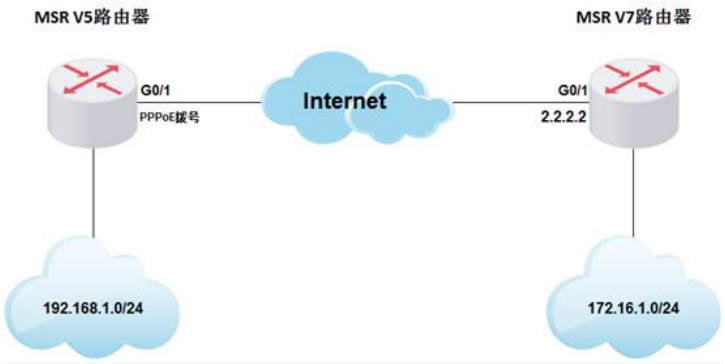
MSR V5和MSR V7路由器IPSec VPN野蛮模式怎么对接?

IPSec VPN　骆翔　2019-01-02 发表

问题描述

MSR V5和MSR V7路由器IPSec VPN野蛮模式怎么对接?

1. **组网需求**



MSR V5路由器采用PPPoE拨号方式上网，IP地址不固定，MSR V7路由器采用固定IP地址上网，两台设备采用野蛮模式建立IPSec VPN保护内网互访的数据流。

解决方法

1. **配置步骤**

1. MSR V5路由器

配置一个访问控制列表，定义由子网192.168.1.0/24去子网172.16.1.0/24的数据流。
<H3C>**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ACL 3001，用于外网口配置NAT引用，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**
[H3C]**ike local-name v5**　//**配置本端安全网关的名字**
创建一条IKE提议1
[H3C]**ike proposal 1**
[H3C-ike-proposal-1]**authentication-algorithm md5**　//指定IKE提议使用的认证算法为MD5
[H3C-ike-proposal-1]**encryption-algorithm 3des-cbc**　//指定IKE提议使用的加密算法为3des-cbc
[H3C-ike-proposal-1]**quit**
配置IPsec安全提议v5。
[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**　//ESP协议采用的加密算法为3des
[H3C-ipsec-transform-set-v5]**esp authentication-algorithm md5**　//ESP协议采用的认证算法md5
[H3C-ipsec-transform-set-v5]**quit**
创建IKE对等体
[H3C]**ike peer v5**
[H3C-ike-peer-v5]**exchange-mode aggressive**　//配置IKE第一阶段的协商模式为野蛮模式
[H3C-ike-peer-v5]**pre-shared-key 123456**　//配置预共享密码
[H3C-ike-peer-v5]**proposal 1**　//引用IKE安全提议1
[H3C-ike-peer-v5]**id-type name**　//选择IKE第一阶段的协商过程中使用ID的类型为name
[H3C-ike-peer-v5]**remote-address 2.2.2.2**　//配置对端安全网关的IP地址，也就是对端设备的公网地址
[H3C-ike-peer-v5]**remote-name v7**　//配置对端安全网关的名字
[H3C-ike-peer-v5]**local-name v5**　//配置本端安全网关的名字，也就是之前配置的ike local-name
[H3C-ike-peer-v5]**quit**
创建一条IPSec安全策略，协商方式为isakmp。

[H3C]**ipsec policy v5 1 isakmp**
[H3C-ipsec-policy-isakmp-v5-1]**security acl 3000** //引用安全ACL
[H3C-ipsec-policy-isakmp-v5-1]**ike-peer v5** //引用IKE对等体
[H3C-ipsec-policy-isakmp-v5-1]**transform-set v5** //引用IPSec安全提议
[H3C-ipsec-policy-isakmp-v5-1]**quit**
在公网接口GigabitEthernet 0/1上应用IPSec安全策略。
[H3C]**interface GigabitEthernet 0/1**
[H3C-GigabitEthernet0/1]**ipsec policy v5**
[H3C-GigabitEthernet0/1]**nat outbound 3001**
[H3C-GigabitEthernet0/1]**quit**
[H3C]**ip route-static 0.0.0.0 0.0.0.0 dialer X** //添加到公网的静态路由，出接口为实际Dialer拨号口

1. MSR V7路由器
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。
<H3C>**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ACL 3001，用于外网口配置NAT引用，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
[H3C]**ike proposal 1**
[H3C-ike-proposal-1]**authentication-algorithm md5** //指定IKE提议使用的认证算法为MD5,配置必须与V5端一致
[H3C-ike-proposal-1]**encryption-algorithm 3des-cbc** //指定IKE提议使用的加密算法为3des-cbc，配置必须与V5端一致
[H3C-ike-proposal-1]**quit**
[H3C]**ike identity fqdn v7** //配置本端FQDN名称
#创建IKE keychain,由于对端地址不固定，配置成0.0.0.0匹配所有。
[H3C]**ike keychain v7**
[H3C-ike-keychain-v7]**pre-shared-key address 0.0.0.0 0.0.0.0 key simple 123456** //此处配置的预共享密钥必须与V5端IKE对等体视图下配置的预共享密钥相同
[H3C-ike-keychain-v7]**quit**
创建并配置IKE profile，名称为v7。
[H3C]**ike profile v7**
[H3C-ike-profile-v7]**keychain v7** //引用上面配置的keychain
[H3C-ike-profile-v7]**exchange-mode aggressive** //配置IKE第一阶段的协商模式为野蛮模式
[H3C-ike-profile-v7]**local-identity fqdn v7** //配置本端身份信息
[H3C-ike-profile-v7]**match remote identity fqdn v5** //指定需要匹配对端身份类型为FQDN，取值v5
[H3C-ike-profile-v7]**proposal 1** //引用之前配置IKE提议
[H3C-ike-profile-v7]**quit**
配置IPsec安全提议v7。
[H3C]**ipsec transform-set v7**
[H3C-ipsec-transform-set-v7]**encapsulation-mode tunnel**
[H3C-ipsec-transform-set-v7] **esp encryption-algorithm 3des-cbc** //ESP协议采用的加密算法为3des-cbc
[H3C-ipsec-transform-set-v7] **esp authentication-algorithm md5** //ESP协议采用的认证算法为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。
[H3C]**ipsec policy-template 1 1**
[H3C-ipsec-policy-template-1-1]**transform-set v7** //指定引用的ipsec安全提议
[H3C-ipsec-policy-template-1-1]**security acl 3000** //引用安全ACL
[H3C-ipsec-policy-template-1-1]**ike-profile v7** //指定引用的IKE profile
[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**
在接口GigabitEthernet0/1上应用IPsec安全策略
[H3C]interface GigabitEthernet 0/1
[H3C-GigabitEthernet0/1]**nat outbound 3001**

[H3C-GigabitEthernet0/1]**ipsec apply policy v7**
[H3C-GigabitEthernet0/1]**quit**
[H3C]**ip route-static 0.0.0.0 0.0.0.0 X.X.X.X** //添加到公网的静态路由，其中X.X.X.X请配置公网接口的网关地址

注：配置完成之后，由拨号端主动发起访问，触发建立IPSec隧道。