

## 403 Forbidden

本电子书由CyberArticle制作。点击[这里](#)下载CyberArticle。注册版本不会显示该信息。[删除广告](#)

本电子书由CyberArticle制作。点击[这里](#)下载CyberArticle。注册版本不会显示该信息。[删除广告](#)

**防火墙和ERG2采用公网固定地址方式搭建IPSEC VPN配置案例（主模式命令行配置、NAQ保活VPN隧道）**

### 目录

[防火墙和ERG2采用公网固定地址方式搭建IPSEC VPN配置案例（主模式命令行配置、NAQ保活VPN隧道）](#)

#### [1 配置需求及说明](#)

[1.1 适用的产品系列](#)

[1.2 配置需求及实现的效果](#)

#### [2 组网图](#)

#### [3 配置步骤](#)

[3.1 防火墙和ERG2路由器上网配置](#)

[3.2 总部侧创建IPSEC兴趣流匹配到分部的数据](#)

[3.3 总部侧创建IPSEC安全提议](#)

[3.4 总部侧创建IKE安全提议](#)

[3.5 总部侧创建IKE安全密钥](#)

[3.6 总部侧创建IKE安全框架](#)

[3.7 配置全局IKE DPD功能](#)

[3.8 总部侧创建IPSEC安全策略](#)

[3.9 总部侧外网接口调用IPSEC策略和NAT动态转换策略](#)

[3.10 总部侧安全策略配置](#)

[3.11 配置NQA，用于保活IPSEC VPN隧道。](#)

[3.12 分部创建IPSEC虚接口](#)

[3.13 分部创建IKE安全提议](#)

- [3.14 分部创建IKE对等体](#)
- [3.15 分部创建IPSEC安全提议](#)
- [3.16 分部创建IPSEC 安全策略](#)
- [3.17 启用IPSEC安全策略功能](#)
- [3.18 分部创建去往总部的静态路由](#)
- [3.19 隧道验证](#)

## 1 配置需求及说明

### 1.1 适用的产品系列

本案例适用于软件平台为Comware V7系列防火墙：F100-X-G2、F1000-X-G2、F100-X-WiNet、F1000-AK、F10X0等；EGG2系列路由器：ER5200G2、ER8300G2、ER3200G2等

*注：本案例是在F100-C-G2的Version 7.1.064, Release 9510P08版本上进行配置和验证的。*

### 1.2 配置需求及实现的效果

分部是台ER5200G2路由器，总部有一台防火墙部署在互联网出口，因业务需要两端内网需要通过VPN相互访问。IP地址及接口规划如下表所示：

公司名称	外网接口	公网地址/掩码	公网网关	内网接口	内网地址/掩码
总部	1/0/3	101.88.26.34/30	101.88.26.33	1/0/3	192.168.10.0/24
分部	Wan1	198.76.26.90/30	198.76.26.89	Lan1	192.168.20.0/24

## 2 组网图



### 3 配置步骤

#### 3.1 防火墙和ERG2路由器上网配置

防火墙上网配置请参考“2.3.2 防火墙外网使用固定IP地址上网配置方法”进行配置，本文只针对IPSEC VPN配置进行介绍。

ERG2路由器上网配置请参考“2.2.2 路由器使用静态地址方式上网配置方法”进行配置，本文只针对IPSEC VPN配置进行介绍。

#### 3.2 总部侧创建IPSEC兴趣流匹配到分部的数据

#创建IPSEC的感兴趣流，用于匹配IPSEC数据。

```

<H3C>system-view
[H3C]acl advanced 3999
[H3C-acl-ipv4-adv-3999]rule permit ip source
192.168.10.0 0.0.0.255 destination 192.168.20.0
0.0.0.255
[H3C-acl-ipv4-adv-3999]quit
  
```

#创建acl 3888调用在外网接口用于排除IPSEC兴趣流不做NAT。

```

[H3C]acl advanced 3888
[H3C-acl-ipv4-adv-3888]rule deny ip source
192.168.10.0 0.0.0.255 destination 192.168.20.0
0.0.0.255
[H3C-acl-ipv4-adv-3888]rule permit ip source any
[H3C-acl-ipv4-adv-3888]quit
  
