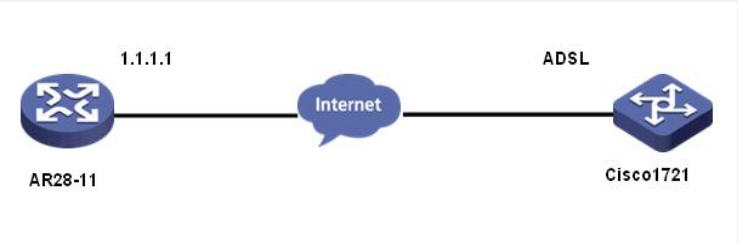
AR系列路由器与CISCO路由器野蛮IPSec互通的典型配置

胡斌B 2006-11-10 发表

AR路由器与CISCO路由器野蛮IPSec互通的典型配置

1.1 Cisco1721作为野蛮IPSec隧道发起方

【组网图】



【需求】

Cisco1721通过ADSL拨号访问Internet，ip地址不固定；AR28-11则通过固定ip地址接入Internet。

IPSec隧道保护的数据流：

中心AR28-11局域网段为10.46.0.0/24；分支Cisco1721局域网段为192.168.1.0/24。

【配置脚本】

AR28-11配置脚本

```
#
sysname Quidway
#
radius scheme system
#
domain system
#
ike proposal 2                  // 创建ike安全提议
authentication-algorithm md5
#
ike peer hnnytset               // 创建ike对等体
exchange-mode aggressive
pre-shared-key hnnytgoodstart
id-type name
remote-name dingannyj
#
ipsec proposal p1               // 创建IPSec安全提议
esp encryption-algorithm 3des
#
ipsec policy policy1 1 isakmp   // 创建IPSec策略
security acl 3000
ike-peer hnnytset
proposal p1
#
acl number 3000            // 建立匹配被保护数据流的ACL规则
rule 0 permit ip source 10.46.0.0 0.0.0.255 destination 192.168.1.0 0.0.0.255
rule 1 deny ip
#
interface Aux0
async mode flow
#
interface Ethernet0/0
ip address 10.46.0.5 255.255.255.0
#
interface Ethernet0/1
ip address 1.1.1.1 255.255.255.248
ipsec policy policy1            // 在接口上应用IPSec策略
#
interface NULL0
#
FTP server enable
#
ip route-static 0.0.0.0 0.0.0.0 1.1.1.2 preference 60
```

Cisco1721配置脚本

```
!
version 12.3
!
hostname dingannyj
!
enable password cisco
!
crypto isakmp policy 100
hash md5
authentication pre-share                  // 配置isakmp策略
!
crypto isakmp peer address 1.1.1.1        //cisco作为发起方必须配置
set aggressive-mode password hnnytgoodstart
set aggressive-mode client-endpoint fqdn dingannyj    // 配置isakmp对等体属性
!
crypto ipsec transform-set hnnytset esp-3des esp-md5-hmac    // 创建IPSec安全提
议
!
crypto map hnnyttrans 10 ipsec-isakmp
set peer 1.1.1.1
set transform-set hnnytset
match address 115                    // 创建IPSec策略
!
interface FastEthernet0
ip address 192.168.1.1 255.255.255.0
ip tcp adjust-mss 1452
speed auto
!
interface Dialer1
mtu 1492
ip address negotiated
encapsulation ppp
dialer pool 1
ppp chap hostname adsl36801864
ppp chap password 0 nongyeju
ppp pap sent-username adsla6531333 password 0 667078
crypto map hnnyttrans                     // 在接口上应用IPSec策略
!
ip route 0.0.0.0 0.0.0.0 Dialer1
ip route 192.168.0.0 255.255.0.0 FastEthernet0
!
!
access-list 115 permit ip 192.168.1.0 0.0.0.255 10.46.0.0 0.0.0.255
access-list 115 deny   ip any any        //建立匹配被保护数据流的访问列表
```

【验证】

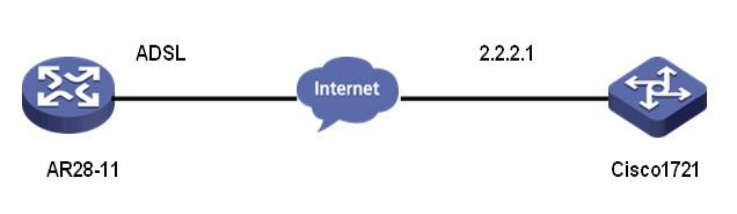
```
<Quidway>dis ike sa
total phase-1 SAs:  1
connection-id  peer           flag       phase   doi
--------------------------------------------------------------
410         2.2.2.1 RD           2     IPSEC
409         2.2.2.1 RD           1     IPSEC

dingannyj#show crypto engine connections active

ID Interface           IP-Address      State  Algorithm           Encrypt  De
crypt
1 Dialer1              2.2.2.1 set    HMAC_MD5+DES_56_CB        0
0
200 Dialer1            2.2.2.1 set    HMAC_MD5+3DES_56_C        0
9
201 Dialer1              2.2.2.1 set    HMAC_MD5+3DES_56_C        9
dingannyj#show crypto isakmp sa
dst             src             state          conn-id slot
1.1.1.1   2.2.2.1 QM_IDLE              1    0
```

