

问题描述

V7设备与Juniper防火墙做ipsec

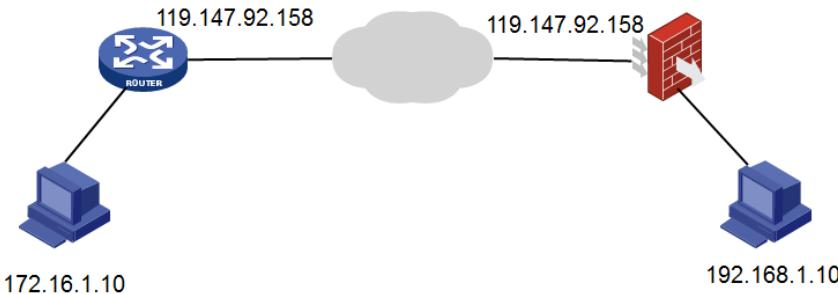
解决方法

功能需求:

总部双出口，分支为Juniper防火墙，为了保证总部于分支的局域网可以正常互通，同时，也要保证数据传输的安全性，需要使用ipsec VPN来实现该功能

组网信息及描述:

总部存在172.16.0.0/16的网段，分支存在192.168.0.0/16的网段，两端通过固定地址建立ipsec VPN。



配置步骤:

第 1 步：我司设备主要配置

```
#  
controller Cellular0/0  
#  
controller Cellular0/1  
#  
interface Aux0  
#  
interface Ethernet1/0  
port link-mode route  
#  
interface Ethernet1/0.1  
ip policy-based-route 1  
#  
interface Ethernet1/0.2  
ip address 172.16.2.1 255.255.255.0  
vlan-type dot1q vid 2  
ip policy-based-route 1  
#  
interface Ethernet1/0.3  
ip address 172.16.3.1 255.255.255.0  
vlan-type dot1q vid 3  
ip policy-based-route 1  
#  
interface Ethernet1/0.4  
ip address 172.16.4.1 255.255.255.0  
vlan-type dot1q vid 4  
ip policy-based-route 1  
#  
interface Ethernet1/0.5  
ip address 172.16.5.1 255.255.255.0  
vlan-type dot1q vid 5  
ip policy-based-route 1  
#
```

```
interface Ethernet1/1
port link-mode route
#
interface Ethernet1/1.1
ip policy-based-route 1
#
interface Ethernet1/1.2
ip policy-based-route 1
#
interface Ethernet1/1.6
ip address 172.16.6.1 255.255.255.0
vlan-type dot1q vid 6
ip policy-based-route 1
#
interface Ethernet1/2
port link-mode route
#
interface Ethernet1/2.7
ip address 172.16.7.1 255.255.255.0
vlan-type dot1q vid 7
ip policy-based-route 1
#
interface Ethernet1/3
port link-mode route
#
interface Virtual-Template1
ppp authentication-mode chap domain system
remote address pool 7
ip address 172.16.10.1 255.255.255.0
#
interface NULL0
#
interface LoopBack0
#
interface GigabitEthernet0/1
port link-mode route
ip address 219.133.71.196 255.255.255.248
nat outbound 3006
ipsec apply policy JJS      //绑定ipsec策略
#
ip route-static 0.0.0.0 Dialer1 //此路由作为备份
ip route-static 0.0.0.0 219.133.71.193 preference 50      //默认路由优先走固定地址接口
ip route-static 119.147.92.158 32 219.133.71.193
#
acl advanced 3005 //配置ipsec的兴趣流
rule 0 permit ip source 172.16.0.0 0.0.255.255 destination 192.168.0.0 0.0.255.255
#
acl advanced 3006 //配置地址转换acl, 禁止ipsec感兴趣流量进行抵制转换
rule 0 deny ip source 172.16.0.0 0.0.255.255 destination 192.168.0.0 0.0.255.255
rule 5 permit ip
#
ipsec transform-set JJS      //创建ipsec安全提议
esp encryption-algorithm 3des-cbc
esp authentication-algorithm sha1
pfs dh-group2
#
ipsec policy JJS 10 isakmp //创建ipsec策略
transform-set JJS
security acl 3005
local-address 219.133.71.196
remote-address 119.147.92.158
ike-profile JJS
sa duration time-based 3600
#
```

```
ike profile JJS      //创建ipsec profile
keychain JJS
local-identity address 219.133.71.196
match remote identity address 119.147.92.158 255.255.255.255
proposal 1
#
ike proposal 1      //创建ike proposal
encryption-algorithm 3des-cbc
dh group2
authentication-algorithm md5
sa duration 28800
#
ike keychain JJS    //创建ike keychain
pre-shared-key address 119.147.92.158 255.255.255.255 key cipher $c$3$YsnapP3lxP/mnLekI3KO
Lxuzakii9rW6NQ==
#
return
```

