# ACG1000系列与V7平台防火墙对接IPSEC VPN配置举例(适用于两端固定 地址组网)

IPSec VPN **叶佳豪** 2019-08-16 发表

# 组网及说明

# 1 配置需求或说明

### 1.1 适用的产品系列

本案例适用于软件平台为ACG1000系列应用控制网关: ACG10X0、ACG1000-AKXXX等。 注:本案例是在ACG1040的Version 1.10, Release 6609P06版本上进行配置和验证的。

#### 1.2 配置需求及实现的效果

因公司业务拓展需要将处于两地的公司网络通过IPSEC VPN连通,使总部和分部网络可以相互访问。I P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 (F1060)       | 1/0/3 | 101.88.26.34/30 | 101.88.26.33 | 1/0/4 | 192.168.10.0/24 |
| 分部 (ACG1040<br>) | ge1   | 198.76.26.90/30 | 198.76.26.89 | ge3   | 192.168.20.0/24 |

2 组网图



#### 配置步骤

### 3 配置步骤

#### 3.1 两端配置上网配置

本文档重点给出两台设备IPSEC VPN配置步骤,上网配置略。

| H <b>BC</b> se | CPATH<br>2 | I F100-C- |        |     | ● ■ 対象     | 日本 |
|----------------|------------|-----------|--------|-----|------------|----|
| 98%            | «          | IPsec策略   |        |     |            |    |
| NO VRE         |            | ●新建 前 删除  |        |     |            |    |
|                |            | 🖻 应用策略接口  | IP地址类型 | 优先级 | 对确IP地址/主机名 | 3  |
| 安全城            |            |           |        |     |            |    |
| [] 🔑 链路        |            |           |        |     |            |    |
| DNS            |            |           |        |     |            |    |
|                |            |           |        |     |            |    |
| 🗈 🔛 IPv6       |            |           |        |     |            |    |
| 💷 📉 VPN        |            |           |        |     |            |    |
| GRE            |            |           |        |     |            |    |
| 🗉 🖽 IPsec      |            | ]         |        |     |            |    |
| 策略             |            |           |        |     |            |    |
| 监控             |            |           |        |     |            |    |
| 高级设置           |            |           |        |     |            |    |

#### 3.2 总部侧防火墙IPSEC VPN策略配置

#在"网络">"VPN">"策略"中点击新建。

#在"基本配置"中"接口"选择接入外网的1/0/3接口,"优先级"设置为1(优先级代表了策略匹配顺序,当存在多条VPN隧道时需要对各VPN隧道优先级进行设置),"认证方式"选择域共享密钥,建立VPN两端隧道的域共享密钥必须一致。对端ID设置对IP地址即分公司公网地址,本端ID默认为本端公网接口IP地址。在保护的数据流中添加源为总部内网网段192.168.10.0/24,目的IP地址为分部内网网段192.168.20.0/24。

