选项减少错误肯定入侵事件

目录

简介

入侵防御系统可能生成在某一喷鼻息规则的额外的警报。警报能是真的正或错误肯定。如果接收许多错误肯定警报，有几个选项可用为了您能减少他们。 此条款提供每个选项优点和缺点的摘要。

选项减少错误肯定警报

> **注意**：这些选项通常不是最好的选择，他们可以是唯一的解决方案在特定情况下。

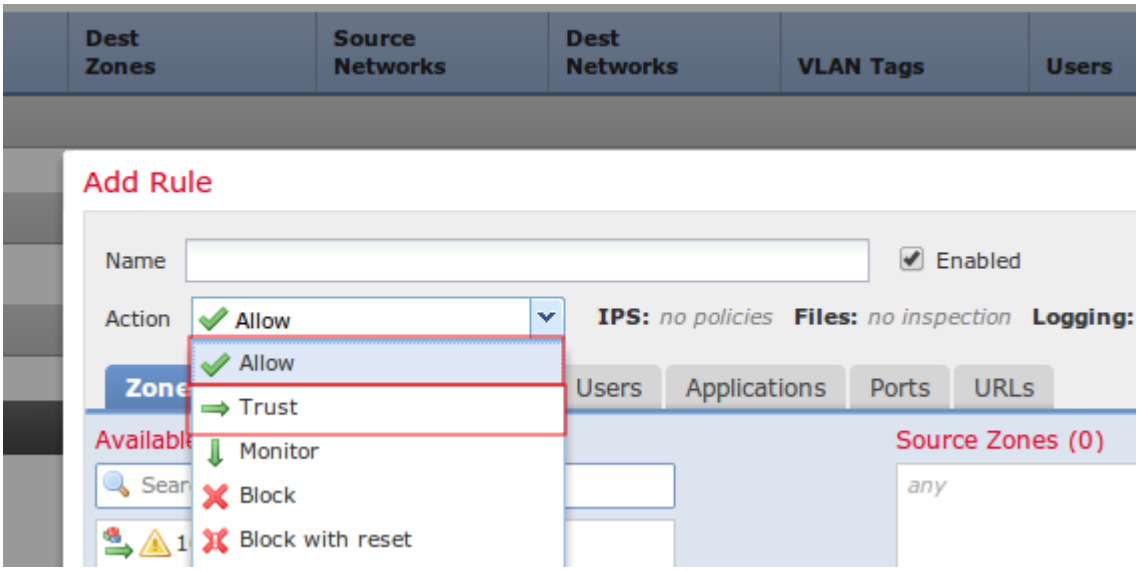
1. 对思科技术支持的报告

如果查找一喷鼻息裁决在良性流量的触发警报，请它向思科技术支持报告。 一旦报告，客户支持工程师升级对漏洞研究小组(VRT)的问题。VRT研究可能的改进对规则。改善的规则是典型可用的对申报人，当他们是可用的和也被添加到下次正式规则更新。

2. 委托或允许规则

允许的委托流量最好的选项穿过Sourcefire设备，不用检查启用**托拉斯**或**允许**操作，不用一项相关的入侵策略。要配置托拉斯或允许规则，请导航对**策略>访问控制>Add规则**。

> **注意**：匹配托拉斯的流量或允许没有配置匹配用户，应用程序，否则URL将有在Sourcefire设备的整体性能的最小影响的规则，因为这样规则可以在火力硬件里处理。