## 第 2 步：Juniper 配置

### 1、创建ike proposal

<http://kms.h3c.com/uploadfile/20151103/141255774001127153738.png>

2、创建ike对等体，使用主模式对接

<http://kms.h3c.com/uploadfile/20151103/141338268401743939179.png>

3、创建ike对等体的预共享密钥

<http://kms.h3c.com/uploadfile/20151103/141418984401214721836.png>

4、在ike对等体中指定对端公网地址

<http://kms.h3c.com/uploadfile/20151103/14153852880398378782.png>

5、配置ipsec proposal

<http://kms.h3c.com/uploadfile/20151103/14165370520175210814.png>

6、配置ipsec策略，使用dh-group2

<http://kms.h3c.com/uploadfile/20151103/14175222080571428251.png>

7、创建ipsec策略，绑定ike对等体和ipsec模版

<http://kms.h3c.com/uploadfile/20151103/141850939201243951793.png>

8、创建ipsec感兴趣流量

return

<http://kms.h3c.com/uploadfile/20151103/142038438801132151374.png>

9、将ipsec策略调用到相应的域间策略上，两个方向都需要调用。

<http://kms.h3c.com/uploadfile/20151103/14212597200793358628.png>

### 第3步：结果验证

```
[H3C-JJS]disp ike sa
Connection-ID  Remote      Flag      DOI
-----
3741          119.147.92.158   RD        IPsec
Flags:
RD--READY RL--REPLACED FD-FADING
[H3C-JJS]disp ips sa
-----
Interface: GigabitEthernet0/1
-----
IPsec policy: JJS
Sequence number: 10
Mode: ISAKMP
-----
Tunnel id: 0
Encapsulation mode: tunnel
Perfect forward secrecy: dh-group2
Inside VPN:
Path MTU: 1443
Tunnel:
  local address: 219.133.71.196
  remote address: 119.147.92.158
Flow:
  sour addr: 172.16.0.0/255.255.0.0 port: 0 protocol: ip
  dest addr: 192.168.0.0/255.255.0.0 port: 0 protocol: ip
[Inbound ESP SAs]
  SPI: 3719319854 (0xddb0512e)
  Connection ID: 7743826034786
  Transform set: ESP-ENCRYPT-3DES-CBC ESP-AUTH-SHA1
  SA duration (kilobytes/sec): 1843200/28800
  SA remaining duration (kilobytes/sec): 1843200/2206
```

```

Max received sequence-number: 0
Anti-replay check enable: Y
Anti-replay window size: 64
UDP encapsulation used for NAT traversal: N
Status: Active
[Outbound ESP SAs]
    SPI: 159650169 (0x09841179)
    Connection ID: 11343008628835
    Transform set: ESP-ENCRYPT-3DES-CBC ESP-AUTH-SHA1
    SA duration (kilobytes/sec): 1843200/28800
    SA remaining duration (kilobytes/sec): 1839651/2206
    Max sent sequence-number: 55990
    UDP encapsulation used for NAT traversal: N
    Status: Active

