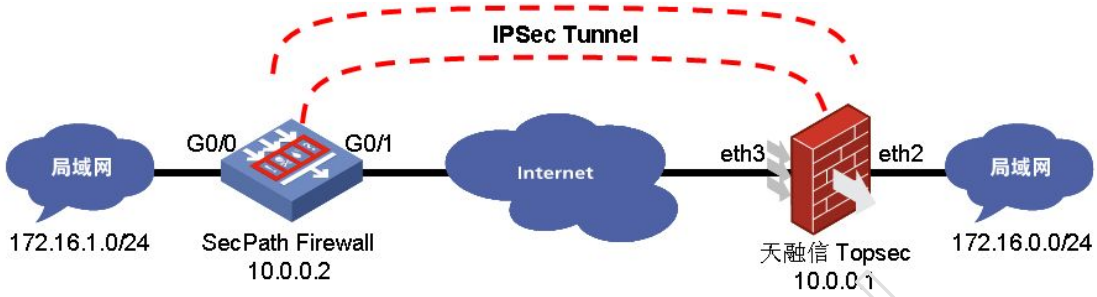
H3C SecPath 防火墙与天融信 Topsec 防火墙 IPSec 对接典型配置



应用环境拓扑

组网模式

1. H3C SecPath 防火墙与天融信防火墙的 IPSec 对接，包括主模式和野蛮模式；其中，野蛮模式时，我司设备为分支端，天融信防火墙为总部端。

详细配置（主模式）

1. SecPath 防火墙的 IPSec 配置(以下文档以 IPSec 配置为主，其他互通性的配置略)；

```
[SecPath]
firewall packet-filter default permit
#
ike peer 1                                  //定义IKE PEER
 pre-shared-key 1                           //预共享密钥为1
 remote-address 10.0.0.1                    //对端地址
 local-address 10.0.0.2                     //本端地址
#
ipsec proposal 1                            //定义安全提议
#
ipsec policy test 1 isakmp                  //定义安全策略
 security acl 3000                          //定义触发的数据流
 ike-peer 1                                 //采用的IKE PEER
 proposal 1                                 //定义使用的安全提议
#
acl number 3000
rule 1 permit ip source 172.16.1.0 0.0.0.255 destination 172.16.0.0 0.0.0.255
#
interface Aux0
 async mode flow
#
interface GigabitEthernet0/0
ip address 172.16.1.1 255.255.255.0
#
interface GigabitEthernet1/1
 ip address 10.0.0.2 255.255.255.0
 ipsec policy test                          //在外网接口上启用IPSec策略
#
```

```
firewall zone trust
 add interface GigabitEthernet0/0
#
firewall zone untrust
 add interface GigabitEthernet0/1
#
ip route-static 0.0.0.0 0.0.0.0 10.0.0.1

 [SecPath]dis ipsec proposal 1
        IPsec proposal name: 1
           encapsulation mode: tunnel
           transform: esp-new
           ESP protocol: authentication md5-hmac-96, encryption des
      [BJtyzx]dis ike proposal
      priority authentication authentication encryption Diffie-Hellman duration
       method                    algorithm      algorithm            group        (seconds)
    ---------------------------------------------------------------------------------------------
    default   PRE_SHARED      SHA            DES_CBC          MODP_768        86400
```

