项目 28　防火墙 IPSec VPN 配置

项目简介

通过在防火墙上配置 IPSec，实现两个公司之间按照需求内部网络互通。IPSec 能够进行数据加密保护，目前使用比较普遍。要实现两个公司之间通过 IPSec 互通数据，前提是互联网要畅通，因为 IPSec 封装加密的数据是通过互联网到达对方。随着公司业务的发展，目前集团化业务部署越来越多，比如公司总部部署 OA 系统，其他分公司通过配置 IPSec，就可以访问公司总部 OA 系统，实现一套系统，全公司使用。

本项目实现公司甲与公司乙之间内网配置安全虚拟专用网（IPSec），IPSec 通过隧道加密技术，形成一个安全互通的隧道在互联网中传输数据。目前防火墙基本上都有 IPSec 模块，通过在不同地域之间的两个防火墙配置 IPSec，实现内网之间数据互通。条件允许的情况下，也可以购买专用 VPN 设备，与分公司之间业务数据加密通信。

一、拓扑图

拓扑图如图 2-3-28-1 所示。

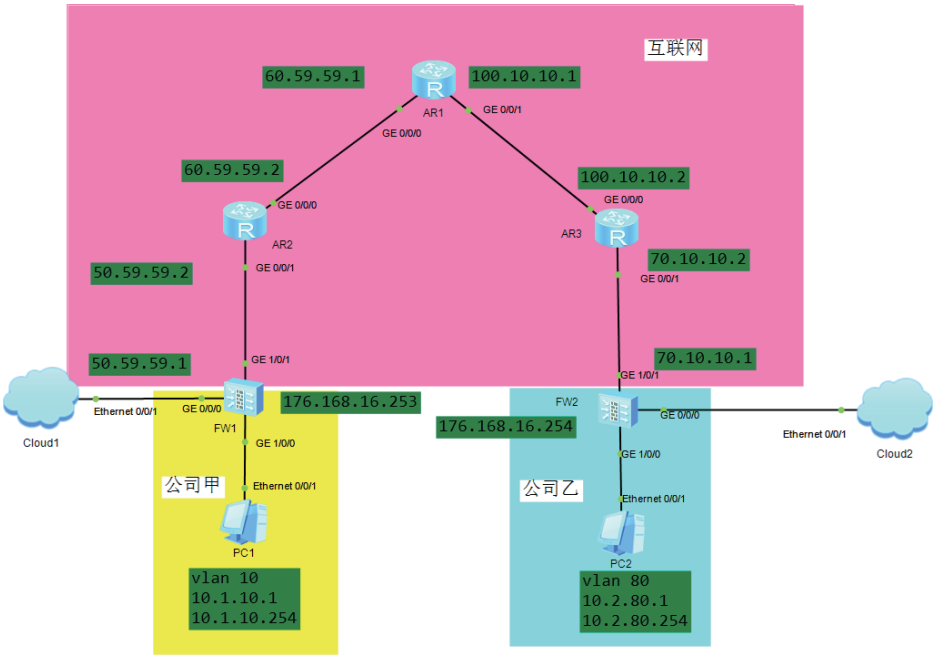
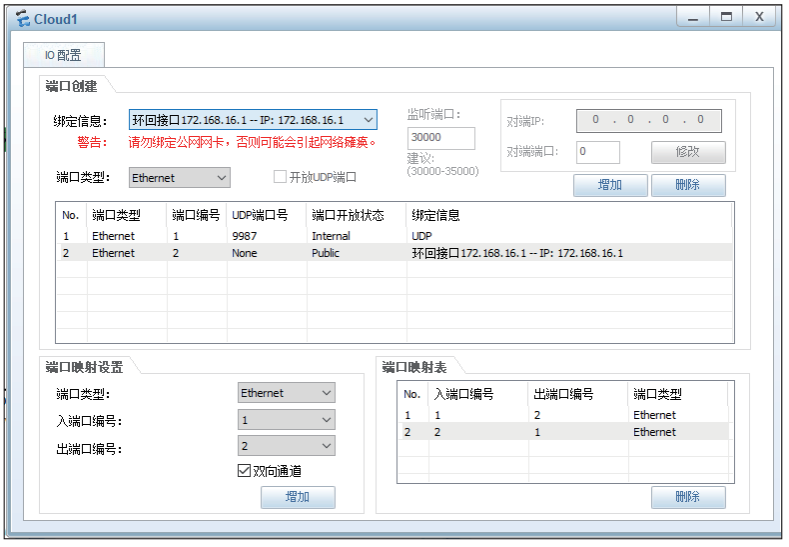


