MSR 系列路由器 IPsec 虚拟隧道接口与 Cisco 互通配置举例

目 录

1 简介

本文档介绍利用 IPsec 虚拟隧道接口与 Cisco 互通的典型配置举例。

IPsec 虚拟隧道接口是一种支持动态路由协议的三层逻辑接口，适用于站点对站点的应用场景，通过配置路由，让站点间的私网数据流通过 IPsec 虚拟隧道接口进行转发，所有通过 IPsec 虚拟隧道接口转发的数据流都会进行 IPsec 加密和解密处理，同时还可以支持对组播流量的保护。

2 配置前提

本文档不严格与具体软、硬件版本对应，如果使用过程中与产品实际情况有差异，请参考相关产品手册，或以设备实际情况为准。

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

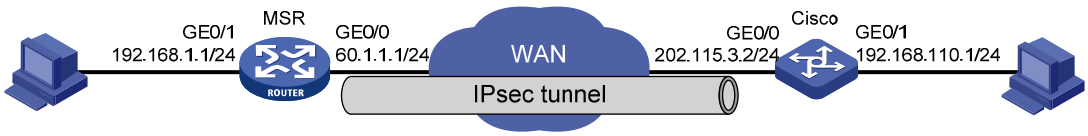
本文档假设您已了解 IPsec 特性。

3 配置举例

3.1 组网需求

如 图 1 所示，总部使用MSR路由器作为网关设备，分支机构使用Cisco路由器作为网关设备，私网路由使用RIPv2 在IPsec虚拟隧道接口间传输。要求：对分支与总部之间的私网数据流进行加密传输。

图1 IPsec 虚拟隧道接口与 Cisco 互通配置组网图



3.2 配置思路

- 将 IPsec 虚拟隧道接口所在网段加入 RIP 进程，通过虚拟隧道接口向对端发布私网路由。
- 配置 IPsec 虚拟隧道所在的广域网路由协议为 ospf。

3.3 使用版本

本举例是在 MSR Release 2317、Cisco12.4 版本上进行配置和验证的。

3.4 配置注意事项

在配置 IPsec 虚拟隧道接口过程中，请注意以下几点：

- IPsec 虚拟隧道接口使用安全框架与 IPsec 关联，安全框架中不需要配置访问控制列表，默认对所有通过 IPsec 虚拟隧道接口转发的数据进行加解密。
- 使用 IPsec 虚拟隧道接口时，IKE 对等体中不需要配置对端地址，IKE 协商时系统向 IPsec 虚拟隧道接口的目的地址发起 IKE 协商。
- 使用 IPsec 虚拟隧道接口时，IKE 协商不需要流量触发，系统会在虚拟隧道接口配置完成后自动向隧道目的地址发起协商。

3.5 配置步骤

3.5.1 MSR的配置

配置接口 GigabitEthernet0/0 的 IP 地址。

```
<MSR> system-view
[MSR] interface gigabitethernet 0/0
[MSR-GigabitEthernet0/0] ip address 60.1.1.1 24
[MSR-GigabitEthernet0/0] quit
```

配置接口 GigabitEthernet0/1 的 IP 地址。

```
[MSR] interface gigabitethernet 0/1
[MSR-GigabitEthernet0/1] ip address 192.168.1.1 24
[MSR-GigabitEthernet0/1] quit
```

配置路由协议 RIPv2。

```
[MSR] rip
[MSR-rip-1] version 2
[MSR-rip-1] network 192.168.1.0
[MSR-rip-1] network 10.0.0.0
[MSR-rip-1] undo summary
[MSR-rip-1] import-route direct
[MSR-rip-1] import-route ospf 1
[MSR-rip-1] quit
```

配置路由协议 OSPF。

```
[MSR] ospf 1
[MSR-ospf-1] area 0.0.0.0
[MSR-ospf-1-area-0.0.0.0] network 60.1.1.0 0.0.0.255
[MSR-ospf-1-area-0.0.0.0] quit
```