```

### 3.3 总部侧创建IPSEC安全提议

#加密类型设置为aes-cbc-128，认证类型设置为sha1。

```
[H3C]ipsec transform-set 1
[H3C-ipsec-transform-set-1]esp encryption-algorithm
aes-cbc-128
[H3C-ipsec-transform-set-1]esp authentication-
algorithm sha1
[H3C-ipsec-transform-set-1]quit
```

### 3.4 总部侧创建IKE安全提议

#IKE安全提议默认的认证类型为sha1，加密类型为DES-CBC，DH组为DH1，所以不需要配置也存在这些参数。

```
[H3C]ike proposal 1
[H3C-ike-proposal-1]quit
```

### 3.5 总部侧创建IKE安全密钥

#创建IKE密钥，地址填写分部侧设备的公网IP，密码设置为123456。

```
[H3C]ike keychain 1
[H3C-ike-keychain-1]pre-shared-key address
198.76.26.90 key simple 123456
[H3C-ike-keychain-1]quit
```

### 3.6 总部侧创建IKE安全框架

#创建IKE安全框架，将本端地址、对端地址、keychain、proposal关联起来。

```
[H3C]ike profile 1
[H3C-ike-profile-1]keychain 1
[H3C-ike-profile-1]local-identity address
101.88.26.34
[H3C-ike-profile-1]match remote identity address
198.76.26.90
[H3C-ike-profile-1]proposal 1
[H3C-ike-profile-1]quit
```

### 3.7 配置全局IKE DPD功能

#创建ike dpd，IKE SA协商成功之后10秒本端会发送DPD探测报文，并等待接收DPD回应报文。若本端在10秒内没有收到DPD回应报文，则会第二次发送DPD探测报文。在此过程中总共会发送三次DPD探测报文，若第三次DPD探测报文发出后10秒仍没收到DPD回应报文，则会删除发送DPD探测报文的IKE SA及其对应的所有IPsec SA。若在此过程中收到了DPD回应报文，则会等待10秒再次发送DPD探测报文

```
[H3C]ike dpd interval 10 retry 10 periodic
```

### 3.8 总部侧创建IPSEC安全策略

#创建IKE安全策略GE1/0/3将transform-set、acl、ike-profile、本端地址、对端地址关联起来。

```
[H3C]ipsec policy GE1/0/3 1 isakmp
[H3C-ipsec-policy-isakmp-GE1/0/3-1]transform-set 1
[H3C-ipsec-policy-isakmp-GE1/0/3-1]security acl 3999
[H3C-ipsec-policy-isakmp-GE1/0/3-1]local-address 101.88.26.34
[H3C-ipsec-policy-isakmp-GE1/0/3-1]remote-address 198.76.26.90
[H3C-ipsec-policy-isakmp-GE1/0/3-1]ike-profile 1
[H3C-ipsec-policy-isakmp-GE1/0/3-1]quit
```

### 3.9 总部侧外网接口调用IPSEC策略和NAT动态转换策略

```
[H3C]interface GigabitEthernet 1/0/3
[H3C-GigabitEthernet1/0/3]ipsec apply policy GE1/0/3
[H3C-GigabitEthernet1/0/3]nat outbound 3888
[H3C-GigabitEthernet1/0/3]quit
```

### 3.10 总部侧安全策略配置

防火墙目前版本存在两套安全策略，请在放通安全策略前确认设备运行那种类型的安全策略？以下配置任选其一。

1. 通过命令“display cu | in security-policy”如果查到命令行存在“security-policy disable”或者没有查到任何信息，则使用下面策略配置。

总部侧配置安全策略放通IPSEC数据

#创建对象组，组名称为192.168.10.0

```
[H3C]object-group ip address 192.168.10.0
[H3C-obj-grp-ip-192.168.10.0]0 network subnet
```

```
192.168.10.0 255.255.255.0
[H3C-obj-grp-ip-192.168.10.0]quit
#创建对象组，名称为192.168.20.0
[H3C]object-group ip address 192.168.20.0
[H3C-obj-grp-ip-192.168.20.0]0      network      subnet
192.168.20.0 255.255.255.0
[H3C-obj-grp-ip-192.168.20.0]quit
```

#创建对象策略，策略名称为Untrust-Trust

```
[H3C]object-policy ip Untrust-Trust
[H3C-object-policy-ip- Untrust-Trust] rule 0 pass
source-ip 192.168.20.0 destination-ip 192.168.10.0
[H3C-object-policy-ip- Untrust-Trust]quit
```

