Options to Reduce False Positive Intrusions

Contents

Introduction

An Intrusion Prevention System may generate excessive alerts on a certain Snort rule. The alerts could be true positive or false positive. If you are receiving many false positive alerts, there are several options available for you to reduce them. This article provides a summary of the advantages and disadvantages of each option.

Options to Reduce False Positive Alerts

> Note: These options are usually not the best choice, they can be the only solution under specific circumstances.

1. Report to Cisco Technical Support

If you find a Snort rule that triggers alerts on benign traffic, please report it to Cisco Technical Support. Once reported, a Customer Support Engineer escalates the issue to Vulnerability Research Team (VRT). VRT researches possible improvements to the rule. Improved rules are typically available to the reporter as soon as they are available, and are also added to the next official rule update.

2. Trust or Allow Rule

The best option for permitting trusted traffic to pass through a Sourcefire appliance without inspection is enabling Trust or Allow action without an associated Intrusion Policy. To configure a Trust or Allow rule, navigate to Policies > Access Control > Add Rule.

> Note: Traffic matching Trust or Allow rules which are not configured to match Users,

Applications, or URLs will have minimal impact on the overall performance of a Sourcefire appliance because such rules can be processed in the FirePOWER hardware.

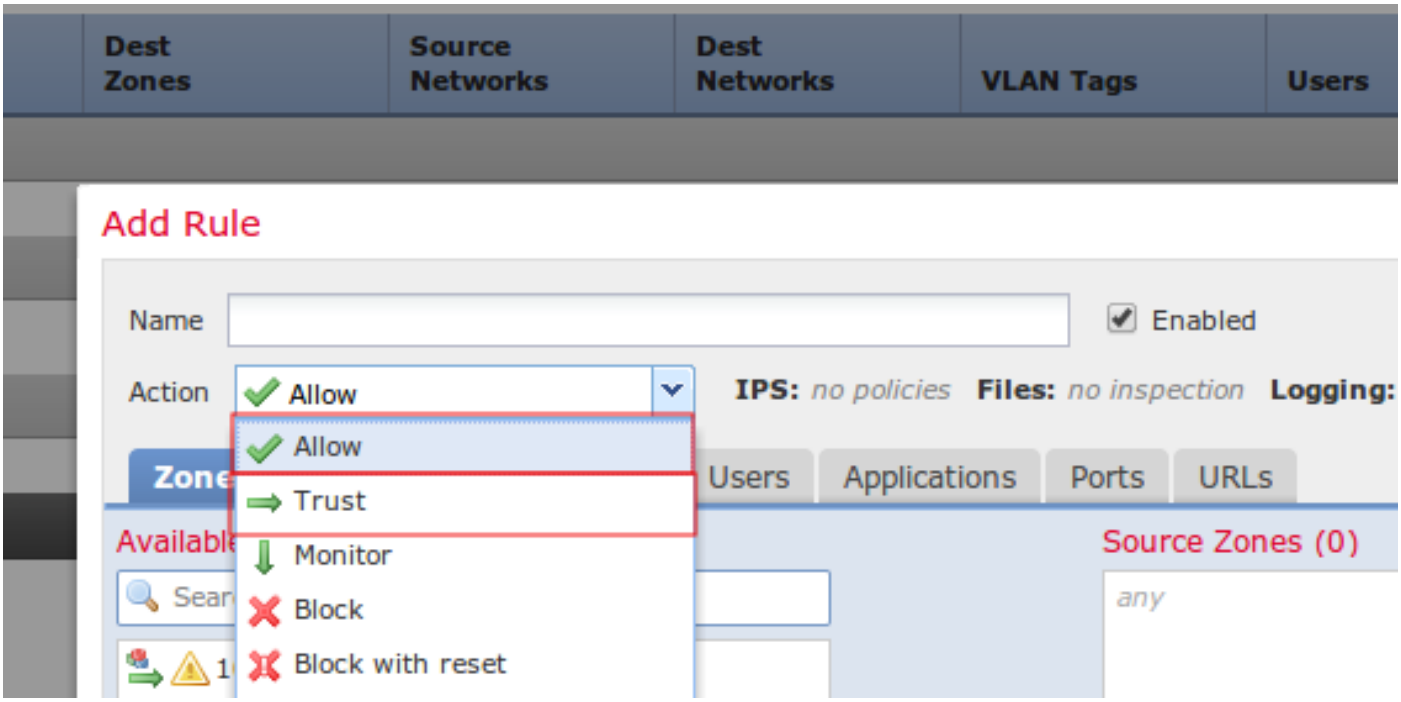

Figure: Configuration of a Trust Rule

3. Disable Unnecessary Rules

You can disable Snort rules that target old and patched vulnerabilities. It improves performance and reduces false positives. Using FireSIGHT recommendations can assist with this task. Additionally, rules which frequently generate low priority alerts or alerts which are not actionable may be good candidates for removal from an Intrusion policy.

4. Threshold

You can use Threshold to reduce the number of intrusion events. This is a good option to configure when a rule is expected to regularly trigger a limited number of events on normal traffic, but could be an indication of a problem if more than a certain number of packets match the rule. You can use this option to reduce the number of events triggered by noisy rules.