```

#### 第1步：我司设备主要配置

```

#
policy-based-route 1 permit node 1
if-match acl 3002
apply output-interface Dialer1
#
policy-based-route 1 permit node 2
if-match acl 3003      //创建空节点，使内网互访的流量不走策略路由
#
policy-based-route 1 permit node 3
if-match acl 3004      //创建空节点，使ipsec互访的流量不走策略路由
#
policy-based-route 1 permit node 4
if-match acl 3001
apply output-interface Dialer1
#
controller Cellular0/0
#
controller Cellular0/1
#
interface Aux0
#
interface Dialer1 //配置拨号
ppp chap password cipher $c$3$wfoaPwdepAprIG9fHN700HiHoIG3KllgtVk
ppp chap user 075506566013@163.gd
ppp pap local-user 075506566013@163.gd password cipher
$c$3$WWO/uBLpX90iMJRESCyeJKLNv3dsxAyNUI+1
dialer bundle enable
dialer-group 1
dialer timer idle 0
dialer timer autodial 60
ip address ppp-negotiate
nat outbound 3001
#
interface Ethernet1/0
port link-mode route
#
interface Ethernet1/0.1
ip policy-based-route 1
#
interface Ethernet1/0.2
ip address 172.16.2.1 255.255.255.0
vlan-type dot1q vid 2
ip policy-based-route 1
#
interface Ethernet1/0.3
ip address 172.16.3.1 255.255.255.0
vlan-type dot1q vid 3
ip policy-based-route 1

