某局点SecPath F1000-AI-75(V7)配置邮件服务器发送DPI日志收不到邮件

IPS防攻击 卢鹏 3天前 发表

问题描述

某局点SecPath F1000-AI-75(V7)配置邮件服务器发送DPI日志收不到邮件

过程分析

ping测试邮箱服务器地址可达，安全策略已经放通，用户名密码没有问题。

手工测试触发设备产生威胁日志，防火墙抓包到邮件服务器的报文，抓包为空。

排查配置发现少了个配置，邮件模板没有被ips引用， ips策略下email parameter-profile email1或者全局下ips email parameter-profile email1

email parameter-profile

email parameter-profile命令用来引用邮件动作参数profile。

undo email parameter-profile命令用来取消引用邮件动作参数profile。

【命令】

email parameter-profile *parameter-profile-name*

undo email parameter-profile

【缺省情况】

未引用邮件动作参数profile。

【视图】

IPS策略视图

【缺省用户角色】

network-admin

context-admin

【参数】

parameter-profile-name：表示邮件动作参数profile名称，为1～63个字符的字符串，不区分大小写。

【使用指导】

非缺省vSystem不支持本命令。

本命令仅在去使能全局动作参数后生效（即执行**undo global-parameter enable**命令）。

配置日志输出方式为邮件后（即配置**log email**命令），需要配置本命令为邮件动作提供执行参数。

本命令引用的邮件动作参数profile由应用层检测引擎动作参数profile提供。有关应用层检测引擎动作参数profile的具体配置请参见“DPI深度安全命令参考”中的“应用层检测引擎”。

多次执行本命令，最后一次执行的命令生效。

【举例】

在IPS策略policy1中引用名为email1的邮件动作参数profile。

<Sysname> system-view

[Sysname] ips policy policy1

[Sysname-ips-policy-policy1] email parameter-profile email1

ips parameter-profile

ips { **block-source** | **capture** | **email** | **logging** | **redirect** } **parameter-profile**命令用来配置IPS动作引用应用层检测引擎动作参数profile。

undo ips { **block-source** | **capture** | **email** | **logging** | **redirect** } **parameter-profile**命令用来取消配置IPS动作引用应用层检测引擎动作参数profile。

【命令】

ips { **block-source** | **capture** | **email** | **logging** | **redirect** } **parameter-profile** *parameter-name*

undo ips { **block-source** | **capture** | **email** | **logging** | **redirect** } **parameter-profile**

【缺省情况】

IPS动作未引用应用层检测引擎动作参数profile。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

vsys-admin

【参数】

block-source：表示设置IPS源阻断动作的参数。

capture：表示设置IPS捕获动作的参数。非缺省vSystem不支持本参数。

email：表示设置IPS邮件动作的参数。非缺省vSystem不支持本参数。

logging：表示设置IPS日志动作的参数。

redirect：表示设置IPS重定向动作的参数。

parameter-profile *parameter-name*：指定IPS动作引用的应用层检测引擎动作参数profile。*parameter-name*表示动作参数profile的名称，为1～63个字符的字符串，不区分大小写。

【使用指导】

每类IPS动作的具体执行参数由应用层检测引擎动作参数profile来定义，可通过引用各动作参数proflle为IPS动作提供执行参数。有关应用层检测引擎动作参数proflle的具体配置请参见“DPI深度安全命令参考”中的“应用层检测引擎”。

如果IPS动作没有引用应用层检测引擎动作参数profile，或者引用的动作参数profile不存在，则使用系

统中各动作参数的缺省值。

【举例】

创建名称为ips1的应用层检测引擎源阻断动作参数profile，配置其阻断源IP地址的时长为1111秒。

```
<Sysname> system-view
[Sysname] inspect block-source parameter-profile ips1
[Sysname-inspect-block-source-ips1] block-period 1111
[Sysname-inspect-block-source-ips1] quit
```

配置IPS源阻断动作引用名称为ips1的应用层检测引擎源阻断动作参数profile。

```
[Sysname] ips block-source parameter-profile ips1
```

解决方法

ips策略下email parameter-profile email1或者全局下ips email parameter-profile email1 增加配置后可以收到邮件