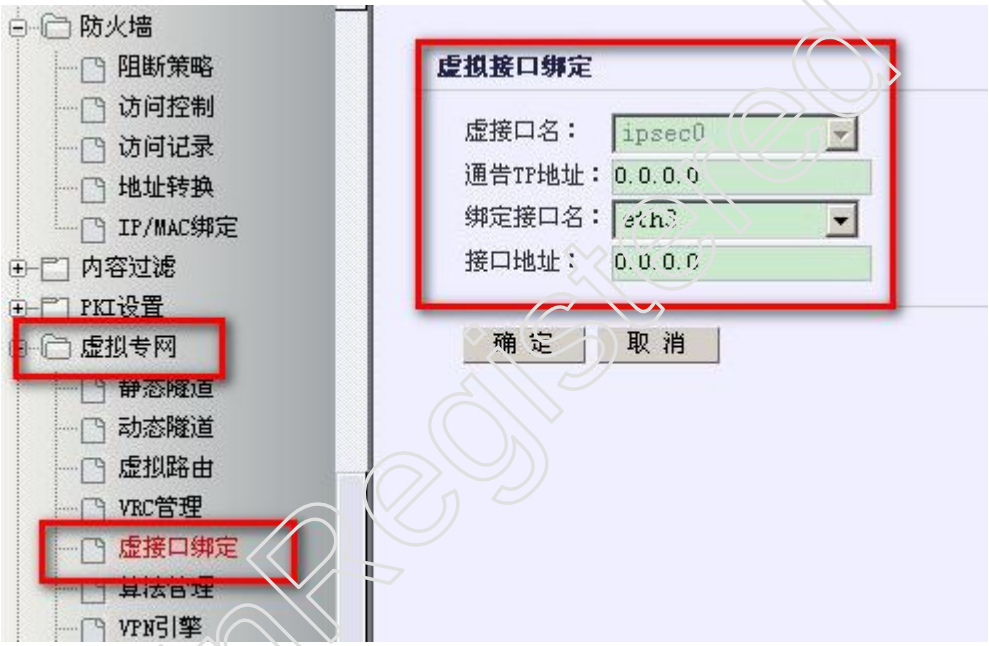
//查看我司设备IPSec/IKE协商的加密算法，天融信TOPSec防火墙的加密算法要和我司的加密算法相同

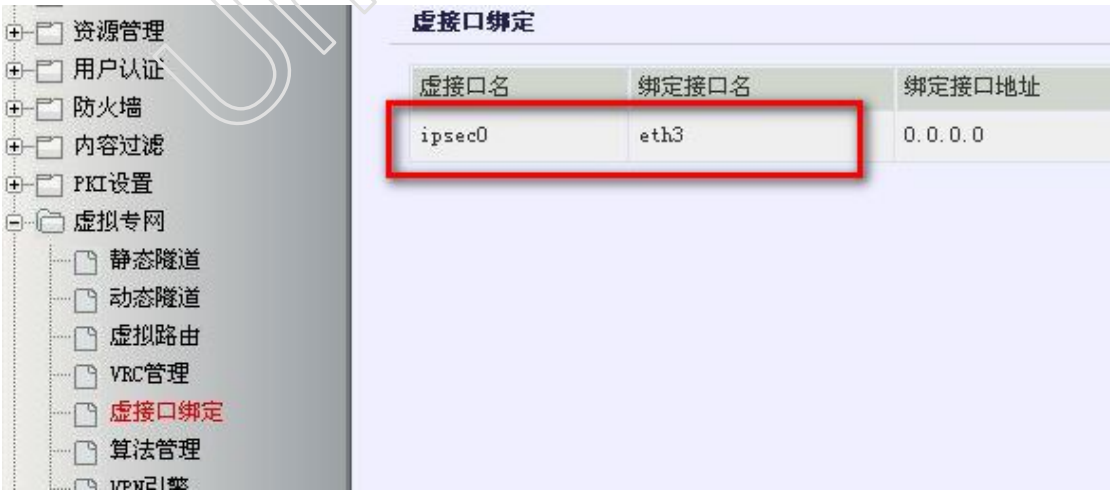
2. 天融信 Topsec 防火墙的 IPSec 配置(以下文档以 IPSec 配置为主，其他互通性的配置略)；

1）在“网络管理>>接口>>物理接口”配置选项卡界面下，配置接口 eth2 和 eth3 的 IP 地址，并保证防火墙域间策略开启 IPSec 相通的策略。

2）在“虚拟专网>>算法管理”配置选项卡界面下，加载 IPSec 相应的算法：在默认的配置情况下，TopSec 是没有加载 DES 算法的，这样可能造成 IPSec 对接不成功。

3）在“虚拟专网>>虚接口绑定”配置选项卡界面下，在 TopSec 防火墙的外网接口启用 IPSec 策略：“接口地址”配置 0.0.0.0 即意味着 TopSec 接收所有 IP 地址发来的 IPSec 协商请求，“绑定接口”即 TopSec 防火墙启用 IPSec 的接口，通常指的是外网接口。

