

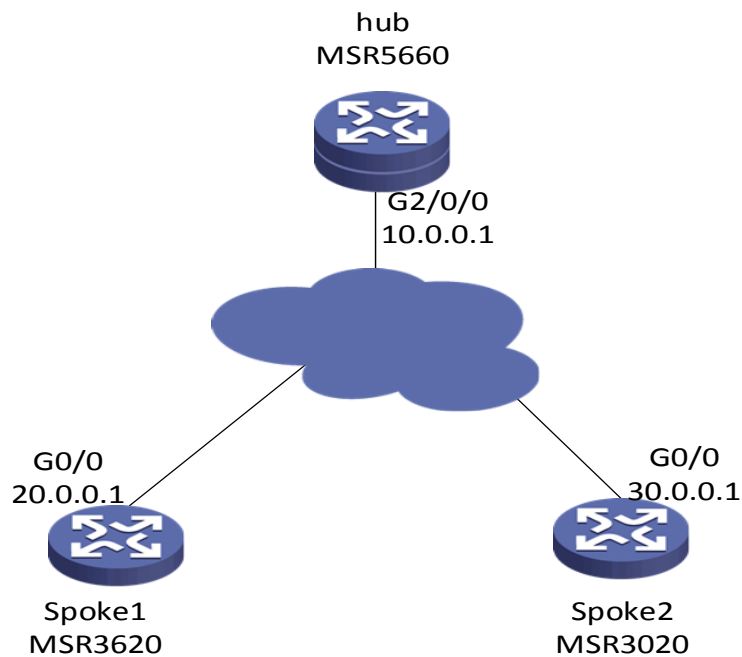
# MSR V7 系列路由器和 MSR V5 系列路由器对接 DVPN 配置

## 一、组网需求：

要求三台路由器之间之间路由可达,PC 使用 loopback 口代替,并且有如下要求:

- 1、dvpn 域名为 abc
- 2、MSR5660 作为 hub 端,MSR3620 和 3020 作为 spoke 端,采用 hub-spoke 结构;
- 3、使用 ipsec 对数据进行加密;
- 4、MSR5660 作为 VAMserver, 采用本地认证。

## 二、组网图：



IP 地址规划：

设备	外网口 IP	内网口 IP	Tunnel 口 IP
MSR5660	10. 0. 0. 1/24	1. 1. 1. 1/24	192. 168. 1. 1/24

MSR3620	20.0.0.1/24	2.2.2.2/24	192.168.1.2/24
MSR3020	30.0.0.1/24	3.3.3.3/24	192.168.1.3/24

### 三、配置步骤：

各设备上 IP 地址和默认路由的配置省略

#### MSR5660 的配置步骤

1、MSR5660 上配置本地认证策略。为 vam client 提供认证

```
#  
domain abc  
    authentication advpn local  
#  
#  
local-user hub class network  
    password cipher $c$3$E94XBBjAX2uaXnYWL1/Pa4n//W1DpQ==  
    service-type advpn  
    authorization-attribute user-role network-operator  
#  
local-user spokel class network  
    password cipher $c$3$AjqXdiz0AapEEfP0hSDGOPYBLbaXA==  
    service-type advpn  
    authorization-attribute user-role network-operator  
#  
local-user spoke2 class network  
    password cipher $c$3$2sk1GhLNtPvmqPSTob81MbnIIta40Q==
```

```
service-type advpn
authorization-attribute user-role network-admin
authorization-attribute user-role network-operator
```

#

## 2、在 MSR5660 上配置 VAMserver 参数，dvpn 域名为 abc id 为 1

#

```
vam server advpn-domain abc id 1
pre-shared-key cipher $c$3$CXwDOAhMccuNG323gs8c/lcT7EIu0A==
authentication-method chap domain abc
server enable
hub-group 0
hub private-address 192.168.1.1
spoke private-address range 192.168.1.0 192.168.1.255
```

