

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](#)

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](#)

V7平台防火墙GRE VPN配置案例 （命令行）

目录

[V7平台防火墙GRE VPN配置案例（命令行）](#)

[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 总部侧防火墙基本网络配置](#)

[3.1.1 设置总部侧外网接口地址](#)

[3.1.2 设置总部侧内网接口地址](#)

[3.1.3 设置总部侧到公网路由](#)

[3.2 总部侧GRE VPN配置](#)

[3.2.1 新建Tunnel 0隧道接口](#)

[3.2.2 新建到tunnel接口的明细路由](#)

- [3.3 总部侧安全策略配置](#)
 - [3.3.1 将外网、内网、tunnel接口加入对应安全](#)
 - [3.3.2 放通安全策略使数据通信正常](#)
- [3.4 结果测试](#)
- [3.5 保存配置](#)

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。

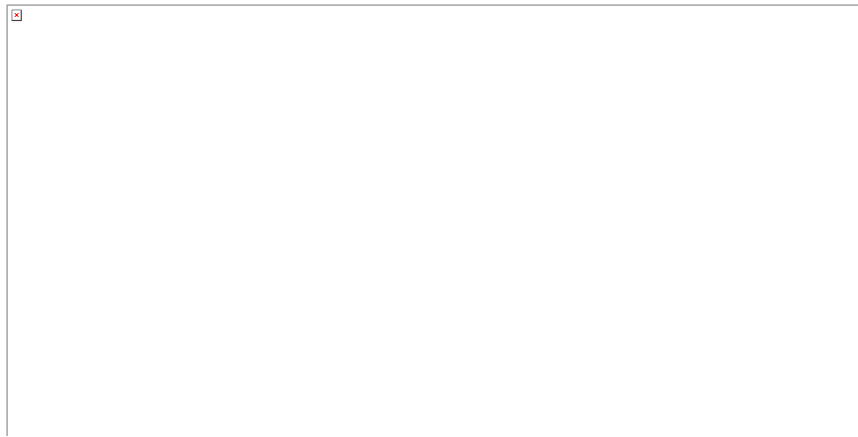
注：本案例是在F100-C-G2的Version 7.1.064, Release 9510P08版本上进行配置和验证的。

1.2 配置需求及实现的效果

总部和分部各有一台防火墙部署在互联网出口，因业务需要两端内网业务需要通过GRE 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	1/0/4	192.168.10.0/24
分部	1/0/3	198.76.26.90/30	198.76.26.89	1/0/4	192.168.20.0/24

2 组网图



3 配置步骤

3.1 总部侧防火墙基本网络配置

3.1.1 设置总部侧外网接口地址

#输入命令“system-view”进入系统视图后为1/0/3接口配置101.88.26.34/30的地址，并配置nat地址转换。

```
<H3C>system-view
[H3C]interface GigabitEthernet 1/0/3
[H3C-GigabitEthernet1/0/3]ip address 101.88.26.34
255.255.255.252
[H3C-GigabitEthernet1/0/3]nat outbound
[H3C-GigabitEthernet1/0/3]quit
```

3.1.2 设置总部侧内网接口地址

#在1/0/4接口配置连接内网地址192.168.10.1/24。

```
[H3C]interface GigabitEthernet 1/0/4
[H3C-GigabitEthernet1/0/4]ip address 192.168.10.1 255.255.255.0
[H3C-GigabitEthernet1/0/4]quit
```

3.1.3 设置总部侧到公网路由

#配置默认路由目的地址及掩码为0.0.0.0、下一跳（网关）地址为

101.88.26.33。

```
[H3C]ip route-static 0.0.0.0 0 101.88.26.33
```

3.2 总部侧GRE VPN配置

3.2.1 新建Tunnel 0隧道接口

#新建Tunnel 0隧道接口，并配置IP地址为1.1.1.1/24，指定Tunnel 0接口源地址与目的地址分别对应总部分支侧的公网地址。

```
[H3C]interface Tunnel 0 mode gre
[H3C-Tunnel0]ip address 1.1.1.1 255.255.255.0
[H3C-Tunnel0]source 101.88.26.34
[H3C-Tunnel0]destination 198.76.26.90
[H3C-Tunnel0]quit
```

