某局点 SecPath F1000-AK125(V7) 手机L2TP over IPSec拨入失败经典案例

L2TP over IPSec VP zhiliao_6a9Vt 2018-09-30 发表

组网及说明

无

问题描述

前期现场部署L2TP over IPSEC后，手机端能够正常拨入访问内网。

后续增加F1000-AK125与分部其他设备建立ipsec 隧道新配置后，发现手机端L2TP over IPSec不能拨入。

过程分析

1、查看配置

ipsec policy-template 1 1
transform-set 1 2 3 4 5
 ike-profile 1
 # 增加的配置加粗
ipsec policy-template 1 10
transform-set 10
 security acl 3501
 ike-profile xiaosunzhuang
#
ipsec policy-template 1 20
transform-set 10
 security acl 3502
 ike-profile dasi
#
ipsec policy 1 1 isakmp template 1
#
l2tp-group 1 mode lns
allow l2tp virtual-template 1
undo tunnel authentication
tunnel name lns
#
l2tp enable
#
ike identity fqdn center
#
ike profile 1
keychain 1
match remote identity address 0.0.0.0 0.0.0.0
proposal 1
#
ike profile dasi
keychain dasi
exchange-mode aggressive
local-identity address 111.33.100.18
match remote identity fqdn dasi
proposal 10
#
ike profile xiaosunzhuang
keychain xiaosunzhuang
exchange-mode aggressive
local-identity address 111.33.100.18
match remote identity fqdn xiaosunzhuang
proposal 10
#
ike proposal 1
encryption-algorithm 3des-cbc
dh group2
authentication-algorithm md5

#
ike proposal 10
encryption-algorithm 3des-cbc
dh group2
#
ike keychain 1
pre-shared-key address 0.0.0.0 0.0.0.0 key cipher c3$L/cA6KnS3tVQGOhuQjfUGtY+H+W1UAxw9g==
#
ike keychain dasi
pre-shared-key hostname dasi key cipher c3$rO1mOi4cuiz6YyHD6LFHbr+dwpwZTyfvs4Tx
#
ike keychain xiaosunzhuang
pre-shared-key hostname xiaosunzhuang key cipher c3$GofP6Rc+l+ZkROdlaEDGqvq10WMO/PltyCFL
#

2、故障时debug ike all信息提示
***Sep 18 12:16:24:052 2018 JingWu IKE/7/ERROR: vrf = 0, local = 111.33.100.18, remote = 106.47.103.91/21227**
Failed to find proposal 10 in profile 1.
……
***Sep 18 12:16:27:258 2018 JingWu IKE/7/ERROR: 2th byte of the structure ISAKMP Identification Payload must be 0.**
***Sep 18 12:16:27:258 2018 JingWu IKE/7/ERROR: vrf = 0, local = 111.33.100.18, remote = 106.47.103.91/21227**
Failed to parse phase 1 packet. Reason INVALID_PAYLOAD_TYPE.

确认现场ike proposal 1和10没有重叠，ike profile 1与ike profile 10、20 local和remote也配置的不一样，并且ike keychain 1的密钥123456，与手机端配置是一致的。

解决方法

*Sep 18 12:16:23:981 2018 JingWu IKE/7/PACKET: vrf = 0, local = 111.33.100.18, remote = 106.47.103.91/21227
Encryption algorithm is 3DES-CBC.
*Sep 18 12:16:23:981 2018 JingWu IKE/7/PACKET: vrf = 0, local = 111.33.100.18, remote = 106.47.103.91/21227
Authentication method is Pre-shared key.
*Sep 18 12:16:23:981 2018 JingWu IKE/7/PACKET: vrf = 0, local = 111.33.100.18, remote = 106.47.103.91/21227
HASH algorithm is HMAC-SHA1.
*Sep 18 12:16:23:981 2018 JingWu IKE/7/PACKET: vrf = 0, local = 111.33.100.18, remote = 106.47.103.91/21227
DH group is 2.
手机协商的时候一次性发了13个请求，分别由不同的算法组成，这13个中筛选出来只有上面这个可以命中proposal 10，所以推测手机端是以枚举的方式来发起请求，前期现场只有peoposal 1，以较靠后的协商。
现场后期加了新策略后，proposal 10在前面就被匹配，导致反向查找ike profile时发现绑定了proposal 1，判断不匹配。ike profile中去除proposal 1的命令后恢复。