```

```
#  
interface Ethernet1/0.4  
ip address 172.16.4.1 255.255.255.0  
vlan-type dot1q vid 4  
ip policy-based-route 1  
#  
interface Ethernet1/0.5  
ip address 172.16.5.1 255.255.255.0  
vlan-type dot1q vid 5  
ip policy-based-route 1  
#  
interface Ethernet1/1  
port link-mode route  
#  
interface Ethernet1/1.1  
ip policy-based-route 1  
#  
interface Ethernet1/1.2  
ip policy-based-route 1  
#  
interface Ethernet1/1.6  
ip address 172.16.6.1 255.255.255.0  
vlan-type dot1q vid 6  
ip policy-based-route 1  
#  
interface Ethernet1/2  
port link-mode route  
#  
interface Ethernet1/2.7  
ip address 172.16.7.1 255.255.255.0  
vlan-type dot1q vid 7  
ip policy-based-route 1  
#  
interface Ethernet1/3  
port link-mode route  
#  
interface Virtual-Template1  
ppp authentication-mode chap domain system  
remote address pool 7  
ip address 172.16.10.1 255.255.255.0  
#  
interface NULL0  
#  
interface LoopBack0  
#  
interface GigabitEthernet0/0 //0口为拨号上网接口  
port link-mode route  
combo enable copper  
tcp mss 1460  
pppoe-client dial-bundle-number 1  
#  
interface GigabitEthernet0/1  
port link-mode route  
mtu 1400  
ip address 219.133.71.196 255.255.255.248  
tcp mss 1024  
nat outbound 3006  
nat server protocol tcp global 219.133.71.196 1521 inside 172.16.7.53 1521  
nat server protocol tcp global 219.133.71.196 8081 inside 172.16.2.218 8081  
nat server protocol tcp global 219.133.71.196 33099 inside 172.16.6.121 3389  
ipsec apply policy JJS //绑定ipsec策略  
#  
interface GigabitEthernet0/2  
port link-mode route
```

```
#  
scheduler logfile size 16  
#  
line class aux  
user-role network-admin  
#  
line class tty  
user-role network-operator  
#  
line class vty  
user-role network-operator  
#  
line aux 0  
user-role network-admin  
#  
line vty 0 4  
authentication-mode scheme  
user-role network-operator  
#  
line vty 5 63  
user-role network-operator  
#  
ip route-static 0.0.0.0 Dialer1 //此路由作为备份  
ip route-static 0.0.0.0 219.133.71.193 preference 50 //默认路由优先走固定地址接口  
ip route-static 119.147.92.158 32 219.133.71.193  
#  
acl advanced 3001  
rule 0 permit ip source 172.16.0.0 0.0.255.255  
rule 10 permit icmp  
#  
acl advanced 3002  
rule 1 permit ip destination 119.147.92.139 0  
rule 3 permit ip destination 119.147.92.141 0  
rule 5 permit ip destination 119.147.92.142 0  
rule 7 permit ip destination 119.147.92.146 0  
rule 9 permit ip destination 119.147.92.148 0  
rule 11 permit ip destination 119.147.92.149 0  
rule 13 permit ip destination 119.147.92.150 0  
rule 15 permit ip destination 119.147.92.154 0  
#  
acl advanced 3003  
rule 0 permit ip source 172.16.0.0 0.0.255.255 destination 172.16.0.0 0.0.255.255  
rule 5 permit ip destination 119.147.92.0 0.0.0.255  
rule 10 deny ip source 172.16.7.53 0 destination 172.16.0.0 0.0.255.255  
rule 15 permit ip source 172.16.7.53 0  
rule 20 deny ip source 172.16.2.218 0 destination 172.16.0.0 0.0.255.255  
rule 25 permit ip source 172.16.2.218 0  
rule 30 deny ip source 172.16.6.121 0 destination 172.16.0.0 0.0.255.255  
rule 35 permit ip source 172.16.6.121 0  
#  
acl advanced 3004  
rule 5 permit ip destination 172.16.10.0 0.0.0.255  
rule 10 permit ip source 172.16.0.0 0.0.255.255 destination 192.168.0.0 0.0.255.255  
#  
acl advanced 3005 //配置ipsec的兴趣流  
rule 0 permit ip source 172.16.0.0 0.0.255.255 destination 192.168.0.0 0.0.255.255  
#  
acl advanced 3006 //配置地址转换acl，禁止ipsec感兴趣流量进行抵制转换  
rule 0 deny ip source 172.16.0.0 0.0.255.255 destination 192.168.0.0 0.0.255.255  
rule 5 permit ip  
#  
ipsec transform-set JJS //创建ipsec安全提议  
esp encryption-algorithm 3des-cbc  
esp authentication-algorithm sha1
```

