某局点F1020 业务经过IPsec vpn之后，无法打开服务器web界面问题处理经验案例

IPSec VPN 刘文峰 2019-06-19 发表

组网及说明

无

问题描述

某局点总部和分部分别采用F1020做出口设备，刚开始分支通过总部fw映射出来的地址访问总部服务器，后期出于安全性考虑，想实现分支访问总部服务器经过ipsec 加密，两边IPsec 能正常建立，分支ping 总部服务器也能ping 通，但是分支的电脑无法打开总部服务器的web界面。

过程分析

之前分支通过总部映射出来可以正常访问，但是通过ipsec 无法访问，所以怀疑是ipsec 加密导致，但是又能ping 通，所以怀疑是两边的TCP、MTU问题导致，让客户修改外网口的tcp mss 1024，mtu 1440，但是还不行，后续mtu 多次测试改其他的也还是不行。

解决方法

按照下面修改之后，问题解决，可以正常打开。

1. 修改内网口的TCP mss，MTU不动
2. TCP mss的值通过dis ipsec sa 看sa 的mtu，然后减去40

tcp mss=mtu-40