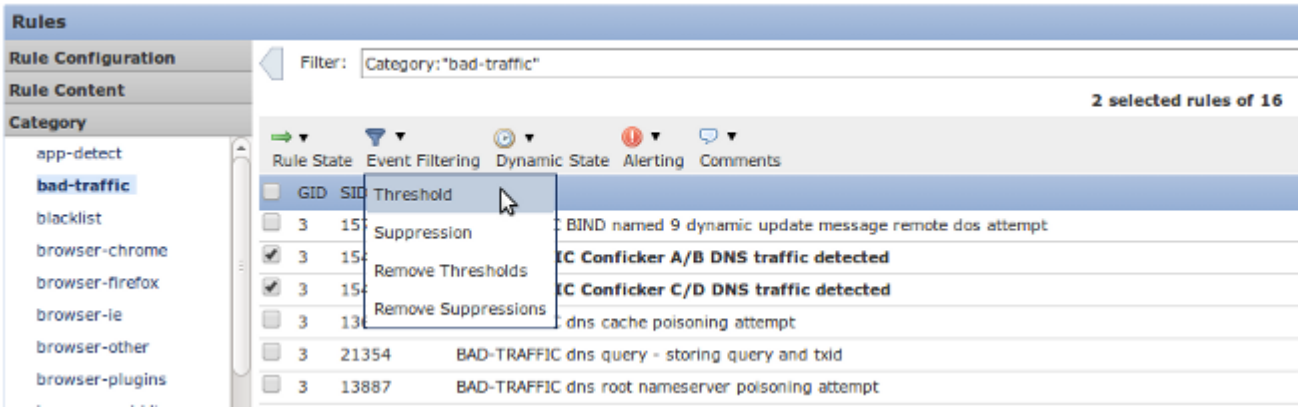
图：托拉斯规则的配置

3. 禁用多余的规则

您能禁用瞄准旧有和被修补的漏洞的喷鼻息规则。它改进性能并且减少错误肯定。使用FireSIGHT建议能协助此任务。 另外，频繁地生成低优先级的警报或警报不是可控诉的规则可能是删除的好候选从入侵策略。

4. 阈值

您能使用**阈值**减少入侵事件数量。这是配置的理想的选择，当规则预计有规律地触发事件有限数量在正常流量时的，但是可能是问题的征兆，如果更多比一定数量的数据包匹配规则。 您能使用此选项减少喧闹的规则触发的事件数量。



图： 阈值的配置

5. 抑制

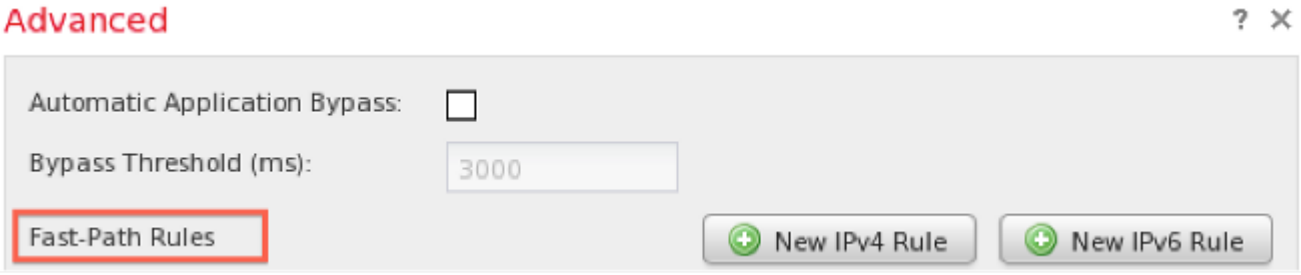
您能使用**抑制**完全排除事件的通知。它配置的类似于**阈值**选项。

> **警告：**抑制可以导致性能问题，因为，当事件没有生成时，喷鼻息必须仍然处理流量。

注意：抑制不防止从降低流量的丢弃规则，因此流量可能静静地降低，当配比与丢弃规则时。

6. Fast-Path规则

类似委托和允许访问控制策略的规则， Fast-Path规则也能旁路检查。 Cisco技术支持一般不建议使用Fast-Path规则，因为他们在**Advanced窗口配置设备**页，并且可能容易地俯视，当访问控制规则是几乎总是满足的时。



图：Fast-Path规定在Advanced窗口的选项。

对使用快速路径规则的唯一的优点是他们能处理更加了不起的最大数据流。 快速路径规则处理流量在硬件级(叫作NMSB)并且能理论上处理至流量200 Gbps。 相反，与**信任的**规则和**允许**操作促进到网络流引擎(NFE)并且能处理流量40 Gbps最大数量。

注意：Fast-Path规则只是可用的在8000系列设备和3D9900。

7. 帕斯规则

为了防止从触发的一个特定规则在流量某一主机(当从该主机的其他流量需要被检查)时，请使用一个*通行证*类型喷鼻息规则。实际上，这是完成它的唯一方法。 当通行证规则有效时，他们可以是非常难维护，因为通行证规则手工写入。 另外，如果规则更新修改通行证规则原始规则，所有相关通行证规则需要手工更新。否则他们可能变得无效。

8. SNORT_BPF变量

在入侵策略的`Snort_BPF`变量使某一流量绕过检查。 当此变量是其中一在传统软件版本时的第一选择，思科技术支持推荐使用访问控制策略规则绕过检查，因为配置是更加粒状，更加可视和更加容易的。