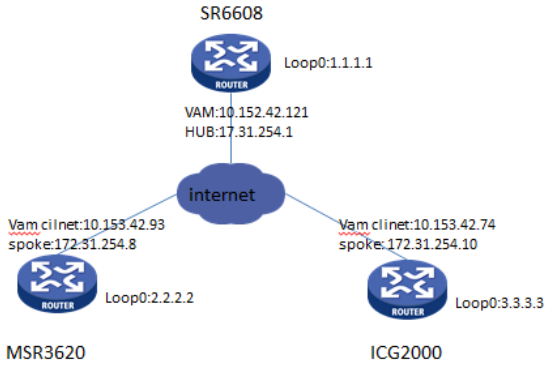
DVPN SR6608 hub MSR G2 spoke

黄磊 2015-09-22 发表

总部SR6608做DVPN HUB和VAM Server，分支点使用Comware v7的MSR3620和Comware v5的ICG 2000做Spoke和VAM client，Spoke和HUB自动建立VPN，为了数据安全，使用IPSec保护VPN数据流。私网路由通过OSPF自动学习。



组网说明：中心和分支之间使用loopback0接口地址默认业务网段，互ping正常表示业务能够正常通信。

使用版本：MSR3620 Release 0106P15

ICG2000 ESS 2207P02

SR6608 Release 3103P08

配置步骤

MSR3620配置

#配置接口地址

```
interface LoopBack0
 ip address 2.2.2.2 255.255.255.255
#
interface GigabitEthernet0/0
ip address 10.153.42.93 255.255.255.0
```

#配置vam client，域名为1，指定vam server为10.153.42.121，预共享密钥123。

```
vam client name hangzhou
 advpn-domain 1
 server primary ip-address 10.153.42.121
 pre-shared-key cipher $c$3$LZRsPI3pWkq8doG+sghjQpvBLPhhfA==
 client enable
```

#配置IPSec模块

```
ike keychain dvpn
 pre-shared-key address 0.0.0.0 0.0.0.0 key cipher $c$3$/BzI9UeIR8cTXqq9Azx2DlVDnLcANw==
#
ike profile dvpn
 keychain dvpn
#
ipsec transform-set dvpn
 encapsulation-mode transport
 esp encryption-algorithm des-cbc
 esp authentication-algorithm sha1
#
ipsec profile dvpn isakmp
 transform-set dvpn
 ike-profile dvpn
```

#配置tunnel口，OSPF网络类型指定p2mp，关联IPSec策略，绑定vam client。

```
interface Tunnel1 mode advpn gre
 ip address 172.31.254.8 255.255.255.0
 ospf network-type p2mp
 source GigabitEthernet0/0
 tunnel protection ipsec profile dvpn
 vam client hangzhou compatible advpn0
```

#配置OSPF，使能loop0口和tunnel口。

```
ospf 1
 area 0.0.0.0
  network 2.2.2.2 0.0.0.0
  network 172.31.254.8 0.0.0.0
#配置指向外网网关的默认路由
 ip route-static 0.0.0.0 0.0.0.0 10.153.42.1
```

SR6608配置

```
#配置接口地址
interface LoopBack0
 ip address 1.1.1.1 255.255.255.255
#
interface GigabitEthernet0/0/0
 ip address 10.153.42.121 255.255.255.0
#配置VAM Server地址
 vam server ip 10.153.42.121
#配置VPN域1，预共享密钥123，指定Hub地址为172.31.254.1
vam server vpn 1
 server enable
 authentication-method none
 pre-shared-key cipher $c$3$Glr9rEhSIGfXV+OLCX6hVkEXYbWT5g==
 hub private-ip 172.31.254.1
#配置VPN域1的客户端beijing，指定服务器地址10.153.42.121，预共享密钥123
vam client name beijing
 client enable
 server primary ip-address 10.153.42.121
 vpn 1
 pre-shared-key cipher $c$3$PvcsqNWL3TNst9PWKKwwVAWXHnWncw==
#配置IPSec模块
ike peer vam
 pre-shared-key cipher $c$3$cw8tajh6I/67q11FiwF4js4I2cg+7g==
#
ipsec transform-set vam
 encapsulation-mode transport
 transform esp
 esp authentication-algorithm sha1
 esp encryption-algorithm des
#
ipsec profile vam
 ike-peer vam
 transform-set vam
#配置tunnel口，OSPF网络类型指定p2mp，关联IPSec策略，绑定vam client。
interface Tunnel1
 ip address 172.31.254.1 255.255.255.0
 tunnel-protocol dvpn gre
 source GigabitEthernet0/0/0
 ospf network-type p2mp
 ipsec profile vam
 vam client beijing
#配置OSPF，使能loop0口和tunnel口。
ospf 1
 area 0.0.0.0
  network 172.31.254.1 0.0.0.0
  network 1.1.1.1 0.0.0.0
#配置指向外网网关的默认路由
 ip route-static 0.0.0.0 0.0.0.0 10.153.42.1
```