3.2.2 新建到tunnel接口的明细路由

#新建一条目的地址为192.168.20.0/24，下一跳（网关）地址为tunnel0接口的路由，用于匹配去往192.168.20.0/24网段的路由客户通过隧道转发。

```
[H3C]ip route-static 192.168.20.0 24 Tunnel 0
```

3.3 总部侧安全策略配置

3.3.1 将外网、内网、tunnel接口加入对应安全

#外网接口加untrust区域、内网接口、tunnel接口加入trust区域。

```
[H3C]security-zone name Untrust
[H3C-security-zone-Untrust]import interface GigabitEthernet 1/0/3
[H3C-security-zone-Untrust]quit
[H3C]security-zone name Trust
[H3C-security-zone-Trust]import interface GigabitEthernet 1/0/4
[H3C-security-zone-Trust]import interface Tunnel 0
[H3C-security-zone-Trust]quit
```

3.3.2 放通安全策略使数据通信正常

1. 放通trust到untrust、local的安全策略，使内网用户访问网络的同时

能管理防火墙设备。

```
[H3C]security-policy ip
[H3C-security-policy-ip]rule 5 name trust-untrust、 local
[H3C-security-policy-ip-5-trust-untrust、 local]action pass
[H3C-security-policy-ip-5-trust-untrust、 local]source-zone trust
[H3C-security-policy-ip-5-trust-untrust、 local]destination-zone
untrust
[H3C-security-policy-ip-5-trust-untrust、 local]destination-zone local
[H3C-security-policy-ip-5-trust-untrust、 local]quit
[H3C-security-policy-ip]quit
```

2. 放通untrust到trust目的地址为192.168.20.0/24网段到

192.168.10.0/24网段的数据

#新建IPV4地址对象组分部网段与总部网段分别对应192.168.20.0/24与192.168.10.0/24网段。

```
[H3C]object-group ip address 分部网段
[H3C-obj-grp-ip-分部网段]0 network subnet 192.168.20.0
255.255.255.0
[H3C-obj-grp-ip-分部网段]quit
[H3C]object-group ip address 总部网段
[H3C-obj-grp-ip-总部网段]0 network subnet 192.168.10.0
255.255.255.0
[H3C-obj-grp-ip-总部网段]quit
```

#新建IPV4地址对象组

```
[H3C]security-policy ip
[H3C-security-policy-ip]rule 10 name untrust-trust
[H3C-security-policy-ip-10-untrust-trust]action pass
[H3C-security-policy-ip-10-untrust-trust]source-zone untrust
[H3C-security-policy-ip-10-untrust-trust]destination-zone trust
[H3C-security-policy-ip-10-untrust-trust]source-ip分部网段
```

```
[H3C-security-policy-ip-10-untrust-trust]destination-ip总部网段
[H3C-security-policy-ip-10-untrust-trust]quit
[H3C-security-policy-ip]quit
#放通同安全域间的安全策略
[H3C]security-zone intra-zone default permit
```

3.4 分部侧防火墙GRE配置

分部防火墙与总部侧防火墙配置方法一致。

3.5 结果测试

#使用总部侧PC机PING测试分部侧PC机测试：

可以看到在总部侧访问分部数据可达，并且通过“display interface Tunnel 0”可以看到收发包数量。

```
<H3C>display interface Tunnel 0
```

```
Tunnel0
```

```
Current state: UP
```

```
Line protocol state: UP
```

```
Description: Tunnel0 Interface
```

```
Bandwidth: 64 kbps
```

```
Maximum transmission unit: 1476
```

```
Internet address: 1.1.1.1/24 (primary)
```

```
Tunnel source 101.88.26.34, destination 198.76.26.90
```

```
Tunnel keepalive disabled
```

```
Tunnel TTL 255
```

```
Tunnel protocol/transport GRE/IP
```

```
GRE key disabled
```

```
Checksumming of GRE packets disabled
```

```
Last clearing of counters: Never
```

```
Last 300 seconds input rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
```

```
Last 300 seconds output rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
```

```
Input: 5 packets, 420 bytes, 0 drops
```

Output: 5 packets, 420 bytes, 0 drops

3.6 保存配置

[H3C]save f