F1000-AK系列防火墙和ERG2路由器IPsec VPN野蛮模式配置

IPSec VPN　程咪　2019-09-23 发表

组网及说明

1 配置需求或说明

1.1 适用的产品系列

本案例适用于如F1000-AK180、F1000-AK170等F1000-AK系列的防火墙。

ERG2 产品系列路由器：ER8300G2-X、ER6300G2、ER3260G2、ER3200G2等。

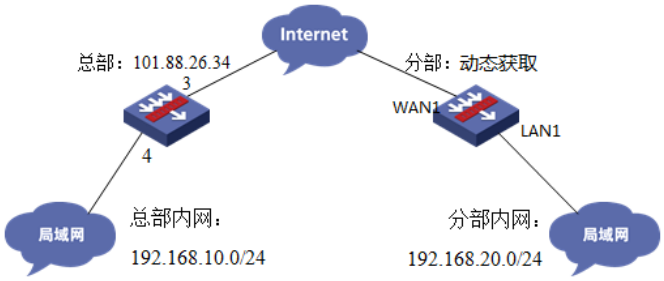
注：本案例是在F100-C-G2的Version 7.1.064, Release 9510P08版本上进行配置和验证的。

1.2 配置需求及实现的效果

总部有一台防火墙，分支有一台ERG2路由器部署在互联网出口，因业务需要两端内网需要通过VPN相互访问。IP地址及接口规划如下表所示：

公司名称	外网接口	公网地址/掩码	公网网关	内网接口	内网地址/掩码
总部	1/0/3	101.88.26.34/30	101.88.26.33	1/0/4	192.168.10.0/24
分部	WAN1	动态获取		LAN1	192.168.20.0/24

2 组网图



配置步骤

3 配置步骤

3.1 总部防火墙侧配置

3.1.1 创建IPSEC安全提议

#加密类型设置为3des-cbc，认证类型设置为sha1。

```
[H3C]ipsec transform-set 1
[H3C-ipsec-transform-set-1]esp encryption-algorithm 3des-cbc
[H3C-ipsec-transform-set-1]esp authentication-algorithm sha1
[H3C-ipsec-transform-set-1]quit
```

3.1.2 创建IKE安全提议

#配置IKE安全提议默认的认证类型为sha1，加密类型为3DES-CBC，DH组为DH2

```
[H3C]ike proposal 1
[H3C-ike-proposal-1] encryption-algorithm 3des-cbc
[H3C-ike-proposal-1] authentication-algorithm sha1
[H3C-ike-proposal-1] dh group2
[H3C-ike-proposal-1]quit
```

3.1.3 创建IKE安全密钥

#创建IKE密钥，分部侧设备的公网IP地址不固定，这边的地址就写为0.0.0.0，密码设置为123456。

```
[H3C]ike keychain 1
[H3C-ike-keychain-1]pre-shared-key address 0.0.0.0  key simple 123456
[H3C-ike-keychain-1]quit
```

3.1.4 配置标识本端身份的FQDN名称

```
[H3C] ike identity fqdn F100
```

3.1.5 创建IKE安全框架

#创建IKE安全框架，将本端名称、对端名称、keychain、proposal关联起来。

```
[H3C]ike profile 1
[H3C-ike-profile-1]keychain 1
[H3C-ike-profile-1]exchange-mode aggressive
[H3C-ike-profile-1] local-identity fqdn F100
[H3C-ike-profile-1] match remote identity fqdn ER
[H3C-ike-profile-1]proposal 1
[H3C-ike-profile-1]quit
```

3.1.6 创建IPSEC安全策略模板

#创建IKE安全策略模板GE1/0/3将transform-set、ike-profile关联起来。

[H3C]ipsec policy-template GE1/0/3 1

[H3C-ipsec-policy-template-GE1/0/3-1]transform-set 1

[H3C-ipsec-policy-template-GE1/0/3-1]ike-profile 1

[H3C-ipsec-policy-template-GE1/0/3-1]quit

#创建一个IPsec安全策略引用策略模板

[H3C]ipsec policy GE1/0/3 1 isakmp template GE1/0/3

3.1.7 创建ACL拒绝IPSEC兴趣流的数据

#创建acl 3888调用在外网接口用于排除IPSEC兴趣流不做NAT。

[H3C]acl advanced 3888

[H3C-acl-ipv4-adv-3888]rule deny ip source 192.168.10.0 0.0.0.255 destination 192.168.20.0 0.0.0.255

