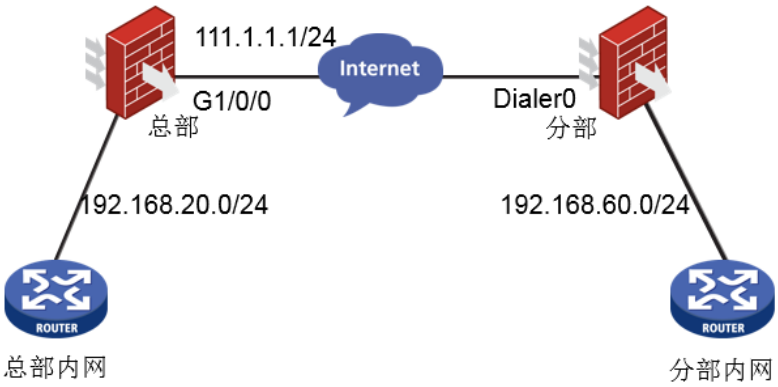
某局点F1000-AK115总部和分部建立IPSEC失败故障排查经验案例

IPSec VPN 王周华 2020-03-30 发表

组网及说明

总部和分部的出口设备是防火墙，为保护内网数据流不被窃听，客户要求通过IPSEC VPN建立隧道传输数据。总部的公网IP地址是固定的IP地址，分部的公网IP地址是通过 PPPOE动态获取的。组网大致拓扑图如下：



本次涉及设备的型号以及版本：F1000-AK115　version 7.1.064, Release 9524P18

问题描述

由于分部的公网IP地址是通过 PPPOE动态获取的，不是固定的IP地址，如果采用IPSEC策略的方式，REMOTE-ADDRESS是必须要指定了，所以总部采用了IPSEC模板的方式，通过野蛮模式建立IPSEC VPN隧道。但是现场反馈配置完成后只能看到第一阶段的IKE SA，第二阶段的IPSEC SA协商失败，导致隧道无法建立成功。

过程分析

1、首先检查两边的配置。分部侧采用FQDN在IKE认证协商阶段向对端标识自己的身份，总部侧采用IP地址标识自己的身份，总部和分部两个阶段采用的加密、验证算法一致。IPSEC VPN关键配置如下：

总部侧：

```
ipsec policy-template zongbu 1
 transform-set 1
 security acl 3010
 local-address 111.1.1.1
 ike-profile zongbu
#
ipsec policy h3c 2 isakmp template zongbu
#
ike profile zongbu
 keychain 1
 exchange-mode aggressive
 local-identity address 111.1.1.1
 match remote identity fqdn fenub
 match local address 111.1.1.1
 proposal 1
ike keychain 1
 pre-shared-key hostname fenbu key cipher $c$3$wxUyCmXoDBXqR/bHFwyOrRzri5oRxPbLEg==
```

分部侧：

```
ipsec policy fenbu 1 isakmp
 transform-set 1
 security acl 3002
 remote-address 111.1.1.1
 ike-profile fenbu
#
 ike identity fqdn fenbu
#
ike profile fenbu
```

keychain 1
exchange-mode aggressive
local-identity fqdn fenbu
match remote identity address 111.1.1.1 255.255.255.255
proposal 1
#
ike keychain 1
pre-shared-key address 111.1.1.1 255.255.255.255 key cipher c3$Po1w5IYWcpzRAg2+yPN1ax8Li6gPvVIJPQ==

2、接下来通过debugging ike all查看隧道的建立过程。现场反馈的debug信息输出如下：

总部侧的报错信息：

ar 26 14:53:18:779 2020 zongbu IKE/7/ERROR: vrf = 0, local = 111.1.1.1, remote = 27.202.76.17/500
Failed to get IPsec policy for phase 2 responder. Delete IPsec SA.

分部侧的报错信息：

*Mar 26 14:27:11:336 2020 fenbu IKE/7/EVENT: vrf = 0, local = 27.202.76.17, remote =111.1.1.1/500
Notification **INVALID_ID_INFORMATION** is received.

总部侧的报错是无法获取阶段2响应的IPsec策略，分部侧的报错INVALID_ID_INFORMATION无效的身份信息可能原因如下：

第二阶段第一个报文后提示的，IPSEC policy下的local-address不对
第二阶段第一个报文后提示的，IPSEC policy下没配置remote-address
第二阶段第一个报文后提示的，接口下配置的IPSEC policy名字不对
第二阶段第一个报文后提示的，IKE SA协商的id-type类型不一致

3、核对分部侧的如上信息没有发现问题，于是排查总部侧无法获取阶段2响应的IPSEC策略的原因。由于总部侧的IP地址是固定的，所以由分部侧发起IPSEC VPN隧道的建立。发现总部侧IPSEC VPN用于匹配保护流量ACL匹配次数没有增加，于是检查两边对应ACL的配置如下：

分部侧：

acl advanced 3002
rule 0 permit ip source 192.168.60.0 0.0.3.255 destination **192.168.20.0 0.0.3.255**

总部侧：

acl advanced 3010
rule 1 permit ip source **192.168.20.0 0.0.0.255** destination 192.168.60.0 0.0.3.255

可以发现两者的ACL没有完全镜像。若IPSEC对等体上的ACL配置非镜像，那么只有在一端的ACL规则定义的范围是另外一端的子集时，SA协商可以成功。需要注意的是，在这种ACL配置下，并不是任何一端发起的SA协商都可以成功，仅当保护范围小（细粒度）的一端向保护范围大（粗粒度）的一端发起的协商才能成功，反之则SA协商失败。而现场分部侧配置的ACL保护范围大于总部侧的ACL保护范围，且是由分部侧发起的协商，所以SA协商失败。

解决方法

将总部侧IPSEC VPN的ACL改为如下后，问题解决。

acl advanced 3010
rule 1 permit ip source 192.168.20.0 0.0.3.255 destination 192.168.60.0 0.0.3.255