F1000-AK系列使用安卓/苹果手机拨入L2TP VPN的配置方法（命令行）

L2TP VPN zhiliao_8mkdB 2018-11-24 发表

组网及说明

1 配置需求及说明

1.1 适用的产品系列

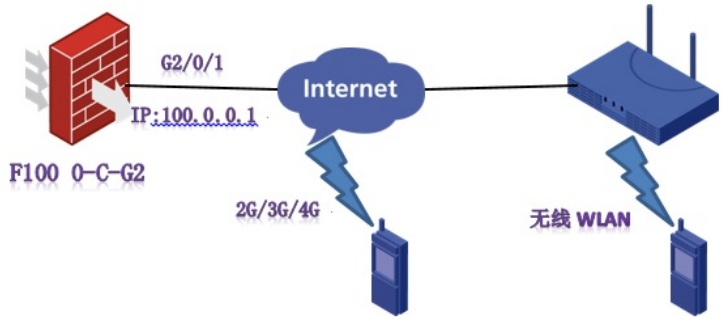
本案例适用于如F1000-AK180、F1000-AK170等F1000-AK系列的防火墙。

1.2 配置需求及实现的效果

将防火墙部署在互联网出口用于L2TP VPN网关，目前需要安卓（Android）\苹果（IOS）手机使用系统自带的L2TP客户端连接VPN访问内网资源。

【小知识】由于安全性考虑，Android 4.0以后的版本和IOS系统L2TP登录方式全部改为L2TP OVER IPSEC方式，所以防火墙只配置L2TP VPN手机终端无法拨入，需要在防火墙增加IPSEC的配置。

2 组网图



注：防火墙外网接口地址为10.0.0.1。

配置步骤

3 防火墙上网配置

略

4 L2TP VPN配置

4.1 启用L2TP VPN

进入系统视图后开启L2TP功能

system-view

[H3C]l2tp enable

4.2 配置地址池用于向L2TP用户下发地址

创建L2TP地址池用于向L2TP用户下发地址，需要注意L2TP下发网段不能与内网网段冲突。

[H3C]ip pool 1 172.16.1.2 172.16.1.254

4.3 配置虚模板

在虚模板下绑定全局下创建的L2TP地址池，服务模板下的ip address为L2TP VPN用户的网关，需要和地址池内地址在同一网段。

[H3C]interface Virtual-Template 1

[H3C-Virtual-Template1]ppp authentication-mode chap pap

[H3C-Virtual-Template1]remote address pool 1

[H3C-Virtual-Template1]ip address 172.16.1.1 24

[H3C-Virtual-Template1]quit

4.4 创建L2TP用户组

创建L2TP组绑定虚模板

[H3C]l2tp-group 1 mode lns

[H3C-l2tp1]undo tunnel authentication

[H3C-l2tp1]allow l2tp virtual-template 1

[H3C-l2tp1]quit

4.5 创建用户

创建的L2TP账号为z，密码为z。

[H3C]local-user z class network

[H3C-luser-network-z]service-type ppp
[H3C-luser-network-z]password simple z
[H3C-luser-network-z]quit

将Virtual-Template接口加入到安全域并放通安全策略

将Virtual-Template 1接口加入Trust区域，如果内网接口也在Trust区域需要放通同域间的安全策略。

[H3C]security-zone name Trust
[H3C-security-zone-Trust]import interface Virtual-Template 1
[H3C-security-zone-Trust]quit
[H3C]security-zone intra-zone default permit

5 IPSEC VPN配置

5.1 配置共享秘钥

配置共享秘钥为123

[H3C]ike keychain 1
[H3C-ike-keychain-1]pre-shared-key address 0.0.0.0 0 key simple 123
[H3C-ike-keychain-1]quit

5.2 配置IKE安全提议

配置多个安全提议用于匹配不同的终端认证\加密算法。

[H3C]ike proposal 1
[H3C-ike-proposal-1]encryption-algorithm aes-cbc-128
[H3C-ike-proposal-1]dh group2
[H3C-ike-proposal-1]authentication-algorithm md5
[H3C-ike-proposal-1]quit
[H3C]ike proposal 2
[H3C-ike-proposal-2]encryption-algorithm 3des-cbc
[H3C-ike-proposal-2]dh group2
[H3C-ike-proposal-2]authentication-algorithm md5
[H3C-ike-proposal-2]quit
[H3C]ike proposal 3
[H3C-ike-proposal-3]encryption-algorithm 3des-cbc
[H3C-ike-proposal-3]dh group2
[H3C-ike-proposal-3]authentication-algorithm sha
[H3C-ike-proposal-3]quit
[H3C]ike proposal 4
[H3C-ike-proposal-4]encryption-algorithm aes-cbc-256
[H3C-ike-proposal-4]dh group2
[H3C-ike-proposal-4]authentication-algorithm sha
[H3C-ike-proposal-4]quit
[H3C]ike proposal 5
[H3C-ike-proposal-5]encryption-algorithm DES-CBC
[H3C-ike-proposal-5]dh group2
[H3C-ike-proposal-5]authentication-algorithm sha
[H3C-ike-proposal-5]quit
[H3C]ike proposal 6
[H3C-ike-proposal-6]encryption-algorithm aes-cbc-192
[H3C-ike-proposal-6]dh group2
[H3C-ike-proposal-6]authentication-algorithm sha
[H3C-ike-proposal-6]quit