| 新建IPsec策略     |                         |                        |           |         |        |     |
|---------------|-------------------------|------------------------|-----------|---------|--------|-----|
| 基本配置          |                         |                        |           |         |        |     |
| 接口            | GE1/0/3                 |                        | ~         |         |        |     |
| IP地址类型        | IPv4                    | © IPv6                 |           |         |        |     |
| 优先级           | 1                       |                        | 1 ( 1     | -65535) |        |     |
| 模式            | ● 对等/分支节点               | ◎ 中心节点                 |           |         |        |     |
| 对鎊IP地址/主机名    | 198.76.26.90            |                        | (1        | -253字符  | )      |     |
| 协商模式          | <ul> <li>主模式</li> </ul> | ◎ 野蛮模式                 |           |         |        |     |
| 认证方式          | 预共享密钥                   |                        | ~         |         |        |     |
| 预共享密钥         | *****                   |                        | (1        | -128字符  | )      |     |
| 再次输入预共享密钥     |                         |                        |           |         |        |     |
| 对銕ID          | IPv4 地址 ¥ 1             | 98.76.26.90            |           |         |        |     |
| 本端ID          | IPv4 地址 ¥ 1             | IPv4 地址 ¥ 101.88.26.34 |           |         | 1.0    |     |
| 描述            |                         |                        | (1-       | 80字符)   |        |     |
|               |                         |                        |           |         |        |     |
|               |                         |                        |           |         |        |     |
| 保护的数据流        |                         |                        |           |         |        |     |
|               | 的数据流                    |                        | ? X       |         | chiltr |     |
| TT 102168 VRF | (八回)                    |                        | ~         | 8LJ     | /Eth   | 121 |
| (V 192.100.   | 1021001000              | 255 255 255 0          |           | _       | 08324  |     |
| 101 M         | 192.168.10.0/           | 255.255.255.0          | -         |         |        |     |
| 目的IP.         | 理址 ④ 192.168.20.0/      | 255.255.255.0          | 1         |         |        |     |
| 协议            | any                     |                        | • (0-255) |         |        |     |
| 动作            | 保护                      |                        | *         |         |        |     |
|               | 油山                      | ROOM                   |           |         |        | 共14 |
|               | 明定                      | 40月                    |           | 司版权所    | 所有,保留一 | 切权利 |

默认防火墙的IPSEC提议为ESP/SHA1/AES-128, IKE安全提议为:

| 优先级     | 认证方式  | 认证算法 | 加密算法    | DH         | IKE SA 生存電明 |
|---------|-------|------|---------|------------|-------------|
| Default | 预共享密钥 | SHA1 | DES-CBC | DH group 1 | 86400       |

## 3.3 总部侧配置安全策略, 放通IPSEC感兴趣流的数据策略

#在"策略">"安全策略">点击"新建","源IP地址"中点击"添加IPV4地址对象组"

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | PATH F100-C-                                                              |                                                                                               |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------|
| <ul> <li>⇒</li> <li>⇒</li></ul> | <ul> <li>◆ 新建</li> <li>前部株</li> <li>内容安全配置支更之后</li> <li>新建安全策略</li> </ul> | □ 如制 ◆ 移动 ✓ E用 ② 菜用 ● 清空除计数据 ◎ 清除列过滤条件 ◎ 開<br>● 清晨 提文才能生效                                     |
| □ ● 市交管理<br>□ ■ ● 印数均衡                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | 源安全域<br>目的安全域<br>策約ID                                                     | Untrust (0-65534) (2)自动编号                                                                     |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | 类型<br>描述信息                                                                | ● IPv4 ◎ IPv6<br>(1-127学符)                                                                    |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | 动作<br>源IP地址<br>目的IP地址                                                     | <ul> <li>● 九许</li> <li>● 拒绝</li> <li>● 九许井泥度检测</li> <li>● 添加Pv4地址対象组</li> <li>(多適)</li> </ul> |

#配置对象组名称为"192.168.20.0",点击"添加",对象地址为192.168.20.0网段,为分支内网段地址

| 新建IPv4地址对象                                                                 | 组                  |                |           | ? X                    |
|----------------------------------------------------------------------------|--------------------|----------------|-----------|------------------------|
| 对象组名称<br>描述                                                                | 192.168.20.0       |                |           | *(1-31字符)<br>(1-127字符) |
| <ul> <li>         → 添加         前 册         →         →         →</li></ul> | 除                  | 内容             | 排除加小      | 编辑                     |
| 添加对象                                                                       |                    | 134            | Junio Dat |                        |
| 对象 (?)<br>排除地址 (?)                                                         | 网段<br>192.168.20.0 | 255.255.255.0  |           | (Pv4地址/掩码长度0-32 )      |
|                                                                            |                    | 确定 取消<br>确定 取消 |           |                        |