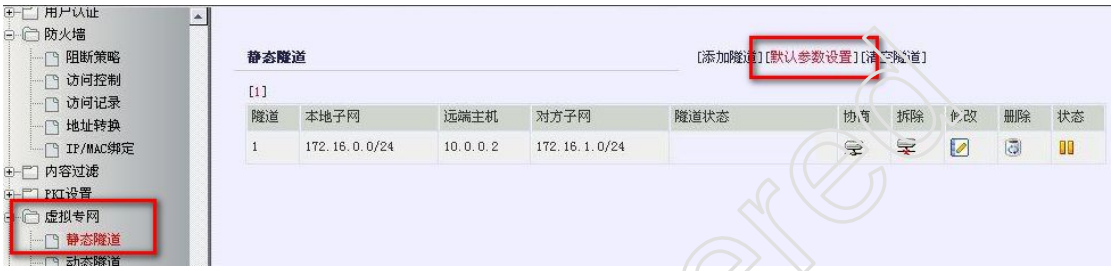


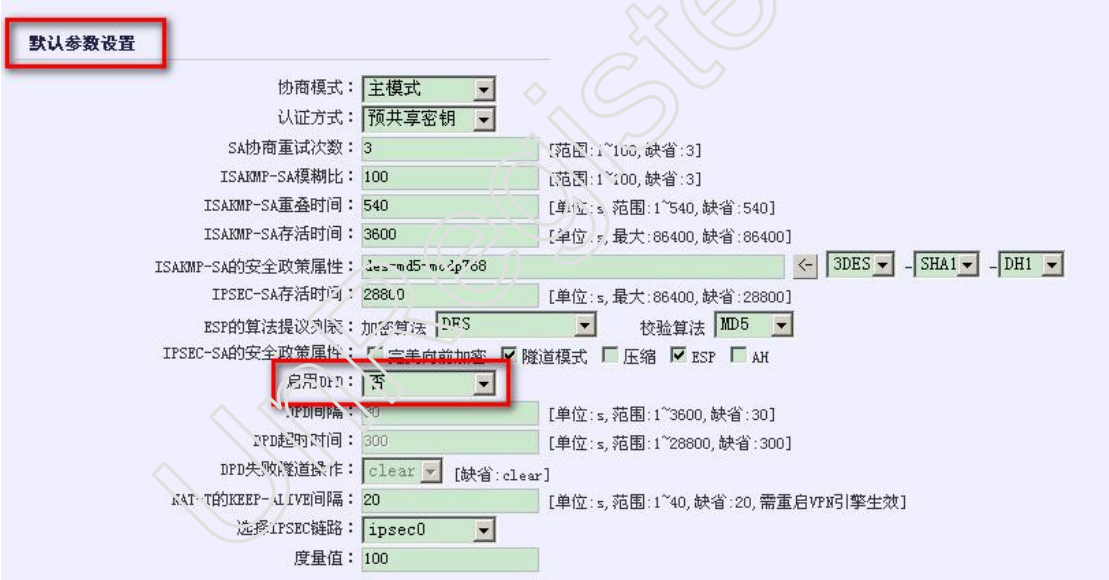


4）在“虚拟专网>>静态隧道>>添加隧道”配置选项卡界面下，新增一条 IPSec 隧道，类似我司的 IPSec proposal 和 ike proposal：唯一需要注意的是几个加密/验证算法要与我

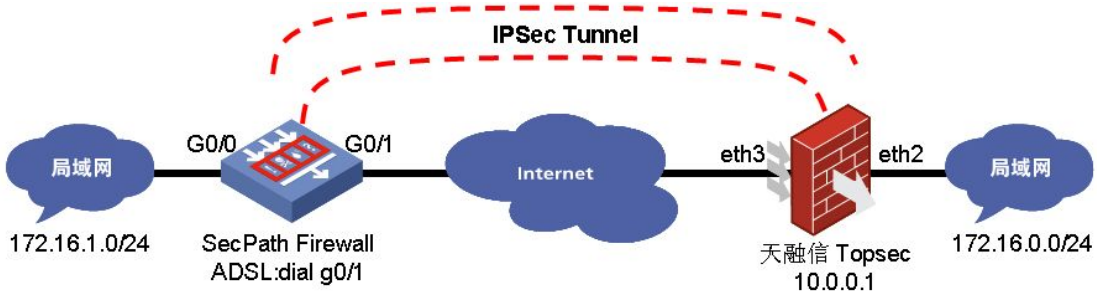
司设备算法保持一致。

5）在“虚拟专网>>静态隧道>>默认参数配置”配置选项卡界面下，调整 Topsec 防火墙 IPSec 参数中的“DPD”配置：**这个配置非常重要，必须将“启用 DPD”配置选项强制为“否”，否则，IPSec 肯定无法协商成功。**





