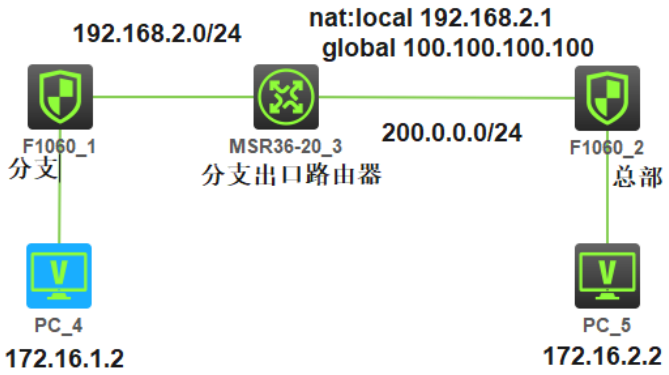
v7 SecPath 防火墙通过user-fqdn穿越nat主模式建立ipsec vpn

IPSec VPN 王永杰 2020-04-08 发表

组网及说明



配置步骤

需求：分支与总部建立ipsec vpn，保护分支内部网段172.16.1.0与总部内部网段172.16.2.2流量通信。分支防火墙非出口设备，需要在出口路由器做nat转换，所以使用user-fqdn的形式穿越nat来协商建立ike sa。

分支防火墙配置:

```
sysname fenzhi
#
interface GigabitEthernet1/0/2
ip address 192.168.2.1 255.255.255.0
tcp mss 1024  //调整接口tcp mss 防止封装esp报头后报文过大分片导致网页打开慢或无法打开
ipsec apply policy fenzhi  //调用ipsec 策略
#
interface GigabitEthernet1/0/3
ip address 172.16.1.1 255.255.255.0
#
security-zone name Trust
import interface GigabitEthernet1/0/3
#
security-zone name Untrust
import interface GigabitEthernet1/0/2
#
ip route-static 0.0.0.0 0 192.168.2.2
#
acl advanced 3000 //定义ipsec 感兴趣流
rule 0 permit ip source 172.16.1.0 0.0.0.255 destination 172.16.2.0 0.0.0.255
#
security-policy ip  //测试时方便，安全策略放全通
rule 0 name permit
action pass
#
ipsec transform-set fenzhi //配置ipsec 安全提议
esp encryption-algorithm 3des-cbc //配置协议（缺省ESP） 采用加密算法
esp authentication-algorithm md5 //配置协议采用的加密算法
#
ipsec policy fenzhi 1 isakmp //创建ipsec策略
transform-set fenzhi //指定ipsec 安全提议
security acl 3000 //指定感兴趣流
remote-address 200.0.0.2 //指定ipsec隧道对端地址
ike-profile fenzhi  //指定ike-profile
#
```

ike identity user-fqdn fenzhi //配置ike user-fqdn
#
ike profile fenzhi //配置ike-profile，缺省就是主模式
keychain fenzhi //指定采用预共享密钥认证时使用的keychain
local-identity user-fqdn fenzhi 指定本端 user-fqdn
match remote identity user-fqdn zongbu 指定对端user-fqdn
proposal 1 //指定ike 提议
#
ike proposal 1 //配置ike提议
encryption-algorithm 3des-cbc //指定ike提议使用的加密算法
dh group2 //指定ike第一阶段密钥协商使用的dh密钥交换参数
authentication-algorithm md5 //指定ike提议使用的认证算法
#
ike keychain fenzhi //配置ike keychain
pre-shared-key address 0.0.0.0 0.0.0.0 key simple 111111 //配置ike keychain的共享密钥
#
ike nat-keepalive 10 //配置向对端发送nat keepalive报文间隔
分支出口路由器配置：
interface GigabitEthernet0/0
ip address 192.168.2.2 255.255.255.0
#
interface GigabitEthernet0/1
ip address 200.0.0.1 255.255.255.0
nat static enable
#
nat static outbound 192.168.2.1 100.100.100.100
总部防火墙配置：
sysname zongbu
#
interface GigabitEthernet1/0/2
ip address 200.0.0.2 255.255.255.0
tcp mss 1024
ipsec apply policy zongbu
#
interface GigabitEthernet1/0/3
ip address 172.16.2.1 255.255.255.0
#
security-zone name Trust
import interface GigabitEthernet1/0/3
#
security-zone name Untrust
import interface GigabitEthernet1/0/2
#
ip route-static 0.0.0.0 0 200.0.0.1
#
acl advanced 3005
rule 0 permit ip source 172.16.2.0 0.0.0.255 destination 172.16.1.0 0.0.0.255
#
security-policy ip
rule 0 name permit
action pass
#
ipsec transform-set zongbu
esp encryption-algorithm 3des-cbc
esp authentication-algorithm md5
#
ipsec policy zongbu 10 isakmp
transform-set zongbu
security acl 3005
remote-address 100.100.100.100
ike-profile zongbu
#
ike identity user-fqdn zongbu
#

```
ike profile zongbu
keychain zongbu
match remote identity user-fqdn fenzhi
proposal 2
#
ike proposal 2
encryption-algorithm 3des-cbc
dh group2
authentication-algorithm md5
#
ike keychain zongbu
pre-shared-key address 0.0.0.0 0.0.0.0 key simple 111111
```

配置关键点

1、 主模式对接两端均可触发ipsec sa建立，需要注意总部fw ipsec 策略 的remote-address 需要写分支路由器nat后的地址

2、 两端设备感兴趣流 security acl 需要对称写，否则只能是更精细的一侧能触发ipsec sa建立后，才能互相通信。如果由粗略的一侧触发只会建立ike sa，无法建立ipsec sa