#在"策略">"安全策略">点击"新建","目的IP地址"中点击"添加IPV4地址对象组"

| 源安全域     | Untrust             |                        |         | ~  | •                |
|----------|---------------------|------------------------|---------|----|------------------|
| 目的安全域    | Trust               |                        |         | ~  | •                |
| 策略ID     |                     |                        |         | _  | (0-65534) 📝 自动编号 |
| 类型       | IPv4                | © IPv6                 |         |    |                  |
| 描述信息     |                     |                        |         |    | (1-127字符)        |
|          |                     |                        |         |    |                  |
| 动作       | ① 允许                | ◎ 拒绝                   | ◎ 允许并深度 | 检测 |                  |
| 源IP地址    | 192.168.2           | 0.0                    |         | ~  | [多选]             |
| 目的IP地址   | 1                   |                        |         | ~  | [多选]             |
| 服务       | + 添加IPv             | /4地址对象组                |         |    | [多选]             |
| 应用       | 本端地址                |                        |         |    | [多选]             |
| 应用组      | 对端内网                |                        |         |    | [多选]             |
| 时间段      | 192.168.20<br>请洗择时间 | 0.0<br>IE\$            |         | ~  |                  |
| VRF      | 公网                  |                        |         | ~  |                  |
| 记录日志     | ◎ 开启                | <ul> <li>关闭</li> </ul> |         |    |                  |
| 开启策略匹配统计 | ◎ 开启                | <ul> <li>关闭</li> </ul> |         |    |                  |
| 启用策略     | ◎ 开启                | ◎ 关闭                   |         |    |                  |

#配置对象组名称为"192.168.10.0",点击"添加",对象地址为192.168.10.0网段,为总部内网网段地址

| 新建IPv4地址对象组                                          |                    |                |      | ? ×                         |
|------------------------------------------------------|--------------------|----------------|------|-----------------------------|
| 对象组名称<br>描述                                          | 192.168.10.0       | ]              |      | * ( 1-31字符 )<br>( 1-127字符 ) |
| <ul> <li>① 添加</li> <li>前 删除</li> <li>一 类型</li> </ul> | t                  | 内容             | 排除地址 | 编辑                          |
| 添加对象                                                 |                    |                |      |                             |
| 对象?                                                  | 网段<br>192.168.10.0 | / 255.255.255. | )    | (IPv4地址/掩码长度0-32            |
| - NFWSHUL ()                                         |                    |                |      |                             |
|                                                      |                    | 确定取消           |      |                             |
|                                                      |                    | 确定取消           |      |                             |

#最后确认一下"源IP地址"为对端内网所在对象组,"目的IP地址"为本端内网地址所在对象组,确定即可

| 源安全域     | Untrust    |                        |        | ~ * |           |        |
|----------|------------|------------------------|--------|-----|-----------|--------|
| 目的安全域    | Trust      |                        |        | ~ * |           |        |
| 策略ID     |            |                        |        | *   | (0-65534) | 🔽 自动编号 |
| 类型       | IPv4       | © IPv6                 |        |     |           |        |
| 描述信息     |            |                        |        |     | (1-127字符) | )      |
|          |            |                        |        |     |           |        |
| 动作       | ④ 允许       | ◎ 拒绝                   | ◎ 允许并深 | 度检测 |           |        |
| 源IP地址    | 192.168.20 | 0.0                    |        | ~   | [多选]      |        |
| 目的IP地址   | 192.168.10 | 0.0                    |        | ~   | [多选]      |        |
| 服务       | 请选择服务      | ł                      |        | ~   | [多选]      |        |
| 应用       | 请选择应用      | 1                      |        | ~   | [多选]      |        |
| 应用组      | 请选择应用      | 组                      |        | ~   | [多选]      |        |
| 时间段      | 请选择时间      | 段                      |        | ~   |           |        |
| VRF      | 公网         |                        |        | ~   |           |        |
| 记录日志     | ◎ 开启       | • 关闭                   |        |     |           |        |
| 开启策略匹配统计 | ◎ 开启       | <ul> <li>关闭</li> </ul> |        |     |           |        |
| 启用策略     | ● 开启       | ◎ 关闭                   |        |     |           |        |
|          | 1          |                        | 1      |     |           |        |

