Options de réduire des intrusions de faux positif

Contenu

Introduction

Un système de prévention des intrusions peut générer des alertes excessives sur un certain reniflent la règle. Les alertes ont pu être positif ou faux positif vrai. Si vous recevez beaucoup d'alertes de faux positif, il y a plusieurs options disponibles pour que vous les réduisiez. Cet article prévoit un résumé des avantages et des inconvénients de chaque option.

Options de réduire des alertes de faux positif

> Remarque: Ces options ne sont habituellement pas le meilleur choix, elles peuvent être la seule solution sous des circonstances spécifiques.

1. État au support technique de Cisco

Si vous trouvez une règle de renifler que les alertes de déclencheurs sur le trafic bénin, le signalent s'il vous plaît au support technique de Cisco. Une fois que signalé, un ingénieur d'assistance clientèle fait suivre la question à l'équipe de recherche de vulnérabilité (VRT). VRT recherche des améliorations possibles à la règle. Les règles améliorées sont en général à la disposition du journaliste dès qu'elles seront disponibles, et sont également ajoutées à la prochaine mise à jour de guide officiel.

2. Faites confiance ou permettez à la règle

La meilleure option pour permettre au trafic de confiance pour traverser une appliance de Sourcefire sans inspection active la **confiance** ou **pour permettre l'**action sans stratégie associée d'intrusion. Pour configurer une confiance ou permettre la règle, naviguez vers les **stratégies > le contrôle d'accès > ajoutent la règle**.

> Remarque: Trafiquez la confiance assortie ou permettez les règles qui ne sont pas configurées pour apparier des utilisateurs, des applications, ou l'URLs aura l'incidence

minimale sur la performance globale d'une appliance de Sourcefire parce que de telles règles peuvent être traitées dans le matériel de puissance de feu.

