

- [首页](#)
- [微信](#)
- [文章分类](#)
 - [华为RS/Wlan/FW](#)
 - [MySQL/MariaDB](#)
 - [Linux/Windows](#)
 - [HTML/CSS/JS](#)
 - [C/C++/Java](#)
 - [PHP/Python](#)
 - [网站/应用/技巧](#)
 - [闲谈/休闲/随笔](#)
- [实用工具](#)
 - [云盘](#)
 - [云音乐](#)
 - [机器人·闲聊](#)
 - [影视Movie系统](#)
 - [VIP视频解析系统](#)
 - [我的『大学毕业留念册』](#)
- [关于本站](#)
 - [免责声明](#)
 - [文章归档](#)
 - [友情链接](#)
 - [网站留言](#)
- [更多功能](#)
 - [微信订阅号](#)
 - [RSS订阅](#)

1. [首页](#)
2. [华为RS/Wlan/FW](#)
3. 华为 | 配置虚拟隧道接口建立GRE over IPSec示例

2019年1月17日 0条评论

华为 | 配置虚拟隧道接口建立GRE over IPSec示例

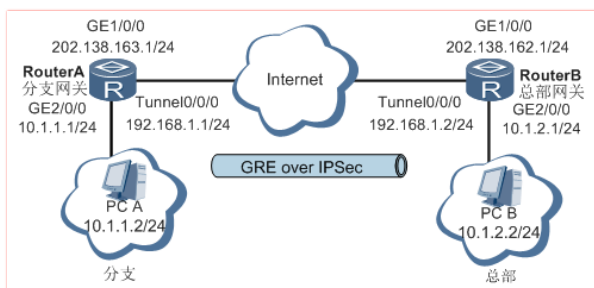
- [内容](#)
- [相关](#)

利用前面所学的知识，进行GRE over IPSec的组网。

一、组网需求

如图所示，RouterA为企业分支网关，RouterB为企业总部网关，分支与总部通过公网建立通信。

企业希望对分支与总部之间相互访问的流量（包括组播数据）进行安全保护。由于组播数据无法直接应用IPSec，所以基于虚拟隧道接口方式建立GRE over IPSec，对Tunnel接口下的流量进行保护。



二、配置思路

采用如下思路配置虚拟隧道接口建立GRE over IPSec:

- 1) 配置物理接口的IP地址和到对端的静态路由，保证两端路由可达；
- 2) 配置GRE Tunnel接口；
- 3) 配置IPSec安全提议，定义IPSec的保护方法；
- 4) 配置IKE对等体，定义对等体间IKE协商时的属性；
- 5) 配置安全框架，并引用安全提议和IKE对等体；
- 6) 在Tunnel接口上应用安全框架，使接口具有IPSec的保护功能；

7) 配置Tunnel接口的转发路由，将需要IPSec保护的数据流引到Tunnel接口。

三、操作步骤

1、分别在RouterA和RouterB上配置物理接口的IP地址和到对端的静态路由

在RouterA上配置接口的IP地址

```
<Huawei> system-view
[Huawei] sysname RouterA
[RouterA] interface gigabitethernet 1/0/0
[RouterA-GigabitEthernet1/0/0] ip address 202.138.163.1 255.255.255.0
[RouterA-GigabitEthernet1/0/0] quit
[RouterA] interface gigabitethernet 2/0/0
[RouterA-GigabitEthernet2/0/0] ip address 10.1.1.1 255.255.255.0
[RouterA-GigabitEthernet2/0/0] quit
```

在RouterA上配置到对端的静态路由，此处假设到对端的下一跳地址为202.138.163.2

```
[RouterA] ip route-static 202.138.162.0 255.255.255.0 202.138.163.2
```

在RouterB上配置接口的IP地址

```
<Huawei> system-view
[Huawei] sysname RouterB
[RouterB] interface gigabitethernet 1/0/0
[RouterB-GigabitEthernet1/0/0] ip address 202.138.162.1 255.255.255.0
[RouterB-GigabitEthernet1/0/0] quit
[RouterB] interface gigabitethernet 2/0/0
[RouterB-GigabitEthernet2/0/0] ip address 10.1.2.1 255.255.255.0
[RouterB-GigabitEthernet2/0/0] quit
```

