SCE 网络攻击问题及解决方法

目录

软硬件平台

硬件平台： SCE1000 SCE2020 SCE8000
软件版本： 所有

问题描述

在客户使用SCE产品进行流量控制的时候，发现流量只是通过SCE设备，并没有被SCE事先定义好的策略所控制，即流量失控，bypass流量现象。
症状：

1. 第三方监控软件发现流量突然增大。
2. 通过SCE报表，看到流量波形图变型。
3. 客户端本来不可以访问的网站，变得可以访问。

故障诊断步骤

首先检查support file 里面的dbglog.txt文件，解压support file之后就可以看到。
或者在SCE上面执行#show logging.

下面给大家举个例子：

我们可以看到从2点14分开始，SCE检测到网络攻击，为了保护自己，它开始bypass网络攻击流量：

```
2011-01-20 02:14:47 | INFO  | CPU #000 | Started filtering packets of type 'UDP
Fragments' received on interface # 1 (network). module # 1. Reason: Started filtering
due to attack detection

2011-01-20 02:29:46 | INFO  | CPU #000 | Started filtering packets of type 'UDP
Fragments' received on interface # 0 (subscriber). module # 1. Reason: Started
filtering due to attack detection
```

在持续一个小时左右后，SCE又恢复了正常，并且我们看到“no shortage events” 的信息。
说明这次bypass流量不是由于流量达到了SCE性能的极限而引起的。

```
2011-01-20 03:17:36 | INFO  | CPU #000 | Stopped filtering packets of type 'UDP
Fragments' received on interface # 0 (subscriber). module # 1. Reason: Back to
normal, no shortage events 2011-01-20 03:17:36 | INFO  | CPU #000 | Stopped filtering
```

```
packets of type 'UDP Fragments' received on interface # 1 (network). module # 1.
Reason: Back to normal, no shortage Events
```

在4点30分的时候，SCE再次检测到网络攻击，bypass流量再次开始了：

```
2011-01-20 04:31:40 | INFO  | CPU  #000 | Started filtering packets of type 'UDP'
received
on interface # 0 (subscriber). module # 1. Reason: Started filtering due  to attack
detection 2011-01-20 04:31:40 | INFO  | CPU #000 | Started filtering packets of type
'TCP Non-SYN' received on interface # 0 (subscriber). module # 1. Reason: Started
filtering due to attack detection
```

在持续一个小时左右，SCE又恢复了正常，

```
2011-01-20 05:34:31 | INFO  | CPU  #000 | Stopped filtering packets of type 'UDP'
received
on interface # 0 (subscriber). module # 1. Reason: Back to normal, no shortage events
2011-01-20 05:34:31 | INFO  | CPU #000 | Stopped filtering packets of type 'TCP Non-
SYN' received on interface # 0 (subscriber). module # 1. Reason: Back to normal, no
shortage
```

经验总结：

SCE platform有一种算法叫做Sanity check，它是SCE的内部算法，在网络攻击发生的时候用来自我保护，当该算法检测到有可能威胁SCE正常工作的流量的时候，该算法就会被启动来过滤流量。

SCE platform还跟踪每个flow的可用资源，如果可用资源利用率达到90%，SCE platform就会检测是否有网络攻击发生，一旦流量被识别为网络攻击，就会开始过滤流量。

过滤流量的缺省时间为一个小时，经过一个小时之后，如果没有检测到网络攻击，过滤流量结束，SCE工作恢复正常，如果仍然能够检测到网络攻击，将继续下一个小时的流量过滤。

解决办法：

- SCE不是网络安全设备，我们应该将SCE放置在一个相对安全的网络环境中。
- 强烈建议将anomaly detaction功能开启,但是请注意，即便开启该功能，仍需将SCE放在相对安全的网络环境中。