3.4 总部侧配置安全策略,放通Untrust到Local,和Local到Utrust的策略,用于建立IPSEC 隧道

| 源安全域     | Untrust                                |           | <b>~</b> *    |          |
|----------|----------------------------------------|-----------|---------------|----------|
| 目的安全域    | Local                                  |           | **            |          |
| 策略ID     |                                        |           | * ( 0-65534 ) | ) 🔽 自动编号 |
| 类型       | IPv4                                   |           |               |          |
| 描述信息     |                                        |           | (1-127字符      | )        |
|          |                                        |           |               |          |
| 动作       | <ul> <li>① 介许</li> <li>⑦ 拒绝</li> </ul> | ◎ 允许并深度检测 | RI            |          |
| 源IP地址    | 请选择或输入对象组                              |           | ▼ [多选]        |          |
| 目的IP地址   | 请选择或输入对象组                              |           | ▼ [多选]        |          |
| 服务       | 请选择服务                                  |           | ▼ [多选]        |          |
| 应用       | 请选择应用                                  |           | ▼ [多选]        |          |
| 应用组      | 请选择应用组                                 |           | ▼ [多选]        |          |
| 时间段      | 请选择时间段                                 |           | *             |          |
| VRF      | 公网                                     |           | *             |          |
| 记录日志     | <ul> <li>一 开启</li> <li>● 关闭</li> </ul> |           |               |          |
| 开启策略匹配统计 | 开启 ● 并启 ● 关闭                           |           |               |          |
| 启用策略     | <ul> <li>开启</li> <li>关闭</li> </ul>     |           |               |          |

| 源安全域     | Local   |                        | ~       | *           |        |
|----------|---------|------------------------|---------|-------------|--------|
| 目的安全域    | Untrust |                        | ~       | •           |        |
| 策略ID     |         |                        |         | * (0-65534) | ✔ 自动编号 |
| 类型       | IPv4    | © IPv6                 |         |             |        |
| 描述信息     |         |                        |         | (1-127字符)   |        |
|          |         |                        |         |             |        |
| 动作       | • 允许    | ◎ 拒绝   ◎               | 允许并深度检测 |             |        |
| 源IP地址    | 请选择或    | 俞入对象组                  | ~       | [多选]        |        |
| 目的IP地址   | 请选择或    | 俞入对象组                  | ~       | [多选]        |        |
| 服务       | 请选择服务   | 5                      | *       | [多选]        |        |
| 应用       | 请选择应用   | ŧ                      | ~       | [多选]        |        |
| 应用组      | 请选择应用   | 用组                     | *       | [多选]        |        |
| 时间段      | 请选择时间   | 同段                     | *       |             |        |
| VRF      | 公网      |                        | *       |             |        |
| 记录日志     | ◎ 开启    | <ul> <li>美闭</li> </ul> |         |             |        |
| 开启策略匹配统计 | ◎ 开启    | <ul><li>美闭</li></ul>   |         |             |        |
| 启用策略     | ◎ 开启    | ◎ 关闭                   |         |             |        |

## 3.5 分部侧IPSEC VPN策略配置

#在 "VPN">"IPsec第三方对接"中新建IKE对等体。

| VPN > IPsec-VPN > IPsec第       | 方对接                                   |  |
|--------------------------------|---------------------------------------|--|
| -NAT                           | ▲ IPsec 配置 IPsec 隧道接口 IKE SA IPsec SA |  |
| DNS<br>DHCP 服务器                | ● 新建IKE                               |  |
| — IPv6网络                       | 名称 详细信息                               |  |
|                                |                                       |  |
|                                | 20 🗸 🖌 🤞 1 共1页 🕨 🔰 👌                  |  |
| └── IPsec-VPN<br>└─ IPsec笛三方对接 | IKE : -                               |  |
| IPsec快速配置                      | ● 新建IPsec                             |  |

