防火墙 IPSEC VPN 证书验证主模式单端触发建立不了问题处理案例

IKE 证书 PKI 刘晨 2020-03-19 发表

组网及说明

无

问题描述

客户现场我司F1030防火墙与多点对接ipsec主模式，ike验证方式为证书认证，在对接其中一台锐捷路由器的时候发现两端配置完成后， 本端触发能够正常建立ipsec，对端触发无法建立ipsec。对端触发的时候ike sa及ipsec sa都没有。

过程分析

对端为锐捷设备，在核对了ike profile 及ipsec policy等配置无误的情况下，收集debug信息

*Mar 13 16:18:36:958 2020 4GYW_F1030_A PKI/7/PKI_DEBUG: -COntext=1; PKI_Certificate_ACP: Matches the attribute 1 in attribute group "group134". Checking the next attribute.

*Mar 13 16:18:36:959 2020 4GYW_F1030_A PKI/7/PKI_DEBUG: -COntext=1; PKI_Certificate_ACP: Matched rule number: 1, which has the action permit, in access control policy "**policy134**". The certificate is trusted. //**匹配了 policy134**

*Mar 13 16:18:36:959 2020 4GYW_F1030_A IKE/7/PACKET: -COntext=1; vrf = 0, local = 2.2.2.254, remote = 1.1.1.1134/500 The profile **RJ_140 is matched**. //**根据policy 134match到了 RJ_140 的ike profile**

*Mar 13 16:18:36:960 2020 4GYW_F1030_A IKE/7/PACKET: -COntext=1; vrf = 0, local = 2.2.2.254, remote = 1.1.1.1134/500 Process certificate payload. *Mar 13 16:18:36:961 2020 4GYW_F1030_A PKI/7/PKI_DEBUG: -COntext=1; Get verify result from cache successfully.

*Mar 13 16:18:36:963 2020 4GYW_F1030_A PKI/7/PKI_DEBUG: -COntext=1; Failed to verify certificate by domain **dom2**. //**通过 RJ_140 的profile去域名为dom2 域下查找证书，命中错了域导致证书验证失败从而ike协商失败**

pki certificate access-control-policy **policy134**
rule 1 permit **group134**

实际对的ike profile下的配置域为 h3c-rsa，从debug信息分析为policy同时调用在两个ike profile下，对端触发时证书验证的时候匹配到另外一个ike profile下的域从而匹配错了证书
从debug信息可以得出，当ipsec结合证书的方式建立隧道时，被动方是通过对端的发过来的证书的颁发者名、主题名以及备用主题名进行匹配，当匹配上了 证书属性组后再去找到对应的证书访问策略，再通过证书访问策略找到对应的ike profile，根据profile下配置的域去进行证书的查找并验证。

ike profile **RJ_134**
 certificate domain **h3c-rsa**
 local-identity address 2.2.2.254
 match remote certificate **policy134**
 match local address Vlan-interface101
 proposal 20

ike profile **RJ_140**
 certificate domain **dom2**
 exchange-mode gm-main
 local-identity address 2.2.2.254
 match remote certificate **policy134**
 match local address Vlan-interface101
 proposal 10

解决方法

将命为 **RJ_140** 的ike profile里调用的pki certificate access-control-policy 修改为正确的后正常建立。