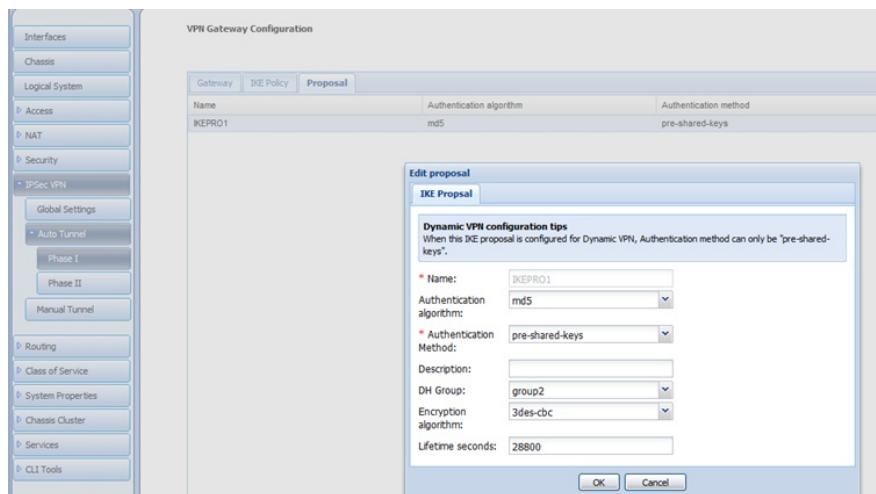
```

pfs dh-group2
#
ipsec policy JJS 10 isakmp //创建ipsec策略
transform-set JJS
security acl 3005
local-address 219.133.71.196
remote-address 119.147.92.158
ike-profile JJS
sa duration time-based 3600
#
l2tp-group 1 mode lns
allow l2tp virtual-template 1
undo tunnel authentication
tunnel name LNS
#
l2tp enable
#
ike profile JJS //创建ipsec profile
keychain JJS
local-identity address 219.133.71.196
match remote identity address 119.147.92.158 255.255.255.255
proposal 1
#
ike proposal 1 //创建ike proposal
encryption-algorithm 3des-cbc
dh group2
authentication-algorithm md5
sa duration 28800
#
ike keychain JJS //黄建ike keychain
pre-shared-key address 119.147.92.158 255.255.255.255 key cipher $c$3$YsnapP3lxP/mnLekI3KO
Lxuzaki9rW6NQ==
#
return

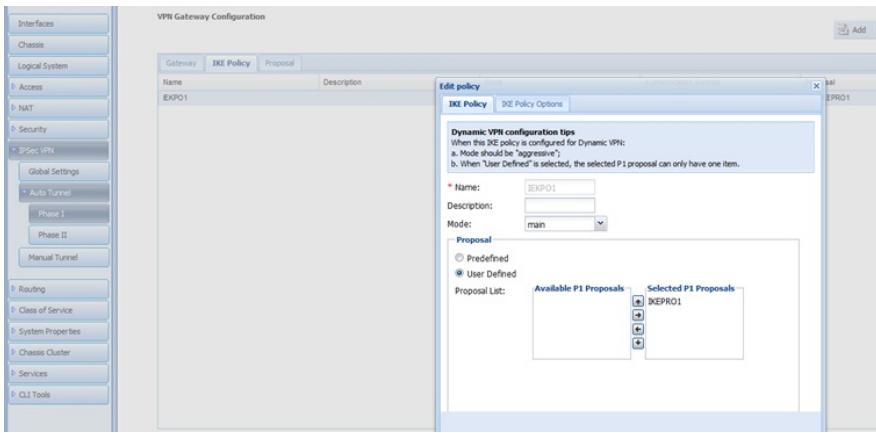
```

