ICG2000D/ICG3000F系列路由器IPSEC 多分支互访配置方法

GRE VPN　史晓虎　2019-08-21 发表

组网及说明

1 配置需求或说明

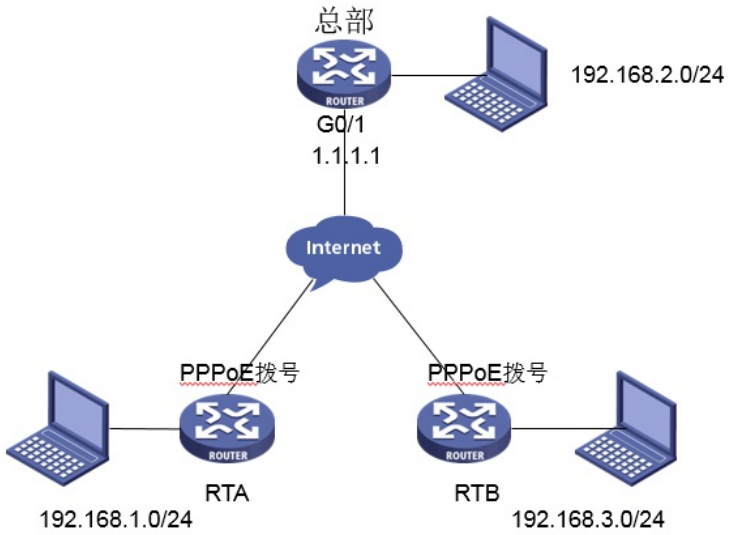
1.1 适用产品系列

本案例适用于如ICG2000D、ICG3000F系列的路由器

1.2 配置需求及实现的效果

MSR 分支路由器采用PPPoE拨号方式上网，IP地址不固定，MSR 总部路由器外网口G0/1的地址为1.1.1.1（模拟运营商公网固定地址环境）。要实现对分支1所在的内网（192.168.1.0/24）与分支2路由器所在的内网（192.168.3.0/24）之间的数据流进行安全保护，实现两端内网终端通过与总部建立IPsec VPN 隧道进行互访。

2 组网图



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 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 设置总部路由器IPSEC VPN

#配置一个访问控制列表3000，定义由总部子网192.168.2.0/24去分支1子网192.168.1.0/24和分支2子网192.168.3.0/24去分支1子网192.168.1.0/24的数据流

system-view

[H3C]acl number 3000

[H3C-acl-adv-3000]rule 0 permit ip source 192.168.2.0 0.0.0.255 destination 192.168.1.0 0.0.0.255

[H3C-acl-adv-3000]rule 1 permit ip source 192.168.3.0 0.0.0.255 destination 192.168.1.0 0.0.0.255

[H3C-acl-adv-3000]quit

#配置一个访问控制列表3001，定义由总部子网192.168.2.0/24去分支2子网192.168.1.0/24和分支1子网192.168.3.0/24去分支2子网192.168.1.0/24的数据流

[H3C]acl number 3001

[H3C-acl-adv-3001]rule 0 permit ip source 192.168.2.0 0.0.0.255 destination 192.168.3.0 0.0.0.255

[H3C-acl-adv-3001]rule 1 permit ip source 192.168.1.0 0.0.0.255 destination 192.168.3.0 0.0.0.255