#基本设置中网关名称设置为"branch",对端网关地址为101.88.26.34,模式设置为主模式,预共享秘 钥与防火墙设置一致,IKE协商交互方案加密算法为DES,认证算法为SHA。

| <b>基本设立</b><br>网关名称 | branch   |          |                          | 0      | 1-31 字符)    |           |   |
|---------------------|----------|----------|--------------------------|--------|-------------|-----------|---|
|                     | 〇本地源     | 接口       | 〇本地源                     | Pttett | ◎无          |           |   |
| 对諦网关                | 静态IPt    | 助        |                          |        |             |           |   |
| IP地址                | 101.88.2 | 26.34    |                          |        |             |           |   |
| 模式                  | ○野蛮模     | 式        | <ul> <li>主模式(</li> </ul> | ID保护   | <b>=</b> )  |           |   |
| 认证方式                | 预共享      | 的        |                          | ~      |             |           |   |
| 预共享密钥               |          |          |                          | ~      | (6-39 字符)   |           |   |
| 「级选项 ン              |          |          |                          |        |             |           |   |
| IKE协商交互方案           |          |          |                          |        |             |           |   |
|                     | 加密算法     | DES      | ~                        | 认证     | SHA         | ✔ 🕣 添加到列表 |   |
|                     |          | 加密算法     |                          |        | 认证          | 操作        |   |
|                     | 1        | DES      |                          |        | SHA         | 删除        |   |
|                     |          |          |                          |        |             |           |   |
|                     |          |          |                          |        |             |           |   |
|                     |          |          |                          |        |             |           |   |
|                     | DH组      | <b>1</b> |                          | C      | 2           | 05        |   |
|                     | 密钥周期     |          | 86400                    |        | (120-86400秒 | )         |   |
|                     | NAT穿越道   | 接频率      | 10                       |        | (10-900 秒)  |           |   |
|                     |          |          |                          |        |             |           | - |

#新建IPsec安全提议。

| IKE : branch |       |  |
|--------------|-------|--|
| ● 新建IPsec    |       |  |
| 名称           | IKE名称 |  |
|              |       |  |

#设置通道名称为"branch", IKE对等体调用"branch", ESP加密和认证算法设置为AES128\_SHA1, 设置完成后点击提交。

| 通道名称                      | branch                                                       |            | (1-31 字符)     |               |
|---------------------------|--------------------------------------------------------------|------------|---------------|---------------|
| IKE                       | branch                                                       |            | -             |               |
| 选项》                       |                                                              |            |               |               |
| IPSEC协商交互方案               |                                                              |            |               |               |
|                           | ESP AES128_S                                                 | HA1 V AH N | ULL V         | ⑦ 添加到列表       |
|                           | ESP                                                          |            | AH            | 操作            |
|                           | 1 AES12                                                      | B_SHA1     | NULL          | 删除            |
| 能美向前保密(PFS)<br>模式<br>家相周期 | <ul> <li>● 无     <li>● 随道機式     <li>● 秒</li> </li></li></ul> | 01         | ○ 2<br>○ 西考都有 | 05            |
| 利                         | 28800                                                        | 0171       |               | (120-85400 秒) |
| 连接方式                      | 自动连接                                                         | ○ 流量触发     | 连接 〇 监控链路     | 故障自动连接        |
|                           | ettial 5                                                     | (2-360     | 0.50)         |               |

#地址选项中添加本地子网到对端子网的规则。

IPsec接口 IPv4地址

| IPv4地址  |                           | (例如:192.1                 | 168.1.1/24)                 |            |
|---------|---------------------------|---------------------------|-----------------------------|------------|
| IPsec   | branch<br>192 168 20 0/24 | ✓<br>192 168 10 0/24 (/s) | 100 - 100 160 1 1/04-100 14 | (9.2.1/24) |
| ALAL AL | )酒trbt/F                  | ENTRI                     | 操作                          |            |
|         |                           |                           |                             |            |
|         |                           |                           |                             |            |
|         |                           |                           |                             |            |
|         |                           |                           |                             |            |
|         |                           |                           |                             |            |

