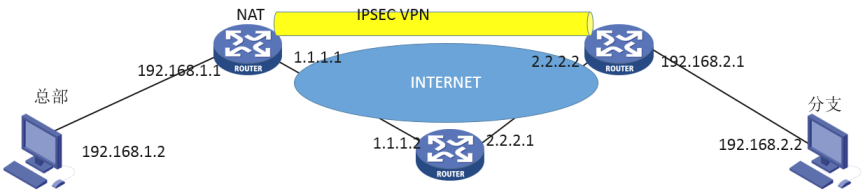
分支通过总部ipsec访问总部内网资源和外网典型配置

IPSec VPN ACL 郑标 2018-06-19 发表

组网及说明



功能需求：

1、分支通过ipsec vpn访问内网资源

2、分支通过ipsec vpn到总部来访问外网

配置步骤

(1)　总部配置

```
#
interface GigabitEthernet0/0
 port link-mode route
 combo enable copper
 ip address 1.1.1.1 255.255.255.0
 nat outbound 3001
 ipsec apply policy map1
#
interface GigabitEthernet0/2
 port link-mode route
 combo enable copper
 ip address 192.168.1.1 255.255.255.0
#
 ip route-static 0.0.0.0 0 1.1.1.2
#
acl advanced 3000
 rule 0 permit ip destination 192.168.2.0 0.0.0.255
#
acl advanced 3001
 rule 0 deny ip destination 192.168.2.0 0.0.0.255
 rule 10 permit ip
#
ipsec transform-set tran1
 esp encryption-algorithm aes-cbc-128
 esp authentication-algorithm sha1
#
ipsec policy map1 10 isakmp
 transform-set tran1
 security acl 3000
 local-address 1.1.1.1
 remote-address 2.2.2.2
 ike-profile profile1
#
ike profile profile1
 keychain keychain1
 match remote identity address 2.2.2.2 255.255.255.0
#
ike keychain keychain1
 pre-shared-key address 2.2.2.2 255.255.255.0 key cipher $c$3$OZlydjTJAKne46C3JSeRRzaQBQO
DJw==
#
return
```

（2）分支配置

```
#
interface GigabitEthernet0/1
 port link-mode route
 combo enable copper
 ip address 2.2.2.2 255.255.255.0
 ipsec apply policy use1
#
interface GigabitEthernet0/2
 port link-mode route
 combo enable copper
 ip address 192.168.2.1 255.255.255.0
#
 ip route-static 0.0.0.0 0 2.2.2.1
#
acl advanced 3000
 rule 0 permit ip source 192.168.2.0 0.0.0.255
#
ipsec transform-set tran1
 esp encryption-algorithm aes-cbc-128
 esp authentication-algorithm sha1
#
ipsec policy use1 10 isakmp
 transform-set tran1
 security acl 3000
 local-address 2.2.2.2
 remote-address 1.1.1.1
 ike-profile profile1
#
ike profile profile1
 keychain keychain1
 match remote identity address 1.1.1.1 255.255.255.0
#
ike keychain keychain1
 pre-shared-key address 1.1.1.1 255.255.255.0 key cipher
$c$3$P/Rehq/mlfZ30RSn8GlrWYPY7EM9LA==
#
return
```

配置关键点

（1）分支感兴趣流只匹配源地址为本端私网地址，目的地址为any；总部感兴趣流只匹配目的地址为对端私网地址，源地址为any；

（2）总部nat中调用的acl注意先把ipsec感兴趣流deny掉。