在RouterB上配置到对端的静态路由，此处假设到对端下一跳地址为202.138.162.2

```
[RouterB] ip route-static 202.138.163.0 255.255.255.0 202.138.162.2
```

2、配置GRE Tunnel接口

配置RouterA

```
[RouterA] interface tunnel 0/0/0
[RouterA-Tunnel0/0/0] ip address 192.168.1.1 255.255.255.0
[RouterA-Tunnel0/0/0] tunnel-protocol gre
[RouterA-Tunnel0/0/0] source 202.138.163.1
[RouterA-Tunnel0/0/0] destination 202.138.162.1
[RouterA-Tunnel0/0/0] quit
```

配置RouterB

```
[RouterB] interface tunnel 0/0/0
[RouterB-Tunnel0/0/0] ip address 192.168.1.2 255.255.255.0
[RouterB-Tunnel0/0/0] tunnel-protocol gre
[RouterB-Tunnel0/0/0] source 202.138.162.1
[RouterB-Tunnel0/0/0] destination 202.138.163.1
[RouterB-Tunnel0/0/0] quit
```

3、分别在RouterA和RouterB上创建IPSec安全提议

在RouterA上配置IPSec安全提议

```
[RouterA] ipsec proposal tran1
[RouterA-ipsec-proposal-tran1] esp authentication-algorithm sha2-256
[RouterA-ipsec-proposal-tran1] esp encryption-algorithm aes-128
[RouterA-ipsec-proposal-tran1] quit
```

在RouterB上配置IPSec安全提议

```
[RouterB] ipsec proposal tran1
[RouterB-ipsec-proposal-tran1] esp authentication-algorithm sha2-256
[RouterB-ipsec-proposal-tran1] esp encryption-algorithm aes-128
[RouterB-ipsec-proposal-tran1] quit
```

4、分别在RouterA和RouterB上配置IKE对等体

在RouterA上配置IKE安全提议。

```
[RouterA] ike proposal 5
[RouterA-ike-proposal-5] authentication-algorithm sha2-256
[RouterA-ike-proposal-5] encryption-algorithm aes-cbc-128
[RouterA-ike-proposal-5] quit
```

在RouterA上配置IKE对等体

```
[RouterA] ike peer spub v2
[RouterA-ike-peer-spub] ike-proposal 5
[RouterA-ike-peer-spub] pre-shared-key cipher huawei
[RouterA-ike-peer-spub] quit
```

在RouterB上配置IKE安全提议

```
[RouterB] ike proposal 5
[RouterB-ike-proposal-5] authentication-algorithm sha2-256
[RouterB-ike-proposal-5] encryption-algorithm aes-cbc-128
[RouterB-ike-proposal-5] quit
```

在RouterB上配置IKE对等体

```
[RouterB] ike peer spua v2
[RouterB-ike-peer-spua] ike-proposal 5
[RouterB-ike-peer-spua] pre-shared-key cipher huawei
[RouterB-ike-peer-spua] quit
```

5、分别在RouterA和RouterB上创建安全框架

在RouterA上配置安全框架

```
[RouterA] ipsec profile profile1
[RouterA-ipsec-profile-profile1] proposal tran1
[RouterA-ipsec-profile-profile1] ike-peer spub
[RouterA-ipsec-profile-profile1] quit
```

在RouterB上配置安全框架

```
[RouterB] ipsec profile profile1
[RouterB-ipsec-profile-profile1] proposal tran1
```

```
[RouterB-ipsec-profile-profile1] ike-peer spua
[RouterB-ipsec-profile-profile1] quit
```

6. 分别在RouterA和RouterB的接口上应用各自的安全框架

在RouterA的接口上引用安全框架

```
[RouterA] interface tunnel 0/0/0
[RouterA-Tunnel0/0/0] ipsec profile profile1
[RouterA-Tunnel0/0/0] quit
```