#创建Untrust到Trust域的域间策略调用Untrust-Trust策略

```
[H3C]zone-pair security source Untrust destination
Trust
[H3C-zone-pair-security-Untrust-Trust]object-policy
apply ip Untrust-Trust
[H3C-zone-pair-security-Untrust-Trust]quit
```

总部侧配置安全策略，放通Untrust到Local，以及Local到Utrust的策略，用于建立IPSEC 隧道

#创建对象策略，策略名称为Untrust-Local

```
[H3C]object-policy ip Untrust-Local
[H3C-object-policy-ip-Untrust-Local] rule 0 pass
[H3C-object-policy-ip-Untrust-Local]quit
```

#创建Untrust到Local域的域间策略调用Untrust- Local策略

```
[H3C]zone-pair security source Untrust destination
Local
[H3C-zone-pair-security-Untrust-Local]object-policy
apply ip Untrust-Local
[H3C-zone-pair-security-Untrust-Local]quit
```

#创建对象策略，策略名称为Local-Untrust

```
[H3C]object-policy ip Local-Untrust
[H3C-object-policy-ip-Local-Untrust] rule 0 pass
[H3C-object-policy-ip-Local-Untrust]quit
```

#创建Local到Untrust域的域间策略调用Local-Untrust策略

```
[H3C]zone-pair security source Local destination
Untrust
```

```
[H3C-zone-pair-security-Local-Untrust]object-policy
apply ip Local-Untrust
[H3C-zone-pair-security-Local-Untrust]quit
```

2. 通过命令“display cu | in security-policy”如果查到命令行存在“security-policy ip”并且没有查到“security-policy disable”，则使用下面策略配置。

```
[H3C]display cu | in security-policy
security-policy ip
```

#创建对象组，组名称为192.168.10.0

```
[H3C]object-group ip address 192.168.10.0
[H3C-obj-grp-ip-192.168.10.0]0      network      subnet
192.168.10.0 255.255.255.0
[H3C-obj-grp-ip-192.168.10.0]quit
```

#创建对象组，名称为192.168.20.0

```
[H3C]object-group ip address 192.168.20.0
[H3C-obj-grp-ip-192.168.20.0]0      network      subnet
192.168.20.0 255.255.255.0
[H3C-obj-grp-ip-192.168.20.0]quit
```

#进入安全策略视图

```
[H3C]security-policy ip
```

#创建rule10，放通ipsec感兴趣流

```
[H3C-security-policy-ip]rule 10 name ipsec
[H3C-security-policy-ip-10-ipsec]source-zone
untrust
[H3C-security-policy-ip-10-ipsec]destination-zone
trust
[H3C-security-policy-ip-10-ipsec]source-ip
192.168.20.0
[H3C-security-policy-ip-10-ipsec]destination-ip
192.168.10.0
[H3C-security-policy-ip-10-ipsec]quit
```

#创建rule20，放通local和untrust之间的流量

```
[H3C-security-policy-ip]rule 20 name local-untrust
[H3C-security-policy-ip-20-local-untrust]source-
zone untrust
[H3C-security-policy-ip-20-local-untrust]source-
zone local
[H3C-security-policy-ip-20-local-untrust]
destination-zone untrust
```

```
[H3C-security-policy-ip-20-local-untrust]
destination-zone local
[H3C-security-policy-ip-20-local-untrust]quit
[H3C-security-policy-ip]quit
```

### 3.11 配置NQA，用于保活IPSEC VPN隧道。

创建ICMP-echo类型的NQA测试组（管理员为admin，操作标签为test1），并配置探测报文的目的地址为分部ERG2内网的ip: 192.168.20.1，源ip是总部内网的ip: 192.168.10.1。

```
<H3C> system-view
[H3C] nqa entry admin test1
[H3C-nqa-admin-test1] type icmp-echo
[H3C-nqa-admin-test1-icmp-echo] destination ip
192.168.20.1
[H3C-nqa-admin-test1-icmp-echo] source ip
192.168.10.1
```

