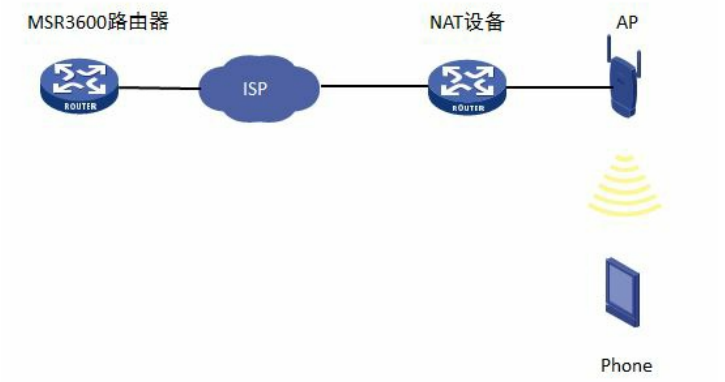
MSR 3600路由器配置L2TP over ipsec vpn手机拨入失败案例分析

IPsec 李聪 2016-04-21 发表



一、 组网以及问题描述：

如图所示，MSR3600路由器上面配置了L2TP over ipsec vpn，方便出差的员工可以使用移动终端拨入vpn访问公司的内网资源。现场按照官网文档的配置之后反馈目前不能成功拨入，接下来分析一下原因。

二、 原因分析：

接下来从配置、网络情况、以及debug方面进行分析。

1. 检查配置以及网络

通过检查现场的配置并没有问题，配置如下：

```
#
ip pool mobile 10.205.8.2 10.205.8.254            //地址池
#
interface Virtual-Template9
 ppp authentication-mode pap
 remote address pool mobile
 ip address 10.205.8.1 255.255.255.0
#
local-user mobile class network
 password cipher 123456
 service-type ppp //服务类型
 authorization-attribute user-role network-operato
#
ipsec transform-set m1  //设置ipsec多种加密算法以及验证算法
 encapsulation-mode transport
 esp encryption-algorithm 3des-cbc
 esp authentication-algorithm md5
#
ipsec transform-set m2
 encapsulation-mode transport
 esp encryption-algorithm aes-cbc-128
```

```
 esp authentication-algorithm sha1
#
ipsec transform-set m3
 encapsulation-mode transport
 esp encryption-algorithm aes-cbc-256
 esp authentication-algorithm sha1
#
ipsec transform-set m4
 encapsulation-mode transport
 esp encryption-algorithm des-cbc
 esp authentication-algorithm sha1
#
ipsec transform-set m5
 encapsulation-mode transport
 esp encryption-algorithm 3des-cbc
 esp authentication-algorithm sha1
#
ipsec transform-set m6
 encapsulation-mode transport
 esp encryption-algorithm aes-cbc-192
 esp authentication-algorithm sha1
#
ipsec policy-template m1 1
 transform-set m1 m2 m3 m4 m5 m6   //不确定终端的提议类型，这里设置多个
#
ipsec policy t1 20 isakmp template m1
#
l2tp-group 9 mode lns  //配置L2TP，这里不使用隧道验证
 allow l2tp virtual-template 9
 undo tunnel authentication
#
 l2tp enable
#
ike profile 1  //ike部分的配置
 keychain 1
match remote identity address 0.0.0.0 0.0.0.0
 proposal 21 22 23 24 25 26
#
ike proposal 21
 encryption-algorithm aes-cbc-128
 dh group2
 authentication-algorithm md5
#
ike proposal 22
 encryption-algorithm 3des-cbc
 dh group2
```

authentication-algorithm md5

#

ike proposal 23

encryption-algorithm 3des-cbc

dh group2

#

ike proposal 24

encryption-algorithm aes-cbc-256

dh group2

#

ike proposal 25

dh group2

#

ike proposal 26

encryption-algorithm aes-cbc-192

dh group2

#

ike keychain 1

pre-shared-key address 0.0.0.0 0.0.0.0 key cipher 123456

#

检查完配置之后，现场反馈目前设备上面还有其他的ipsec vpn，可以建立成功的，而且客户使用的电信线路，设备直接连接的电信光纤，没有防火墙之类的设备做拦截。在外网ping也是没有问题的，目前暂时可以排除网络问题。接下来进行抓包分析。

2. debugging抓包分析匹配的keychain

在抓包分析之前使用display ike sa以及display ipsec sa都发现没有建立隧道。为了分析ikel以及ipsec、l2tp的建立过程，开启了debugging l2tp all、debugging ike all、debugging ipsec all。测试的手机的外网地址是119.4.255.218，以下是提示信息：

*Mar 23 17:07:37:557 2016 JT-ROUTE-A IKE/7/Event: Found pre-shared key that matches address 119.4.255.218 in keychain t1.//现场设备配置中配置的keychain是keychain 1，但是这里匹配的keychain明显不对。因此需要检查ike keychain这一块的配置。

*Mar 23 17:07:37:557 2016 JT-ROUTE-A IKE/7/Packet: Attributes is acceptable.

*Mar 23 17:07:37:557 2016 JT-ROUTE-A IKE/7/Event: Oakley transform 9 is acceptable.