[H3C-acl-ipv4-adv-3888]rule permit ip source any

[H3C-acl-ipv4-adv-3888]quit

3.1.8 外网接口调用IPSEC策略和NAT动态转换策略

[H3C]interface GigabitEthernet 1/0/3

[H3C-GigabitEthernet1/0/3]ipsec apply policy GE1/0/3

[H3C-GigabitEthernet1/0/3]nat outbound 3888

[H3C-GigabitEthernet1/0/3]quit

3.1.9 配置安全策略放通IPSEC数据

#创建对象组，组名称为192.168.10.0

[H3C]object-group ip address 192.168.10.0

[H3C-obj-grp-ip-192.168.10.0]0 network subnet 192.168.10.0 255.255.255.0

[H3C-obj-grp-ip-192.168.10.0]quit

#创建对象组，名称为192.168.20.0

[H3C]object-group ip address 192.168.20.0

[H3C-obj-grp-ip-192.168.20.0]0 network subnet 192.168.20.0 255.255.255.0

[H3C-obj-grp-ip-192.168.20.0]quit

#创建对象策略，策略名称为Untrust-Trust

[H3C]object-policy ip Untrust-Trust

[H3C-object-policy-ip- Untrust-Trust] rule 0 pass source-ip 192.168.20.0 destination-ip 192.168.10.0

[H3C-object-policy-ip- Untrust-Trust]quit

#创建Untrust到Tust域的域间策略调用Untrust-Trust策略

[H3C]zone-pair security source Untrust destination Trust

[H3C-zone-pair-security-Untrust-Trust]object-policy apply ip Untrust-Trust

[H3C-zone-pair-security-Untrust-Trust]quit

3.1.10 配置安全策略，放通Untrust到Local，以及Local到Utrust的策略，用于建立IPSEC 隧道

#创建对象策略，策略名称为Untrust-Local

[H3C]object-policy ip Untrust-Local

[H3C-object-policy-ip-Untrust-Local] rule 0 pass

[H3C-object-policy-ip-Untrust-Local]quit

#创建Untrust到Local域的域间策略调用Untrust- Local策略

[H3C]zone-pair security source Untrust destination Local

[H3C-zone-pair-security-Untrust-Local]object-policy apply ip Untrust-Local

[H3C-zone-pair-security-Untrust-Local]quit

#创建对象策略，策略名称为Local-Untrust

[H3C]object-policy ip Local-Untrust

[H3C-object-policy-ip-Local-Untrust] rule 0 pass

[H3C-object-policy-ip-Local-Untrust]quit

#创建Local到Untrust域的域间策略调用Local-Untrust策略

[H3C]zone-pair security source Local destination Untrust

[H3C-zone-pair-security-Local-Untrust]object-policy apply ip Local-Untrust

[H3C-zone-pair-security-Local-Untrust]quit

3.1.11 保存配置

[H3C]save force

3.2 分部ERG2路由器侧配置

3.2.1 配置IPSec 虚接口

单击【VPN】--【VPN设置】--【虚接口】, 点击【新增】，绑定对应的WAN口，比如WAN1：

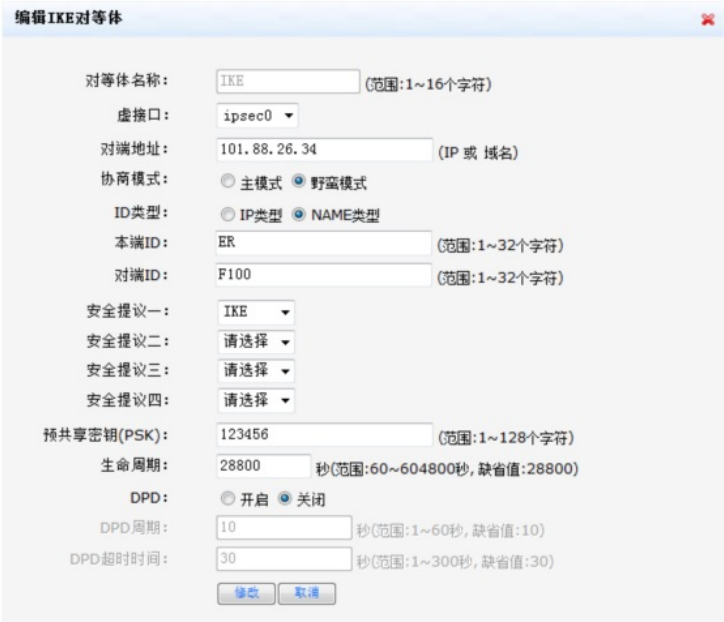
3.2.2 配置IKE安全提议

单击【VPN】--【VPN设置】--【IKE安全提议】，点击【新增】，配置IKE安全提议的各个参数：安全提议名称、IKE验证算法、IKE加密算法、IKE DH组，如下图配置。