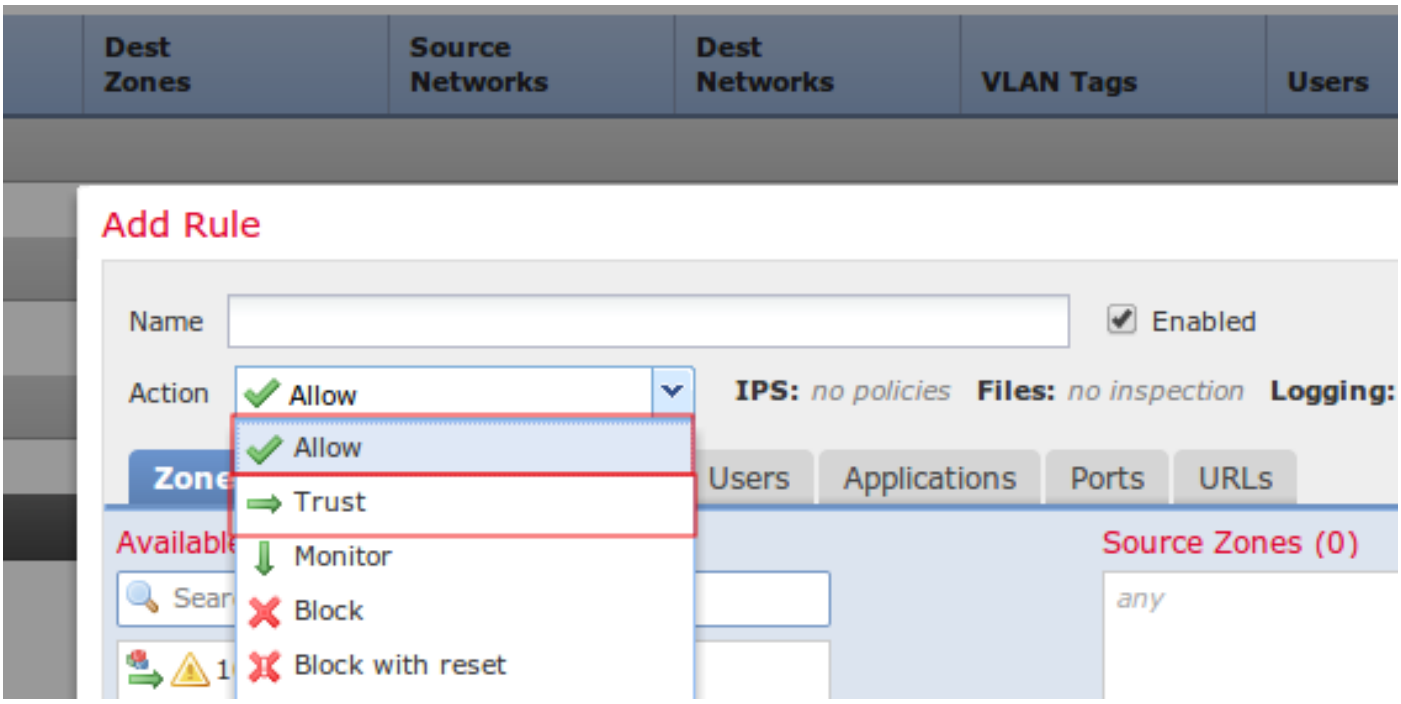

Figure : Configuration d'une règle de confiance

3. Règles inutiles de débronchement

Vous pouvez désactiver reniflez les règles qui visent de vieilles et patchées vulnérabilités. Il améliore la représentation et réduit des faux positifs. Utilisant FireSIGHT les recommandations peuvent assister cette tâche. Supplémentaire, les règles qui génèrent fréquemment les alertes de faible priorité ou les alertes qui ne sont pas recevables peuvent être de bons candidats pour la suppression d'une stratégie d'intrusion.

4. Seuil

Vous pouvez employer le **seuil** pour réduire le nombre d'événements d'intrusion. C'est une bonne option de configurer quand une règle est prévue de déclencher régulièrement un nombre limité d'événements sur le trafic normal, mais pourrait être une indication d'un problème si plus qu'un certain nombre de paquets apparient la règle. Vous pouvez utiliser cette option de réduire le nombre d'événements déclenchés par des règles bruyantes.

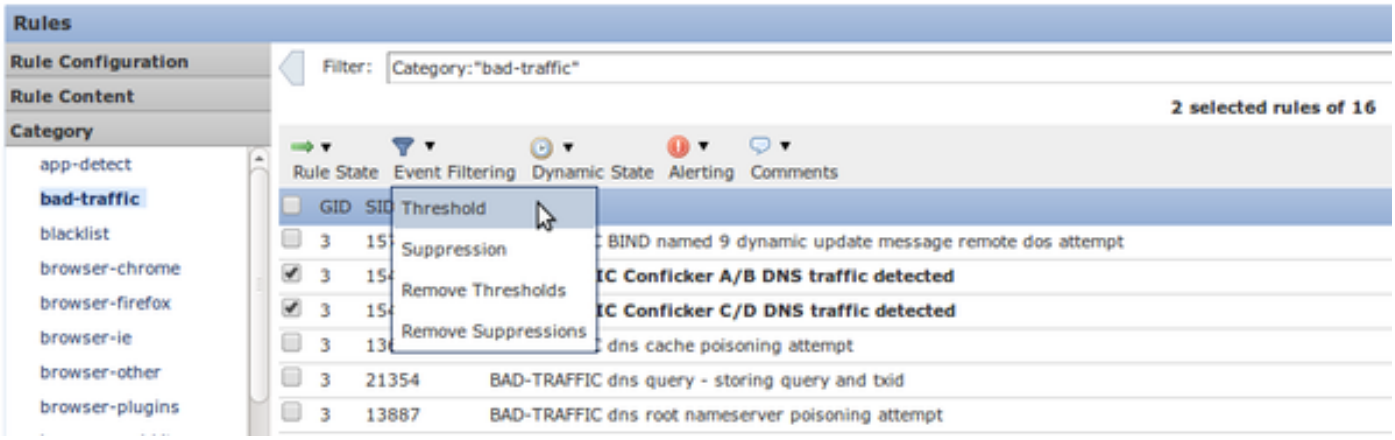

Figure : Configuration de seuil

5. Suppression

Vous pouvez employer la **suppression** pour éliminer complètement la notification des événements. Il est semblable configuré à l'option de **seuil**.