5.3 配置IKE安全框架

配置IKE安全框架调用创建的6个安全提议。

[H3C]ike profile 1
[H3C-ike-profile-1]keychain 1
[H3C-ike-profile-1]match remote identity address 0.0.0.0 0
[H3C-ike-profile-1]proposal 1 2 3 4 5 6
[H3C-ike-profile-1]quit

配置IPSEC安全提议

[H3C]ipsec transform-set 1
[H3C-ipsec-transform-set-1]encapsulation-mode transport
[H3C-ipsec-transform-set-1]esp encryption-algorithm 3des-cbc
[H3C-ipsec-transform-set-1]esp authentication-algorithm MD5
[H3C-ipsec-transform-set-1]quit
[H3C]ipsec transform-set 2

[H3C-ipsec-transform-set-2]encapsulation-mode transport
[H3C-ipsec-transform-set-2]esp encryption-algorithm aes-cbc-128
[H3C-ipsec-transform-set-2]esp authentication-algorithm sha1
[H3C-ipsec-transform-set-2]quit
[H3C]ipsec transform-set 3
[H3C-ipsec-transform-set-3]encapsulation-mode transport
[H3C-ipsec-transform-set-3]esp encryption-algorithm aes-cbc-256
[H3C-ipsec-transform-set-3]esp authentication-algorithm sha1
[H3C-ipsec-transform-set-3]quit
[H3C]ipsec transform-set 4
[H3C-ipsec-transform-set-4]encapsulation-mode transport
[H3C-ipsec-transform-set-4]esp encryption-algorithm des-cbc
[H3C-ipsec-transform-set-4]esp authentication-algorithm sha1
[H3C-ipsec-transform-set-4]quit
[H3C]ipsec transform-set 5
[H3C-ipsec-transform-set-5]encapsulation-mode transport
[H3C-ipsec-transform-set-5]esp encryption-algorithm 3des-cbc
[H3C-ipsec-transform-set-5]esp authentication-algorithm sha1
[H3C-ipsec-transform-set-5]quit
[H3C]ipsec transform-set 6
[H3C-ipsec-transform-set-6]encapsulation-mode transport
[H3C-ipsec-transform-set-6]esp encryption-algorithm aes-cbc-192
[H3C-ipsec-transform-set-6]esp authentication-algorithm sha1
[H3C-ipsec-transform-set-6]quit

5.4 配置IPSEC模板

配置IPSEC模板并调用之前创建的6个模板
[H3C]ipsec policy-template z 1
[H3C-ipsec-policy-template-z-1]transform-set 1 2 3 4 5 6
[H3C-ipsec-policy-template-z-1]ike-profile 1
[H3C-ipsec-policy-template-z-1]quit
配置IPSEC策略
[H3C]ipsec policy a 10 isakmp template z

5.5 将IPSEC策略在外网接口调用

[H3C]interface GigabitEthernet 2/0/1
[H3C-GigabitEthernet2/0/1]ipsec apply policy a
[H3C-GigabitEthernet2/0/1]quit
外网接口NAT中添加ACL拒绝掉L2TP数据流量做地址转换。
因为在防火墙处理流程上是先进行NAT后进行IPSEC VPN，如果出接口不拒绝掉L2TP数据流会导致回包无法匹配IPSEC兴趣流。
[H3C]acl advanced 3000
[H3C-acl-ipv4-adv-3000]rule deny udp destination-port 1701
[H3C-acl-ipv4-adv-3000]rule permit ip source any
[H3C-acl-ipv4-adv-3000]quit
[H3C]interface GigabitEthernet 2/0/1
[H3C-GigabitEthernet2/0/1]nat outbound 3000
[H3C-GigabitEthernet2/0/1]quit

