



防火墙基于地域限制访问

域间策略/安全域 刘昆 2022-09-09 发表

问题描述

需求：防火墙基于地域限制访问。

如：限制境外地址访问

过程分析

支持地区 (geo-location) ,对应包含的IP地址集合, 直接引用

解决方法

防火墙从B64D071分支开始支持地区 (geo-location) , 可以在安全策略中通过配置source-location/destination-location命令实现基于地区的控制。

【举例】限制中国境内以外的地区访问

```
#
Security-policy ip
rule 100 name 放行国内地址
action pass
source-zone untrust
source-location China
rule 101 name denyall
action drop
source-zone untrust
#
```

版本判断方法:

(1) 粗略判断: 版本号为RaabbPcc时, bb \geq 71时为支持。

举例F5030 R9660P30版本为60分支, 不支持; F9671P10版本为71分支, 支持。

(2) 详细判断: probe视图下display system internal version查看内部版本号。

如下举例为45分支, 小于71, 所以不支持。

```
[F5020-IRF-probe]display system internal version  
H3C SecPath F5020 V900R003B02D645SP2415  
Comware V700R001B64D045SP2415
```