*Mar 23 17:07:37:557 2016 JT-ROUTE-A IKE/7/Packet: Construct SA payload

*Mar 23 17:07:37:557 2016 JT-ROUTE-A IKE/7/Packet: Construct NAT-T rfc3947 vendor ID payload.

以下是ike keychain的配置：

#

ike keychain 1

pre-shared-key address 0.0.0.0 0.0.0.0 key cipher c3$nsDnONpQI6pTw0IAhPrYGMx8ujyOUHc9Rw==

#

ike keychain t1

pre-shared-key address 0.0.0.0 0.0.0.0 key cipher c3$Q9EwwSCk+9oblBfPMVSgNqAYiric7xnxmsXT

#

Ike profile的配置：

#

ike profile 1

keychain 1

local-identity address 171.221.201.249

match remote identity address 0.0.0.0 0.0.0.0

proposal 21 22 23 24 25 26

#

#

ike profile t1

keychain t1

exchange-mode aggressive

match remote identity address 0.0.0.0 0.0.0.0

match remote identity fqdn shoufeizhan

proposal 1

以上的ike keychain t1以及ike profile t1是建立野蛮模式的ipsec使用的。对比以上的ike keychain以及ike profile的配置之后发现l2tp over ipsec vpn和野蛮模式的ipsec vpn的profile匹配的对方地址是一致的，都是匹配全部地址0.0.0.0/0，但是ipsec限制当系统配置了多个ike profile时，ike profile中match remote identity address配置地址范围不能有交集。因此，我们需要将野蛮模式的ipsec vpn配置进行修改，修改为匹配对方fqdn name的方式。修改如下：

#

ike keychain t1

pre-shared-key hostname shoufeizhan key cipher c3$8eT/7r9F4lWawFv3Pp7lVG3CsxTjTF2O+Q==

#

ike profile t1

keychain t1

exchange-mode aggressive

match remote identity fqdn shoufeizhan

proposal 1

#

以上修改完成之后依然还是不能成功拨入，但是这次看到匹配正确的ike keychain以及ike profile了。

3. debugging抓包分析匹配的验证加密算法以及其他参数

修改完ike keychain之后接下来继续查看debug的抓包信息：

*Apr 5 14:35:10:399 2016 JT-ROUTE-A IKE/7/Packet: The profile 1 is matched.

*Apr 5 14:35:10:399 2016 JT-ROUTE-A IKE/7/Error: Failed to find proposal 15 in profile 1./这里看出匹配了profile了，但是发现匹配的提议有问题，没有找到合适的proposal 15。

*Apr 5 14:35:10:400 2016 JT-ROUTE-A IKE/7/Packet: Encrypt the packet.

*Apr 5 14:35:10:400 2016 JT-ROUTE-A IKE/7/Packet: Construct notification packet: PAYLOAD_MALFORMED.//一般为密钥错误或者加密验证算法有问题。

*Apr 5 14:35:10:400 2016 JT-ROUTE-A IKE/7/Packet: Sending packet to 119.4.255.86 remote port 15843, local port 4500.

从以上的错误看出没有建立成功的原因就是profile里面没找到合适的profile的参数，我们对比设备的配置发现proposal 15以及配置在l2tp中使用的proposal 24一样的：

#

ike proposal 15

encryption-algorithm aes-cbc-256

dh group2

#

ike proposal 24

encryption-algorithm aes-cbc-256

dh group2

但是ike profile 1里面调用的是proposal 24。为什么没有调用配置的proposal 24，而是调用了提议一样序号比较小的proposal 15？原因是主模式下IKE提议在配置的时候具有优先级，使用主模式建立IKE一阶段SA时，发送时按照优先级顺序发送所有的IKE提议，响应端将收到的IKE提议，依据收到的顺序与本端所有提议进行比较，选中符合的一个继续协商。根据现场提供的ike proposal的优先级如下：

Priority Authentication Authentication Encryption Diffie-Hellman Duration

method algorithm algorithm group (seconds)

---

15 PRE-SHARED-KEY SHA1 AES-CBC-256 Group 2 86400

24 PRE-SHARED-KEY SHA1 AES-CBC-256 Group 2 86400

可以看出配置相同的proposal，是以序号为小的优先级高。因此当移动终端发起访问，协商的参数命中优先级高的proposal就以序号小的proposal 15协商，但是因为ike profile里面没有相应的proposal 15的配置，因此协商失败。

解决的办法就是在ike profile里面添加序号小优先级高的proposal 15即可。现场修改完成之后就可以正常拨入访问公司内网了。

三、 解决办法：

1. ipsec限制当系统配置了多个ike profile时，ike profile中match remote identity address配置地址范围不能有交集。因此，我们需要将野蛮模式的ipsec vpn配置进行修改，修改为匹配对方fqdn name的方式。

2.主模式下IKE提议在配置的时候具有优先级，使用主模式建立IKE一阶段SA时，发送时按照优先级顺序发送所有的IKE提议，响应端将收到的IKE提议，依据收到的优先级顺序与本端所有提议进行比较，选中符合的一个继续协商。因此L2TP的ipsec配置中ike profile中的proposal需要包括优先级高的协商参数。