ORB305 与 H3C Router 构建 IPSEC VPN 配置指导手册

东用科技有限公司

发布日期 2020-08-21

一、H3C Router 配置：

<H3CRouter>system-view　　//进入配置模式

[H3CRouter]local-user admin　　//添加本地用户

[H3CRouter-luser-cisco]password simple admin　//为添加的用户设置密码

[H3CRouter-luser-cisco]service-type web　　//开启网页配置功能

[H3CRouter-luser-cisco]quit

[H3CRouter]Ethernetinterface Ethernet 0/0　//进入接口配置模式

[H3CRouter-Ethernet0/0] ip address 123.15.36.140 255.255.255.128//配置外网接口地址

[H3CRouter-Ethernet0/0] quit　　//退出接口配置模式

[H3CRouter-Ethernet0/1] ip address 172.18.253.1 255.255.255.0 //配置内外接口地址

[H3CRouter-Ethernet0/0] quit　　//退出接口配置模式

[H3CRouter] ip route-static 0.0.0.0 0.0.0.0 123.15.36.129 //配置静态路由

[H3CRouter]acl number 3000　　//创建访问控制列表

[H3CRouter-acl-3000]rule 5 permit ip source 172.18.253.0 0.0.0.255//允许内网网段访问公网

[H3CRouter-Ethernet0/0] quit　　//退出接口配置模式

[H3CRouter]acl number 3001　　//创建访问控制列表

[H3CRouter-acl-3001] rule 0 permit ip source 172.18.253.0 0.0.0.255 destination 192.168.0.0 0.0.255.255

rule 5 deny ip　　//拒绝除内网网段以为的网段访问远端子网

[H3CRouter]Ethernetinterface Ethernet 0/0　//进入接口配置模式

[H3CRouter-Ethernet0/0]nat outbound 3000 //在外网接口上启用 ACL 3000

[H3CRouter-Ethernet0/0]quit //退出接口配置模式

[H3CRouter]ike proposal 1 //创建 IKE 提议，并进入 IKE 提议视图

[H3CRouter]ike peer fenzhi //创建一个 IKE 对等体，并进入 IKE-Peer 视图

[H3CRouter-ike-peer-fenzhi]exchange-mode aggressive //配置 IKE 第一阶段的协商为野蛮模式

[H3CRouter-ike-peer-fenzhi]proposal 1 //配置 IKE 对等体引用的 IKE 安全提议

[H3CRouter-ike-peer-fenzhi]pre-shared-key simple abc123 //配置采用预共享密钥认证时，所使用的预共享密钥

[H3CRouter-ike-peer-fenzhi]id-type name //选择 IKE 第一阶段的协商过程中使用 ID 的类型

[H3CRouter-ike-peer-fenzhi]remote-name fenzhi //配置对端安全网关的名字

[H3CRouter-ike-peer-fenzhi]remote-address fenzhi dynamic //配置对端安全网关的 IP 地址

[H3CRouter-ike-peer-fenzhi]local-address 123.15.36.140 //配置本端安全网关的 IP 地址

H3CRouter-ike-peer-fenzhi] local-name center //配置本端安全网关的名字

[H3CRouter-ike-peer-fenzhi] nat traversal //配置 IKE/IPsec 的 NAT 穿越功能

[H3CRouter-ike-peer-fenzhi]quit

[H3CRouter] ipsec transform-set fenzhi //配置 IPsec 安全提议 fenzhi

[H3CRouter-ipsec-transform-set-tran1] encapsulation-mode tunnel //报文封装形式采用隧道模式

[H3CRouter-ipsec-transform-set-tran1] transform esp // 安全协议采用 ESP 协议

[H3CRouter-ipsec-transform-set-tran1] esp encryption-algorithm 3des //选择 ESP 协议采用的加密算法

[H3CRouter-ipsec-transform-set-tran1] esp authentication-algorithm md5 //选择 ESP 协议采用的认证算法