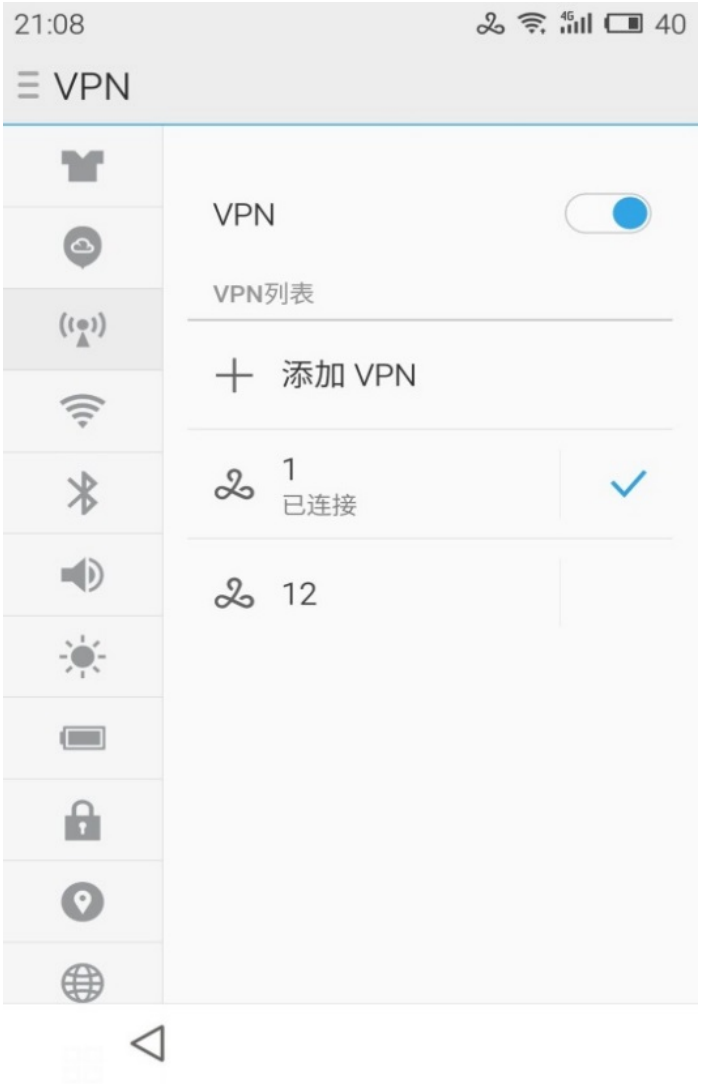
6 保存配置

[H3C]quit
save force

7 实验验证

使用安卓手机拨入VPN


21:09
40
L2TP/IPSec PSK类型
名称 1
服务器地址 100.0.0.1
用户名 z
密码 •
L2TP 密钥
IPSec 标识符
IPSec 预共享密钥 123
DNS 搜索域
保存



使用苹果手机拨入VPN

8 注意事项

协商模式

安卓手机自带的客户端默认为传输模式，和IKE主模式协商。

关于IKE安全提议

安卓手机IKE第一阶段协商的加密算法和验证算法，安卓自带客户端会发送8种组合方式，所以本次案例选取6种以便与更多的系统兼容。

```
    Transform ID: KEY_IKE (1)
  ⊞ Transform IKE Attribute Type (t=11,l=2) Life-Type : Seconds
  ⊞ Transform IKE Attribute Type (t=12,l=2) Life-Duration : 28800
  ⊞ Transform IKE Attribute Type (t=1,l=2) Encryption-Algorithm : 3DES-CBC
  ⊞ Transform IKE Attribute Type (t=3,l=2) Authentication-Method : PSK
  ⊞ Transform IKE Attribute Type (t=2,l=2) Hash-Algorithm : SHA
  ⊞ Transform IKE Attribute Type (t=4,l=2) Group-Description : Alternate 1024-bit MODP group
⊟ Type Payload: Transform (3) # 2
    Next payload: Transform (3)
    Payload length: 32
    Transform number: 2
    Transform ID: KEY_IKE (1)
  ⊞ Transform IKE Attribute Type (t=11,l=2) Life-Type : Seconds
  ⊞ Transform IKE Attribute Type (t=12,l=2) Life-Duration : 28800
  ⊞ Transform IKE Attribute Type (t=1,l=2) Encryption-Algorithm : 3DES-CBC
  ⊞ Transform IKE Attribute Type (t=3,l=2) Authentication-Method : PSK
  ⊞ Transform IKE Attribute Type (t=2,l=2) Hash-Algorithm : MD5
  ⊞ Transform IKE Attribute Type (t=4,l=2) Group-Description : Alternate 1024-bit MODP group
⊟ Type Payload: Transform (3) # 3
    Next payload: Transform (3)
    Payload length: 32
    Transform number: 3
    Transform ID: KEY_IKE (1)
  ⊞ Transform IKE Attribute Type (t=11,l=2) Life-Type : Seconds
  ⊞ Transform IKE Attribute Type (t=12,l=2) Life-Duration : 28800
  ⊞ Transform IKE Attribute Type (t=1,l=2) Encryption-Algorithm : DES-CBC
  ⊞ Transform IKE Attribute Type (t=3,l=2) Authentication-Method : PSK
  ⊞ Transform IKE Attribute Type (t=2,l=2) Hash-Algorithm : SHA
  ⊞ Transform IKE Attribute Type (t=4,l=2) Group-Description : Alternate 1024-bit MODP group
⊟ Type Payload: Transform (3) # 4
    Next payload: Transform (3)
    Payload length: 32
    Transform number: 4
    Transform ID: KEY_IKE (1)
  ⊞ Transform IKE Attribute Type (t=11,l=2) Life-Type : Seconds
  ⊞ Transform IKE Attribute Type (t=12,l=2) Life-Duration : 28800
  ⊞ Transform IKE Attribute Type (t=1,l=2) Encryption-Algorithm : DES-CBC
  ⊞ Transform IKE Attribute Type (t=3,l=2) Authentication-Method : PSK
  ⊞ Transform IKE Attribute Type (t=2,l=2) Hash-Algorithm : MD5
```

