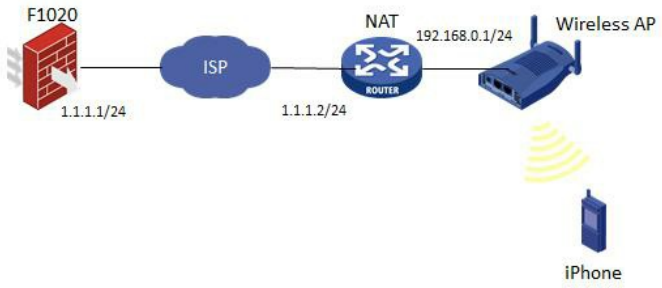
Comware V7平台FW与iPhone对接IPSec配置案例

L2TP IPSec 莘启跃 2016-04-27 发表

Comware V7防火墙设备作为VPN总部，客户通过移动终端iPhone拨入，中间跨越运营商nat。



如图所示，F1020通过G1/0/1与NAT设备G0/1相连，NAT设备下挂一台无线AP，iPhone通过AP接入网络，自动获取地址。由于终端地址不固定，总部F1020采用模板方式建立IPSec。

1、NAT上配置基本上网所需的NAT及路由功能即可，此处略，AP配置同略。

2、F1020 IPSec相关配置

```
#
domain system     //配置domain的ike认证/授权类型
 authentication ike none
 authorization ike local
#
ike address-group ikepool 3.3.3.3 3.3.3.10 255.255.255.255 //配置ike地址池
#
local-user client class network   //创建用户并指定service-type为ike
 password cipher $c$3$7oUi/Qkp1cvEi2b6Ep2T/HKO0+dOf0QXxQ==
 service-type ike
 authorization-attribute user-role network-operator
 authorization-attribute ip-pool ikepool
#
ike proposal 1                 //配置ike proposal
 encryption-algorithm 3des-cbc
 dh group2
 authentication-algorithm md5
#
ike keychain 1             //配置ike key keychain
 pre-shared-key address 0.0.0.0 0.0.0.0 key cipher
$c$3$pEmDV1qqz2vxVM5yiSU+aEOikiUjHK4AJw==
#
ike profile 1              //配置ike profile
 keychain 1
 match remote identity address 0.0.0.0 0.0.0.0
 proposal 1
 client-authentication xauth                  //指定为xauth认证类型
 aaa authorization domain system username client
#
```

ipsec transform-set 1

esp encryption-algorithm aes-cbc-256

esp authentication-algorithm sha1

#

ipsec policy-template 1 1

transform-set 1

ike-profile 1

#

ipsec policy 1 1 isakmp template 1

#

interface GigabitEthernet1/0/1

port link-mode route

ip address 1.1.1.1 255.255.255.0

ipsec apply policy 1

#

3、接口加入安全区域，并放通域间策略

4、iPhone配置

添加VPN时，选择为“IPSec”，账户为local-user，密钥为F1020上配置的pre-shared-key。

5、验证

其中，“指定的IP地址”就是从F1020上配置的ike address-group中自动获取的。

display ike sa verbose

Connection ID: 29

Outside VPN:

Inside VPN:

Profile: 1

Transmitting entity: Responder

Local IP: 1.1.1.1

Local ID type: IPV4_ADDR

Local ID: 1.1.1.1

Remote IP: 1.1.1.2

Remote ID type: IPV4_ADDR

Remote ID: 192.168.1.101

Authentication-method: PRE-SHARED-KEY

Authentication-algorithm: MD5

Encryption-algorithm: 3DES-CBC

Life duration(sec): 3600

Remaining key duration(sec): 3573

Exchange-mode: Main

Diffie-Hellman group: Group 2

NAT traversal: Detected

Extend authentication: Enabled

Assigned IP address: 3.3.3.3

display ipsec sa

Interface: GigabitEthernet1/0/1

IPsec policy: 1

Sequence number: 1

Mode: template

Tunnel id: 0

Encapsulation mode: tunnel

Perfect forward secrecy:

Path MTU: 1419

Tunnel:

local address: 1.1.1.1

remote address: 1.1.1.2

Flow:

sour addr: 0.0.0.0/0.0.0.0 port: 0 protocol: ip

dest addr: 3.3.3.3/255.255.255.255 port: 0 protocol: ip

[Inbound ESP SAs]

SPI: 227698188 (0x0d92660c)

Transform set: ESP-ENCRYPT-AES-CBC-256 ESP-AUTH-SHA1

SA duration (kilobytes/sec): 1843200/3600

SA remaining duration (kilobytes/sec): 1843193/3514

Max received sequence-number: 144

Anti-replay check enable: Y

Anti-replay window size: 64

UDP encapsulation used for NAT traversal: Y

Status: Active

[Outbound ESP SAs]

SPI: 223889891 (0x0d5849e3)

Transform set: ESP-ENCRYPT-AES-CBC-256 ESP-AUTH-SHA1

SA duration (kilobytes/sec): 1843200/3600

SA remaining duration (kilobytes/sec): 1843200/3514

Max sent sequence-number: 0

UDP encapsulation used for NAT traversal: Y

Status: Active

终端拨入VPN时，F1020 debug ike信息见附件。

1、配置认证类型为xauth。

2、V7设备老版本不支持xauth，具体参考版本说明书。不同版本开启xauth的命令可能不一样：aa
a authentication xauth 或者 client-authentication xauth