V7防火墙IPS自定义特征库的写作规则

特征库 孔梦龙 2022-05-18 发表

问题描述

IPS自定义特征库的写作

解决方法

按照这种模版写进去，后面如果有新的域名客户就可以自己添加了。

例子：|11|代表 advainvienvaiebai 是17个字符，|02|代表 md 是2个字符，采用16进制；sid:1计数，相当于编写一个ID(和原本库的ID不一样)，自定义中不能有重复的

advainvienvaiebai.md

丢弃类：

drop udp any any -> any any (msg:"DNS Query for advainvienvaiebai.md"; content:"|11|advainvienvaiebai|02|md"; classtype:bad-unknown; sid:101; rev:1;)

告警类：

alert udp any any -> any any (msg:"DNS Query for aefobfboabobfaoua.name"; content:"|11|aefobfboabobfaoua |04|name"; classtype:bad-unknown; sid:102; rev:1;)

上述的放在一个txt，然后命名后缀改成.rules