#

## 3、在 MSR5660 上配置 VAM client 参数，自己作为 hub 端。

#

```
vam client name hub
advpn-domain abc
server primary ip-address 10.0.0.1
pre-shared-key cipher $c$3$bWr5WXMFR/aUYs7f404ktGLFqRVeg==
user hub password cipher $c$3$aVtfVTH2c+z+1PYMAWKCMxEj/FERTA==
client enable
```

#

## 4、在 MSR5660 上配置 ipsec 安全框架

#

```
ipsec transform-set 1
esp encryption-algorithm des-cbc
esp authentication-algorithm md5
```

#

```
ipsec profile 1 isakmp
  transform-set 1
  ike-profile 1
#
ike profile 1
  keychain 1
#
ike keychain 1
  pre-shared-key address 0.0.0.0 0.0.0.0 key cipher
  $c$3$tdT0/1od2V5nncno4Jl/xviWb3tS6g==
#
```

5、在 MSR5660 上配置 dvpn 隧道，采用 udp 模式封装。隧道上调用 ipsec 安全框架，并开启对 V5 版本的 dvpn 的兼容。

```
#
interface Tunnel1 mode advpn udp
  ip address 192.168.1.1 255.255.255.0
  ospf network-type p2mp
  source GigabitEthernet2/0/0
  tunnel protection ipsec profile 1
  vam client hub compatible advpn0
#
```

6、在 MSR5660 上配置 OSPF，将 tunnel 口和内网接口宣告进 ospf。

```
#
ospf 1
  area 0.0.0.0
  network 1.1.1.0 0.0.0.255
  network 192.168.1.1 0.0.0.0
#
```

## MSR3620 的配置步骤

### 1、在 MSR3620 上配置 VAM client, 自己作为 spoke 端

```
#  
vam client name spokel  
advpn-domain abc  
server primary ip-address 10.0.0.1  
pre-shared-key cipher $c$3$dAX5ZBSKxv1MfkirBj6bMox17un3Nw==  
user spokel password cipher $c$3$tpAUD0x7rQbXGMm+WzzBVgi9vYuKUQ==  
client enable  
#
```

### 2、在 MSR3620 上配置 ipsec 安全框架

```
#  
ipsec transform-set 1  
esp encryption-algorithm des-cbc  
esp authentication-algorithm md5  
#  
ipsec profile 1 isakmp  
transform-set 1  
ike-profile 1  
#  
ike profile 1  
keychain 1  
#  
ike keychain 1  
pre-shared-key address 0.0.0.0 0.0.0.0 key cipher  
$c$3$tAelqptq/gvntIZEeq01IrFXw5nqug==  
#
```

### 3、在 MSR3620 上配置 dvpn 隧道, 采用 udp 封装模式, 并在隧道接口上调用 ipsec

## 安全框架

```
#  
interface Tunnel1 mode advpn udp  
ip address 192.168.1.2 255.255.255.0  
ospf network-type p2mp  
source GigabitEthernet0/0  
tunnel protection ipsec profile 1  
vam client spokel
```

```
#
```

4、在 MSR3620 上配置 OSPF，将 tunnel 口和内网接口宣告进 ospf。

```
#
```

```
ospf 1  
area 0.0.0.0  
network 2.2.2.0 0.0.0.255  
network 192.168.1.2 0.0.0.0
```

```
#
```

## MSR3020 的配置步骤

1、在 MSR3620 上配置 VAM client，自己作为 spoke 端

```
#
```

```
vam client name spoke2  
client enable  
server primary ip-address 10.0.0.1  
user spoke2 password cipher $c$3$JrAPoBzo8JMktfhDYpGyCyBck8LYTA==  
vpn abc  
pre-shared-key cipher $c$3$jC7Ix9gaoRob0xNinoC7qwXeVNsZdQ==
```

```
#
```

