

Seccenter攻击事件明细中查到大量“未定义事件”解决方法

Seccenter A1000 黄磊 2016-12-26 发表

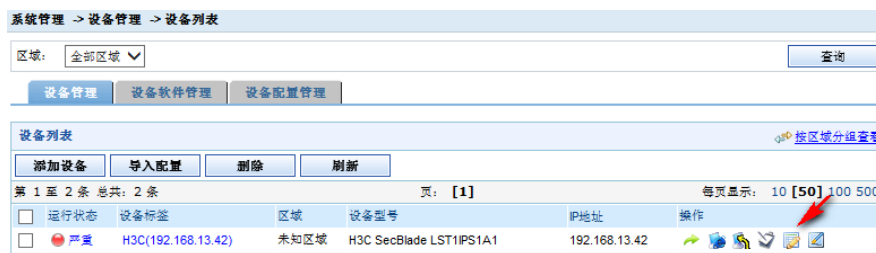
客户网络部署了IPS安全设备，开启了防火攻击防护功能，通过Seccenter统一纳管。在使用过程中发现该IPS在Seccenter上的攻击事件明细中看到大量的“未定义事件”的防攻击日志，如下图。但是在IPS设备本地的查看防攻击日志显示正常。



时间	源IP/MAC	目的IP/MAC	方向	事件	目的端口	协议	Vlan	事件数	代理IP	设备IP	详细
2016-12-15 15:53:25	78.188.169.7774:1f.4a:2f63:71	10.0.0.41/0c:c4:7a:56:19:c	从外到内	未定义事件: 832	443	TCP	1	1		22.9.42.4	
2016-12-15 15:53:24	78.188.169.7774:1f.4a:2f63:71	10.0.0.42/0c:c4:7a:56:19:c	从外到内	未定义事件: 832	443	TCP	1	1		22.9.42.4	

导致Seccenter上未能正常解析出IPS设备发送的防攻击日志信息，显示“未定义事件”的原因主要是Seccenter攻击特征库和设备上不一致。特征库记录了可识别的攻击特征，如果IPS发送的防攻击日志在Seccenter上的攻击特征库中未定义，则会显示成未定义事件+对应ID。

可以在Seccenter的设备管理列表中，手动点击同步设备的特征库，操作位置如下图：



如果需要Seccenter以后自动同步设备上的特征库，可以开启自动同步。



另外如果Seccenter同时管理多台IPS等安全设备，建议安全设备更新使用相同版本的特征库。