## 第 2 步: Juniper配置

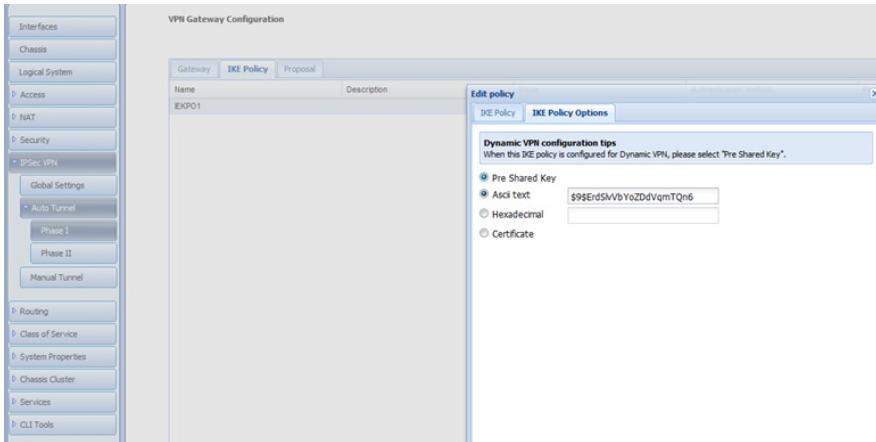
### 1、创建ike proposal



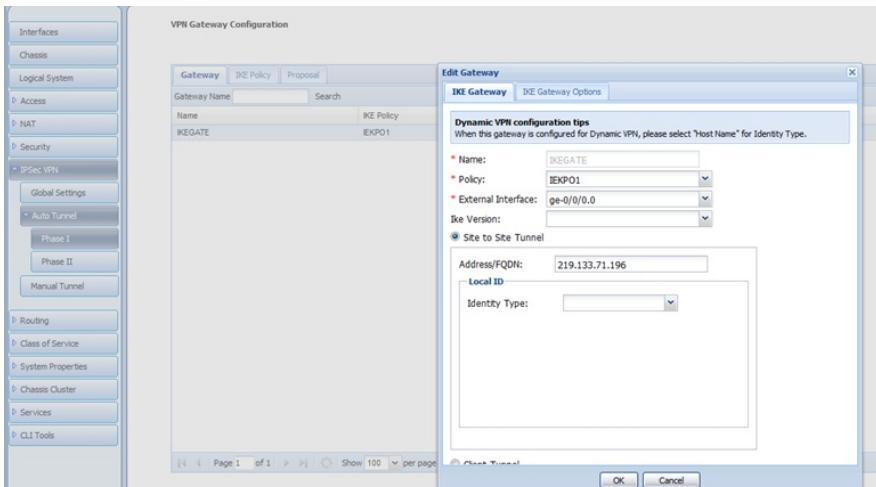
### 2、创建ike对等体，使用主模式对接



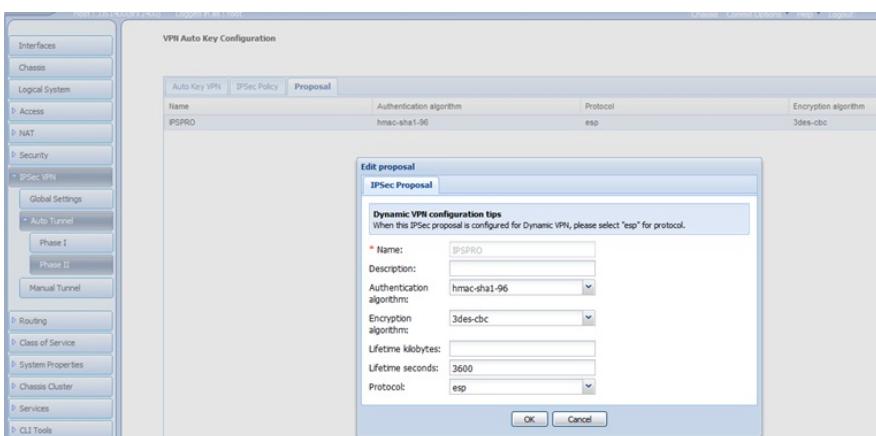
### 3、创建ike对等体的预共享密钥



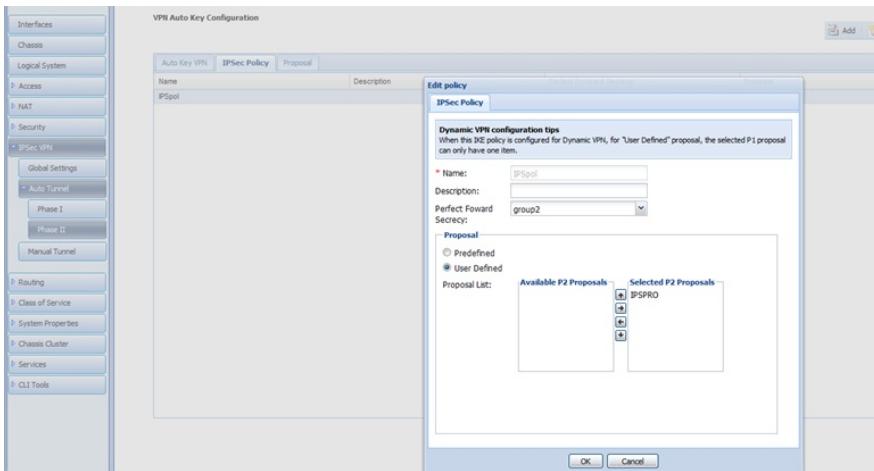
### 4、在ike对等体中指定对端公网地址



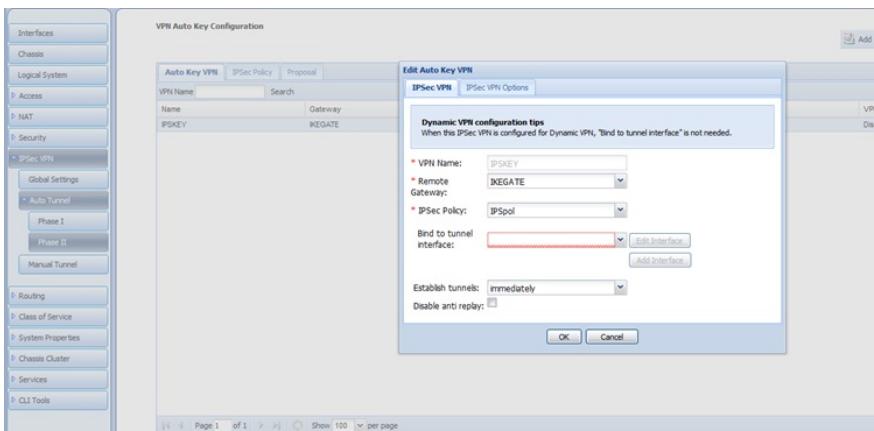
### 5、配置ipsec proposal



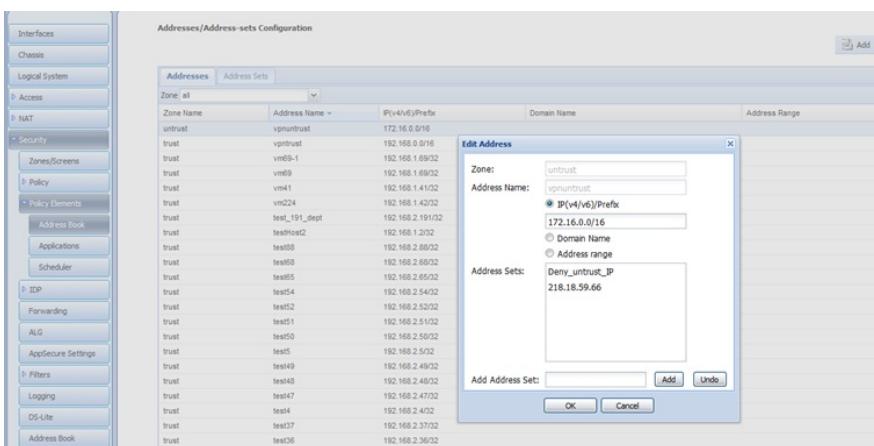
### 6、配置ipsec策略，使用dh-group2



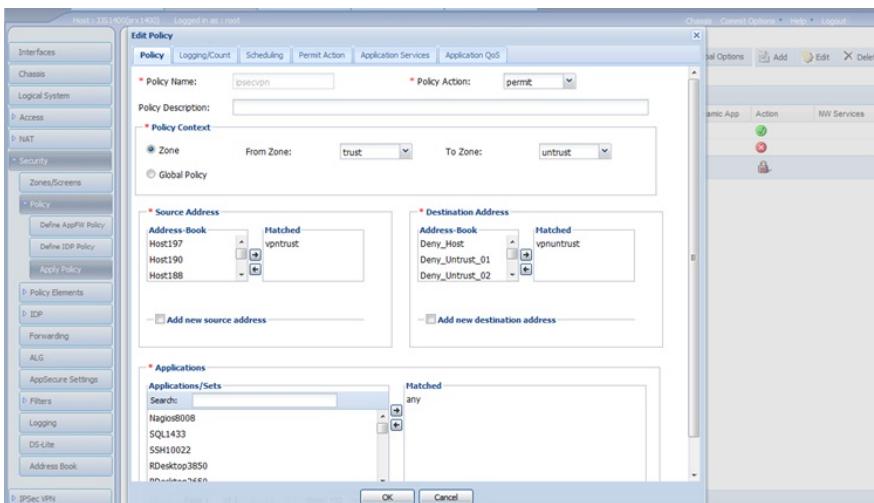
## 7、创建ipsec策略，绑定ike对等体和ipsec模版

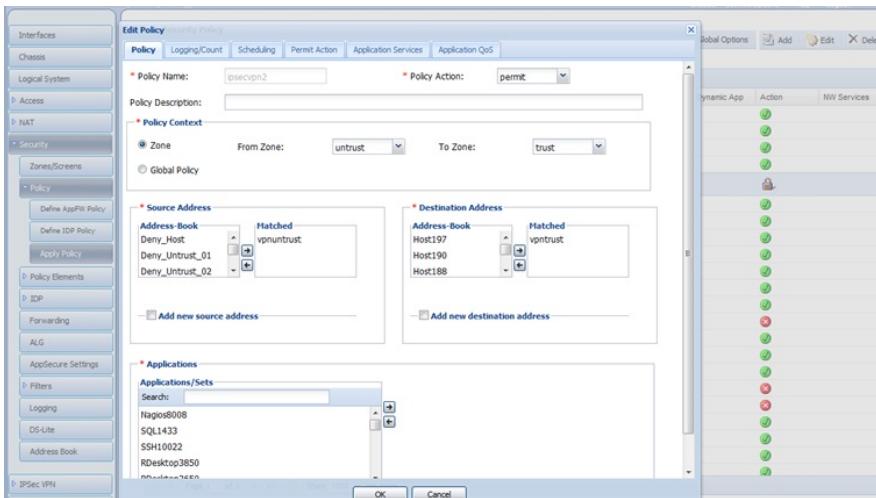


## 8、创建ipsec感兴趣流量



## 9、将ipsec策略调用到相应的域间策略上，两个方向都需要调用。





### 第3步：结果验证

```