[H3CRouter-ipsec-transform-set-tran1] quit

[H3CRouter]ipsec policy 983040 1 isakmp //创建一条 IPsec 安全策略,协商方式为 isakmp

[H3CRouter-ipsec-policy-isakmp-use1-10] security acl 3001 //引用访问控制列表 3001

[H3CRouter-ipsec-policy-isakmp-use1-10] transform-set fenzhi //引用 IPsec 安全提议

[H3CRouter-ipsec-policy-isakmp-use1-10] ike-peer fenzhi // 引用 IKE 对等体

[H3CRouter-ipsec-policy-isakmp-use1-10] quit

[H3CRouter] interface ethernet 0/0 //进入外部接口

[H3CRouter-Ethernet0/1] ipsec policy 983040 //在外部接口上应用 IPsec 安全策略组

验证配置结果

```
[H3CRouter] display ike proposal
  priority authentication authentication encryption Diffie-Hellman duration
                           method             algorithm       algorithm
      group              (seconds)
-------------------------------------------------------------------------
--
   10              PRE_SHARED          MD5                  DES_CBC
        MODP_768              5000
```

```
  default   PRE_SHARED          SHA                   DES_CBC
  MODP_768              86400
[H3CRouter] display ike proposal
  priority authentication authentication encryption Diffie-Hellman duration
                           method             algorithm       algorithm
      group              (seconds)
------------------------------------------------------------------------
--
  default   PRE_SHARED          SHA                   DES_CBC
  MODP_768              86400
```

可通过如下显示信息查看到 IKE 协商成功后生成的两个阶段的 SA。

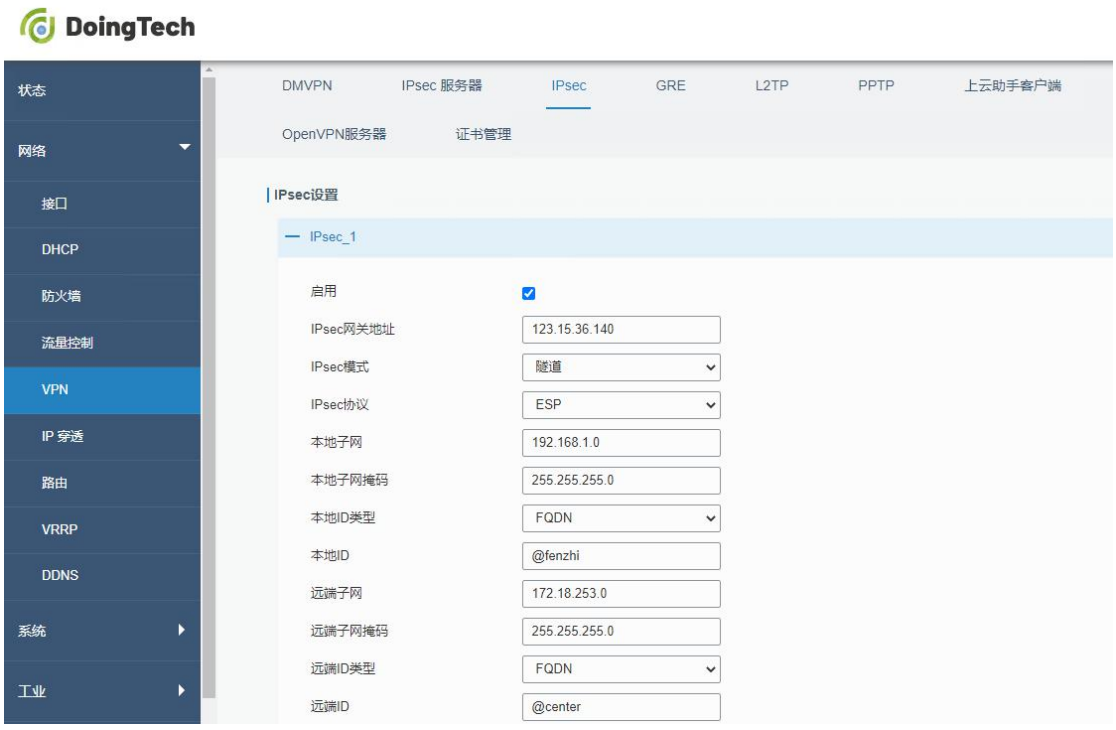
```
[H3CRouter] display ike sa
      total phase-1 SAs:   1
      connection-id   peer                       flag                phas
e     doi
   -----------------------------------------------------
        1                          219.140.142.211             RD|ST
            1         IPSEC
        2                          219.140.142.211             RD|ST
            2         IPSEC

   flag meaning
   RD--READY ST--STAYALIVE RL--REPLACED FD--FADING TO—TIMEOUT RK-REKEY
```