ICG2000C配置

```
#配置互联口地址
interface Ethernet0/0
 port link-mode route
 ip address 10.153.42.74 255.255.255.0
#
interface LoopBack0
```

```
 ip address 3.3.3.3 255.255.255.255
#创建VPN域1的客户端shanghai，指定服务器地址10.153.42.121，预共享密钥123。
vam client name shanghai
 client enable
 server primary ip-address 10.153.42.121
 vpn 1
 pre-shared-key simple 123
#配置IPSec模块
ike peer dvpn
 pre-shared-key simple 123
#
ipsec proposal dvpn
 encapsulation-mode transport
 esp authentication-algorithm sha1
#
ipsec profile dvpn
 ike-peer dvpn
 proposal dvpn
#配置OSPF，使能loop0口和tunnel口。
ospf 1
 area 0.0.0.0
  network 3.3.3.3 0.0.0.0
  network 172.31.254.10 0.0.0.0
#配置tunnel口，OSPF网络类型指定p2mp，关联IPSec策略，绑定vam client。
interface Tunnel1
 ip address 172.31.254.10 255.255.255.0
 tunnel-protocol dvpn gre
 source Ethernet0/0
 ospf network-type p2mp
 ipsec profile dvpn
 vam client shanghai
#
#配置指向外网网关的默认路由
 ip route-static 0.0.0.0 0.0.0.0 10.153.42.1
```

结果验证

```
[SR6608]disp vam server address-map all
 VPN name:  1
 Total address-map number:  3

 Private-ip     Public-ip        Type        Holding time

 172.31.254.1   10.153.42.121    Hub         48H 55M  8S
 172.31.254.8   10.153.42.93     Spoke       3H  5M  5S
 172.31.254.10  10.153.42.74     Spoke       0H 56M  1S
[SR6608]ping -a 1.1.1.1 2.2.2.2
  PING 2.2.2.2: 56  data bytes, press CTRL_C to break
    Reply from 2.2.2.2: bytes=56 Sequence=0 ttl=255 time=1 ms
    Reply from 2.2.2.2: bytes=56 Sequence=1 ttl=255 time=1 ms
    Reply from 2.2.2.2: bytes=56 Sequence=2 ttl=255 time=1 ms
    Reply from 2.2.2.2: bytes=56 Sequence=3 ttl=255 time=1 ms
    Reply from 2.2.2.2: bytes=56 Sequence=4 ttl=255 time=1 ms

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

[SR6608]ping -a 1.1.1.1 3.3.3.3
  PING 3.3.3.3: 56  data bytes, press CTRL_C to break
    Reply from 3.3.3.3: bytes=56 Sequence=0 ttl=255 time=2 ms
    Reply from 3.3.3.3: bytes=56 Sequence=1 ttl=255 time=2 ms
```

Reply from 3.3.3.3: bytes=56 Sequence=2 ttl=255 time=2 ms
Reply from 3.3.3.3: bytes=56 Sequence=3 ttl=255 time=2 ms
Reply from 3.3.3.3: bytes=56 Sequence=4 ttl=255 time=2 ms

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

1、MSR G2和V5设备建立DVPN时tunnel绑定vam client 时必须使用 compatible advpn0，必然建立失败，debug可以看到如下提示。

<MSR3620>debugging advpn all
*Jan 17 18:10:25:657 2015 H3C ADVPN/7/EVENT: Compatibility was not configured.

2、MSR G2的advpn-domain名称和V5 VAM client下配置了VPN域名保证一致。