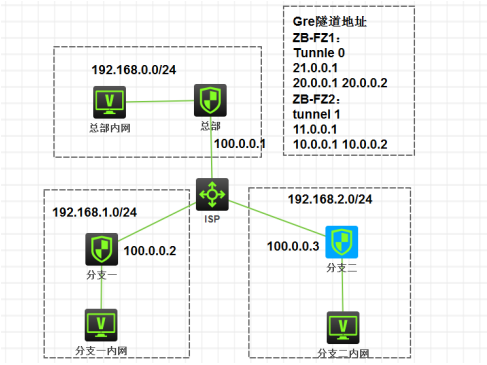
GRE over ipsec

GRE VPN IPSec VPN 李旭东 2018-05-14 发表

组网及说明

多分支接入的情况下，如果设备支持点到多点GRE隧道，则总部只需要配置一个GRE Tunnle，但是设备不支持此特性的话，只能在总部为每个分支建立一个GRE Tunnle。



总部:

公网地址：100.0.0.1

私网地址:192.168.0.0/24

GRE tunnel 0:去往分支1

地址：21.0.0.1

封装源地址:20.0.0.1 目的地址:20.0.0.2

GRE tunnel 1:去往分支2

地址：11.0.0.1

封装源地址:10.0.0.1 目的地址:10.0.0.2

分支一:

公网地址：100.0.0.2

私网地址:192.168.1.0/24

GRE tunnel 0:去往总部

地址：21.0.0.2

封装源地址:20.0.0.2 目的地址:20.0.0.1

分支二:

公网地址：100.0.0.2

私网地址:192.168.1.0/24

GRE tunnel 0:去往总部

地址：11.0.0.2

封装源地址:10.0.0.2 目的地址:10.0.0.1

配置步骤

配置基本的IP地址以及域间策略

总部:

```
interface GigabitEthernet1/0/1
ip address 192.168.0.1 255.255.255.0
#
interface GigabitEthernet1/0/2  #公网口
 ip address 100.0.0.1 255.255.255.0

interface LoopBack0  #GRE封装时的源地址
 description GRE
 ip address 20.0.0.1 255.255.255.255
#
interface LoopBack1 # #GRE封装时的源地址
 description GRE
 ip address 10.0.0.1 255.255.255.255
```

```
interface Tunnel0 mode gre
 description ToFenZhi_1
 ip address 21.0.0.1 255.255.255.0
 source 20.0.0.1
 destination 20.0.0.2
#
interface Tunnel1 mode gre
 description ToFenZhi_2
 ip address 11.0.0.1 255.255.255.0
 source 10.0.0.1
     destination 10.0.0.2

#域间策略
security-zone name Trust
 import interface GigabitEthernet1/0/1
#
security-zone name Untrust
 import interface GigabitEthernet1/0/2
 import interface Tunnel0
 import interface Tunnel1

zone-pair security source Any destination Any
 packet-filter 3010

acl advanced 3010
 description yujiancelue
 rule 0 permit ip
```

分支一：

```
interface GigabitEthernet1/0/1
ip address 192.168.1.1 255.255.255.0
#
interface GigabitEthernet1/0/2
ip address 100.0.0.2 255.255.255.0


interface LoopBack0
 description GRE
 ip address 20.0.0.2 255.255.255.255


interface Tunnel0 mode gre  #这里封装的地址源目和总部反过来
 ip address 21.0.0.2 255.255.254.0
 source  20.0.0.2
 destination 20.0.0.1

security-zone name Trust
 import interface GigabitEthernet1/0/1
#
security-zone name Untrust
 import interface GigabitEthernet1/0/2
 import interface Tunnel0

acl advanced 3010
 description yujiancelue
 rule 0 permit ip

zone-pair security source Local destination Any
 packet-filter 3010
```

分支二：

```
interface GigabitEthernet1/0/1
ip address 192.168.2.1 255.255.255.0
#
interface GigabitEthernet1/0/2
ip address 100.0.0.3 255.255.255.0


interface LoopBack0
 description GRE
 ip address 10.0.0.2 255.255.255.255



interface Tunnel0 mode gre
 ip address 11.0.0.2 255.255.255.0
 source 10.0.0.2
 destination 10.0.0.1

security-zone name Trust
 import interface GigabitEthernet1/0/1#
security-zone name Untrust
 import interface GigabitEthernet1/0/2
 import interface Tunnel0
#
acl advanced 3010
 description yujiancelue
 rule 0 permit ip
#
zone-pair security source Any destination Any
 packet-filter 3010
```