图2-3-28-1　拓扑图

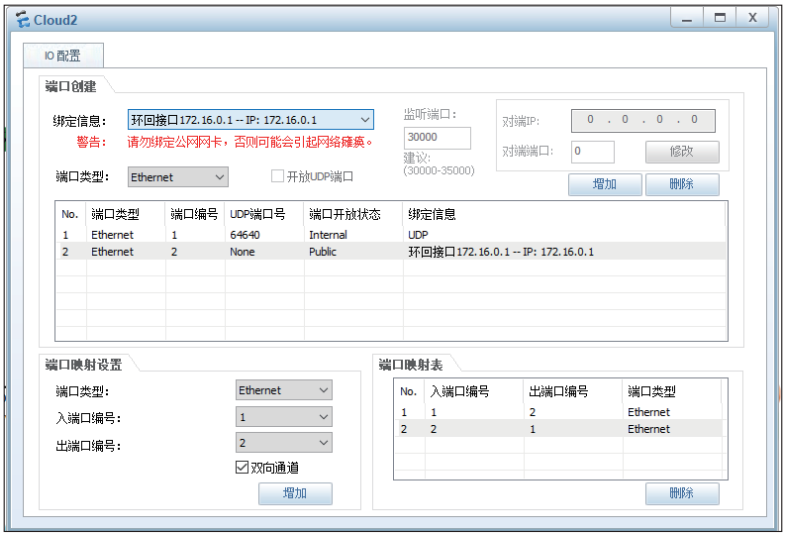
本项目在模拟器上完成，首先在物理主机上新建两个环回接口，如图 2-3-28-2 所示。

图2-3-28-2　环回接口

模拟器中两个防火墙通过“Cloud”，与物理主机通信，然后通过 web 界面进行防火墙配置，如图 2-3-28-3 所示。



（a）

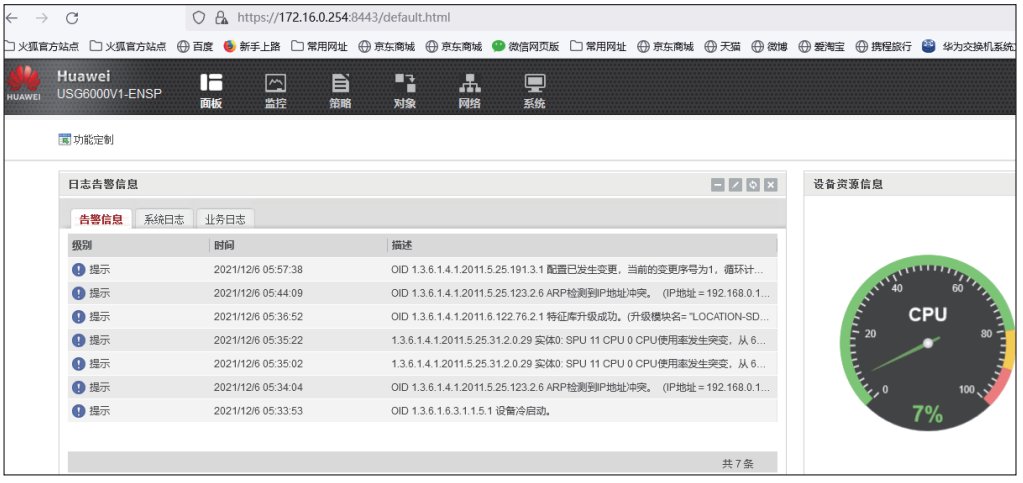


（b）

图2-3-28-3　“Cloud”配置

当防火墙管理接口配置地址后（允许 https 功能），在 IE 浏览器输入 https://IP:8843，访问防火墙。图 2-3-28-4 所示是配置完毕后，分别为 FW1 与 FW2 防火墙界面。

（a）FW1 登录界面



（b）FW2 登录界面

图2-3-28-4　防火墙登录界面

二、因特网（公网）之间互通配置

步骤 1　AR1 路由器 IP 地址配置。

```
<Huawei>sys
Enter system view, return user view with Ctrl+Z.
[Huawei]sysname AR1
# 关闭信息提示
[AR1]un in en
Info: Information center is disabled.
[AR1]interface GigabitEthernet 0/0/0
[AR1-GigabitEthernet0/0/0]ip address 60.59.59.1 24
[AR1-GigabitEthernet0/0/0]quit
[AR1]interface GigabitEthernet 0/0/1
[AR1-GigabitEthernet0/0/1]ip address 100.10.10.1 24
[AR1-GigabitEthernet0/0/1]quit
[AR1]quit
<AR1>save
```

步骤 2　AR2 路由器 IP 地址配置

```
< AR2>system-view
Enter system view, return user view with Ctrl+Z.
[AR2]interface GigabitEthernet  0/0/0
[AR2-GigabitEthernet0/0/0]ip address 60.59.59.2 24
[AR2-GigabitEthernet0/0/0]quit
[AR2]interface GigabitEthernet 0/0/1
[AR2-GigabitEthernet0/0/1]ip address 50.59.59.2 24
[AR2-GigabitEthernet0/0/1]quit
[AR2]quit
<AR2>sa
```

步骤 3　AR3 路由器 IP 地址配置。

```
<Huawei>
<Huawei>sys
<Huawei>system-view
[Huawei]sysname AR3
[AR3]interface GigabitEthernet 0/0/0
[AR3-GigabitEthernet0/0/0]ip address 100.10.10.2 24
[AR3-GigabitEthernet0/0/0]quit
[AR3]interface GigabitEthernet 0/0/1
[AR3-GigabitEthernet0/0/1]ip address 70.10.10.2 24
[AR3-GigabitEthernet0/0/1]quit
[AR3]quit
<AR3>sa
```