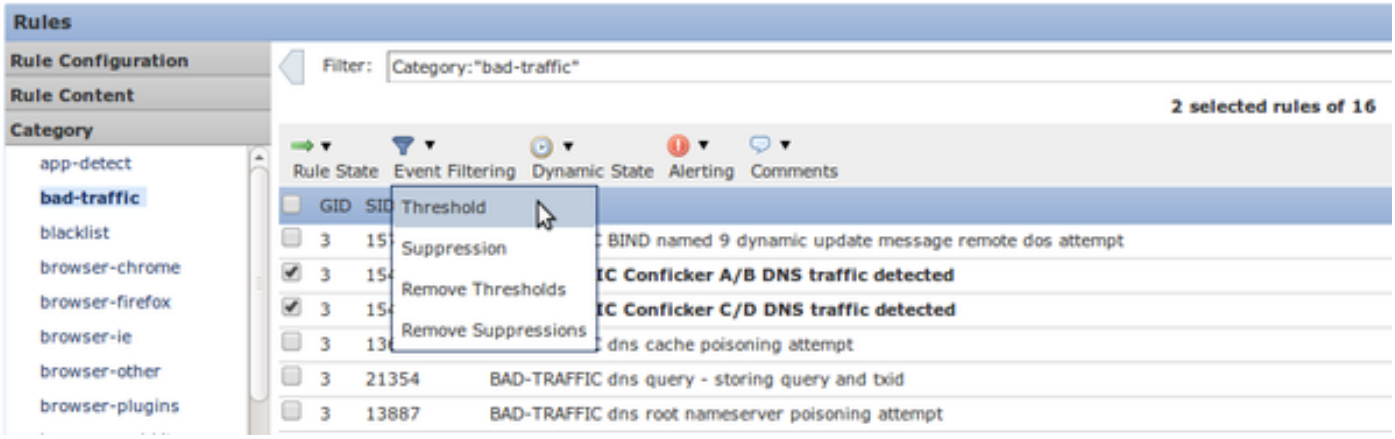

Figure: Configuration of Threshold

5. Suppression

You can use Suppression to completely eliminate the notification of events. It is configured similar to Threshold option.

> Caution: Suppression can lead performance issues, because while no events are generated, Snort still has to process the traffic.

> Note: Suppression does not prevent drop rules from dropping traffic, so traffic may be silently dropped when it matches with drop rule.

---

6. Fast-Path rules

Similar to Trust and Allow rules of an Access Control policy, Fast-Path rules can also bypasses inspection. Cisco Technical Support does not generally recommend using Fast-Path rules because they are configured in the Advanced window of the Device page and may be easily overlooked while Access Control rules are almost always sufficient.

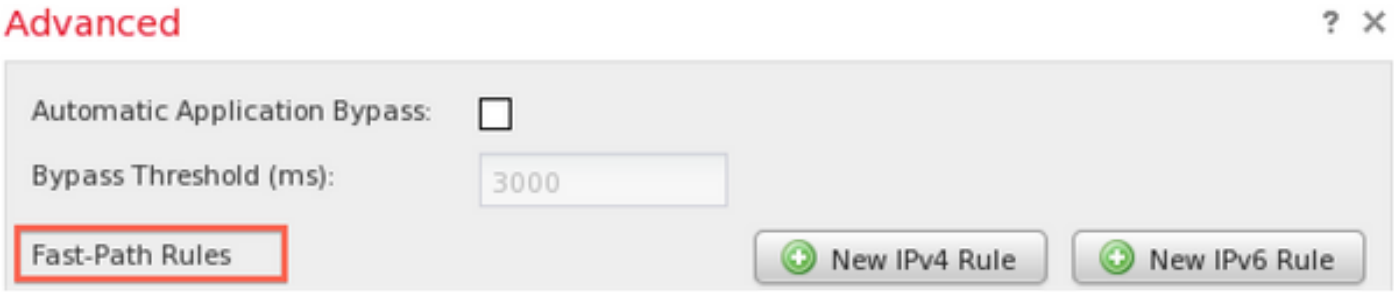

Figure: Fast-Path Rules option in the Advanced window.

The only advantage to using fast-path rules is that they can handle a greater maximum volume of traffic. Fast-path rules process traffic at the hardware level (known as NMSB) and can theoretically handle up to 200 Gbps of traffic. In contrast, rules with Trust and Allow actions are promoted to the Network Flow Engine (NFE) and can handle a maximum of 40 Gbps of traffic.

Note: Fast-Path rules are only available on 8000 series devices and the 3D9900.

7. Pass Rules

In order to prevent a specific rule from triggering on traffic from a certain host (while other traffic from that host needs to be inspected), use a pass type Snort rule. In fact, this is the only way to accomplish it. While pass rules are effective, they can be very difficult to maintain because pass rules are manually written. Additionally, if the original rules of pass rules are modified by a rule update, all related pass rules need to be updated manually. Otherwise they may become ineffective.

8. SNORT_BPF Variable

The `Snort_BPF` variable in an intrusion policy enables certain traffic to bypass inspection. While this variable was one of the first choices on legacy software versions, Cisco Technical Support recommends to use an Access Control policy rule to bypass inspection, because it is more granular, more visible, and much easier to configure.

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).