在RouterB的接口上引用安全框架

```
[RouterB] interface tunnel 0/0/0
[RouterB-Tunnel0/0/0] ipsec profile profile1
[RouterB-Tunnel0/0/0] quit
```

此时在RouterA和RouterB上执行display ipsec profile会显示所配置的信息

7. 配置Tunnel接口的转发路由，将需要IPSec保护的数据流引到Tunnel接口

在RouterA上配置Tunnel接口的转发路由

```
[RouterA] ip route-static 10.1.2.0 255.255.255.0 tunnel 0/0/0
```

在RouterB上配置Tunnel接口的转发路由

```
[RouterB] ip route-static 10.1.1.0 255.255.255.0 tunnel 0/0/0
```

8. 检查配置结果

配置成功后，分别在RouterA和RouterB上执行display ike sa v2会显示所配置的信息，以RouterA为例。

```
[RouterA] display ike sa v2
Conn-ID Peer      VPN  Flag(s)      Phase
-----
  22  202.138.162.1  0   RD|ST        2
  21  202.138.162.1  0   RD|ST        1
Flag Description:
RD--READY  ST--STAYALIVE  RL--REPLACED  FD--FADING  TO--TIMEOUT
```

配置成功后，分别在RouterA和RouterB上执行display ipsec sa会显示所配置的信息，以RouterA为例。

```
[RouterA] display ipsec sa
=====
Interface: Tunnel0/0/0
Path MTU: 1500
=====
-----
IPSec profile name: "profile1"
Mode           : PROF-ISAKMP
-----
Connection ID   : 22
Encapsulation mode: Tunnel
Tunnel local    : 202.138.163.1
Tunnel remote   : 202.138.162.1
Qos pre-classify : Disable
[Outbound ESP SAs]
SPI: 1599804596 (0x5f5b14b4)
```

```
Proposal: ESP-ENCRYPT-AES-128 SHA2-256-128
SA remaining key duration (bytes/sec): 1887436800/2489
  Max sent sequence-number: 0
UDP encapsulation used for NAT traversal: N
[Inbound ESP SAs]
SPI: 2169616882 (0x8151b9f2)
Proposal: ESP-ENCRYPT-AES-128 SHA2-256-128
SA remaining key duration (bytes/sec): 1887436800/2489
  Max received sequence-number: 0
Anti-replay window size: 32
UDP encapsulation used for NAT traversal: N
```

四、配置文件


RouterA的配置文件

```
#
sysname RouterA
#
ipsec proposal tran1
  esp authentication-algorithm sha2-256
  esp encryption-algorithm aes-128
#
ike proposal 5
  encryption-algorithm aes-cbc-128
  authentication-algorithm sha2-256
#
ike peer spub v2
  pre-shared-key cipher Huawei
  ike-proposal 5
#
ipsec profile profile1
  ike-peer spub
  proposal tran1
#
interface Tunnel0/0/0
  ip address 192.168.1.1 255.255.255.0
  tunnel-protocol gre
  source 202.138.163.1
  destination 202.138.162.1
  ipsec profile profile1
#
interface GigabitEthernet1/0/0
  ip address 202.138.163.1 255.255.255.0
#
interface GigabitEthernet2/0/0
  ip address 10.1.1.1 255.255.255.0
#
ip route-static 202.138.162.0 255.255.255.0 202.138.163.2
ip route-static 10.1.2.0 255.255.255.0 tunnel0/0/0
#
return
```