步骤 4　FW1 防火墙配置。

华为防火墙默认用户名：admin，密码：Admin@123，密码修改为：huawei@123，配置略。

```
[FW1]interface GigabitEthernet 0/0/0
[FW1-GigabitEthernet0/0/0]ip address 172.168.16.253 24
# 允许 ping 功能
[FW1-GigabitEthernet0/0/0]service-manage ping permit
# 允许 ssh 功能
[FW1-GigabitEthernet0/0/0]service-manage ssh permit
# 允许 https 功能
[FW1-GigabitEthernet0/0/0]service-manage https permit
[FW1-GigabitEthernet0/0/0]quit
# 配置 FW1 防火墙出口地址
[FW1-GigabitEthernet1/0/1]ip address 50.59.59.1 24
#  GigabitEthernet1/0/1 允许 ping。
[FW1-GigabitEthernet1/0/1]service-manage ping permit
[FW1-GigabitEthernet1/0/1]quit
# 进入到 untrust 区域
[FW1]firewall zone untrust
# 将 GigabitEthernet  1/0/1 加入到 untrust 区域
[FW1-zone-untrust]add interface GigabitEthernet 1/0/1
[FW1-zone-untrust]quit
[FW1]quit
<FW1>save
```

步骤 5　FW1 通过 ssh 协议远程访问配置。

用户名 :firewall1，密码：huawei@123。

```
[FW1]stelnet server enable
[FW1]aaa
# 配置 ssh 远程访问用户名 firewall1
[FW1-aaa]manager-user firewall1
# 开启 ssh 服务
[FW1-aaa-manager-user-firewall1]service-type ssh
# 配置 ssh 访问权限
[FW1-aaa-manager-user-firewall1]level 15
[FW1-aaa-manager-user-firewall1]password
# 修改新密码：huawei@123
Enter Password:
Confirm Password:
[FW1-aaa-manager-user-firewall1]quit
[FW1-aaa]quit
[FW1]user-interface vty 0 4
[FW1-ui-vty0-4]authentication-mode aaa
[FW1-ui-vty0-4]quit
# 生成秘钥
[FW1]rsa local-key-pair create
The key name will be: FW1_Host
The range of public key size is (2048 ~ 2048).
NOTES: If the key modulus is greater than 512,
       it will take a few minutes.
Input the bits in the modulus[default = 2048]:2048
Generating keys...
..+++++
.........................++
....++++
...........++
[FW1]quit
<FW1>save
```

使用 SecureCRT 远程登录 FW1, 如图 2-3-28-5 所示。

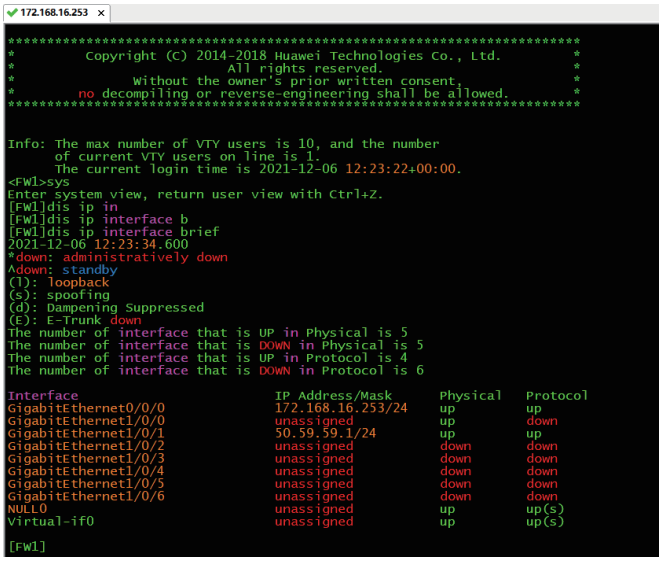


图2-3-28-5　使用SecureCRT 远程登录FW1

步骤 6　配置 AR2、AR3 和 AR1 三个路由器路由信息。

```
[AR2]display current-configuration | include ip rou
ip route-static 70.10.10.0 255.255.255.0 60.59.59.1
ip route-static 100.10.10.0 255.255.255.0 60.59.59.1
[AR3]display current-configuration | include ip rou
ip route-static 50.59.59.0 255.255.255.0 100.10.10.1
ip route-static 60.59.59.0 255.255.255.0 100.10.10.1
[AR1]display current-configuration | include ip rou
ip route-static 50.59.59.0 255.255.255.0 60.59.59.2
ip route-static 70.10.10.0 255.255.255.0 100.10.10.2
[AR1]
网络测试 - 通
<AR2>ping 100.10.10.2
  PING 100.10.10.2: 56  data bytes, press CTRL_C to break
  Reply from 100.10.10.2: bytes=56 Sequence=1 ttl=254 time=30 ms
  ……省略……
  --- 100.10.10.2 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
round-trip min/avg/max = 20/24/30 ms
网络测试 - 通
<AR3>ping 60.59.59.2
  PING 60.59.59.2: 56  data bytes, press CTRL_C to break
    Reply from 60.59.59.2: bytes=56 Sequence=1 ttl=254 time=30 ms
    ……省略……
  --- 60.59.59.2 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 20/24/30 ms
```