> **Attention** : La suppression peut mener des problèmes de performance, parce que tandis qu'aucun événement n'est généré, reniflent doit traiter toujours le trafic.

> Remarque: La suppression n'empêche pas des règles de baisse du trafic chutant, ainsi le trafic peut être silencieusement abandonné quand il s'assortit avec la règle de baisse.

6. Règles de Rapide-chemin

Semblable pour faire confiance et permettre à des règles d'une stratégie de contrôle d'accès, les règles de Rapide-chemin mettent en boîte également l'inspection de contournements. Le support technique de Cisco généralement ne recommande pas utilisant des règles de Rapide-chemin parce qu'ils sont configurés dans la fenêtre **avancée de la** page de **périphérique** et peut être facilement donné sur tandis que les règles de contrôle d'accès sont presque toujours suffisantes.

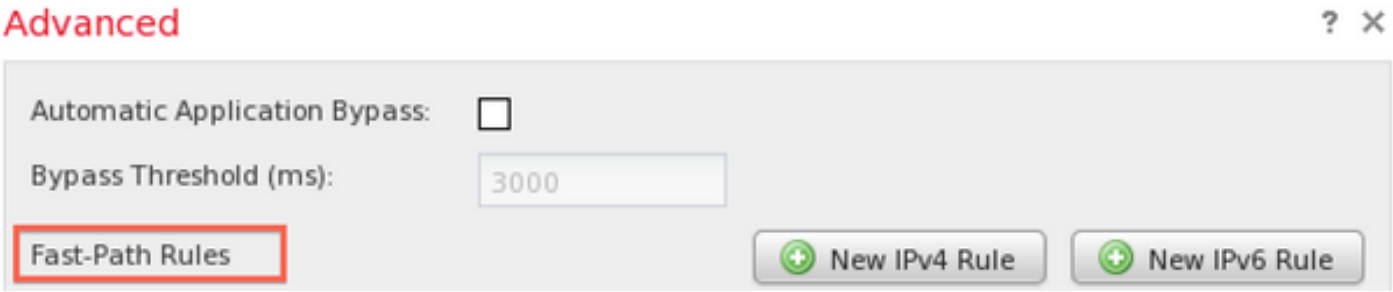

Figure : Le Rapide-chemin ordonne l'option dans la fenêtre avancée.

Le seul avantage à utiliser des règles de rapide-chemin est qu'elles peuvent traiter un plus grand volume maximum du trafic. le trafic de processus de règles de Rapide-chemin au niveau matériel (connu sous le nom de NMSB) et peut théoriquement traiter jusqu'à 200 GBP du trafic. En revanche, les règles avec la **confiance** et **permettent des** actions sont favorisées à l'engine de flux de réseau (NFE) et peuvent manipuler un maximum de 40 GBP du trafic.

> Remarque: Les règles de Rapide-chemin sont seulement disponibles sur des périphériques de gamme 8000 et le 3D9900.

7. Passez les règles

Afin d'empêcher une règle spécifique du déclenchement sur le trafic d'un certain hôte (tandis qu'autre le trafic de cet hôte doit être examiné), utilisez un type de *passage* reniflent la règle. En fait, c'est la seule manière de l'accomplir. Tandis que les règles de passage sont efficaces, il peut être très difficiles les mettre à jour parce que des règles de passage sont manuellement écrites. Supplémentaire, si les règles d'origine des règles de passage sont modifiées par une mise à jour de règle, toutes les règles relatives de passage doivent être mises à jour manuellement.

Autrement ils peuvent devenir inefficaces.

8. Variable SNORT_BPF

La variable de `Snort_BPF` dans une stratégie d'intrusion permet à certain trafic de sauter l'inspection. Tandis que cette variable était l'un des premiers choix sur des versions de logiciel hérité, le support technique de Cisco recommande d'utiliser une règle de stratégie de contrôle d'accès de sauter l'inspection, parce qu'il est plus granulaire, plus visible, et beaucoup plus facile de configurer.