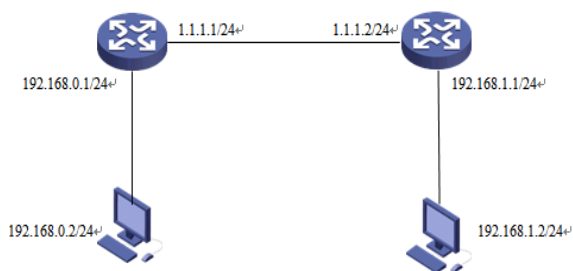


# 知 ACG1000与V7平台设备使用IPSEC主模式VPN对接案例

ACG1000 IPsec 刘嘉伟 2015-11-08 发表

客户目前使用ACG1000-S作为网络出口设备，现在要与对端MSR设备建立IPSEC VPN



配置任务 (ACG1040) :

- 1、配置接口地址
- 2、配置路由
- 3、配置IKE
- 4、配置IPSEC
- 5、配置IPSEC安全策略

配置步骤:

- 1) 配置接口地址

接口名称	IP地址	IPv6地址	MAC地址	工作模式	双工模式	速率(Mbps)	连接状态	启动状态	操作
1 ge0	192.168.1.1/24		586eb1x440e2	route	full	1000	up	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
2 ge1	1.1.1.2/24		586eb1x440e3	route	full	1000	up	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
3 ge2			586eb1x440e4	route	full	1000	down	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
4 ge3			586eb1x440e5	route	full	1000	down	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

配置外网口ge1的ip地址为1.1.1.2/24，配置内网口ge0的ip地址为192.168.1.1/24

- 2) 设置路由

网络配置 > 路由 > 静态路由

静态路由

目的地址: 0.0.0.0

子网掩码: 0.0.0.0

下一跳/出接口:  下一跳  出接口

下一跳: 1.1.1.1

权重: 1 (1-255)

距离: 1 (1-255)

地址探测: -

提交 取消

- 3) 配置IKE

点击设备左侧导航栏张的 VPN>IPSEC>新建IKE

### 基本设置

网关名称  (1-31 字符)

对端网关 **静态IP地址**

IP地址

模式  野蛮模式  主模式(ID保护)

认证方式 **预共享密钥**

预共享密钥  (6-39 字符)

### 高级选项

#### IKE协商交互方案

加密算法 **3DES** 认证 **MD5** [+ 添加到列表](#)

	加密算法	认证	操作
1	3DES	MD5	<a href="#">删除</a>

DH组  1  2  5

密钥周期  (120-86400 秒)

NAT穿越连接频率  (10-900 秒)

### 4) 新建IPSEC

注意这里的密钥周期必须要创建

### 基本设置

通道名称  (1-31 字符)

IKE **soho**

### 高级选项

#### IPSEC协商交互方案

ESP **NULL\_NULL** AH **NULL** [+ 添加到列表](#)

	ESP	AH	操作
1	3DES_MD5	NULL	<a href="#">删除</a>

完美向前保密(PFS)  无  1  2  5

模式  隧道模式

密钥周期  秒  千字节  两者都有

秒  (120-86400 秒)

自动连接

时间  (2-3600 秒)

[提交](#)

[取消](#)

### 5) 创建IPSEC隧道接口

IPsec接口

IPv4地址  (例如: 192.168.1.1/24)

IPsec **soho**

地址项目  -  (例如: 192.168.1.1/24-192.168.2.1/24)

[+ 添加到列表](#)

	源地址	目的地址	操作
1	192.168.1.0/24	192.168.0.0/24	<a href="#">删除</a>

[提交](#)

[取消](#)

### 6) 创建路由

在网络设置>静态路由>新建

目的地址

子网掩码

下一跳/出接口  下一跳  出接口

出接口  (支持3G、tunnel、pppoe接口，黑洞路由)

权重  (1-255)

距离  (1-255)

地址探测

显示的状态:

目的地址	掩码	下一跳	出接口	权重	距离	地址探测	状态	操作
1	0.0.0.0	0.0.0.0	1.1.1.1	ge1	1	1	-	<input checked="" type="checkbox"/> <input type="checkbox"/>
2	192.168.0.0	255.255.255.0	tunnel1	1	1	-	<input checked="" type="checkbox"/> <input type="checkbox"/>	