步骤 7　FW2 防火墙基本配置。

```
# FW2-GigabitEthernet0/0/0 配置
[FW2-GigabitEthernet0/0/0]display this
2021-12-06 12:15:52.590
#
interface GigabitEthernet0/0/0
 undo shutdown
 ip binding vpn-instance default
 ip address 172.16.0.254 255.255.255.0
 alias GE0/METH
 service-manage https permit
 service-manage ping permit
 service-manage ssh permit
#
return
[FW2-GigabitEthernet1/0/1]ip address 70.10.10.1 24
[FW2-GigabitEthernet1/0/1]service-manage ping permit
[FW2-GigabitEthernet1/0/1]quit
[FW2]firewall zone untrust
```

```
[FW2-zone-untrust]add interface GigabitEthernet 1/0/1
[FW2-zone-untrust]quit
[FW2]quit
<FW2>sa
```

步骤 8　两个防火墙配置默认路由。

```
[FW1]ip route-static 0.0.0.0 0 50.59.59.2
[FW2]ip route-static 0.0.0.0 0 70.10.10.2
```

步骤 9　FW1 与 FW2 放通 untrust/trust/local 三个区域 ping 功能。

如图 2-3-28-6、图 2-3-28-7 所示，分别是 FW1 与 FW2 配置界面。

FW2 通过 ssh 协议远程访问配置，用户名 :firewall2，密码：huawei@123，配置略。

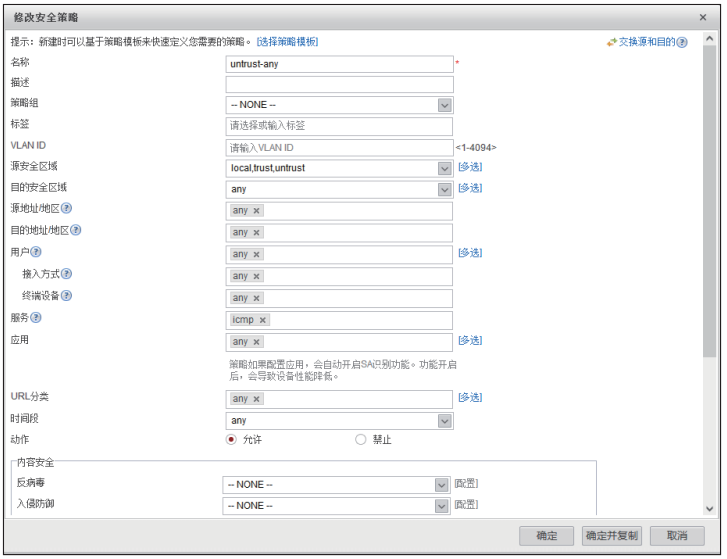


图2-3-28-6　FW1放通untrust/trust/local三个区域ping

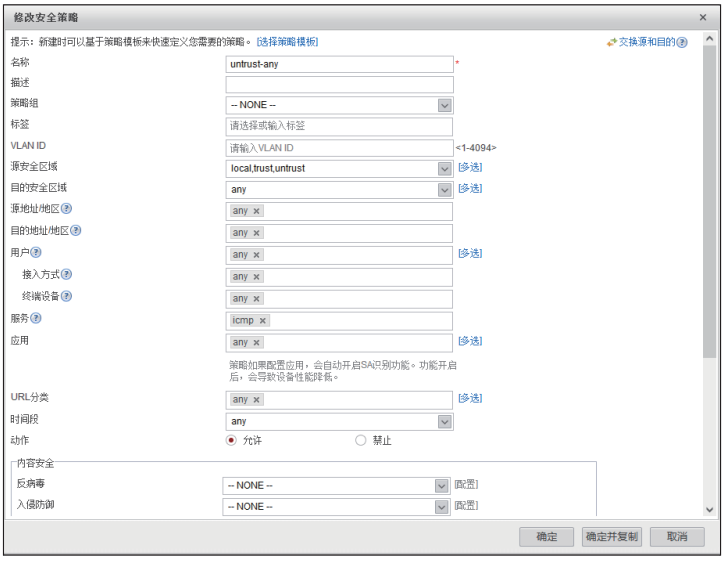


图2-3-28-7　FW2放通untrust/trust/local三个区域ping

步骤 10　因特网之间网络测试。

```
FW1-ping-FW2- 通
<FW1>ping 70.10.10.1
  PING 70.10.10.1: 56  data bytes, press CTRL_C to break
    Reply from 70.10.10.1: bytes=56 Sequence=1 ttl=252 time=19 ms
……省略……
  --- 70.10.10.1 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 17/17/19 ms
```

三、内部网络配置

步骤 1　FW1 内网地址配置。

```
# 配置 vlan 以及网关
[FW1]interface Vlanif 10
[FW1-Vlanif10]display this
2021-12-07 01:52:13.410
#
interface Vlanif10
ip address 10.1.10.254 255.255.255.0
#
Return
# 将 vlan 10 加入到 trust 区域
[FW1-zone-trust]add interface Vlanif 10
[FW1-Vlanif10]service-manage ping permit
# 将接口变为二层接口
[FW1-GigabitEthernet1/0/0]portswitch
[FW1-GigabitEthernet1/0/0]port link-type access
[FW1-GigabitEthernet1/0/0]port default vlan 10
[FW1-GigabitEthernet1/0/0]quit
```

