[2011-06-15]ComwareV5防火墙与iOS iPhone建立L2TP over IPSec VPN典型配置案例

金山 2011-06-15 发表

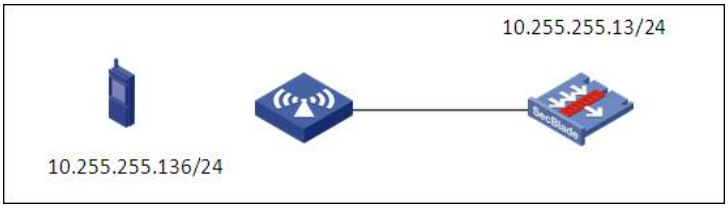
ComwareV5防火墙与iOS iPhone建立L2TP over IPSec VPN典型配置案例

一、 组网需求：

随着苹果公司的iPhone、iPad、iPod Touch等运行iOS操作系统的手持式终端设备的流行，越来越多的客户希望利用这些手持终端设备与防火墙直接建立VPN连接，从而访问公司内部网络资源。本案例用于指导网络工程师对上述组网需求进行配置。

二、 组网图：

iPhone通过无线与SecBlade II FW三层连接，路由可达。



设备版本：

H3C SecBlade FW：Comware Software, Version 5.20, Feature 3169P07

iPhone3GS: iOS 4.3(8F190)

三、 配置步骤：

1. 配置iPhone无线接入

1.1 在AP上配置无线接入服务，使iPhone正常接入无线网络。（略）

1.2 配置DHCP服务，为iPhone无线接入分配IP地址；也可以手工为iPhone配置IP地址。（略）

1.3 检查iPhone与防火墙是否三层路由可达。下图为本案例中iPhone接入无线后的状态截屏。

2. 配置SecBlader提供L2TP over IPSec VPN服务

1.1 SecBlade II FW上配置接口IP地址并加入某一防火墙安全区域。（略）

```
interface GigabitEthernet0/1
 port link-mode route
 ip address 10.255.255.13 255.255.255.0
```

1.2 L2TP相关配置。

```
#
 l2tp enable
#
 domain default enable system

#
domain system
```

```
 access-limit disable
 state active
 idle-cut disable
 self-service-url disable
 ip pool 0 172.31.255.2 172.31.255.254
#
local-user jshan
 password simple qwerty
 authorization-attribute level 3
 service-type ppp
#
l2tp-group 1
 undo tunnel authentication
 allow l2tp virtual-template 0
#
interface Virtual-Template0
 ppp authentication-mode chap domain system
 remote address pool
 ip address 172.31.255.1 255.255.255.0
```

1.3 IPSec相关配置。

```
#
 ike local-name center
#
ike proposal 1
 encryption-algorithm aes-cbc 256
 dh group2
#
ike peer ikeiphone
 pre-shared-key cipher xz8n+yXxN+I=
 remote-address 10.255.255.136
 local-address 10.255.255.13
#
ipsec proposal 1
 encapsulation-mode transport
 esp authentication-algorithm sha1
 esp encryption-algorithm aes 128
#
ipsec policy-template temp 1
 ike-peer ikeiphone
 proposal 1
#
ipsec policy policy 1 isakmp template temp
#
interface GigabitEthernet0/1
 port link-mode route
 ip address 10.255.255.13 255.255.255.0
 ipsec policy policy
```

3. 配置iPhone接入VPN

进入iPhone主界面，进入“设置”、“通用”、“网络”、“VPN”，进入VPN配置页面。

服务器地址就是IPSec服务的公网地址。

账户和密码是和l2tp部分的配置相通的，也就是说，iphone客户IPSEC这边配置的是什么，会直接同步给L2TP和PPTP那两个页签，这三页里只能用相同的。因此配置为L2TP的用户名和密码。

密钥是IKE的预共享密钥。

请参考如下两幅截图进行配置。

4. 验证VPN接入效果

在本案例中，当iPhone接入VPN后的效果如下图所示。注意在iPhone右上角会出现一个“VPN”的标识

。

此时就可以通过iPhone上安装的Web浏览器等其他应用客户端访问VPN内部资源了。

四、 配置关键点：

1. iPhone在进行IKE一阶段协商时，仅支持主模式，不支持野蛮模式。

2. iPhone在进行IKE一阶段、二阶段SA协商时，支持的安全提议中，加密及验证算法安全性级别较高，防火墙如果采用默认安全提议无法协商成功，需手工配置安全提议。

iPhone默认有6个ike proposal，下面显示的只是其中之一。

```
<H3C>dis ike proposal 1
 priority authentication authentication encryption Diffie-Hellman duration
          method       algorithm    algorithm       group       (seconds)
--------------------------------------------------------------------------------
  1      PRE_SHARED    SHA    AES_CBC_256   MODP_1024    86400
```

iPhone默认有3个ipsec proposal，下面显示的只是其中之一。

```
<H3C>dis ipsec proposal 1

  IPsec proposal name: 1
    encapsulation mode: transport
    transform: esp-new
    ESP protocol: authentication sha1-hmac-96, encryption 128-bits aes
```

3. 在使用GPRS、EDGE、WCDMA等2G、3G接入条件下，如果广域网存在NAT，由于iPhone不支持野蛮模式，因此也无法与我司防火墙配置实现NAT穿越。