MER8300 开启上网行为管理功能后内网全部断网

安全域 郭尧 2021-06-28 发表

组网及说明

路由器作出口设备

问题描述

正常情况下能够正常访问外网，在路由器设备上全局控制开启上网行为管理功能后，内网全部断网

过程分析

查看配置无误

上网行为管理策略配置为any，并且动作为不阻断

其他策略，黑白名单等均未进行配置

路由器能够与外网114地址互通，内网设备无法ping通外网，下行交换机也无法与外网互通，但是能够ping通路由器内网接口地址

WEB页面查看设备状态均正常，CPU内网均正常，路由器正常获取公网地址

WEB页面查看设备配置均无异常，关闭上网行为管理功能后业务恢复正常

版本升级到最新版本

后进入命令行查看是否有异常配置

发现设备居然配置了any到any的域间测试，且接口未加入安全域，内外网接口无法互通

尝试关闭上网行为管理功能后，域间策略配置消失，判断该功能会自动启用域间策略

V7路由器默认没有开启安全功能，也没有安全域。所以接口不加入域能正常上网。但是上网行为管理要通过域间策略的方式来生效，所以当配置上网行为管理策略时，设备会下发动作是inspect的域间策略。此时相当于设备启用了安全功能，类似于防火墙。需要将接口加入安全域，才能根据域间策略访问外网。

解决方法

该设备web页面无法配置安全域、域间策略等配置，若要开启上网行为管理功能，需要在命令行把内外网接口加入安全域，通过域间策略放通，开启上网行为管理功能后，能够正常访问外网

注：

在官网用户手册配置没有相关说明，V7路由器使用上网行为管理功能时，需要先在配置的设备接入的接口未加入安全域的情况下，在web管理界面配置好对应的上网行为管理策略。让后将内外网口加入对应的安全域，上网行为管理策略才会正确生效。接口如果未加入安全域会导致内网断网。将上网行为管理策略删除之后，必须把这些接口从安全域移除，否则也会造成网络中断。