V7防火墙通过主模式和多个分支建立ipsec时断时通

李超 2018-01-07 发表

客户总部部署了一台v7防火墙，总部和多个分支建立ipsec vpn，分支有v5和v7设备，客户反馈reset ipsec sa和reset ike sa后，vpn有时候需要很长时间才能起来，有时候又很快就可以起来。

通过登录总部和有问题的分支，发现ipsec起不来有两种情况：第一种情况是分支没有配置pfs；另一种分支配置了pfs，但是分支是V5设备。

第一种情况下：

总部配置

ipsec transform-set GE1/0/2_IPv4_5

esp encryption-algorithm des-cbc

esp authentication-algorithm md5

pfs dh-group1

分支配置

ipsec transform-set gzbggds

esp encryption-algorithm des-cbc

esp authentication-algorithm md5

缺省情况下，使用IPsec安全策略发起协商时不使用PFS特性，发起方的PFS强度必须大于或等于响应方的PFS强度，否则协商会失败，不配置PFS特性的一端，按照对端的PFS特性要求进行IKE协商，大概意思就是PFS强的向PFS弱的或者有PFS的向没有的发起是可以正常协商的，反之则协商失败。

现场情况下，分支没有配置PFS特性，总部配置了PFS特性，所以当分支主动去触发ipsec时，协商就会失败，只有等总部主动去触发时协商才会成功，最后给客户带来的感觉就是ipsec中断后，有时候需要很长时间才能恢复，有时候又很快就恢复。

第二种情况：

现场总部为V7设备配置了多个算法相同的ike proposal，V7和V7设备对接，分支主动ping总部时，总部有如下多个相同的算法优先级不同的ike proposal，V7设备优先会选择优先级比较高的ike proposal，如果ike profile中未包含该优先级的proposal，则协商失败；

V5和V7设备对接，分支主动ping总部时，会选择优先级比较低的ike proposal，如果ike profile中未包含该优先级的proposal，则协商失败；

总部ping分支能通，是因为分支相同算法proposal只有一个，所以协商可以成功。

<F1000-AK130>dis ike proposal

Priority	Authentication method	Authentication algorithm	Encryption algorithm	Diffie-Hellman group	Duration (seconds)
65518	PRE-SHARED-KEY	SHA1	DES-CBC	Group 1	86400
65519	PRE-SHARED-KEY	SHA1	DES-CBC	Group 1	86400
65520	PRE-SHARED-KEY	SHA1	DES-CBC	Group 1	86400
65521	PRE-SHARED-KEY	SHA1	DES-CBC	Group 1	86400
65522	PRE-SHARED-KEY	SHA1	DES-CBC	Group 1	86400
65523	PRE-SHARED-KEY	SHA1	DES-CBC	Group 1	86400
65524	PRE-SHARED-KEY	SHA1	DES-CBC	Group 1	86400
65525	PRE-SHARED-KEY	SHA1	DES-CBC	Group 1	86400
65526	PRE-SHARED-KEY	SHA1	DES-CBC	Group 1	86400
65527	PRE-SHARED-KEY	SHA1	DES-CBC	Group 1	86400
65528	PRE-SHARED-KEY	SHA1	DES-CBC	Group 1	86400
65529	PRE-SHARED-KEY	SHA1	DES-CBC	Group 1	86400
65530	PRE-SHARED-KEY	SHA1	DES-CBC	Group 1	86400
65531	PRE-SHARED-KEY	SHA1	DES-CBC	Group 1	86400
65532	PRE-SHARED-KEY	SHA1	DES-CBC	Group 1	86400
65533	PRE-SHARED-KEY	SHA1	DES-CBC	Group 1	86400
65534	PRE-SHARED-KEY	SHA1	DES-CBC	Group 1	86400
65535	PRE-SHARED-KEY	SHA1	DES-CBC	Group 1	86400
default	PRE-SHARED-KEY	SHA1	DES-CBC	Group 1	86400

这种情况下，给客户带来的感觉也是ipsec中断后，有时候需要很长时间才能恢复，有时候又很快就恢复。

针对第一种情况，将分支的PFS特性配置的跟总部一致，第二种情况，在总部的每个ike profile中均添加优先级最高和最低的proposal。