步骤 2　FW1 防火墙 NAT 转化功能配置（可以忽略，配置原因：测试网络通畅性）见图 2-3-28-8，新建地址（内部地址组），创建完毕方便在策略中调用。

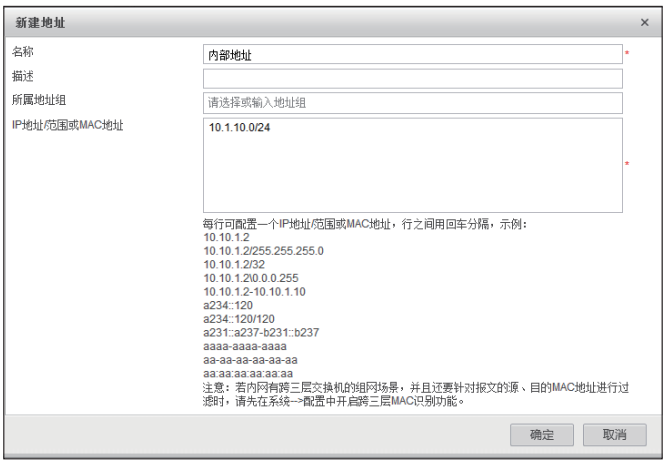


图2-3-28-8　新建地址

图 2-3-28-9 是创建 NAT 策略。源地址直接调用图 2-3-28-7 新建地址组。

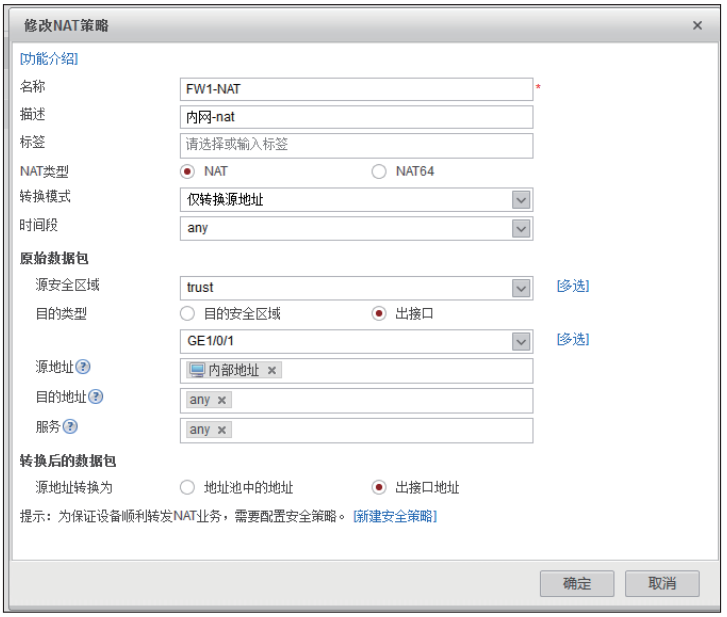


图2-3-28-9　创建NAT策略（配置内容按照图中填写）

图 2-3-28-10，是查询新建的 NAT 策略。

图2-3-28-10　查询新建的NAT策略

网络测试

PC1（IP：10.1.10.1）-ping-FW2 - 通，见图 2-3-28-11。

```
PC>ping 70.10.10.1

Ping 70.10.10.1: 32 data bytes, Press Ctrl_C to break
From 70.10.10.1: bytes=32 seq=1 ttl=251 time=32 ms
From 70.10.10.1: bytes=32 seq=2 ttl=251 time=15 ms
From 70.10.10.1: bytes=32 seq=3 ttl=251 time=32 ms
From 70.10.10.1: bytes=32 seq=4 ttl=251 time=31 ms
From 70.10.10.1: bytes=32 seq=5 ttl=251 time=15 ms

--- 70.10.10.1 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 15/25/32 ms

PC>
```

图2-3-28-11　网络测试

查询防火墙 FW1-NAT 会话转换信息，见图 2-3-28-12。

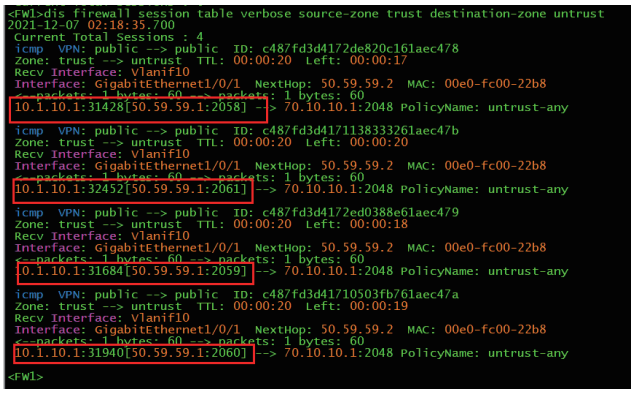


图2-3-28-12　防火墙FW1-NAT会话转换信息

步骤 3　FW2 内网地址配置。

```
[FW2]vlan 80
Info: This operation may take a few seconds. Please wait for a moment...done.
[FW2-vlan80]quit
[FW2]interface Vlanif 80
[FW2-Vlanif80]ip ad
[FW2-Vlanif80]ip address 10.2.80.254 24
[FW2-Vlanif80]service-manage ping permit
[FW2-Vlanif80]quit
[FW2]firewall zone trust
[FW2-zone-trust]add interface Vlanif 80
[FW2-zone-trust]quit
[FW2]interface  GigabitEthernet 1/0/0
[FW2-GigabitEthernet1/0/0]portswitch
[FW2-GigabitEthernet1/0/0]port link-type access
[FW2-GigabitEthernet1/0/0]port default vlan 80
[FW2-GigabitEthernet1/0/0]quit
[FW2]quit
<FW2>save
```

