[20140710]关于H3C Comware V5平台防火墙变更默认域间策略转发规则的公告

金山 2014-07-10 发表

关于H3C Comware V5平台防火墙变更默认域间策略转发规则的公告

【产品型号】

以下Comware V5平台防火墙产品(共计25款)将涉及本次变更，具体型号包括：

SecBlade Enhanced

SecBlade II

SecPath F5000-S/C

SecPath F1000-E

SecPath F1000-E-SI/A-EI/S-AI

SecPath F1000-C-SI

SecPath F1000-A/S/C-G

SecPath F100-E/A/M/S/C-G

SecPath F100-A/M-SI

SecPath U200-A/M/S/CA/CM/CS

特别注意，以下防火墙产品（共计3款）不涉及变更，具体型号包括：

SecPath F5000-A5

SecPath F1000S-EI

SecPath F100-C-AI

【涉及版本】

产品型号	策略变更起始版本号（含）
SecBlade Enhanced	CMW520-R3820
SecBlade II	CMW520-R3180
SecPath F5000-S/C	CMW520-R3811
SecPath F1000-E	CMW520-R3180
SecPath F1000-E-SI/A-EI/S-AI	CMW520-R3733
SecPath F1000-C-SI	CMW520-R5142P01
SecPath F1000-A/S/C-G	CMW520-R3733
SecPath F100-E/A/M/S/C-G	CMW520-R5142
SecPath F100-A/M-SI	CMW520-R5142P01
SecPath U200-A/M/S/CA/CM/CS	CMW520-R5116P23（F5123系列版本不变更）

【问题描述】

本次Comware V5平台防火墙默认域间策略转发规则变更如下：

变更前：系统默认安全区域之间**按照优先级进行转发**，即“高优先级安全域可以访问低优先级安全域”、“相同级别安全域之间可以互访”等。

变更后：系统默认域间策略转发规则**更改为全部阻断**，即任意安全区域之间和相同安全域之内都不允许通信。

【原因分析】

1、为满足市场需求，提高防火墙设备在网运行稳定性及客户业务安全性，特进行此次生产版本变更操作。

2、为实现在网防火墙设备运行配置兼容性，前述“变更前”、“变更后”默认规则可通过命令进行切换。

恢复至“变更前”的按优先级的默认互访规则：

[H3C] interzone policy default by-priority

切换至“变更后”的全部阻断的默认互访规则：

[H3C] undo interzone policy default by-priority

【规避措施 / 解决方案】

1. 新发货设备运行“涉及版本（或更新的版本）”，以出厂空配置启动后，将遵循全部阻断的默认域间策略互访规则。

2. 对在网运行防火墙执行升级操作时，当设备从早期版本升级至“涉及版本（或更新的版本）”时，软件会自动在原有配置中添加“interzone policy default by-priority”命令，维持变更前默认互访规则，确保版本升级操作不影响当前业务转发。完成升级操作后须注意保存此配置。