[H3C-acl-adv-3001]quit

#配置公网口NAT要关联的ACl 3002，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 3002
[H3C-acl-adv-3002]rule 0 deny ip source 192.168.2.0 0.0.0.255 destination 192.168.1.0 0.0.0.255
[H3C-acl-adv-3002]rule 1 deny ip source 192.168.3.0 0.0.0.255 destination 192.168.1.0 0.0.0.255
[H3C-acl-adv-3002]rule 2 deny ip source 192.168.2.0 0.0.0.255 destination 192.168.3.0 0.0.0.255
[H3C-acl-adv-3002]rule 3 deny ip source 192.168.1.0 0.0.0.255 destination 192.168.3.0 0.0.0.255
[H3C-acl-adv-3002]rule 4 permit ip
[H3C-acl-adv-3002]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zongbu
[H3C]ike identity fqdn zongbu
#创建并配置IKE keychain，名称为RTA和RTB
[H3C]ike keychain RTA
#配置与分支之间协商采用的预共享密钥，(由于分支设备无固定IP，这里需要采用name的方式)，这里配置分支1的name为RTA，分支2的name为RTB，分支name需要与分支侧设置的一致，使用的预共享密钥为明文123456
[H3C-ike-keychain-RTA]pre-shared-key hostname RTA key simple 123456
[H3C-ike-keychain-RTA]quit
[H3C]ike keychain RTB
[H3C-ike-keychain-RTB]pre-shared-key hostname RTB key simple 123456
[H3C-ike-keychain-RTB]quit
#创建并配置IKE profile，名称分别为RTA和RTB，引用上面配置的keychain，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zongbu，指定需要匹配对端身份类型为FQDN且取值RTA和RTB，引用之前配置IKE提议1
[H3C]ike profile RTA
[H3C-ike-profile-RTA]keychain RTA
[H3C-ike-profile-RTA]exchange-mode aggressive
[H3C-ike-profile-RTA]local-identity fqdn zongbu
[H3C-ike-profile-RTA]match remote identity fqdn RTA
[H3C-ike-profile-RTA]proposal 1
[H3C-ike-profile-RTA]quit
[H3C]ike profile RTB
[H3C-ike-profile-RTB]keychain RTB
[H3C-ike-profile-RTB]exchange-mode aggressive
[H3C-ike-profile-RTB]local-identity fqdn zongbu
[H3C-ike-profile-RTB]match remote identity fqdn RTB
[H3C-ike-profile-RTB]proposal 1
[H3C-ike-profile-RTB]quit
#配置IPsec安全提议1，ESP协议采用的加密算法为3des-cbc，认证算法为md5
[H3C]ipsec transform-set 1
[H3C-ipsec-transform-set-1]encapsulation-mode tunnel
[H3C-ipsec-transform-set-1]esp encryption-algorithm 3des-cbc
[H3C-ipsec-transform-set-1]esp authentication-algorithm md5
[H3C-ipsec-transform-set-1]quit
#创建两个模板名字分别为t1和t2，顺序号为1的安全策略模板，引用之前创建的ACL3000和3001，引用之前创建的IKE profile，引用之前的IPSec安全提议1
[H3C]ipsec policy-template t1 1
[H3C-ipsec-policy-template-t1-1]security acl 3000
[H3C-ipsec-policy-template-t1-1]ike-profile RTA
[H3C-ipsec-policy-template-t1-1]transform-set 1
[H3C-ipsec-policy-template-t1-1]quit
[H3C]ipsec policy-template t2 1
[H3C-ipsec-policy-template-t2-1]security acl 3001
[H3C-ipsec-policy-template-t2-1]ike-profile RTB
[H3C-ipsec-policy-template-t2-1]transform-set 1
[H3C-ipsec-policy-template-t2-1]quit
#引用IPSec策略模板t1和t2，创建名字为policy zongbu、顺序号为1和2的IPsec安全策略

[H3C] ipsec policy zongbu 1 isakmp template t1
[H3C] ipsec policy zongbu 2 isakmp template t2
#设置外网口做NAT转换的时候关联ACL 3002（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 3002
[H3C-GigabitEthernet0/1]ipsec apply policy zongbu
[H3C-GigabitEthernet0/1]quit
#保存配置
[H3C]save force

3.3 设置分支1路由器IPSEC VPN

#配置一个访问控制列表，定义由分支1子网192.168.1.0/24去总部子网192.168.2.0/24，分支1子网192.168.1.0/24去分支2子网192.168.3.0/24的数据流
system-view
[H3C]acl advanced 3000
[H3C-acl-ipv4-adv-3000]rule 0 permit ip source 192.168.1.0 0.0.0.255 destination 192.168.2.0 0.0.0.255
[H3C-acl-ipv4-adv-3000]rule 1 permit ip source 192.168.1.0 0.0.0.255 destination 192.168.3.0 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 192.168.1.0 0.0.0.255 destination 192.168.2.0 0.0.0.255
[H3C-acl-ipv4-adv-3001]rule 1 deny ip source 192.168.1.0 0.0.0.255 destination 192.168.3.0 0.0.0.255
[H3C-acl-ipv4-adv-3001]rule 2 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RTA
[H3C]ike identity fqdn RTA
#创建并配置IKE keychain，名称为RTA。
[H3C]ike keychain RTA
#配置对端IP地址为1.1.1.1，使用的预共享密钥为明文123456
[H3C-ike-keychain-RTA]pre-shared-key address 1.1.1.1 key simple 123456
[H3C-ike-keychain-RTA]quit
#创建并配置IKE profile，名称为RTA，引用上面配置的keychain RTA，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RTA，指定需要匹配对端身份类型为FQDN且取值zongbu，引用之前配置IKE提议1
[H3C]ike profile RTA
[H3C-ike-profile-RTA]keychain RTA
[H3C-ike-profile-RTA]exchange-mode aggressive
[H3C-ike-profile-RTA]local-identity fqdn RTA
[H3C-ike-profile-RTA]match remote identity fqdn zongbu
[H3C-ike-profile-RTA]proposal 1
[H3C-ike-profile-RTA]quit
#配置IPsec安全提议1，ESP协议采用的加密算法为3des-cbc，认证算法为md5
[H3C]ipsec transform-set 1
[H3C-ipsec-transform-set-1]esp encryption-algorithm 3des-cbc
[H3C-ipsec-transform-set-1]esp authentication-algorithm md5
[H3C-ipsec-transform-set-1]quit
#创建一条IPSec安全策略RTA，协商方式为isakmp。引用之前创建的感兴趣数据流ACL3000，指定对端公网ip地址，引用之前创建的IKE profile，引用之前的IPSec安全提议1
[H3C]ipsec policy RTA 1 isakmp
[H3C-ipsec-policy-isakmp-RTA-1]security acl 3000
[H3C-ipsec-policy-isakmp-RTA-1]remote-address 1.1.1.1
[H3C-ipsec-policy-isakmp-RTA-1]ike-profile RTA