RouterB的配置文件

```
#
sysname RouterB
#
ipsec proposal tran1
  esp authentication-algorithm sha2-256
  esp encryption-algorithm aes-128
#
```

```
ike proposal 5
  encryption-algorithm aes-cbc-128
  authentication-algorithm sha2-256
#
ike peer spua v2
  pre-shared-key cipher Huawei
  ike-proposal 5
#
ipsec profile profile1
  ike-peer spua
  proposal tran1
#
interface Tunnel0/0/0
  ip address 192.168.1.2 255.255.255.0
  tunnel-protocol gre
  source 202.138.162.1
  destination 202.138.163.1
  ipsec profile profile1
#
interface GigabitEthernet1/0/0
  ip address 202.138.162.1 255.255.255.0
#
interface GigabitEthernet2/0/0
  ip address 10.1.2.1 255.255.255.0
#
ip route-static 202.138.163.0 255.255.255.0 202.138.162.2
ip route-static 10.1.1.0 255.255.255.0 tunnel0/0/0
#
return
```

 您阅读这篇文章共花了：0小时00分03秒

赞 (5) [打赏](#) [分享](#)

-
-
-



• [支付宝扫一扫](#)



•
微信扫一扫



•
企鹅扫一扫

上一篇: [华为 | IPSEC Over GRE与GRE Over IPSEC区别比较](#)

下一篇: [华为 | Snmp的基本概念](#)