MSR2630上的配置:

```

interface GigabitEthernet0/0 //配置内网接口
port link-mode route
ip address 192.168.0.1 255.255.255.0
#
interface GigabitEthernet0/1 //配置外网接口
port link-mode route
ip address 1.1.1.1 255.255.255.0
ipsec apply policy 1 //绑定ipsec策略
#
ip route-static 0.0.0.0 0 1.1.1.2 //配置路由
#
acl number 3000 //创建感兴趣流
rule 0 permit ip source 192.168.0.0 0.0.0.255 destination 192.168.1.0 0.0.0.255
#
ipsec transform-set 1 //创建ipsec安全提议
esp encryption-algorithm 3des-cbc
esp authentication-algorithm md5
#
ipsec policy 1 1 isakmp //创建ipsec安全策略
transform-set 1 //绑定安全提议
security acl 3000 //绑定安全ACL
remote-address 1.1.1.2 //写远端地址
#
ike proposal 1
encryption-algorithm 3des-cbc
authentication-algorithm md5
#
ike keychain 1 //配置共享密钥
pre-shared-key address 1.1.1.2 255.255.255.255 key cipher $c$3$+x9YocATZDyMsPBX4G3UcDKL
raWt2QJqgw==

```

测试结果:

查看IPSEC安全联盟:

名称	对端网关	本地网关	状态	过期时间	流量(入/出/B)	源网端	目的网端	操作
1 soho	1.1.1.1	1.1.1.2	连接		31346/1843200.1 0.0/0.0	192.168.1.0/24	192.168.0.0/24	<input type="checkbox"/> <input checked="" type="checkbox"/>

查看ike:

名称	对端网关	本地网关	状态	过期时间/s	操作
1 soho	1.1.1.1	1.1.1.2	连接	82353	<input type="checkbox"/> <input checked="" type="checkbox"/>

MSR上查看配置:

```

<H3C>display ike sa
Connection-ID Remote Flag DOI
-----
2 1.1.1.2 RD IPSEC
Flags:
RD--READY RL--REPLACED FD-FADING

```

```

<H3C>display ipsec sa
-----
Interface: GigabitEthernet0/1
-----

IPsec policy: 1
Sequence number: 1
Mode: isakmp
-----
Tunnel id: 0
Encapsulation mode: tunnel
Perfect forward secrecy:
Path MTU: 1443
Tunnel:
  local address: 1.1.1.1
  remote address: 1.1.1.2
Flow:
sour addr: 192.168.0.0/255.255.255.0 port: 0 protocol: ip
dest addr: 192.168.1.0/255.255.255.0 port: 0 protocol: ip

[Inbound ESP SAs]
SPI: 3992791942 (0xedfd2b86)
Transform set: ESP-ENCRYPT-3DES-CBC ESP-AUTH-MD5
SA duration (kilobytes/sec): 1843200/3600
SA remaining duration (kilobytes/sec): 1843199/3375
Max received sequence-number: 3
Anti-replay check enable: Y
Anti-replay window size: 64
UDP encapsulation used for NAT traversal: N
Status: active

[Outbound ESP SAs]
SPI: 137057985 (0x082b56c1)
Transform set: ESP-ENCRYPT-3DES-CBC ESP-AUTH-MD5
SA duration (kilobytes/sec): 1843200/3600
SA remaining duration (kilobytes/sec): 1843199/3375
Max sent sequence-number: 3
UDP encapsulation used for NAT traversal: N
Status: active
-----

```

ACG命令行显示的配置:

```

interface ge0
ip address 192.168.1.1/24
!
interface ge1
traffic-mode extern
ip address 1.1.1.2/24
!
interface tunnel 1 mode ipsec
mtu 1420
!
vpn ipsec phase1
edit gateway soho
set mode main
set remotegw 1.1.1.1
authentication pre-share
set preshared-key secret kTgxl5p34DqlzzT+XZ0R14cv6Qal7urj9YogDjQGHYyVxSLYlpmOxTPwro
4b0aN
lifetime 86400
set dpd retry 5
set nat 10
group 1
set policy 1
  encrypt 3des
  hash md5
  exit
set modecfg-server
modecfg-server disable
exit
!
vpn ipsec phase2
edit tunnel soho
set peer soho
mode tunnel
set lifetime seconds 86400
set proposal1 esp-3des-md5 ah-null
!
interface tunnel1
tunnel-ipsec soho
tunnel-ipsec interested-subnet pair 192.168.1.0/24 192.168.0.0/24
!
policy default-action permit
policy white-list enable
!
ip route 0.0.0.0/0 1.1.1.1
ip route 192.168.0.0/24 tunnel1

```