步骤 4　FW2 防火墙 NAT 转换功能配置（可以忽略，配置原因：测试网络通畅性）。新建地址，见图 2-3-28-13。

图2-3-28-13　新建地址

新建 NAT 策略，见图 2-3-28-14。

图2-3-28-14　新建NAT策略（按照图中内容配置）

```
PC2（IP：10.2.80.1）-ping-FW1-通
PC>ping 50.59.59.1
Ping 50.59.59.1: 32 data bytes, Press Ctrl_C to break
From 50.59.59.1: bytes=32 seq=1 ttl=251 time=31 ms
……省略……
--- 50.59.59.1 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 16/25/31 ms
```

查询 FW2 防火墙 NAT 转换信息，如图 2-3-28-15 所示。

```
[FW2]dis firewall session table verbose source-zone trust destination-zone untru
st
2021-12-07 02:29:40.490
 Current Total Sessions : 5
 icmp  VPN: public --> public  ID: c487f913633e790232761aec70f
 Zone: trust --> untrust  TTL: 00:00:20  Left: 00:00:16
 Recv Interface: Vlanif80
 Interface: GigabitEthernet1/0/1  NextHop: 70.10.10.2  MAC: 00e0-fcaf-223c
 <--packets: 1 bytes: 60 --> packets: 1 bytes: 60
 10.2.80.1:4807[70.10.10.1:2056] --> 50.59.59.1:2048 PolicyName: untrust-any

 icmp  VPN: public --> public  ID: c487f913633e6a8237961aec70e
 Zone: trust --> untrust  TTL: 00:00:20  Left: 00:00:15
 Recv Interface: Vlanif80
 Interface: GigabitEthernet1/0/1  NextHop: 70.10.10.2  MAC: 00e0-fcaf-223c
 <--packets: 1 bytes: 60 --> packets: 1 bytes: 60
 10.2.80.1:4551[70.10.10.1:2055] --> 50.59.59.1:2048 PolicyName: untrust-any

 icmp  VPN: public --> public  ID: c487f913633e4d835cc61aec70c
 Zone: trust --> untrust  TTL: 00:00:20  Left: 00:00:13
 Recv Interface: Vlanif80
 Interface: GigabitEthernet1/0/1  NextHop: 70.10.10.2  MAC: 00e0-fcaf-223c
 <--packets: 1 bytes: 60 --> packets: 1 bytes: 60
 10.2.80.1:4039[70.10.10.1:2053] --> 50.59.59.1:2048 PolicyName: untrust-any

 icmp  VPN: public --> public  ID: c487f913633e5c0374161aec70d
 Zone: trust --> untrust  TTL: 00:00:20  Left: 00:00:14
 Recv Interface: Vlanif80
 Interface: GigabitEthernet1/0/1  NextHop: 70.10.10.2  MAC: 00e0-fcaf-223c
 <--packets: 1 bytes: 60 --> packets: 1 bytes: 60
 10.2.80.1:4295[70.10.10.1:2054] --> 50.59.59.1:2048 PolicyName: untrust-any

 icmp  VPN: public --> public  ID: c487f913633e8783b6a61aec710
 Zone: trust --> untrust  TTL: 00:00:20  Left: 00:00:17
 Recv Interface: Vlanif80
 Interface: GigabitEthernet1/0/1  NextHop: 70.10.10.2  MAC: 00e0-fcaf-223c
 <--packets: 1 bytes: 60 --> packets: 1 bytes: 60
 10.2.80.1:5063[70.10.10.1:2057] --> 50.59.59.1:2048 PolicyName: untrust-any
```

图2-3-28-15　FW2防火墙NAT转换信息

将原来配置 NAT 策略禁止，进行 IPSec 配置。因为内网 NAT 转换权限高于 VPN 协议，内网流量将 NAT 转换后，无法进入 VPN 隧道（可以自行查阅防火墙相关资料，考虑 NAT 穿越技术实现与 NAT 策略共存）。

四、防火墙 IPSec-VPN 配置，实现两个内网之间网络互通

在未配置之前测试内网之间是不通的。PC1（IP：10.1.10.1）-ping-PC2(10.2.80.1)- 不通，如图 2-3-28-16 所示。

PC2（IP：10.2.80.1）-ping-PC1(10.1.10.1)- 不通，见图 2-3-28-17。

```
PC>ping 10.2.80.1

Ping 10.2.80.1: 32 data bytes, Press Ctrl_C to break
Request timeout!
Request timeout!
Request timeout!
Request timeout!
Request timeout!

--- 10.2.80.1 ping statistics ---
  5 packet(s) transmitted
  0 packet(s) received
  100.00% packet loss

PC>
```