# 配置下一跳地址为101.88.26.33，以便测试报文使用ipsec vpn隧道发给分部设备。

```
[H3C-nqa-admin-test1-icmp-echo] next-hop ip
101.88.26.33
```

# 配置可选参数：一次NQA测试中探测的次数为10，探测的超时时间为500毫秒，测试组连续两次测试开始时间的时间间隔为5000毫秒。

```
[H3C-nqa-admin-test1-icmp-echo] probe count 10
[H3C-nqa-admin-test1-icmp-echo] probe timeout 500
[H3C-nqa-admin-test1-icmp-echo] frequency 5000
```

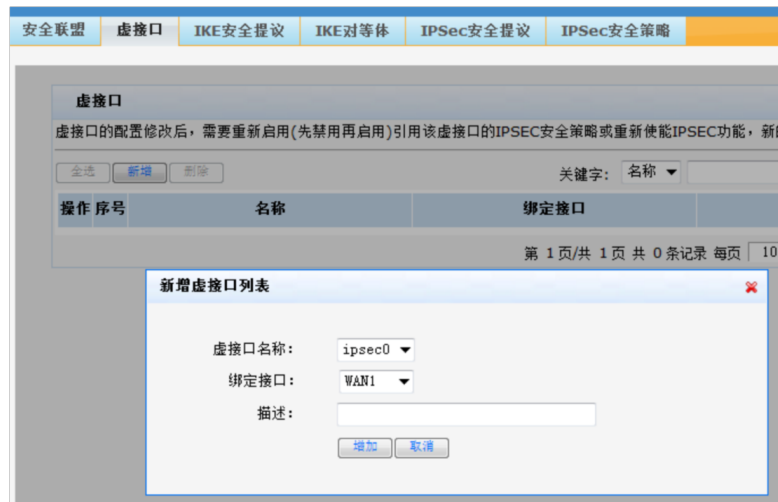
# 启动ICMP-echo测试操作，并一直进行测试。

```
[H3C] nqa schedule admin test1 start-time now
lifetime forever
```

### 3.12 分部创建IPSEC虚接口

#在“VPN” > “IPSEC VPN” > “虚接口”中点击新建，绑定到外网接口WAN1





### 3.13 分部创建IKE安全提议

#在“VPN” > “IPSEC VPN” > “IKE安全提议” 中点击新建  
IKE安全提议的认证类型为SHA1，加密类型为DES，DH组为DH1。



### 3.14 分部创建IKE对等体

#在“VPN” > “IPSEC VPN” > “IKE对等体” 中点击新建  
对端地址选择总部公网IP，选择配置好的IKE安全提议，使用主模式，  
输入IKE 预共享密钥，开启DPD，和总部进行匹配。

安全联盟 虚接口 IKE安全提议 IKE对等体 IPsec安全提议 IPsec安全策略

关键字: 名称 查询

操作	序号	名称	虚接口	对端地址	模式	ID类型
第 1 页/共 1 页 共 0 条记录 每页 10						

**新增IKE对等体**

对等体名称: peer (范围:1~16个字符)

虚接口: ipsec0

对端地址: 101.88.26.34 (IP 或 域名)

协商模式: ☒ 主模式 ☐ 野蛮模式

安全提议一: tiyi

安全提议二: 请选择

安全提议三: 请选择

安全提议四: 请选择

预共享密钥(PSK): 123456 (范围:1~128个字符)

生命周期: 28800 秒(范围:60~604800秒, 缺省值:28800)

DPD: ☒ 开启 ☐ 关闭

DPD周期: 10 秒(范围:1~60秒, 缺省值:10)

DPD超时时间: 30 秒(范围:1~300秒, 缺省值:30)

增加 取消

### 3.15 分部创建IPSEC安全提议

#在“VPN” > “IPSEC VPN” > “IPSEC安全提议” 中点击新建  
#加密类型设置为aes128，认证类型设置为sha1。

安全联盟 虚接口 IKE安全提议 IKE对等体 IPsec安全提议 IPsec安全策略

安全提议

安全提议的配置修改后，需要重新启用(先禁用再启用)引用该安全提议的IPsec安全策略或重新使能IPsec功能，新

关键字: 名称 查询

操作	序号	名称	安全协议	AH算法
第 1 页/共 1 页 共 0 条记录 每页 10 行				

**新增IPSEC安全提议**

安全提议名称: esp (范围:1~31个字符)