创建 IKE 对等体，并配置共享密钥。

```
[MSR] ike peer test
[MSR-ike-peer-test] pre-shared-key test
[MSR-ike-peer-test] quit
```

采用 IPsec 安全提议的缺省配置。

```
[MSR] ipsec proposal test
[MSR-ipsec-proposal-test] quit
```

创建 IPsec 安全框架，并关联 IKE 对等体和 IPsec 安全提议。

```
[MSR] ipsec profile test
[MSR-ipsec-profile-test] ike-peer test
[MSR-ipsec-profile-test] proposal test
[MSR-ipsec-profile-test] quit
```

创建 IPsec 虚拟隧道接口，并关联 IPsec 安全框架。

```
[MSR] interface tunnel 0
[MSR-Tunnel0] ip address 10.1.3.1 255.255.255.0
[MSR-Tunnel0 ]tunnel-protocol ipsec ipv4
[MSR-Tunnel0] source 60.1.1.1
[MSR-Tunnel0] destination 202.115.3.2
[MSR-Tunnel0] ipsec profile test
[MSR-Tunnel0] quit
```

3.5.2 Cisco的配置

配置接口 GigabitEthernet0/0 的 IP 地址。

```
Cisco> enable
Cisco# configure terminal
Cisco(config)# interface gigabitethernet 0/0
Cisco(config-if)# ip address 202.115.3.2 255.255.255.0
Cisco(config-if)# exit
```

配置接口 GigabitEthernet0/1 的 IP 地址。

```
Cisco(config)# interface gigabitethernet 0/1
Cisco(config-if)# ip address 192.168.110.1 255.255.255.0
Cisco(config-if)# exit
```

配置路由协议 RIPv2。

```
Cisco(config)# router rip
Cisco(config-router)# version 2
Cisco(config-router)# network 10.0.0.0
Cisco(config-router)# network 192.168.110.0
Cisco(config-router)# no auto-summary
Cisco(config-router)# exit
```

配置路由协议 OSPF。

```
Cisco(config)# router ospf 1
Cisco(config-router)# network 202.115.3.0 0.0.0.255 area 0
Cisco(config-router)# exit
```

创建 isakmp 策略，认证方式选择共享密钥方式。

```
Cisco(config)# crypto isakmp policy 1
Cisco(config-isakmp)# authentication pre-share
Cisco(config-isakmp)# exit
```

配置预共享密钥。

```
Cisco(config)# crypto isakmp key xq address 0.0.0.0 0.0.0.0
```

配置 IPsec 安全提议。

```
Cisco(config)# crypto ipsec transform-set tunnel esp-des esp-md5-hmac
```

```
Cisco(cfg-crypto-trans)# mode tunnel
Cisco(cfg-crypto-trans)# exit
```

创建 IPsec 框架。

```
Cisco(config)# crypto ipsec profile test
Cisco(ipsec-profile)# set transform-set tunnel
Cisco(ipsec-profile)# exit
```

创建 IPsec 虚拟隧道接口，并关联 IPsec 框架。

```
Cisco(config)# interface tunnel 0
Cisco(config-if)# ip address 10.1.3.2 255.255.255.0
Cisco(config-if)# tunnel source 202.115.3.2
Cisco(config-if)# tunnel destination 60.1.1.1
Cisco(config-if)# tunnel mode ipsec ipv4
Cisco(config-if)# tunnel protection ipsec profile test
Cisco(config-if)# exit
```

3.6 验证配置

以 MSR 为例，可通过以下方式验证上述配置：

配置完成后，IPsec 虚拟隧道接口协议 UP。

```
<MSR> display interface Tunnel0
Tunnel0 current state: UP
Line protocol current state: UP
Description: Tunnel0 Interface
The Maximum Transmit Unit is 64000
Internet Address is 10.1.3.1/24 Primary
Encapsulation is TUNNEL, service-loopback-group ID not set.
Tunnel source 60.1.1.1, destination 202.115.3.2
Tunnel bandwidth 64 (kbps)
Tunnel keepalive disabled
Tunnel protocol/transport IPsec/IP
Output queue : (Urgent queuing : Size/Length/Discards)  0/100/0
Output queue : (Protocol queuing : Size/Length/Discards)  0/500/0
Output queue : (FIFO queuing : Size/Length/Discards)  0/75/0
Last clearing of counters:  16:44:43 Thu 09/20/2011
    Last 300 seconds input:  0 bytes/sec, 0 packets/sec
    Last 300 seconds output:  0 bytes/sec, 0 packets/sec
    12915 packets input,  4115576 bytes
    0 input error
    12898 packets output,  4009208 bytes
    0 output error
```

