MSR V5平台和MSR V7平台路由器IPSec VPN对接典型配置(野蛮模式)方法

IPSec VPN　zhiliao_xv35y　2018-11-25 发表

组网及说明

1 配置需求或说明

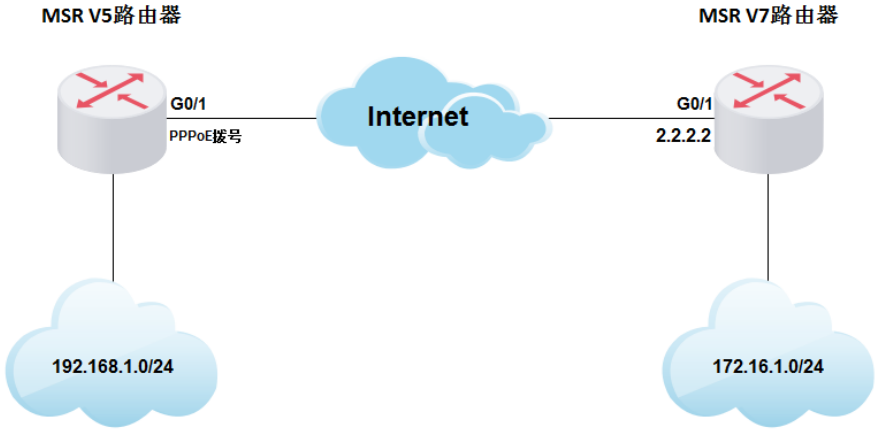
1.1 适用产品系列

本案例提到的MSR v5平台路由器是指Comware V5 软件平台MSR WiNet系列路由器，如MSR830-WiNet 、MSR 830-10-WiNet 、MSR 930-WiNet 、MSR 930-10-WiNet 、MSR 930-WiNet-W 、MSR 2600-10-WiNet等

本案例提到的MSR V7平台路由器是指Comware V7平台的MSR830-WiNet系列路由器，如MSR830-10BEI-WiNet 、MSR830-6EI-WiNet 、MSR830-5BEI-WiNet 、MSR830-6BHI-WiNet 、MSR830-10BHI-WiNet等

1.2 配置需求及实现的效果

MSR V5路由器采用PPPoE拨号方式上网，IP地址不固定，MSR V7路由器外网口G0/1的地址为2.2.2.2（模拟运营商公网固定地址环境）。要实现对MSR V5所在的内网（192.168.1.0/24）与MSR V7路由器所在的内网（172.16.1.0/24）之间的数据流进行安全保护，实现两端内网终端通过IPsec VPN 隧道进行互访。



配置步骤

3 配置步骤

3.1 配置路由器基本上网

#路由器基本上网配置省略，MSR V5路由器的上网具体设置步骤请参考“2.1.1 路由器外网使用拨号上网配置方法”章节中“MSR830[930][2600]系列路由器基本上网（PPPoE拨号）命令行配置（V5）”案例，MSR V7路由器的上网具体设置步骤请参考“2.1.2 路由器外网使用固定IP地址上网配置方法”章节中“MSR830-WiNet系列路由器基本上网（静态IP）命令行配置（V7）”案例

3.2 设置MSR V5路由器IPSEC VPN

配置一个访问控制列表3000，定义由子网192.168.1.0/24去子网172.16.1.0/24的数据流。
system-view
[H3C]acl number 3000
[H3C-acl-adv-3000]rule 0 permit ip source 192.168.1.0 0.0.0.255 destination 172.16.1.0 0.0.0.255
[H3C-acl-adv-3000]quit
#配置公网口NAT要关联的ACl 3001，作用是把IPSec感兴趣流从NAT转换的数据流deny掉，防止IPSec数据流被NAT优先转换
[H3C]acl number 3001
[H3C-acl-adv-3001]rule 0 deny ip source 192.168.1.0 0.0.0.255 destination 172.16.1.0 0.0.0.255
[H3C-acl-adv-3001]rule 1 permit ip
[H3C-acl-adv-3001]quit
#配置本端安全网关的名字
[H3C]ike local-name v5
创建一条IKE提议1，指定IKE提议使用的认证算法为MD5，加密算法为3des-cbc
[H3C]ike proposal 1
[H3C-ike-proposal-1]authentication-algorithm md5
[H3C-ike-proposal-1]encryption-algorithm 3des-cbc
[H3C-ike-proposal-1]quit
配置IPSec安全提议v5，配置ESP协议采用的加密算法为3des，采用的认证算法md5
[H3C]ipsec transform-set v5

[H3C-ipsec-transform-set-v5]encapsulation-mode tunnel
[H3C-ipsec-transform-set-v5]transform esp
[H3C-ipsec-transform-set-v5]esp encryption-algorithm 3des
[H3C-ipsec-transform-set-v5]esp authentication-algorithm md5
[H3C-ipsec-transform-set-v5]quit
创建IKE对等体v5，配置IKE第一阶段的协商模式为野蛮模式，预共享密钥为123456，引用之前创建的IKE安全提议1，选择IKE第一阶段的协商过程中使用ID的类型为name，配置对端地址为对端公网接口地址2.2.2.2，配置对端安全网关的名字为v7，配置本端安全网关的名字为v5
[H3C]ike peer v5
[H3C-ike-peer-v5]exchange-mode aggressive
[H3C-ike-peer-v5]pre-shared-key 123456
[H3C-ike-peer-v5]proposal 1
[H3C-ike-peer-v5]id-type name
[H3C-ike-peer-v5]remote-address 2.2.2.2
[H3C-ike-peer-v5]remote-name v7
[H3C-ike-peer-v5]local-name v5
[H3C-ike-peer-v5]quit
创建一条IPSec安全策略v5，协商方式为isakmp。引用之前创建的感兴趣数据流ACL3000，引用之前创建的对等体v5，引用之前的IPSec安全提议v5
[H3C]ipsec policy v5 1 isakmp
[H3C-ipsec-policy-isakmp-v5-1]security acl 3000
[H3C-ipsec-policy-isakmp-v5-1]ike-peer v5
[H3C-ipsec-policy-isakmp-v5-1]transform-set v5
[H3C-ipsec-policy-isakmp-v5-1]quit
#设置外网口（在本例中假设拨号口为Dialer 10）做NAT转换的时候关联ACL 3001 （如果之前已经在外网口配置了 nat outbound，需要先undo掉），并将IPSec安全策略v5应用在外网接口，
[H3C]interface Dialer 10
[H3C-Dialer10]undo nat outbound
[H3C-Dialer10]nat outbound 3001
[H3C-Dialer10]ipsec policy v5
[H3C-Dialer10]quit