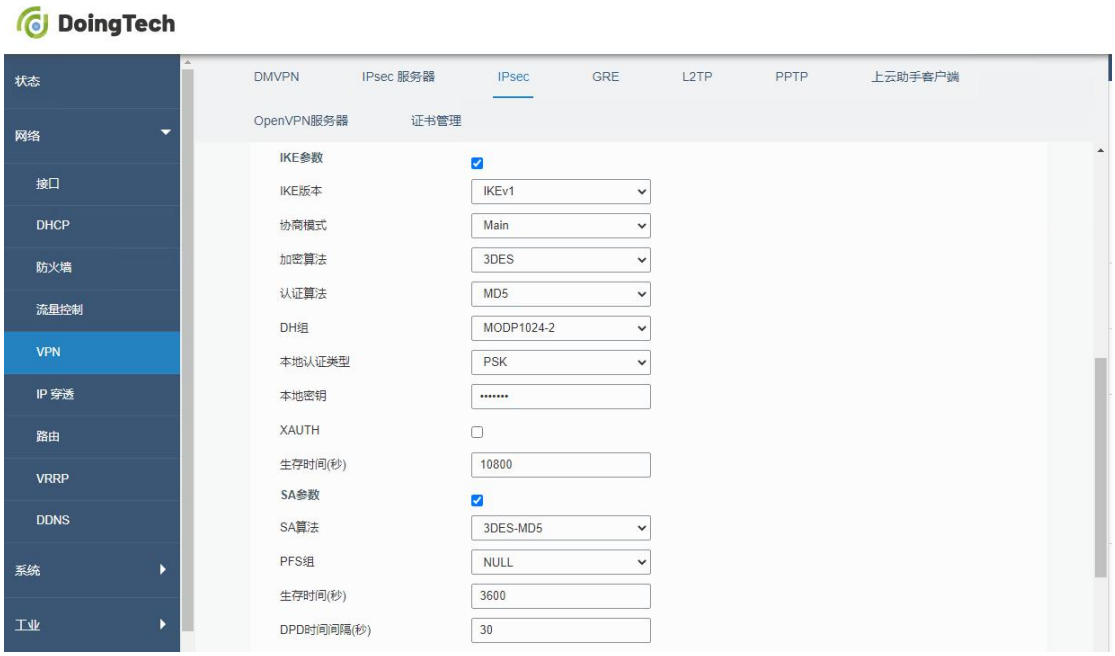
IKE 第二阶段协商生成的 IPsec SA 用于保护子网 10.1.1.0/24 与子网 10.1.2.0/24 之间的数据流，可通过如下显示信息查看。

