isakmp)#encryption 3des （设置加密使用的算法，此密码手工指定）  
Router(config-isakmp)#lifetime 3600 （生存时间）  
  
  
  
Router(config)#crypto isakmp key 0 cisco address 12.12.12.2  
  
  
Router(config)#access-list 1 permit ip any any  
  
Router(config)#crypto ipsec transform-set cisco esp-3des   
  
Router(cfg-crypto-trans)#mode tunnel （隧道模式）  
  
  
Router(config)#crypto map cisco 1 ipsec-isakmp （cisco为名，1为优先级，值越小约优先，）  
Router(config-crypto-map)#set peer 12.12.12.2 （vpn对端IP）  
Router(config-crypto-map)#set transform-set cisco （cisco与transform-set cisco一致）  
Router(config-crypto-map)#match address 1 （匹配的访问列表）  
  
Router(config)#int e0/0  
Router(config-if)#crypto map cisco （匹配map名）

R2：

Router(config)#crypto isakmp enable

Router(config)#crypto isakmp policy 1   
Router(config-isakmp)#group 1   
Router(config-isakmp)#hash md5 （设置密钥认证使用的算法）  
Router(config-isakmp)#authentication pre-share （使用预先设置的密钥）  
Router(config-isakmp)#encryption 3des （设置加密使用的算法，此密码手工指定）  
Router(config-isakmp)#lifetime 3600 （生存时间）  
  
  
  
Router(config)#crypto isakmp key 0 cisco address 12.12.12.1  
  
  
Router(config)#access-list 1 permit ip any any  
  
Router(config)#crypto ipsec transform-set cisco esp-3des   
  
Router(cfg-crypto-trans)#mode tunnel （隧道模式）  
  
  
Router(config)#crypto map cisco 1 ipsec-isakmp （cisco为名，1为优先级，值越小约优先，）  
Router(config-crypto-map)#set peer 12.12.12.1 （vpn对端IP）  
Router(config-crypto-map)#set transform-set cisco （cisco与transform-set cisco一致）  
Router(config-crypto-map)#match address 1 （匹配的访问列表）  
  
Router(config)#int e0/0  
Router(config-if)#crypto map cisco （匹配map名）

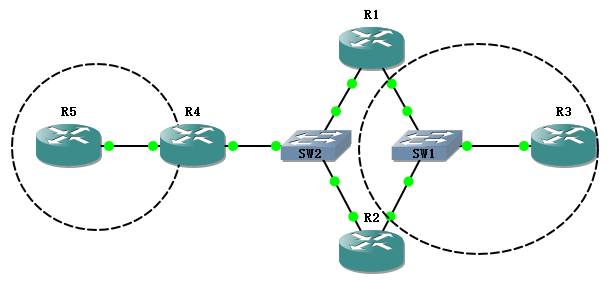
测试：



三。Vpn穿越nat

在nat上将感兴趣流配置bypass

四。HSRP冗余



R1：

//下面就是纯HSRP的配置了

Int e/0

Standby 100 ip 124.124.124.254

//在这里虚拟网关并没有用，只是HSRP配置格式要求

//因为并没有PC的arp请求

Standby 100 priority 255

Standby 100 preempt

Standby 100 name IPsecVPN

//给组起个名字

track 1 interface e0/1 line-protocol

int e0/0

standby 100 track 1

//配置下行链路的接口跟踪

R2：

Int e/0

Standby 100 ip 124.124.124.254

Standby 100 priority 254

Standby 100 preempt

Standby 100 name IPsecVPN

track 1 interface e0/1 line-protocol

int e0/0

standby 100 track 1