2、在 MSR3020 上配置 ipsec 安全框架

```
#
```

```
ike peer 1
  pre-shared-key cipher $c$3$xAx7reyenG3PFL9Sq5akSY+hZ9UxVQ==
#
ipsec transform-set 1
  encapsulation-mode tunnel
  transform esp
  esp authentication-algorithm md5
  esp encryption-algorithm des
#
ipsec profile 1
  ike-peer 1
  transform-set 1
#
```

### 3、在 MSR3020 上配置 dvpn 隧道,采用 udp 封装模式,并在隧道接口上调用 ipsec 安全框架

```
#
interface Tunnel1
  ip address 192.168.1.3 255.255.255.0
  tunnel-protocol dvpn udp
  source GigabitEthernet0/0
  ospf network-type p2mp
  ipsec profile 1
  vam client spoke2
#
```

### 4、在 MSR3020 上配置 OSPF, 将 tunnel 口和内网接口宣告进 ospf。

```
#
ospf 1
  area 0.0.0.0
  network 192.168.1.3 0.0.0.0
```

```
network 3.3.3.0 0.0.0.255
```

```
#
```

## 四、配置验证

1、在 VAM sever (MSR5660) 上查看 vam client 的注册情况。所有 hub 端和 spoke 端都应注册上。

```
<MSR56>display vam server address-map
```

```
ADVPN domain name: abc
```

```
Total private address mappings: 3
```

Group	Private address	Public address	Type	NAT	Holding time
0	192.168.1.1	10.0.0.1	Hub	No	0H 17M 49S
0	192.168.1.2	20.0.0.1	Spoke	No	0H 11M 38S
0	192.168.1.3	30.0.0.1	Spoke	No	0H 29M 8S

2、在 hub 端 (MSR5660) 上查看 advpn 会话状态。State 应该为 success。

```
<MSR56>display advpn session verbose
```

```
Interface : Tunnell
```

```
Client name : hub
```

```
ADVPN domain name : abc
```

```
Link protocol : IPsec-UDP
```

```
Number of sessions: 2
```

```
Private address: 192.168.1.2
```

```
Public address : 20.0.0.1
```

```
ADVPN port : 18001
```

```
SA's SPI:
```

```
inbound: 1736220816 (0x677ca090) [ESP]
```

```
outbound: 871375101 (0x33f020fd) [ESP]
```

```
Behind NAT : No
```

```
Session type : Hub-Spoke
```



**State : Success**

Holding time : 0H 7M 53S

Input : 68 packets, 65 data packets, 3 control packets  
27 multicasts, 0 errors

Output: 74 packets, 71 data packets, 2 control packets  
35 multicasts, 1 errors

Private address: 192.168.1.3

Public address : 30.0.0.1

ADVPN port : 4571

SA's SPI:

inbound: 2877476916 (0xab82d034) [ESP]

outbound: 1028202610 (0x3d492072) [ESP]

Behind NAT : No

Session type : Hub-Spoke

**State : Success**

Holding time : 0H 8M 26S

Input : 53 packets, 52 data packets, 1 control packets  
19 multicasts, 0 errors

Output: 60 packets, 59 data packets, 1 control packets  
38 multicasts, 0 errors

### 3、在 vam clien 端 (MSR3620) 查看 vam 注册状态, current state 应该为 ONLINE

```
<MSR36>display vam client fsm
```

Client name : spokel

Status : Enabled

ADVPN domain name: abc

Primary server: 10.0.0.1

Private address: 192.168.1.2

Interface : Tunnell

**Current state** : **ONLINE (active)**  
Client type : Spoke  
Holding time : 0H 1M 31S  
Encryption-algorithm : AES-CBC-256  
Authentication-algorithm: HMAC-SHA1  
Keepalive : 180 seconds, 3 times  
Hub number : 1