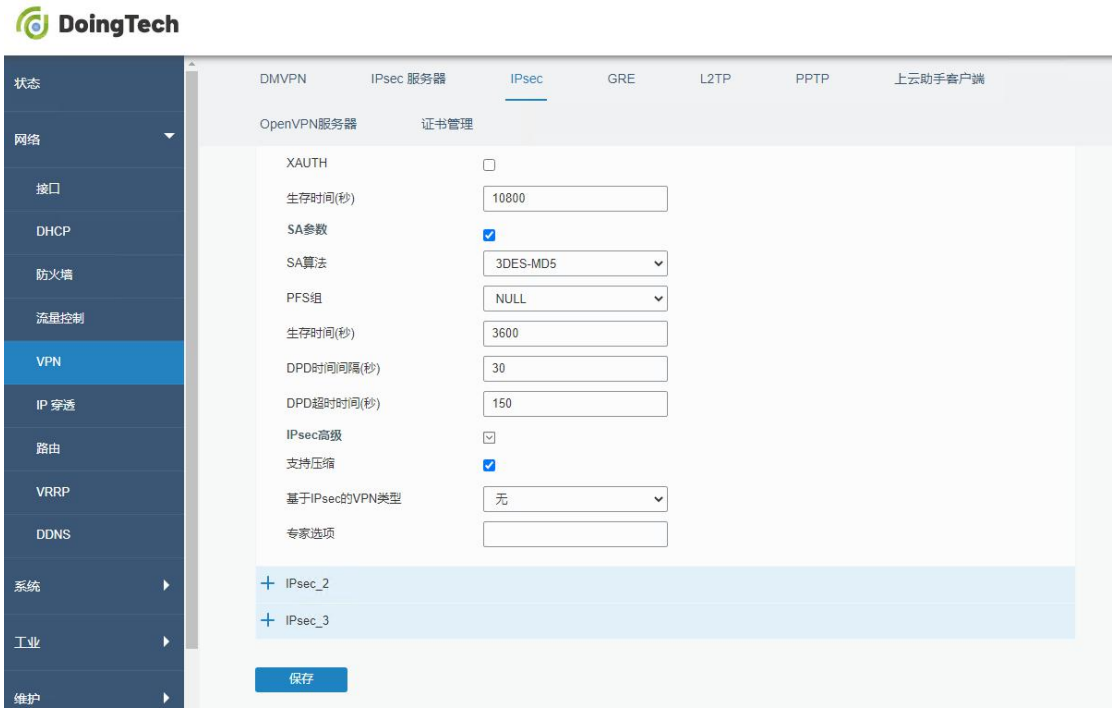
```
[H3CRouter] display ipsec sa
==============================
Interface: Ethernet0/1
       path MTU: 1500
==============================

   ----------------------------
   IPsec policy name: "map1"
    sequence number: 10
   acl version: ACL4
   mode: isakmp
   ----------------------------
       PFS: N, DH group: none
       tunnel:
              local    address: 123.15.36.140
```

```
            remote address: 219.140.142.211
        flow:
            sour addr: 172.18.253.0/255.255.255.0    port: 0    protocol:
IP
            dest addr: 192.168.2.0/255.255.255.0    port: 0    protocol:
IP

        [inbound ESP SAs]
            spi: 0x3D6D3A62(1030568546)
            transform: ESP-ENCRYPT-DES ESP-AUTH-SHA1
            in use setting: Tunnel
            connection id: 1
            sa duration (kilobytes/sec): 1843200/3600
            sa remaining duration (kilobytes/sec): 1843199/3590
            anti-replay detection: Enabled
                anti-replay window size(counter based): 32
            udp encapsulation used for nat traversal: N

        [outbound ESP SAs]
            spi: 0x553FAAE(89389742)
            transform: ESP-ENCRYPT-DES ESP-AUTH-SHA1
            in use setting: Tunnel
            connection id: 2
            sa duration (kilobytes/sec): 1843200/3600
            sa remaining duration (kilobytes/sec): 1843199/3590
            anti-replay detection: Enabled
                anti-replay window size(counter based): 32
            udp encapsulation used for nat traversal: N
```

二、ORB305 IPSEC VPN 配置






DoingTech
状态
网络
接口
DHCP
防火墙
流量控制
VPN
IP 穿透
路由
VRRP
DDNS
系统
工业
维护
DMVPN
IPsec 服务器
IPsec
GRE
L2TP
PPTP
上云助手客户端
OpenVPN服务器
证书管理
XAUTH
生存时间(秒)
10800
SA参数
SA算法
3DES-MD5
PFS组
NULL
生存时间(秒)
3600
DPD时间间隔(秒)
30
DPD超时时间(秒)
150
IPsec高级
支持压缩
基于IPsec的VPN类型
无
专家选项
IPsec_2
IPsec_3
保存