[H3C-ipsec-policy-isakmp-RTA-1]transform-set 1
[H3C-ipsec-policy-isakmp-RTA-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RTA应用在外网接口，
[H3C]interface Dialer 10
[H3C-Dialer10]undo nat outbound
[H3C-Dialer10]nat outbound 3001
[H3C-Dialer10]ipsec apply policy RTA
[H3C-Dialer10]quit
#保存配置
[H3C]save force

3.4 设置分支2路由器IPSEC VPN

#配置一个访问控制列表，定义由分支2子网192.168.3.0/24去总部子网192.168.2.0/24，分支2子网192.168.3.0/24去分支1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 192.168.3.0 0.0.0.255 destination 192.168.2.0 0.0.0.255
[H3C-acl-ipv4-adv-3000]rule 1 permit ip source 192.168.3.0 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 192.168.3.0 0.0.0.255 destination 192.168.2.0 0.0.0.255
[H3C-acl-ipv4-adv-3001]rule 1 deny ip source 192.168.3.0 0.0.0.255 destination 192.168.1.0 0.0.0.255
[H3C-acl-ipv4-adv-3001]rule 2 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RTB
[H3C]ike identity fqdn RTB
#创建并配置IKE keychain，名称为RTB。
[H3C]ike keychain RTB
#配置对端IP地址为1.1.1.1，使用的预共享密钥为明文123456
[H3C-ike-keychain-RTB]pre-shared-key address 1.1.1.1 key simple 123456
[H3C-ike-keychain-RTB]quit
#创建并配置IKE profile，名称为RTA，引用上面配置的keychain RTB，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RTB，指定需要匹配对端身份类型为FQDN且取值zongbu，引用之前配置IKE提议1
[H3C]ike profile RTB
[H3C-ike-profile-RTB]keychain RTB
[H3C-ike-profile-RTB]exchange-mode aggressive
[H3C-ike-profile-RTB]local-identity fqdn RTB
[H3C-ike-profile-RTB]match remote identity fqdn zongbu
[H3C-ike-profile-RTB]proposal 1
[H3C-ike-profile-RTB]quit
#配置IPsec安全提议1，ESP协议采用的加密算法为3des-cbc，认证算法为md5
[H3C]ipsec transform-set 1
[H3C-ipsec-transform-set-1]esp encryption-algorithm 3des-cbc
[H3C-ipsec-transform-set-1]esp authentication-algorithm md5
[H3C-ipsec-transform-set-1]quit
#创建一条IPSec安全策略RTB，协商方式为isakmp。引用之前创建的感兴趣数据流ACL3000，指定对端公网ip地址，引用之前创建的IKE profile，引用之前的IPSec安全提议1
[H3C]ipsec policy RTB 1 isakmp
[H3C-ipsec-policy-isakmp-RTB-1]security acl 3000
[H3C-ipsec-policy-isakmp-RTB-1]ike-profile RTB
[H3C-ipsec-policy-isakmp-RTB-1]remote-address 1.1.1.1

[H3C-ipsec-policy-isakmp-RTB-1]transform-set 1
[H3C-ipsec-policy-isakmp-RTB-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RTA应用在外网接口，
[H3C]interface Dialer 10
[H3C-Dialer10]undo nat outbound
[H3C-Dialer10]nat outbound 3001
[H3C-Dialer10]ipsec apply policy RTB
[H3C-Dialer10]quit
#保存配置
[H3C]save force

3.5 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，在分支路由器上带源ping 总部路由器内网网关地址

配置关键点