## 一、拓扑



## 二、配置步骤

### 1、vpn tunnel的配置

H3C的配置如下：

ike peer rt7

 exchange-mode aggressive

 pre-shared-key cipher $c$3$INAXVOVsmP35Q3O2a8FL0NiKLMf/QQNyv81o

 id-type name

 remote-name rt7

 nat traversal

ipsec transform-set 1

 encapsulation-mode tunnel

 transform esp

 esp authentication-algorithm sha1

 esp encryption-algorithm des

ipsec policy-template temp 7

 ike-peer rt7

 transform-set 1

在防火墙采用接口模式配置，配置如下图所示。在阶段2中配置源目标和目标地址是GRE-tunnel的起始IP和终止IP。





### 2、GRE配置

GRE是从172.16.0.7到172.16.0.254，在h3c设备上配置为

interface Tunnel7

 ip address 172.16.1.25 255.255.255.252

 source 172.16.0.254

 destination 172.16.0.7

 keepalive 10 3

防火墙上配置为

define system gre-tunnel

 edit "gre-vpn"

 set interface "Branch\_to\_HQ\_p1"

 set local-gw 172.16.0.7

 set remote-gw 172.16.0.254

 next

end

define system interface

 edit "gre-vpn"

 set vdom "root"

 set ip 172.16.1.26 255.255.255.255

 set type tunnel

 set remote-ip 172.16.1.25

 set interface "Branch\_to\_HQ\_p1"

 next

end

注：172.16.1.26是在172.16.1.25/30一个网段的另外一个IP，所以配置我们防火墙这边的GRE接口IP为172.16.1.26。

但是172.16.0.7这个IP地址必须存在防火墙的某个接口上。所以我们将IP地址配置在ipsec的虚拟接口上。

define system interface

 edit "Branch\_to\_HQ\_p1"

 set vdom "root"

 set ip 172.16.0.7 255.255.255.255

 set type tunnel

 set remote-ip 172.16.0.254

 set interface "port1"

 next

end

### 3、添加策略



策略应该涵盖从GRE到IPsec接口，和从IPsec接口到GRE接口。这是保证GRE隧道流量能够通过IPsec通道。

内网通过vpn通道访问对端内网，则通过内网到GRE的策略来控制。

### 4、路由

添加一个172.16.0.0/24的路由，目的是让对端GRE隧道通讯流量能被接收。192.168.0.0/16是让192.168.0.0网段的流量进入GRE通道。



如果配置OSPF，则不需要192.168.0.0/16路由。

在H3C上配置如下：

ospf 1

 silent-interface Vlan-interface1

 silent-interface Vlan-interface2

 area 0.0.0.0

 network 192.168.0.0 0.0.255.255

 network 172.16.1.0 0.0.0.255

在防火墙配置如下：



配置动态路由后，可以学习到路由：



## 三、原配置文件

H3C的配置文件：



我们防火墙的配置文件：

