

问题描述

我们安全设备和对端路由器建立ipsec，之前正常，突然出问题的，两端都是固定ip，debug看我们这边回给对端的ike profile信息不正确

过程分析

```
最初我们防火墙用ike profile ipsec2715350323_IPv4_47和对端建立ike
ipsec policy-template ipsec2715350323 47
transform-set ipsec2715350323_IPv4_47
local-address 2.161.75.18
remote-address 1.52.142.90
ike-profile ipsec2715350323_IPv4_47
policy alias baicheng-bg
```

通过debug信息看：对端发过的ike协商报文，我们设备用ike profile ipsec2715350323_IPv4_21回给对端的，导致ike协商一直起不来

```
*May 14 11:06:40:551 2024 L2-8-S1-ZTNA-AK8010-14 IKE/7/EVENT: -COntext=1; vrf = 0, local =
2.161.75.18, remote = 1.52.142.90/500
The profile ipsec2715350323_IPv4_21 is matched.
```

```
ike profile ipsec2715350323_IPv4_21
keychain ipsec2715350323_IPv4_21
exchange-mode aggressive
local-identity fqdn crCenter
match remote identity address 0.0.0.0 0.0.0.0
match remote identity fqdn yangguang-br
match local address GigabitEthernet1/0/9
```

proposal 2

后面创建了一个编号小的ipsec2715350323_IPv4_19和对端建立vpn，依旧是匹配ike profile ipsec2715350323_IPv4_21，不匹配明细

解决方法

IKE profile的匹配优先级首先取决于其中是否配置了match local address，其次决定于配置的优先级值，最后决定于配置IKE profile的先后顺序。

如果想让某个ike命中某个profile，可以调整优先级数值

2.1.44 priority (IKE profile view)

priority 命令用来指定IKE profile的优先级。

undo priority 命令用来恢复缺省情况。

【命令】

```
priority priority
undo priority
```

【缺省情况】

IKE profile的优先级为100。

【视图】

IKE-Profile视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

priority priority: IKE profile优先级号，取值范围为1~65535。该数值越小，优先级越高。

【使用指导】

配置了**match local address**的IKE profile，优先级高于所有未配置**match local address**的IKE profile。即IKE profile的匹配优先级首先决定于其中是否配置了**match local address**，其次决定于它的优先级。

【举例】

```
# 指定在IKE profile prof1的优先级为10。
<Sysname> system-view
[Sysname] ike profile prof1
```

[Sysname-ike-profile-prof1] priority 10

把ike profile ipsec2715350323_IPv4_19的优先级调成50解决的

ike profile ipsec2715350323_IPv4_19

priority 50