[H3C-JJS]disp ike sa
Connection-ID Remote      Flag      DOI
-----
3741      119.147.92.158   RD       IPsec
Flags:
RD--READY RL--REPLACED FD-FADING
[H3C-JJS]disp ips sa
-----
Interface: GigabitEthernet0/1
-----
IPSec policy: JJS
Sequence number: 10
Mode: ISAKMP
-----
Tunnel id: 0
Encapsulation mode: tunnel
Perfect forward secrecy: dh-group2
Inside VPN:
Path MTU: 1443
Tunnel:
local address: 219.133.71.196
remote address: 119.147.92.158
Flow:
sour addr: 172.16.0.0/255.255.0.0 port: 0 protocol: ip
dest addr: 192.168.0.0/255.255.0.0 port: 0 protocol: ip
[Inbound ESP SAs]
SPI: 3719319854 (0xddb0512e)
Connection ID: 7743826034786
Transform set: ESP-ENCRYPT-3DES-CBC ESP-AUTH-SHA1
SA duration (kilobytes/sec): 1843200/28800
SA remaining duration (kilobytes/sec): 1843200/2206
Max received sequence-number: 0
Anti-replay check enable: Y
Anti-replay window size: 64
UDP encapsulation used for NAT traversal: N
Status: Active
[Outbound ESP SAs]
SPI: 159650169 (0x09841179)
Connection ID: 11343008628835
Transform set: ESP-ENCRYPT-3DES-CBC ESP-AUTH-SHA1
SA duration (kilobytes/sec): 1843200/28800
SA remaining duration (kilobytes/sec): 1839651/2206
Max sent sequence-number: 55990
UDP encapsulation used for NAT traversal: N
Status: Active
```