- 搜索

请善用搜索功能

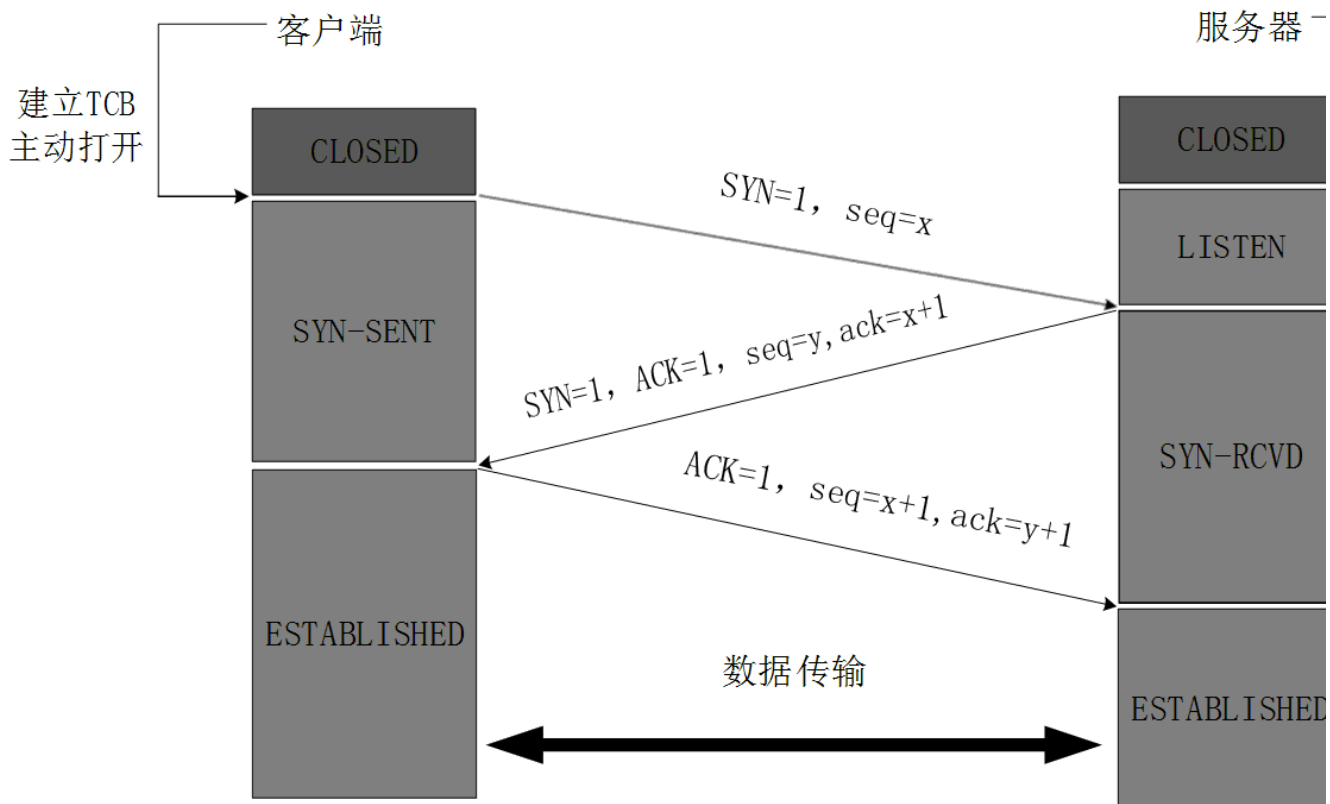
搜索

- 随机文章



。 [休闲 | 打饱勃](#)

o



[华为网络基础 | TCP连接管理机制](#)

• 存档

- o [2021年8月\(1\)](#)
- o [2021年7月\(2\)](#)
- o [2021年6月\(1\)](#)
- o [2021年3月\(1\)](#)
- o [2020年12月\(2\)](#)
- o [2020年11月\(3\)](#)
- o [2020年10月\(1\)](#)
- o [2020年9月\(2\)](#)
- o [2020年7月\(2\)](#)
- o [2020年6月\(1\)](#)
- o [2020年5月\(1\)](#)
- o [2020年4月\(1\)](#)
- o [2020年3月\(5\)](#)
- o [2020年2月\(11\)](#)
- o [2020年1月\(1\)](#)
- o [2019年12月\(1\)](#)
- o [2019年11月\(4\)](#)
- o [2019年10月\(4\)](#)
- o [2019年9月\(3\)](#)
- o [2019年8月\(3\)](#)
- o [2019年7月\(3\)](#)
- o [2019年6月\(15\)](#)
- o [2019年5月\(5\)](#)
- o [2019年4月\(3\)](#)
- o [2019年3月\(3\)](#)
- o [2019年2月\(15\)](#)
- o [2019年1月\(18\)](#)
- o [2018年12月\(9\)](#)
- o [2018年11月\(2\)](#)
- o [2018年10月\(7\)](#)
- o [2018年9月\(13\)](#)
- o [2018年8月\(58\)](#)
- o [2018年7月\(25\)](#)
- o [2018年6月\(1\)](#)
- o [2018年5月\(1\)](#)
- o [2018年3月\(7\)](#)
- o [2018年1月\(1\)](#)
- o [2017年10月\(6\)](#)
- o [2017年9月\(1\)](#)
- o [2017年8月\(1\)](#)
- o [2017年7月\(4\)](#)
- o [2017年6月\(3\)](#)

- [2017年5月\(19\)](#)

×

用户登陆

请输入用户名

请输入密码

请填写验证码

bWU7P

记住密码

用户登陆

[忘记密码?](#)

还没有账号?

暂不开放注册

您还可以使用其他方式登陆

请珍惜本站账号,一经发现账号共享,取消VIP资格.

- [首页](#)
- [微语](#)
- [搜索](#)
- [关于](#)
- [用户](#)

Copyright © 2017-2021 [飞翔...吾爱的Blog](#) 渝ICP备14002470号-2  渝公网安备50011802010177号 Powered by [Emlog](#)& Theme by [Fishyoung](#) | [sitemap](#) | [网站地图](#) | [联系站长](#)

-
- [去顶部](#)

键入搜索关键词

大家都在搜

- [linux](#)
- [打鲍勃](#)
- [拥塞控制](#)
- [查找](#)
- [NQA联动](#)
- [无线故障](#)
- [区别比较](#)
- [远程桌面](#)
- [iframe](#)
- [utf-8](#)
- [win2012](#)
- [单播](#)
- [防火墙](#)
- [cost](#)
- [伪首部](#)
- [matplotlib](#)
- [jar](#)
- [vi](#)
- [内存](#)
- [RYU](#)
- [Snmpservice](#)
- [注释](#)
- [Docker](#)
- [WireShark实战](#)
- [离线安装](#)
- [vlan](#)
- [快速](#)
- [总结](#)
- [运维工程师](#)
- [gcc](#)