3.3 设置MSR V7路由器IPSEC VPN
配置一个访问控制列表，定义由子网172.16.1.0/24去子网192.168.1.0/24的数据流。
system-view
[H3C]acl advanced 3000
[H3C-acl-ipv4-adv-3000]rule 0 permit ip source 172.16.1.0 0.0.0.255 destination 192.168.1.0 0.0.0.255
[H3C-acl-ipv4-adv-3000]quit
#配置公网口NAT要关联的ACl 3001，作用是把IPSec感兴趣流从NAT转换的数据流deny掉，防止IPSec数据流被NAT优先转换
[H3C]acl advanced 3001
[H3C-acl-ipv4-adv-3001]rule 0 deny ip source 172.16.1.0 0.0.0.255 destination 192.168.1.0 0.0.0.255
[H3C-acl-ipv4-adv-3001]rule 1 permit ip
[H3C-acl-adv-3001]quit
创建一条IKE提议1，指定IKE提议使用的认证算法为MD5，加密算法为3des-cbc
[H3C]ike proposal 1
[H3C-ike-proposal-1]authentication-algorithm md5
[H3C-ike-proposal-1]encryption-algorithm 3des-cbc
[H3C-ike-proposal-1]quit
#配置本端FQDN名称为v7
[H3C]ike identity fqdn v7
#创建并配置IKE keychain，名称为v7。
[H3C]ike keychain v7
#配置对端IP地址为0.0.0.0（由于对端地址不固定，所以配置对端地址为0.0.0.0，其目的是匹配所有地址），使用的预共享密钥为明文123456
[H3C-ike-keychain-v7]pre-shared-key address 0.0.0.0 0.0.0.0 key simple 123456
[H3C-ike-keychain-v7]quit
创建并配置IKE profile，名称为v7，引用上面配置的keychain v7，配置IKE第一阶段的协商模式为野蛮模式，本端身份类型为FQDN且取值为v7，指定需要匹配对端身份类型为FQDN且取值v5，引用之前配置IKE提议1
[H3C]ike profile v7
[H3C-ike-profile-v7]keychain v7
[H3C-ike-profile-v7]exchange-mode aggressive

[H3C-ike-profile-v7]local-identity fqdn v7
[H3C-ike-profile-v7]match remote identity fqdn v5
[H3C-ike-profile-v7]proposal 1
[H3C-ike-profile-v7]quit
配置IPsec安全提议v7，ESP协议采用的加密算法为3des-cbc，认证算法为md5
[H3C]ipsec transform-set v7
[H3C-ipsec-transform-set-v7]encapsulation-mode tunnel
[H3C-ipsec-transform-set-v7]esp encryption-algorithm 3des-cbc
[H3C-ipsec-transform-set-v7]esp authentication-algorithm md5
[H3C-ipsec-transform-set-v5]quit
创建一个模板名字为1，顺序号为1的安全策略模板，引用之前创建的ACL3000，引用之前创建的IKE profile v7，引用之前的IPSec安全提议v7
[H3C]ipsec policy-template 1 1
[H3C-ipsec-policy-template-1-1]transform-set v7
[H3C-ipsec-policy-template-1-1]security acl 3000
[H3C-ipsec-policy-template-1-1]ike-profile v7
[H3C-ipsec-policy-template-1-1]quit
引用IPSec策略模板1，创建名字为policy v7、顺序号为1的IPsec安全策略
[H3C] ipsec policy v7 1 isakmp template 1
#设置外网口做NAT转换的时候关联ACL 3001 （如果之前已经在外网口配置了 nat outbound，需要先undo掉），并将IPSec安全策略v7应用在外网接口
[H3C]interface GigabitEthernet 0/1
[H3C-GigabitEthernet0/1]undo nat outbound
[H3C-GigabitEthernet0/1]nat outbound 3001
[H3C-GigabitEthernet0/1]ipsec apply policy v7
[H3C-GigabitEthernet0/1]quit

3.4 验证配置结果

#配置完成之后，由拨号端主动发起访问，触发建立IPSec隧道，在MSR V5路由器上带源ping MSR V7路由器内网网关地址

```
[H3C]ping -a 192.168.1.1 172.16.1.1
  PING 172.16.1.1: 56  data bytes, press CTRL_C to break
    Reply from 172.16.1.1: bytes=56 Sequence=0 ttl=255 time=1 ms
    Reply from 172.16.1.1: bytes=56 Sequence=1 ttl=255 time=1 ms
    Reply from 172.16.1.1: bytes=56 Sequence=2 ttl=255 time=1 ms
    Reply from 172.16.1.1: bytes=56 Sequence=3 ttl=255 time=1 ms
    Reply from 172.16.1.1: bytes=56 Sequence=4 ttl=255 time=1 ms

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

配置关键点