1.2 AR28-11作为野蛮IPSec隧道发起方

【组网图】



【需求】

AR28-11通过ADSL拨号访问Internet，ip地址不固定；Cisco1721则通过固定ip地址接入Internet。

IPSec隧道保护的数据流：

中心AR28-11局域网段为10.46.0.0/24；分支Cisco1721局域网段为192.168.1.0/24。

【配置脚本】

AR28-11配置脚本

```
#
sysname Quidway
#
ike local-name hnnytgoodstart           // 创建ike协商本端网关的名字
#
radius scheme system
#
domain system
#
ike proposal 2                  // 创建ike安全提议
authentication-algorithm md5
#
ike peer hnnytset               // 创建ike对等体
exchange-mode aggressive
pre-shared-key hnnytgoodstart
id-type name
remote-name dingannyj
remote-address  2.2.2.1
#
ipsec proposal p1                   // 创建IPSec安全提议
esp encryption-algorithm 3des
#
ipsec policy policy1 1 isakmp    // 创建IPSec策略
security acl 3000
ike-peer hnnytset
proposal p1
#
acl number 3000                 // 建立匹配被保护数据流的ACL规则
rule 0 permit ip source 10.46.0.0 0.0.0.255 destination 192.168.1.0 0.0.0.255
rule 1 deny ip
#
interface Aux0
async mode flow
#
interface Ethernet0/0
ip address 10.46.0.5 255.255.255.0
#
interface Dialer0
link-protocol ppp
ip address ppp-negotiate
mtu 1450
dialer enable-circular
dialer-group 1
ipsec policy policy1                // 在接口上应用IPSec策略
#
interface NULL0
#
FTP server enable
#
ip route-static 0.0.0.0 0.0.0.0 dialer0 preference 60
```

Cisco1721配置脚本

```
!
version 12.3
!
hostname dingannyj
!
enable password cisco
!
crypto isakmp policy 100
hash md5
authentication pre-share                // 配置isakmp策略
!
crypto isakmp key huawei hostname hnnytgoodstart      // Cisco作响应方必须配置
crypto isakmp identity hostname
!
crypto ipsec transform-set hnnytset esp-3des esp-md5-hmac    // 创建IPSec安全提
议
!
crypto dynamic-map dyna 1
set transform-set hnnytset
match address 115
crypto map hnnyttrans 10 ipsec-isakmp dynamic dyna        // 创建IPSec策略
!
interface FastEthernet0
ip address 192.168.1.1 255.255.255.0
ip tcp adjust-mss 1452
speed auto
!
interface FastEthernet1
ip address 2.2.2.1 255.255.255.248
ip tcp adjust-mss 1452
speed auto
crypto map hnnyttrans        // 在接口上应用IPSec策略
!
ip route 0.0.0.0 0.0.0.0 FastEthernet1
ip route 192.168.0.0 255.255.0.0 FastEthernet0
!
!
access-list 115 permit ip 192.168.1.0 0.0.0.255 10.46.0.0 0.0.0.255
access-list 115 deny   ip any any        //建立匹配被保护数据流的访问列表
```

【配置关键点】

采用野蛮模式和Cisco互通时，Cisco作为隧道发起方和响应方的配置是有区别的。

Cisco作为隧道发起方：

crypto isakmp peer address 1.1.1.1   //Cisco作为发起方必须配置

set aggressive-mode password hnnytgoodstart

set aggressive-mode client-endpoint fqdn dingannyj

Cisco作为隧道响应方：

crypto isakmp key huawei hostname hnnytgoodstart   //Cisco作为响应方必须配置

crypto isakmp identity hostname

【提示】

1、cisco不区分aggressive模式和main模式。

2、cisco isakmp policy提供多种验证策略（pre-share、rsa-encr、rsa-sig）

Quidway的ike仅支持pre-shared-key方式。

3、cisco 路由器上isakmp policy必须配置，由于需要指定pre-share验证策略，两者必须匹配。

Quidway的ike proposal可以不配，默认方式也能满足协商的要求。

4、在cisco 的isakmp policy环境下和Quidway的ike proposal环境下，支持的加密算法会有一定的区别。

5、ike sa keepalive不是RFC标准，因此各厂商关于其的实现程度不同，难以配合。

Cisco不支持此功能。

6、cisco 的“show crypto isakmp sa”只显示ike阶段的sa信息。

Quidway的“display ike sa”显示两个ike和ipsec两个阶段的sa信息。