IPsec的配置

总部

#总部使用模板方式建立ipsec，只需要写一个策略，不需要安全acl。

```
ike keychain 1
 pre-shared-key address 0.0.0.0 0.0.0.0 key  simple  123  #0.0.0.0代表接受任何地址建立ipsec

ike profile 1
 keychain 1
 local-identity address 100.0.0.1
 match remote identity address 0.0.0.0 0.0.0.0
#
ipsec transform-set 1
 esp encryption-algorithm 3des-cbc
 esp authentication-algorithm md5
#
ipsec policy-template 1 1
 transform-set 1
 local-address 100.0.0.1
 ike-profile 1
#
ipsec policy 1 1 isakmp template 1

#接口下调用ipsec
interface GigabitEthernet1/0/2
ip address 100.0.0.1 255.255.255.0
 ipsec apply policy 1
```

最重要的一步：

ip route-static 192.168.1.0 24 Tunnel0　　#192.168.1.0是分支一的私网地址，将其下一跳指向Tun nle 0，即去往分支一的GRE隧道。

ip route-static 192.168.2.0 24 Tunnel1　　#192.168.1.0是分支二的私网地址，将其下一跳指向Tun

nle 0，即去往分支一的GRE隧道。

分支一：

```
ike profile 1
 keychain 1
 match remote identity address 100.0.0.1 255.255.255.255
#
ike keychain 1
 pre-shared-key address 100.0.0.1 255.255.255.255 key simple 123

ipsec transform-set 1
 esp encryption-algorithm 3des-cbc
 esp authentication-algorithm md5
#
ipsec policy 1 1 isakmp
 transform-set 1
 security acl 3020
 remote-address 100.0.0.1
 ike-profile 1


acl advanced 3020
 description IPsec
 rule 0 permit ip source 20.0.0.2 0 destination 20.0.0.1 0
```

#这里安全ACl匹配的流和GRE的源目地址一致，即由GRE封装之后的报文。

最重要的一步：

```
 ip route-static 192.168.0.0 24 Tunnel0
```

#不管是去往总部192.168.0.0还是去往其他分支192.168.2.0，下一跳全部指向Tunnle 0，全部指向总部，再由总部转发。

```
 ip route-static 192.168.2.0 24 Tunnel0
```

分支二：

类似分支一

```
ipsec transform-set 1
 esp encryption-algorithm 3des-cbc
 esp authentication-algorithm md5
#
ipsec policy 1 1 isakmp
 transform-set 1
 security acl 3020
 remote-address 100.0.0.1
 ike-profile 1
#
ike profile 1
 keychain 1
 match remote identity address 100.0.0.1 255.255.255.255
#
ike keychain 1
 pre-shared-key address 100.0.0.1 255.255.255.255 key simple 123


acl advanced 3020
 description IPsec
 rule 0 permit ip source 20.0.0.2 0 destination 20.0.0.1 0


 ip route-static 192.168.0.0 24 Tunnel0
 ip route-static 192.168.2.0 24 Tunnel0
#
```

验证效果：

#总部使用模板方式时，只能被动建立IPSEC隧道，不能主动呼叫。

分支一：

[H3C]ping -a 192.168.1.1 192.168.0.1
Ping 192.168.0.1 (192.168.0.1) from 192.168.1.1: 56 data bytes, press CTRL_C to break
56 bytes from 192.168.0.1: icmp_seq=0 ttl=255 time=2.000 ms
56 bytes from 192.168.0.1: icmp_seq=1 ttl=255 time=8.000 ms
56 bytes from 192.168.0.1: icmp_seq=2 ttl=255 time=2.000 ms
56 bytes from 192.168.0.1: icmp_seq=3 ttl=255 time=1.000 ms
56 bytes from 192.168.0.1: icmp_seq=4 ttl=255 time=1.000 ms

--- Ping statistics for 192.168.0.1 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 1.000/2.800/8.000/2.638 ms
[H3C]%May 9 18:41:03:921 2018 H3C PING/6/PING_STATISTICS: -COntext=1; Ping statistics for 1
92.168.0.1: 5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss, round-trip min/avg/max/st
d-dev = 1.000/2.800/8.000/2.638 ms.