IKE 两个阶段的 SA 正常建立。

```
<MSR> display ike sa
    total phase-1 SAs:  1
    connection-id  peer            flag        phase   doi
  --------------------------------------------------------------
     6385          202.115.3.2     RD|ST         1     IPSEC
```

```
     6559          202.115.3.2     RD|ST         2     IPSEC

  flag meaning
  RD--READY ST--STAYALIVE RL--REPLACED FD--FADING TO--TIMEOUT
```

查看路由表，私网数据通过 RIP 学习到，且出接口为 Tunnel 接口。

```
<MSR> dis ip routing-table 192.168.110.0
Routing Table : Public
Summary Count : 2

Destination/Mask    Proto  Pre  Cost         NextHop         Interface

192.168.110.0/24    RIP    100  1            10.1.3.2        Tun0
```

总部和分支的私网间可以相互 ping 通。

```
<MSR> ping 192.168.110.1
  PING 192.168.110.1: 56  data bytes, press CTRL_C to break
    Reply from 192.168.110.1: bytes=56 Sequence=1 ttl=255 time=1 ms
    Reply from 192.168.110.1: bytes=56 Sequence=2 ttl=255 time=2 ms
    Reply from 192.168.110.1: bytes=56 Sequence=3 ttl=255 time=1 ms
    Reply from 192.168.110.1: bytes=56 Sequence=4 ttl=255 time=1 ms
    Reply from 192.168.110.1: bytes=56 Sequence=5 ttl=255 time=1 ms

  --- 192.168.110.1 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 1/1/2 ms
```

3.7 配置文件

- MSR：

```
#
ike peer test
 pre-shared-key cipher O1v1Lr98JRU=
#
ipsec proposal test
#
ipsec profile test
 ike-peer test
 proposal test
#
interface GigabitEthernet0/0
 port link-mode route
 ip address 60.1.1.1 255.255.255.0
#
interface GigabitEthernet0/1
 port link-mode route
 ip address 192.168.1.1 255.255.255.0
```

```
#
interface Tunnel0
 ip address 10.1.3.1 255.255.255.0
 tunnel-protocol ipsec ipv4
 source 60.1.1.1
 destination 202.115.3.2
 ipsec profile test
#
ospf 1
 area 0.0.0.0
  network 60.1.1.0 0.0.0.255
#
rip 1
 undo summary
 version 2
 network 192.168.1.0
 network 10.0.0.0
 import-route direct
 import-route ospf 1
#
```

- Cisco：

```
!
crypto isakmp policy 1
 authentication pre-share
crypto isakmp key xq address 0.0.0.0 0.0.0.0
!
crypto ipsec transform-set tunnel esp-des esp-md5-hmac
!
crypto ipsec profile test
 set transform-set tunnel
!
interface Tunnel0
 ip address 10.1.3.2 255.255.255.0
 tunnel source 202.115.3.2
 tunnel destination 60.1.1.1
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile test
!
interface GigabitEthernet0/0
 ip address 202.115.3.2 255.255.255.0
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 ip address 192.168.110.1 255.255.255.0
 duplex auto
 speed auto
!
```

```
router ospf 1
 log-adjacency-changes
 network 202.115.3.0 0.0.0.255 area 0
!
router rip
 version 2
 network 10.0.0.0
 network 192.168.110.0
 no auto-summary
!
end
```

4 相关资料

- H3C MSR 系列路由器 命令参考(V5)-R2311
- H3C MSR 系列路由器 配置指导(V5)-R2311