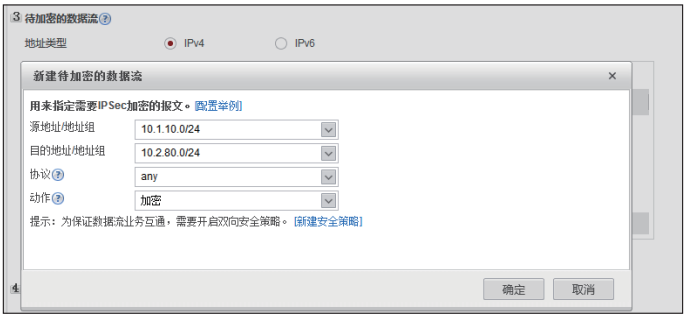
图2-3-28-16　网络测试（一）

```
PC>ping 10.1.10.1

Ping 10.1.10.1: 32 data bytes, Press Ctrl_C to break
Request timeout!
Request timeout!
Request timeout!
Request timeout!
Request timeout!

--- 10.1.10.1 ping statistics ---
  5 packet(s) transmitted
  0 packet(s) received
  100.00% packet loss

PC>
```

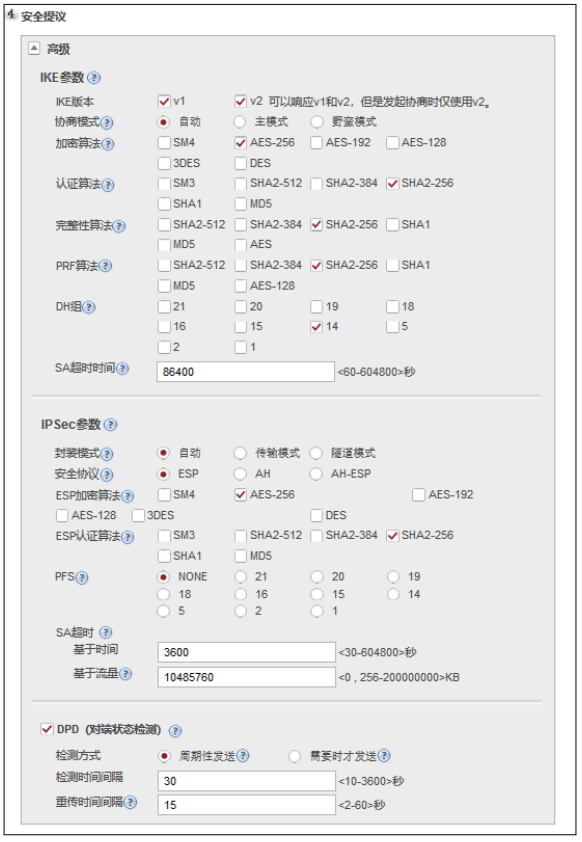
图2-3-28-17　网络测试（二）

步骤 1　FW1 防火墙 IPSec 配置（预共享密钥：a123456789），如图 2-3-28-18 所示。

(a)



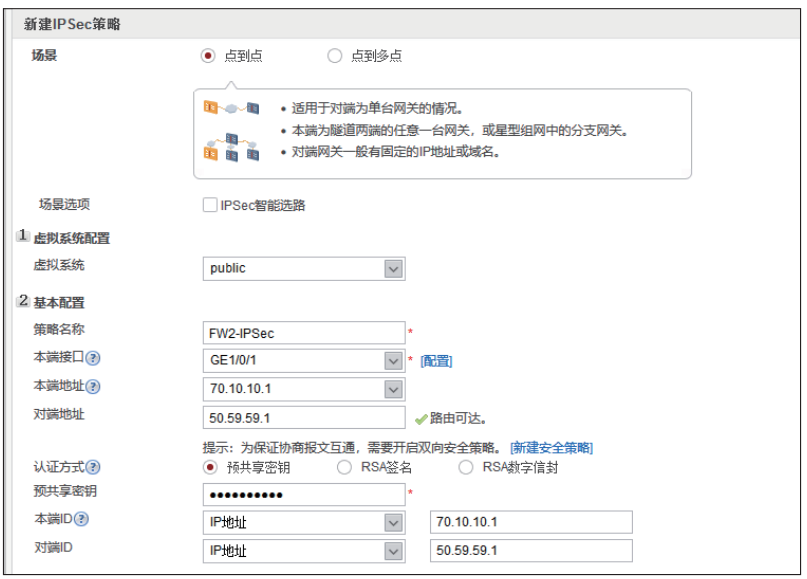
(b)



(c)