关于IPSEC安全提议

安卓手机自带客户端第二阶段协商为3DES加密算法，SHA1验证算法。也支持AES-CBC-256加密算法和SHA1验证算法（苹果手机也是支持这个）。如果苹果手机需要接入，只需再增加一个transform-set配置为传输模式AES-CBC-256加密算法和SHA1验证算法。

```
    Transform number: 5
    Transform ID: KEY_IKE (1)
  ⊞ Transform IKE Attribute Type (t=11,l=2) Life-Type : Seconds
  ⊞ Transform IKE Attribute Type (t=12,l=2) Life-Duration : 28800
  ⊞ Transform IKE Attribute Type (t=1,l=2) Encryption-Algorithm : AES-CBC
  ⊞ Transform IKE Attribute Type (t=14,l=2) Key-Length : 128
  ⊞ Transform IKE Attribute Type (t=3,l=2) Authentication-Method : PSK
  ⊞ Transform IKE Attribute Type (t=2,l=2) Hash-Algorithm : SHA
  ⊞ Transform IKE Attribute Type (t=4,l=2) Group-Description : Alternate 1024-bit MODP group
⊟ Type Payload: Transform (3) # 6
    Next payload: Transform (3)
    Payload length: 36
    Transform number: 6
    Transform ID: KEY_IKE (1)
  ⊞ Transform IKE Attribute Type (t=11,l=2) Life-Type : Seconds
  ⊞ Transform IKE Attribute Type (t=12,l=2) Life-Duration : 28800
  ⊞ Transform IKE Attribute Type (t=1,l=2) Encryption-Algorithm : AES-CBC
  ⊞ Transform IKE Attribute Type (t=14,l=2) Key-Length : 128
  ⊞ Transform IKE Attribute Type (t=3,l=2) Authentication-Method : PSK
  ⊞ Transform IKE Attribute Type (t=2,l=2) Hash-Algorithm : MD5
  ⊞ Transform IKE Attribute Type (t=4,l=2) Group-Description : Alternate 1024-bit MODP group
⊟ Type Payload: Transform (3) # 7
    Next payload: Transform (3)
    Payload length: 36
    Transform number: 7
    Transform ID: KEY_IKE (1)
  ⊞ Transform IKE Attribute Type (t=11,l=2) Life-Type : Seconds
  ⊞ Transform IKE Attribute Type (t=12,l=2) Life-Duration : 28800
  ⊞ Transform IKE Attribute Type (t=1,l=2) Encryption-Algorithm : AES-CBC
  ⊞ Transform IKE Attribute Type (t=14,l=2) Key-Length : 256
  ⊞ Transform IKE Attribute Type (t=3,l=2) Authentication-Method : PSK
  ⊞ Transform IKE Attribute Type (t=2,l=2) Hash-Algorithm : SHA
  ⊞ Transform IKE Attribute Type (t=4,l=2) Group-Description : Alternate 1024-bit MODP group
⊟ Type Payload: Transform (3) # 8
    Next payload: NONE / No Next Payload  (0)
    Payload length: 36
    Transform number: 8
    Transform ID: KEY_IKE (1)
  ⊞ Transform IKE Attribute Type (t=11,l=2) Life-Type : Seconds
```

关于V5平台设备是否支持手机端拨入

V5平台的设备例如部分防火墙和部分MSR设备使用传输模式配置l2tp over ipsec时，封装会出现问题，将会导致l2tp报文无法正常封装。故无法实现手机使用自带客户端l2tp over ipsec拨号需求。

配置关键点