IPsec

#### 3.6 配置保存

● 新建 ⑧ 删除

#在设备管理界面右上角点击配置保存,保存当前配置。

|  |   | 副署伊友     | 调业  |
|--|---|----------|-----|
|  | ( | BUELTKIT | IВШ |

# 3.7 结果测试

#总部侧分支侧电脑可以正常通信。 <H3C>ping -a 192.168.10.1 192.168.20.2 Ping 192.168.20.2 (192.168.20.2) from 192.168.10.1: 56 data bytes, press CTRL\_C to break 56 bytes from 192.168.20.2: icmp\_seq=0 ttl=127 time=1.550 ms 56 bytes from 192.168.20.2: icmp\_seq=2 ttl=127 time=0.876 ms 56 bytes from 192.168.20.2: icmp\_seq=3 ttl=127 time=0.876 ms 56 bytes from 192.168.20.2: icmp\_seq=3 ttl=127 time=0.894 ms 56 bytes from 192.168.20.2: icmp\_seq=4 ttl=127 time=0.966 ms #在总部侧查看IKE与IPSEC SA。 <H3C>display ike sa Connection-ID Remote Flag DOI

107 198.76.26.90 RD IPsec Flags: RD--READY RL--REPLACED FD-FADING RK-REKEY <H3C>dius <H3C>dis <H3C>display ipse <H3C>display ipsec sa Interface: GigabitEthernet1/0/3 \_\_\_\_\_ -----IPsec policy: branch Sequence number: 1 Mode: ISAKMP Tunnel id: 0 Encapsulation mode: tunnel Perfect Forward Secrecy: Inside VPN: Extended Sequence Numbers enable: N Traffic Flow Confidentiality enable: N Path MTU: 1428 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 #分部侧设备查看IPSEC连接状态:

| IPse  | < 122  | IPsec腰道擦口                        | IKE SA             | IPsec SA    |    |              |                 |     |        |
|-------|--------|----------------------------------|--------------------|-------------|----|--------------|-----------------|-----|--------|
|       |        | 名称                               | 3                  | 讨病网关        |    | 本地网关         | 状态              |     | 过期时间/s |
| 1     |        | branch                           | 1                  | 01.88.26.34 |    | 198.76.26.90 | 连接              |     | 86041  |
| -     | 10-10  | Phone State Billion              | INC. CA.           |             |    |              |                 |     |        |
|       | - BUEL | In activities and activities and | INE SA INS         | ec SA       |    |              |                 |     |        |
| IPser |        | a称 对                             | ine sa lina<br>調网关 | 本地网关        | 状态 | 过期时间/过期流量    | <b>流量(</b> 入/出) | 遼网络 | 目的网络   |

#### 3.8 注意事项

### 3.8.1 外网接口配置动态地址转换导致VPN无法建立问题

在配置IPSEC VPN时需要注意外网口配置地址转换时一定要排除掉VPN的感兴趣流,因为NAT转换在接口出方向优先于IPSEC策略,如果不修改会导致数据先经过NAT地址转换后无法匹配兴趣流。 在"对象">"ACL">"IPv4"中点击新建按钮。

| H <b>3C</b> s                                    | ECPATH F1 | .00-C-           |      | ()<br>概览 | <b>十</b><br>监控 | 策略 | 对象  |
|--------------------------------------------------|-----------|------------------|------|----------|----------------|----|-----|
| 孙                                                | « IPv4    | ACL组             |      |          |                |    |     |
|                                                  | (+) #     | 所建 前 删除<br>ACL分类 | ACL  |          | 規則数量           | Ł  | 规则匹 |
| □ ● 対象组<br>□ ● 対象组<br>□ M ACL<br>IPv4            |           | 高级               | 3000 |          | 1              |    | 配置原 |
| - IPv6<br>二层<br>III SSL<br>III V\$公明管理<br>III KI |           |                  |      |          |                |    |     |