3.2.3 配置IKE对等体

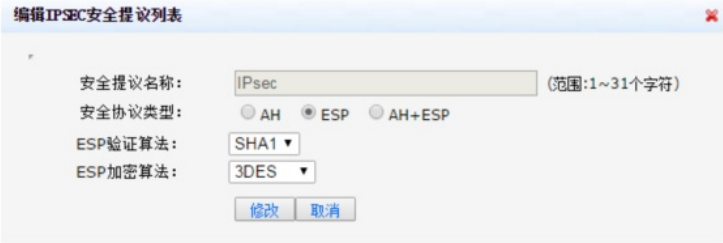
单击【VPN】--【VPN设置】--【IKE对等体】，点击【新增】，配置IKE对等体：

对等体名称为IKE、绑定虚接口为ipsec0（前面已经创建）、对端地址为总部的公网ip，即101.88.26.34；协商模式选择野蛮模式，ID类型为name类型并配置本段的ID为ER对端的ID为F100；安全提议选择ike（前面已经创建）、配置预共享秘钥，此处配置为123456，其余选择默认即可。



3.2.4 配置IPSec安全提议

单击【VPN】--【VPN设置】--【IPSec安全提议】，点击【新增】，配置IPSEC安全提议：安全提议名称、安全协议类型、ESP验证算法、ESP加密算法配置如下图：



3.2.5 配置IPSec安全策略

单击【VPN】--【VPN设置】--【IPSec安全策略】，勾选启【用IPSec功能】，点击【新增】，配置IPSec安全策略：本地子网IP即为分支内网网段，此处配置为192.168.20.0/24，对端子网IP即为总部内网网段，此处配置为192.168.10.0/24，其余参数按照下图所示配置：

3.2.6 配置去往对端子网的静态路由

单击【高级设置】--【路由设置】--【静态路由】，目的地址配置成对端子网，即192.168.10.0，子网掩码为255.255.255.0，出接口为ipsec0虚接口。

3.3 测试VPN是否连通

3.3.1 数据访问触发IPsec建立

在分部内网中任意找一台电脑访问对端网络资源。

举例：在分支侧电脑ping总部侧电脑，IPSEC初始建立时会丢1-2个包，建立后通信正常。

```
C:\Users\sfw1081>ping 192.168.10.3

正在 Ping 192.168.10.3 具有 32 字节的数据:
请求超时。
请求超时。
来自 192.168.10.3 的回复: 字节=32 时间<1ms TTL=255
来自 192.168.10.3 的回复: 字节=32 时间<1ms TTL=255

192.168.10.3 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 2, 丢失 = 2 (50% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 0ms, 最长 = 0ms, 平均 = 0ms
```

3.3.2 查看IPSEC监控信息

#V7防火墙通过命令行查看display ike sa可以看到隧道状态为RD状态表示ike建立完成。

```
[H3C]dis ike sa
    Connection-ID   Remote                  Flag         DOI
-----------------------------------------------------------------------------
    29              198.76.26.90            RD           IPsec
Flags:
RD--READY RL--REPLACED FD-FADING RK-REKEY
```

#V7防火墙通过display ipsec sa可以看到IPSEC SA基本状态。

```
[H3C]dis ipsec sa
-------------------------------
Interface: GigabitEthernet1/0/3
-------------------------------

  -----------------------------
  IPsec policy: GE1/0/3
  Sequence number: 1
  Mode: Template
  -----------------------------
    Tunnel id: 0
    Encapsulation mode: tunnel
    Perfect Forward Secrecy:
    Inside VPN:
    Extended Sequence Numbers enable: N
    Traffic Flow Confidentiality enable: N
    Path MTU: 1444
    Tunnel:
        local  address: 101.88.26.34
        remote address: 198.76.26.90
    Flow:
        sour addr: 192.168.10.0/255.255.255.0  port: 0  protocol: ip
        dest addr: 192.168.20.0/255.255.255.0  port: 0  protocol: ip


    [Inbound ESP SAs]
      SPI: 4032357769 (0xf058e589)
      Connection ID: 158913789952
      Transform set: ESP-ENCRYPT-3DES-CBC ESP-AUTH-SHA1
      SA duration (kilobytes/sec): 1843200/3600
      SA remaining duration (kilobytes/sec): 1843199/3545
      Max received sequence-number: 8
      Anti-replay check enable: Y
      Anti-replay window size: 64
      UDP encapsulation used for NAT traversal: N
      Status: Active

    [Outbound ESP SAs]
      SPI: 1786751150 (0x6a7fa8ae)
      Connection ID: 64424509441
      Transform set: ESP-ENCRYPT-3DES-CBC ESP-AUTH-SHA1
      SA duration (kilobytes/sec): 1843200/3600
      SA remaining duration (kilobytes/sec): 1843199/3545
      Max sent sequence-number: 8
      UDP encapsulation used for NAT traversal: N
      Status: Active
```

ERG2侧:

在【VPN】--【VPN设置】--【IPSec安全策略】--【安全联盟】里查看隧道建立情况

配置关键点