安全协议类型: ☐ AH ☒ ESP ☐ AH+ESP

ESP验证算法: SHA1

ESP加密算法: AES128

增加 取消

### 3.16 分部创建IPSEC 安全策略

#在“VPN”>“IPSEC VPN”>“IPSEC 安全策略”中点击新建  
本端子网IP为本端需要走VPN的内网地址，对端子网为总部需要走VPN的地址，调用之前创建的IKE对等体和IPSEC的安全提议。

新增IPSEC安全策略

安全策略名称: ipsec (范围:1~16个字符)

是否启用: 启用

本地子网IP/掩码: 192.168.20.0 / 255.255.255.0

对端子网IP/掩码: 192.168.10.1 / 255.255.255.0

协商类型: ☒ IKE协商 ☐ 手动模式

对等体: peer

安全提议一: esp

安全提议二: 请选择

安全提议三: 请选择

安全提议四: 请选择

PFS: 禁止

生命周期: 28800 秒 (范围:120~604800, 缺省值:28800)

触发模式: 流量触发

增加 取消

### 3.17 启用IPSEC安全策略功能

IPSec设置

☒ 启用IPSec功能

应用

### 3.18 分部创建去往总部的静态路由

#在“高级设置”>“路由设置”>“静态路由”中点击新建  
新增一条静态路由。目的地址为对端的VPN网段。出接口选择IPSEC虚接口。

### 3.19 隧道验证

V7防火墙侧:

通过命令行查看display ike sa可以看到隧道状态为RD状态表示ike建立完成。

```
[H3C]dis ike sa
Connection-ID  Remote      Flag      DOI
-----
29             198.76.26.90  RD        IPsec
Flags:
RD--READY RL--REPLACED FD--FADING RK--REKEY
```

#V7防火墙通过display ipsec sa可以看到IPSEC SA基本状态。

```
[H3C]dis ipsec sa

-----
Interface: GigabitEthernet1/0/3
-----

IPsec policy: GE1/0/3
Sequence number: 1
Mode: Template
-----

Tunnel id: 0
Encapsulation mode: tunnel
Perfect Forward Secrecy:
Inside VPN:
Extended Sequence Numbers enable: N
Traffic Flow Confidentiality enable: N
Path MTU: 1444
Tunnel:
    local address: 101.88.26.34
    remote address: 198.76.26.90
Flow:
    sour addr: 192.168.10.0/255.255.255.0 port: 0 protocol: ip
    dest addr: 192.168.20.0/255.255.255.0 port: 0 protocol: ip

[Inbound ESP SAs]
SPI: 4032357769 (0xf058e589)
Connection ID: 158913789952
Transform set: ESP-ENCRYPT-3DES-CBC ESP-AUTH-SHA1
SA duration (kilobytes/sec): 1843200/3600
SA remaining duration (kilobytes/sec): 1843199/3545
Max received sequence-number: 8
Anti-replay check enable: Y
Anti-replay window size: 64
UDP encapsulation used for NAT traversal: N
Status: Active

[Outbound ESP SAs]
SPI: 1786751150 (0x6a7fa8ae)
Connection ID: 64424509441
Transform set: ESP-ENCRYPT-3DES-CBC ESP-AUTH-SHA1
SA duration (kilobytes/sec): 1843200/3600
SA remaining duration (kilobytes/sec): 1843199/3545
Max sent sequence-number: 8
UDP encapsulation used for NAT traversal: N
Status: Active
```

## ERG2侧:

在【VPN】--【VPN设置】--【IPSec安全策略】--【安全联盟】里查看隧道建立情况

安全联盟

虚接口

IKE安全提议

IKE对等体

IPSec安全提议

IPSec安全策略

安全联盟SA

通过安全联盟SA，IPSec能够对不同的数据流提供不同级别的安全保护。在这里可以查询到相应隧道的当前状态，了解隧道建立的各种参数。

刷新

名称	方向	隧道两端	AH SPI	AH 算法	ESP SPI	ESP 算法	数据流
ipsec	in	101.88.26.34 =>198.76.26.90	----	----	0x6a7fa8ae	3DES_SHA1	192.168.10.0/24 =>192.168.20.0/24
ipsec	out	198.76.26.90 =>101.88.26.34	----	----	0xf058e589	3DES_SHA1	192.168.20.0/24 =>192.168.10.0/24

第 1 页 / 共 1 页 共 2 条记录 每页 10