[H3C]ping -a 192.168.1.1 192.168.2.1
Ping 192.168.2.1 (192.168.2.1) from 192.168.1.1: 56 data bytes, press CTRL_C to break
56 bytes from 192.168.2.1: icmp_seq=0 ttl=254 time=5.000 ms
56 bytes from 192.168.2.1: icmp_seq=1 ttl=254 time=2.000 ms
56 bytes from 192.168.2.1: icmp_seq=2 ttl=254 time=4.000 ms
56 bytes from 192.168.2.1: icmp_seq=3 ttl=254 time=2.000 ms
56 bytes from 192.168.2.1: icmp_seq=4 ttl=254 time=3.000 ms

--- Ping statistics for 192.168.2.1 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 2.000/3.200/5.000/1.166 ms
[H3C]%May 9 18:41:07:906 2018 H3C PING/6/PING_STATISTICS: -COntext=1; Ping statistics for 1
92.168.2.1: 5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss, round-trip min/avg/max/st
d-dev = 2.000/3.200/5.000/1.166 ms.

分支二：

[H3C]ping -a 192.168.2.1 192.168.0.1
Ping 192.168.0.1 (192.168.0.1) from 192.168.2.1: 56 data bytes, press CTRL_C to break
56 bytes from 192.168.0.1: icmp_seq=0 ttl=255 time=1.000 ms
56 bytes from 192.168.0.1: icmp_seq=1 ttl=255 time=1.000 ms
56 bytes from 192.168.0.1: icmp_seq=2 ttl=255 time=1.000 ms
56 bytes from 192.168.0.1: icmp_seq=3 ttl=255 time=2.000 ms
56 bytes from 192.168.0.1: icmp_seq=4 ttl=255 time=1.000 ms

--- Ping statistics for 192.168.0.1 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 1.000/1.200/2.000/0.400 ms
[H3C]\%May 9 18:42:47:047 2018 H3C PING/6/PING_STATISTICS: -COntext=1; Ping statistics for 1
92.168.0.1: 5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss, round-trip min/avg/max/st
d-dev = 1.000/1.200/2.000/0.400 ms.

[H3C]ping -a 192.168.2.1 192.168.1.1
Ping 192.168.1.1 (192.168.1.1) from 192.168.2.1: 56 data bytes, press CTRL_C to break
56 bytes from 192.168.1.1: icmp_seq=0 ttl=254 time=11.000 ms
56 bytes from 192.168.1.1: icmp_seq=1 ttl=254 time=2.000 ms
56 bytes from 192.168.1.1: icmp_seq=2 ttl=254 time=2.000 ms
56 bytes from 192.168.1.1: icmp_seq=3 ttl=254 time=5.000 ms
56 bytes from 192.168.1.1: icmp_seq=4 ttl=254 time=4.000 ms

--- Ping statistics for 192.168.1.1 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 2.000/4.800/11.000/3.311 ms
[H3C]%May 9 18:42:50:726 2018 H3C PING/6/PING_STATISTICS: -COntext=1; Ping statistics for 1
92.168.1.1: 5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss, round-trip min/avg/max/st
d-dev = 2.000/4.800/11.000/3.311 ms.

配置关键点

总结与建议：

一：注意loopback口的建立，和GRE**封装**时的源目地址保持一致，而不是GRE Tunnle的ip地址。

二：安全策略，Tunnle口需要加入安全域并且放通策略

三：这种方式下的IPSEC，后续网段变动时，只需要配置不同的静态路由指向GRE Tunnle口，IPsec的配置无需改变，适合私网地址较大的拓扑。

四：IPsec的各种加密参数注意保持一致。以及IPsec的安全ACL匹配的是GRE封装之后的源目地址。

五：对于各种访问控制，建议IPsec这块不用动，等IPsec成功后，在防火墙的域间策略上统一控制。