图2-3-28-18　FW1防火墙IPSec配置

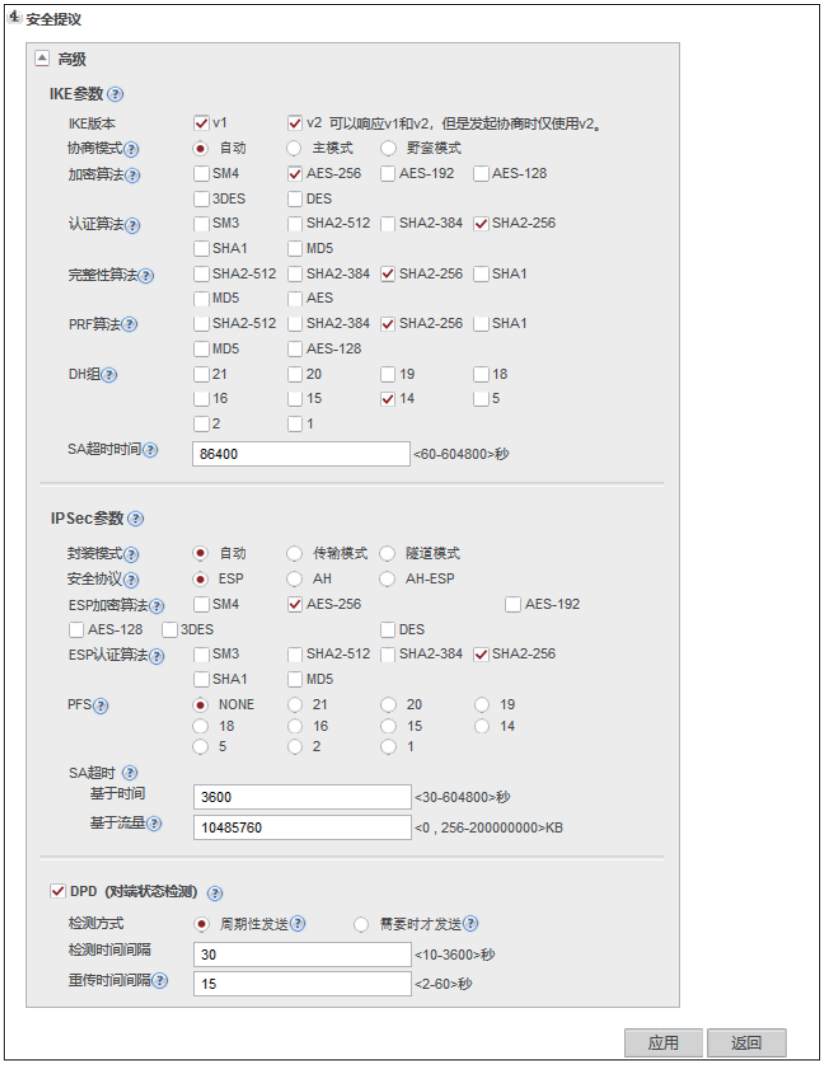
步骤 2　FW2 防火墙 IPSec 配置，见图 2-3-28-19



(a)

图2-3-28-19

(b)



(c)

图2-3-28-19　FW2防火墙IPSec配置

步骤 3　在安全策略中放通流量。

FW1(在生产中，要根据服务类型进行相关流量放通) 安全策略允许流量通过，如图 2-3-28-20 所示。

图2-3-28-20　FW1安全策略允许流量通过

FW2(在生产中，要根据服务类型进行相关流量放通) 安全策略允许流量通过，如图 2-3-28-21 所示。

图2-3-28-21　FW2安全策略允许流量通过

步骤 4　查看协商状态。

FW1 防火墙协商“成功”，如图 2-3-28-22 所示。

图2-3-28-22　FW1防火墙协商“成功”

FW2 防火墙协商“成功”，如图 2-3-28-23 所示。

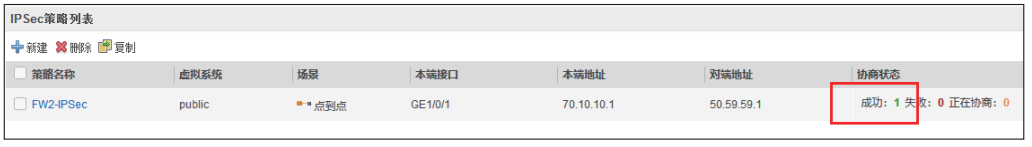


图2-3-28-23　FW2防火墙协商“成功”

网络测试

测试 PC1（IP：10.1.10.1）-ping-PC2（10.2.80.1）- 通，如图 2-3-28-24 所示。

测试 PC2（10.2.80.1）-ping- PC1（IP：10.1.10.1）- 通，如图 2-3-28-25 所示。

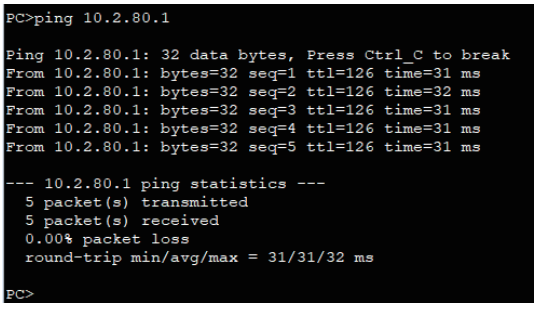


图2-3-28-24　网络测试（一）

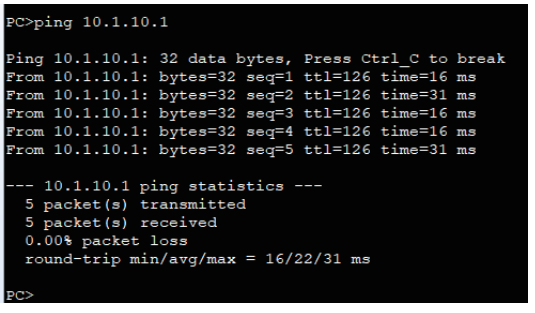


图2-3-28-25　网络测试（二）