#在"类型"中选择高级ACL, ACL编号输入3999。

| IPv4 ACL组   |                     |                    |
|-------------|---------------------|--------------------|
| 🛨 新建   🏛 删除 |                     |                    |
| 新建IPv4ACL   |                     | ×                  |
| 类型          | ◎ 基本ACL ● 高级ACL     |                    |
| ACL 🕐       | 3999                | *(3000-3999或1-63个字 |
|             |                     | 符)                 |
| 规则匹配顺序      | ◎ 按照配置顺序     ◎ 自动排序 |                    |
| 规则编号步长      | 5                   | (1-20)             |
| 描述          |                     | (1-127字符)          |
|             |                     |                    |

#以总部防火墙为例,动作选择拒绝,IP协议类型选择拒绝,匹配条件匹配总部侧内网到分部侧内网的 网段(在分部侧防火墙匹配条件取反)后点击确定添加下一条策略。

| 新建IPv4高级ACL的规 | 则              |     |           |   |                         | × |
|---------------|----------------|-----|-----------|---|-------------------------|---|
| ACL编号         | 3999           |     |           |   | (3000-3999或<br>1-63个字符) | ^ |
| 规则编号          | 🔽 自动编号         |     |           |   | * (0-65534)             |   |
| 描述            |                |     |           |   | (1-127字符)               |   |
| 动作            | ◎ 允许           | (   | )拒绝       |   | ]                       |   |
| IP协议类型        | ip             |     |           | ~ | *(0-256,256代            |   |
| 匹配条件 🕐        | ☑ 匹配源IP地址/通    | 配符推 | 範码        |   | 表任意ip)                  |   |
|               | 192.168.10.0   | /   | 0.0.0.255 | * |                         |   |
|               | ☑ 匹配目的IP地址/j   | 通配济 | 掩码        |   |                         |   |
|               | 192.168.20.0   | /   | 0.0.0.255 | * |                         |   |
|               | III 匹配TCP/UDP报 | 文的》 | 就満口号      |   |                         |   |
|               | III 匹配TCP/UDP报 | 文的目 | 目的端口号     |   |                         |   |
|               | 匹配TCP报文的道      | 接建  | 立标识       |   |                         | Ť |
|               | 确定             |     | 取消        |   |                         |   |

#不需要改变此页面配置,可以直接点击确定按钮。当有多个网段访问VPN的需求时,需要先添加拒绝的策略,再添加全部允许的策略。

| 新建IPv4高级ACL的 | 规则                  |                         | ×      |
|--------------|---------------------|-------------------------|--------|
| ACL编号        | 3999                | (3000-3999或<br>1-63个字符) | ^      |
| 规则编号         | ☑ 自动编号              | * (0-65534)             |        |
| 描述           |                     | (1-127字符)               |        |
| 动作           | ◎ 允许 ◎ 拒绝           |                         |        |
| IP协议类型       | 请选择                 | ▼*(0-256,256代           |        |
| 匹配条件 🕐       | 匹配源IP地址/通配符掩码       | 表任意ip )                 |        |
|              | 📄 匹配目的IP地址/通配符掩码    |                         |        |
|              | I 匹配TCP/UDP报文的源端口号  |                         |        |
|              | 🥅 匹配TCP/UDP报文的目的端口号 |                         |        |
|              | 匹配TCP报文的连接建立标识      |                         |        |
|              | I 匹配TCP报文标识         |                         |        |
|              | 匹配ICMP报文的消息类型和消息码   |                         | $\sim$ |
|              | 确定取消                |                         |        |

#在"策略">"NAT">"NAT动态转换">"策略配置"中点击新建按钮。接口选择外网接口,ACL选择之前创 建的3999,转换后地址选择接口IP地址。

注意:如果配置策略中已经存在动态转换策略,请在此策略的基础上添加或者更换ACL选项。该操作可能导致断网请谨慎操作。



配置关键点