关于安全产品安全策略和域间策略混配出现业务中断问题的技术公告

域间策略/安全域 包过滤 王晗 2021-12-03 发表

问题描述

【产品型号】

涉及F100系列、L100系列、F1000系列、T1000系列、L1000系列、F5000系列、T5000系列、L5000系列、vFW系列、vLB系列、SecBlade FW系列、SecBlade IPS系列、SecBlade ADE系列、M9000系列、T9000系列 等安全全系列Comware V7产品。

【涉及版本】

所有Comware V7 支持安全策略版本

【问题描述】

上述设备使用域间策略（包括包过滤及对象策略）时，有如下三种情况混配会导致业务中断。

1、域间策略调用包过滤时，在命令行配置安全策略，并且新建rule。由于新建的rule初始全阻断且全匹配，导致包过滤业务全部中断。

2、域间策略调用对象策略时，在命令行新建安全策略。由于对象策略和安全策略互斥，对象策略全部失效，导致对象策略业务全部中断。

3、域间策略调用对象策略时，在web界面新建安全策略，由于对象策略和安全策略互斥，对象策略全部失效，导致对象策略业务全部中断。

原因分析

【原因分析】

1、安全策略功能与对象策略功能在设备上不能同时使用，当安全策略功能处于开启状态时，首次进入安全策略视图后，对象策略功能立即失效。

2、当安全策略与包过滤同时配置时，因为安全策略对报文的处理在包过滤之前，报文与安全策略规则匹配成功后，不再进行包过滤处理。

规避措施/解决方案

【解决方案】

域间策略全部转换为安全策略，避免域间策略和安全策略混配。