#### 4、在 vam clien 端 (MSR3620) 查看 dvpn 会话， state 应该为 Success

<MSR36>display advpn session verbose

Interface : Tunnell  
Client name : spokel  
ADVPN domain name : abc  
Link protocol : IPsec-UDP  
Number of sessions: 1  
Private address: 192.168.1.1  
Public address : 10.0.0.1  
ADVPN port : 18001  
SA's SPI:  
inbound: 1389802046 (0x52d6b23e) [ESP]  
outbound: 3204125641 (0xbefb13c9) [ESP]  
Behind NAT : No  
Session type : Spoke-Hub  
**State** : **Success**  
Holding time : 0H 1M 33S  
Input : 22 packets, 20 data packets, 2 control packets  
6 multicasts, 0 errors  
Output: 19 packets, 17 data packets, 2 control packets  
5 multicasts, 0 errors

5、在 vam clien 端 (MSR3020) 查看 vam 注册状态, current state 应该为 ONLINE

```
<MSR30>dis vam client fsm
Client name: spoke2
VPN name: abc
Interface: Tunnell
Resend interval(seconds): 5
Client type: Spoke
Username: spoke2
```

```
Primary server: 10.0.0.1
```

```
Current state: ONLINE
```

```
Holding time: 0h 31m 33s
```

```
Encryption-algorithm: AES-256
```

```
Authentication-algorithm: SHA1
```

6、在 vam clien 端 (MSR3020) 查看 dvpn 会话, state 应该为 Success

```
<MSR30>display dvpn session all
```

```
Interface: Tunnell VPN name: abc Total number: 1
```

```
Private IP: 192.168.1.1
```

```
Public IP: 10.0.0.1
```

```
Session type: Spoke-Hub
```

```
State: SUCCESS
```

```
Holding time: 0h 10m 36s
```

```
Input: 64 packets, 63 data packets, 1 control packets
```

```
42 multicasts, 0 errors
```

```
Output: 57 packets, 56 data packets, 1 control packets
```

```
23 multicasts, 0 errors
```

## 7、连通性测试。Hub 端和两个 spoke 端都能互通

```
<MSR56>ping -a 1.1.1.1 2.2.2.2
```

```
Ping 2.2.2.2 (2.2.2.2) from 1.1.1.1: 56 data bytes, press CTRL_C to break
```

```
56 bytes from 2.2.2.2: icmp_seq=0 ttl=255 time=0.918 ms
```

```
56 bytes from 2.2.2.2: icmp_seq=1 ttl=255 time=0.707 ms
```

```
56 bytes from 2.2.2.2: icmp_seq=2 ttl=255 time=0.695 ms
```

```
56 bytes from 2.2.2.2: icmp_seq=3 ttl=255 time=1.354 ms
```

```
56 bytes from 2.2.2.2: icmp_seq=4 ttl=255 time=0.740 ms
```

```
<MSR56>ping -a 1.1.1.1 3.3.3.3
```

```
Ping 3.3.3.3 (3.3.3.3) from 1.1.1.1: 56 data bytes, press CTRL_C to break
```

```
56 bytes from 3.3.3.3: icmp_seq=0 ttl=255 time=1.347 ms
```

```
56 bytes from 3.3.3.3: icmp_seq=1 ttl=255 time=1.280 ms
```

```
56 bytes from 3.3.3.3: icmp_seq=2 ttl=255 time=1.233 ms
```

```
56 bytes from 3.3.3.3: icmp_seq=3 ttl=255 time=1.233 ms
```

```
56 bytes from 3.3.3.3: icmp_seq=4 ttl=255 time=6.516 ms
```

## 五、配置关键点

- 1、V5 和 V7 对接 DVPN，V7 设备的 tunnel 口上需要使用命令 `vam client xxx compatible advpn0` 开启兼容模式。否则会出现 VAM 能注册上，但是 dvpn 会话协商不起来的情况。
- 2、如果采用 hub-spoke 结构，tunnel 接口上需要配置 ospf 网络类型为 P2MP。
- 3、配置 ipsec 安全框架时，不需要指明对端地址，也不需要配置感兴趣流。