6）在“虚拟专网>>静态隧道”配置选项卡界面下，可以查看到 IPSec 隧道已经协商成功：



应用环境拓扑

详细配置（野蛮模式）

1. SecPath 防火墙的 IPSec 配置(以下文档以 IPSec 配置为主，其他互通性的配置略)；

```
[SecPath]
firewall packet-filter default permit
#
ike peer 1                                  //定义 IKE PEER
 exchange-mode aggressive                   //IKE 交换模式为野蛮模式
 pre-shared-key 1                           //预共享密钥为 1
 id-type name                               //ID 的类型为名字
 remote-address 10.0.0.1                    //对端地址
 remote-name zhongxin                       //对端名字为 zhongxin
 nat traversal                              //支持 NAT 穿越
#
ipsec proposal 1                            //定义安全提议
#
ipsec policy test 1 isakmp                  //定义安全策略
 security acl 3000                          //定义触发的数据流
 ike-peer 1                                 //采用的IKE PEER
 proposal 1                                 //定义使用的安全提议
#
acl number 3000
rule 1 permit ip source 172.16.1.0 0.0.0.255 destination 172.16.0.0 0.0.0.255
#
interface Aux0
 async mode flow
#
interface GigabitEthernet0/0
ip address 172.16.1.1 255.255.255.0
#
interface GigabitEthernet1/1
 pppoe-client dial-bundle-number 1          //绑定拨号口
#
interface Dialer1                           //定义拨号口
link-protocol ppp
ppp pap local-user 123 password simple 123  //拨号的用户和密码
ip address ppp-negotiate                    //定义协商地址
dialer user test
dialer-group 1
dialer bundle 1
ipsec policy policy1                        //在外网接口上启用IPSec策略
#
firewall zone trust
```

```
 add interface GigabitEthernet0/0
#
firewall zone untrust
 add interface GigabitEthernet0/1
 add interface Dialer1
#
ip route-static 0.0.0.0 0.0.0.0 Dialer 1

 [SecPath]dis ipsec proposal 1
        IPsec proposal name: 1
           encapsulation mode: tunnel
           transform: esp-new
           ESP protocol: authentication md5-hmac-96, encryption des
       [BJtyzx]dis ike proposal
       priority authentication authentication encryption Diffie-Hellman duration
        method                    algorithm      algorithm            group        (seconds)
     ------------------------------------------------------------------------------------------
     default   PRE_SHARED      SHA            DES_CBC          MODP_768        86400
```

*//查看我司设备**IPSec/IKE**协商的加密算法，天融信**TOPSec**防火墙的加密算法要和我司的加密算法相同*

2. 天融信 Topsec 防火墙的 IPSec 配置(以下文档以 IPSec 配置为主，其他互通性的配置略)；

注意点：在以H3C SecPath防火墙为IPSec分支端情况下，天融信的防火墙上的IPSec配置与主模式的配置几乎完全完全一致，唯一不同地方的配置如下截图：

1）在“虚拟专网>>静态隧道>>添加隧道”配置选项卡界面下，新增IPSec隧道时，“对方地址或者域名”选项中配置的IPSec对端地址为：0.0.0.0.

2）特别注意：

即便是野蛮模式的IPSec对接，天融信防火墙IPSec“第一阶段协商”依然应该选择“主模式”，如果选择“野蛮模式”则会对接失败；

我分析天融信这块的配置实际上不是指IPSec协商方式，而是指天融信防火

墙设备所处的状态：在我司设备为分支端，而天融信防火墙为中心端时，对于天融信防火墙而言，不主动发起协商请求，与主模式相比，工作机制完全一致，所以，这里就应该选择“主模式”。

如果分支端是天融信防火墙，而中心端是我司设备，那么这里可能就要选择“野蛮模式”了。